

KATA PENGANTAR

Segala puji dan syukur ke hadirat Allah SWT atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Buku Tugas Akhir Capstone Design yang berjudul "Pengujian Keamanan Server Berbasis *Website*" dengan baik dan tepat waktu. Buku tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik (S.T) pada Program Studi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Telkom Univeristy.

Penulis menyadari bahwa dalam penyusunan pengembangan Tugas Akhir ini masih terdapat kekurangan baik dari sisi materi, teknik penulisan, dan keterbatasan ilmu yang penulis miliki. Oleh karena itu, penulis sangat terbuka dan mengharapkan kritik dan saran yang membangun demi memperbaiki pengembangan Tugas Akhir ini di masa yang akan datang. Penulis berharap bahwa pengembangan Tugas Akhir ini dapat memberikan manfaat bagi pembaca dan menjadi sumber referensi bagi perkembangan ilmu pengetahuan.

UCAPAN TERIMA KASIH

Dalam pengembangan Tugas Akhir ini, penulis menyadari bahwa pengembangan Tugas Akhir Capstone Design “Pengujian Keamanan Server Berbasis *Website*” ini tidak dapat terwujud tanpa dukungan, bimbingan, bantuan dan do’a yang diberikan oleh berbagai pihak selama proses penyelesaian. Oleh karena itu, penulis ingin mengungkapkan rasa terimakasih yang mendalam kepada :

1. Tuhan Yang Maha Esa atas rahmat dan karunia-Nya yang telah memberikan Penulis kemampuan dan kesempatan untuk menyelesaikan Tugas Akhir Capstone Design “Pengujian Keamanan Server Berbasis *Website*” ini.
2. Bapak Dr.Eng. Favian Dewanta, S.T., M.Eng. selaku Pembimbing I dan Bapak Bagus Aditya, S.T., M.T. selaku Pembimbing II yang dengan sabar memberikan arahan, nasihat, pengetahuan, dan masukan yang berharga selama proses pengerjaan Tugas Akhir ini.
3. Seluruh dosen di Program Studi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom Bandung, yang telah memberikan ilmu dan wawasan yang sangat berarti dalam perjalanan akademik penulis.
4. Rekan tim Tugas Akhir yang telah bekerjasama dengan baik untuk menyelesaikan Tugas Akhir ini.
5. Kedua orang tua penulis atas dukungan, doa, motivasi dan nasihat kepada Penulis yang menjadi sumber kekuatan dan motivasi dalam menyelesaikan studi ini.
6. Teman – teman seperjuangan yang selalu memberikan dukungan moral, bantuan dan kebersamaan selama masa studi hingga penyusunan Tugas Akhir ini.
7. Seluruh pihak lainnya yang tidak dapat disebutkan satu per satu, tetapi turut berperan dalam memberikan dukungan dan motivasi selama proses penyelesaian Tugas Akhir ini.

DAFTAR ISI

LEMBAR PENGESAHAN	i
BUKU CAPSTONE DESIGN	i
LEMBAR PERNYATAAN ORISINALITAS	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
LEMBAR PERNYATAAN ORISINALITAS	iv
ABSTRAK.....	v
ABSTRACT.....	vi
KATA PENGANTAR	vii
UCAPAN TERIMA KASIH	viii
DAFTAR ISI.....	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL.....	xvi
DAFTAR SINGKATAN	xvii
BAB 1 USULAN GAGASAN	1
1.1 Deskripsi Umum Masalah.....	1
1.2 Analisis Masalah.....	1
1.2.1 Aspek Keamanan	1
1.2.2 Aspek Teknis	2
1.2.3 Aspek Lingkungan	2
1.3 Analisis Solusi yang Ada	2
1.4 Tujuan Tugas Akhir	2
1.5 Batasan Tugas Akhir.....	3
BAB 2 TINJAUAN PUSTAKA.....	4
2.1 Vulnerability <i>Scanning</i>	4

2.2	OWASP.....	4
2.3	Nmap <i>scanner</i>	6
2.4	Nikto <i>Scanner</i>	7
2.5	CVSS.....	8
2.6	Django.....	8
2.7	Docker.....	9
BAB 3 SPESIFIKASI DAN DESAIN SISTEM		10
3.1	Spesifikasi Sistem	10
3.2	Desain Sistem.....	11
3.2.1	<i>Usecase</i> Diagram	12
3.2.2	<i>Activity</i> Diagram	13
3.3	Metode Pengukuran yang Sesuai dengan Solusi Terpilih.....	14
BAB 4 IMPLEMENTASI		17
4.1	Deskripsi umum implementasi	17
4.2	Detail Implementasi	18
4.2.1	Backend.....	18
4.2.2	Frontend	23
4.2.3	Docker.....	27
4.3	Prosedur Pengoperasian Solusi	31
BAB 5 PENGUJIAN		39
5.1	Skema Pengujian Sistem.....	39
5.1.1	Daftar Pengujian	39
5.1.2	Skenario Pengujian	39
5.2	Proses Pengujian dan Analisis Hasil.....	40
5.2.1	Pengujian Menggunakan Nikto <i>Scanner</i>	40
5.2.2	Pengujian Menggunakan Nmap <i>Scanner</i>	59
5.2.3	Pengujian Komparasi Nmap dan Nikto	81

5.2.4	Pengujian Reliability Menggunakan ApacheJmeter	94
5.2.5	Pengujian Backend.....	98
5.2.6	Pengujian Frontend	102
5.2.7	Pengujian Docker.....	106
5.2.8	Rangkuman Hasil Pengujian.....	111
BAB 6 KESIMPULAN DAN SARAN		113
6.1	Kesimpulan.....	113
6.2	Saran	115
DAFTAR PUSTAKA		116
LAMPIRAN.....		118

DAFTAR GAMBAR

Gambar 3. 1 Usecase Diagram	12
Gambar 3. 2 Activity Diagram	13
Gambar 4. 1 Struktur Frontend.....	23
Gambar 4.2 Login Page.....	31
Gambar 4.3 Menu Bar	31
Gambar 4.4 Home Page.....	32
Gambar 4.5 Fitur-fitur Nikto Scanner	32
Gambar 4.6 Fitur-fitur Nmap Scanner.....	33
Gambar 4.7 Opsi Lanjutan Nmap Scanner	33
Gambar 4.8 Fitur Port Scan	34
Gambar 4.9 Hasil Pemindaian	34
Gambar 4. 10 Diagram Kerentanan.....	35
Gambar 4.11 Analisis Keamanan Detail	35
Gambar 4.12 Rekomendasi Perbaikan Berbasis Generative AI	36
Gambar 4.13 Unduh Ringkasan Pemindaian.....	36
Gambar 4.14 Menu Riwayat Pemindaian.....	37
Gambar 4.15 Menu About US.....	37
Gambar 4.16 Menu Contact Us	38
Gambar 5.1 Pengujian Pertama Website 1 Device (Localhost:5001) dengan Nikto scanner	41
Gambar 5.2 Pengujian kedua Website 1 device (Localhost:5001) dengan Nikto Scanner	41
Gambar 5.3 Pengujian ketiga Website 1 device (Localhost:5001) dengan Nikto Scanner.....	42
Gambar 5.4 Pengujian pertama Website 1 device (Localhost:5002) dengan Nikto Scanner.....	43
Gambar 5.5 Pengujian kedua Website 1 device (Localhost:5002) dengan Nikto Scanner	43
Gambar 5.6 Pengujian ketiga Website 1 device (Localhost:5002) dengan Nikto Scanner.....	44
Gambar 5.7 Pengujian pertama Website 1 device (Localhost:5003) dengan Nikto Scanner.....	45
Gambar 5.8 Pengujian kedua Website 1 device (Localhost:5003) dengan Nikto Scanner	45
Gambar 5.9 Pengujian ketiga Website 1 device (Localhost:5003) dengan Nikto Scanner.....	46
Gambar 5.10 Pengujian pertama Website beda device (Localhost:5001) dengan Nikto Scanner	47
Gambar 5.11 Pengujian kedua Website beda device (Localhost:5001) dengan Nikto Scanner	48
Gambar 5.12 Pengujian ketiga Website beda device (Localhost:5001) dengan Nikto Scanner.....	48
Gambar 5.13 Pengujian pertama Website beda device (Localhost:5002) dengan Nikto Scanner	49
Gambar 5.14 Pengujian kedua Website beda device (Localhost:5002) dengan Nikto Scanner	50

Gambar 5.15 Pengujian ketiga Website beda device (Localhost:5002) dengan Nikto Scanner.....	50
Gambar 5.16 Pengujian pertama Website beda device (Localhost:5003) dengan Nikto Scanner	51
Gambar 5.17 Pengujian kedua Website beda device (Localhost:5003) dengan Nikto Scanner	52
Gambar 5.18 Pengujian ketiga Website beda device.....	52
Gambar 5.19 Pengujian pertama Website internet (https://www.pln.co.id) dengan Nikto Scanner.....	53
Gambar 5.20 Pengujian kedua Website internet (https://www.pln.co.id) dengan Nikto Scanner	54
Gambar 5.21 Pengujian ketiga Website internet (https://www.pln.co.id) dengan Nikto Scanner.....	55
Gambar 5.22 Pengujian pertama Website internet (http://httpbin.org) dengan Nikto Scanner	55
Gambar 5.23 Pengujian kedua Website internet (http://httpbin.org) dengan Nikto Scanner.....	56
Gambar 5.24 Pengujian ketiga Website internet (http://httpbin.org) dengan Nikto Scanner.....	57
Gambar 5.25 Pengujian pertama Website internet (https://www.komdigi.go.id/) dengan Nikto Scanner..	57
Gambar 5.26 Pengujian kedua Website internet (https://www.komdigi.go.id/) dengan Nikto Scanner....	58
Gambar 5.27 Pengujian ketiga Website internet (https://www.komdigi.go.id/) dengan Nikto Scanner.....	59
Gambar 5.28 Pengujian pertama Website 1 device (Localhost:8081) dengan nmap Scanner.....	60
Gambar 5.29 Pengujian pertama Website 1 device (Localhost:8081) dengan nmap Scanner.....	60
Gambar 5.30 Pengujian kedua Website 1 device (Localhost:8081) dengan nmap Scanner.....	61
Gambar 5.31 Pengujian kedua Website 1 device (Localhost:8081) dengan nmap Scanner.....	61
Gambar 5.32 Pengujian ketiga Website 1 device (Localhost:8081) dengan nmap Scanner.....	62
Gambar 5.33 Pengujian ketiga Website 1 device (Localhost:8081) dengan nmap Scanner.....	62
Gambar 5.34 Pengujian pertama Website 1 device (Localhost:8082) dengan nmap Scanner.....	63
Gambar 5. 35 Pengujian kedua Website 1 device (Localhost:8082) dengan nmap Scanner.....	64
Gambar 5.36 Pengujian ketiga Website 1 device (Localhost:8082) dengan nmap Scanner.....	64
Gambar 5.37 Pengujian pertama Website 1 device (Localhost:8083) dengan nmap Scanner.....	65
Gambar 5.38 Pengujian kedua Website 1 device (Localhost:8083) dengan nmap Scanner.....	66
Gambar 5.39 Pengujian ketiga Website 1 device (Localhost:8083) dengan nmap Scanner.....	66
Gambar 5.40 Pengujian pertama Website beda device (Localhost:8081) dengan nmap Scanner	67
Gambar 5.41 Pengujian pertama Website beda device (Localhost:8081) dengan nmap Scanner	68
Gambar 5.42 Pengujian kedua Website beda device (Localhost:8081) dengan nmap Scanner.....	69
Gambar 5.43 Pengujian kedua Website beda device (Localhost:8081) dengan nmap Scanner.....	69
Gambar 5.44 Pengujian ketiga Website beda device (Localhost:8081) dengan nmap Scanner	70
Gambar 5.45 Pengujian ketiga Website beda device (Localhost:8081) dengan nmap Scanner	70
Gambar 5.46 Pengujian pertama Website beda device (Localhost:8082) dengan nmap Scanner	71
Gambar 5.47 Pengujian kedua Website beda device (Localhost:8082) dengan nmap Scanner.....	71
Gambar 5.48 Pengujian ketiga Website beda device (Localhost:8082) dengan nmap Scanner	72
Gambar 5.49 Pengujian pertama Website beda device (Localhost:8083) dengan nmap Scanner	73
Gambar 5.50 Pengujian kedua Website beda device (Localhost:8083) dengan nmap Scanner.....	73

Gambar 5.51 Pengujian ketiga Website beda device (Localhost:8083) dengan nmap Scanner	74
Gambar 5.52 Pengujian pertama Website internet (scanme.nmap.org) dengan nmap Scanner.....	75
Gambar 5.53 Pengujian kedua Website internet (scanme.nmap.org) dengan nmap Scanner.....	75
Gambar 5.54 Pengujian ketiga Website internet (scanme.nmap.org) dengan nmap Scanner.....	76
Gambar 5.55 Pengujian pertama Website internet (neverssl.com) dengan nmap Scanner.....	77
Gambar 5.56 Pengujian kedua Website internet (neverssl.com) dengan nmap Scanner	77
Gambar 5.57 Pengujian ketiga Website internet (neverssl.com) dengan nmap Scanner.....	78
Gambar 5.58 Pengujian pertama Website internet (www.detik.com) dengan nmap Scanner	78
Gambar 5.59 Pengujian kedua Website internet (www.detik.com) dengan nmap Scanner.....	79
Gambar 5. 60 Pengujian ketiga Website internet (www.detik.com) dengan nmap Scanner	79
Gambar 5. 61 Skor Keamanan Website Https://Sman1pyk.Sch.Id/ Berdasarkan Hasil Pemindaian Nikto 81	
Gambar 5. 62 Hasil Temuan Kerentanan Website Https://Sman1pyk.Sch.Id/ Berdasarkan Hasil Pemindaian Nikto	81
Gambar 5. 63 Hasil Rekomendasi AI Website Https://Sman1pyk.Sch.Id/ Berdasarkan Hasil Pemindaian Nikto	82
Gambar 5. 64 Skor Keamanan Website Https://Sman1pyk.Sch.Id/ Berdasarkan Hasil Pemindaian Nmap83	
Gambar 5. 65 Hasil Temuan Kerentanan Website Https://Sman1pyk.Sch.Id/ Berdasarkan Hasil Pemindaian Nmap.....	83
Gambar 5. 66 Hasil Rekomendasi AI Website Https://Sman1pyk.Sch.Id/ Berdasarkan Hasil Pemindaian Nmap.....	84
Gambar 5. 67 Skor Keamanan Website Https://Expired.Badssl.Com Berdasarkan Pemindaian Nikto	85
Gambar 5. 68 Hasil Temuan Kerentanan Website Https://Expired.Badssl.Com Berdasarkan Hasil Pemindaian Nikto.....	85
Gambar 5. 69 Hasil Rekomendasi AI Website Https://Expired.Badssl.Com Berdasarkan Hasil Pemindaian Nikto	86
Gambar 5. 70 Skor Keamanan Website Https://Expired.Badssl.Com Berdasarkan Pemindaian Nmap.....	87
Gambar 5. 71 Hasil Temuan Kerentanan Website Https://Expired.Badssl.Com Berdasarkan Hasil Pemindaian Nmap	87
Gambar 5. 72 Hasil Rekomendasi AI Website Https://Expired.Badssl.Com Berdasarkan Hasil Pemindaian Nmap.....	88
Gambar 5. 73 Skor Keamanan Website Https://Google-Gruyere.Appspot.Com/ Berdasarkan Hasil Pemindaian Nikto.....	89
Gambar 5. 74 Hasil Temuan Kerentanan Website Https://Google-Gruyere.Appspot.Com/ Berdasarkan Hasil Pemindaian Nikto	89
Gambar 5. 75 Hasil Rekomendasi AI Website Https://Google-Gruyere.Appspot.Com/ Berdasarkan Hasil Pemindaian Nikto.....	90
Gambar 5. 76 Skor Keamanan Website Https://Google-Gruyere.Appspot.Com/ Berdasarkan Hasil Pemindaian Nmap	91

Gambar 5. 77 Hasil Temuan Kerentanan Website Https://Google-Gruyere.Appspot.Com/ Berdasarkan Hasil Pemindaian Nmap.....	91
Gambar 5. 78 Hasil Rekomendasi AI Website Https://Google-Gruyere.Appspot.Com/ Berdasarkan Hasil Pemindaian Nmap	92
Gambar 5. 79 Pengujian 1	95
Gambar 5.80 Pengujian 6	96
Gambar 5. 81 Grafik Average Response Time.....	97
Gambar 5.82 Grafik System Throughput	98
Gambar 5.83 Summary Report Pengujian Level 1	99
Gambar 5.84 Graph Result Pengujian Level 1	99
Gambar 5.85 Monitoring Penggunaan CPU dan Memori	101
Gambar 5.86 Flowchart Alur Pengujian Frontend.....	103
Gambar 5.87 Hasil Pengujian 1	103
Gambar 5.88 Grafik Hasil Pengujian 1.....	104
Gambar 5.89 Hasil Pengujian Tanpa Proses Pemindaian 1	107
Gambar 5.90 Grafik CPU dan Memory.....	107

DAFTAR TABEL

Tabel 1. 1 QWASP Top 10 Vulnerability	5
Tabel 3. 1 Spesifikasi Sistem.....	10
Tabel 3. 2 Pengukuran Scanning	14
Tabel 3. 3 Reporting.....	15
Tabel 3. 4 Rekomendasi Perbaikan	16
Tabel 5.1 Pengujian Website Localhost 1 Device Menggunakan Nikto Scanner	46
Tabel 5.2 Pengujian Website Localhost Beda Device Menggunakan Nikto Scanner	53
Tabel 5. 3 Pengujian Website Internet Menggunakan Nikto Scanner.....	59
Tabel 5.4 Tabel Pengujian Website 1 Device Menggunakan Nmap Scanner	66
Tabel 5.5 Pengujian Website Beda Device Menggunakan Nmap Scanner	74
Tabel 5. 6 Pengujian Website Internet Menggunakan Nmap Scanner	80
Tabel 5. 7 Rekap Hasil Analisis Pengujian Website	80
Tabel 5.8 Rekap Hasil Pengujian Performa Website	95
Tabel 5.9 Rekap Hasil Pengujian Menggunakan Apache JMeter	97
Tabel 5.10 Hasil Analisis pengujian menggunakan Apache JMeter	97
Tabel 5.11 data pengujian load testing sistem backend.....	100
Tabel 5.12 Data Penggunaan CPU	101
Tabel 5.13 Data Penggunaan Memori	102
Tabel 5. 14 Skenario Pengujian Interface.....	102
Tabel 5.15 Rekapitulasi Data Hasil Pengujian Frontend.....	105
Tabel 5. 16 Rekapitulasi Performa Setiap Endpoint.....	105
Tabel 5.17 Hasil Pengujian Tanpa Proses Pemindaian 1	107
Tabel 5.18 Hasil 1 (Pengujian Docker Aktif dengan Pemindaian Menggunakan Nikto).....	108
Tabel 5.19 Hasil 1 (Pengujian Docker aktif dengan Pemindaian Menggunakan Nmap).....	109
Tabel 5.20 Hasil 2 (Pengujian Docker Aktif Dengan Pemindaian Menggunakan Nmap Dan Nikto Bersamaan).....	110
Tabel 5. 25 Perbandingan Spesifikasi dan Realisasi	112

DAFTAR SINGKATAN

SQL injection	: <i>Structured Query Language Injection</i>
SSL	: <i>Secure Socket Layer</i>
TLS	: <i>Transport Layer Security</i>
DDoS	: <i>Distribution Denial Of Service</i>
Nmap	: <i>Network Mapper</i>
AI	: <i>Artificial Intelligence</i>
OWASP	: <i>Open Web Application Security Project</i>
CI/CD	: <i>Continuous Integration / Continuous Deployment</i>
SSRF	: <i>Server-Side Request Forgery</i>
OS	: <i>Operating System</i>
GPL	: <i>General Public License</i>
HTTP	: <i>Hypertext Transfer Protocol</i>
CVSS	: <i>Common Vulnerability Scoring System</i>
MVC	: <i>Model-View-Controller</i>
MVT	: <i>Models-View-Template</i>
URL	: <i>Uniform Resource Locator</i>
ORM	: <i>Object-Relational Mapping</i>
PDF	: <i>Portable Document Format</i>
IP	: <i>Internet Protocol</i>
FGD	: <i>Focus Group Discussion</i>
HTML	: <i>HyperText Markup Language</i>
CRUD	: <i>Create, Read, Update, Delete</i>
API	: <i>Application Programming Interface</i>
CSS	: <i>Cascading Style Sheets</i>

BAB 1

USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Server merupakan sistem komputer yang menyediakan berbagai layanan dalam jaringan komputer^[19]. Server terdiri dari berbagai jenis, diantaranya *web* server yang berfungsi untuk memberikan konten *web* kepada pengguna, *application* server yang digunakan untuk menjalankan dan mengelola aplikasi, *database* server yang digunakan untuk menyimpan dan mengelola data, email server yang digunakan untuk mengelola pengiriman dan penerimaan pesan, dan masih banyak lagi^[18]. Saat ini, server berperan penting dalam keberlangsungan teknologi pada kehidupan sehari – hari.

Dengan semakin banyaknya penggunaan server dalam kehidupan sehari-hari di kalangan perusahaan, organisasi dan individu, risiko serangan *cyber* pada server semakin meningkat. Kompleksitas masalah dalam keamanan server terletak pada serangan *cyber* seperti pencurian data, peretasan, serangan kerentanan terhadap *malware* dan serangan lainnya yang berkelanjutan. Maka, keamanan server menjadi salah satu hal yang perlu diperhatikan dan ditingkatkan untuk melindungi data pengguna serta memastikan kelangsungan layanan pada server tersebut berjalan dengan baik.

1.2 Analisis Masalah

Pada bagian ini merupakan analisa masalah yang dituangkan berupa aspek – aspek diantaranya aspek keamanan, aspek teknis dan aspek lingkungan. Adapun analisis aspek aspek tersebut yaitu :

1.2.1 Aspek Keamanan

Server merupakan target utama dari berbagai serangan keamanan yang dapat membahayakan integritas, ketersediaan data, dan kerahasiaan. Ancaman – ancaman ini diantaranya *SQL injection* yang merupakan salah satu serangan umum yang terjadi pada server, dimana penyerang menyisipkan kode berbahaya untuk mengakses dan merusak basis data, selain itu ancaman *Cross-site Scripting*, serangan *brute force*, tidak ada implementasi enkripsi seperti SSL/TLS yang dapat membuat data yang dikirim antara server dan klien rentan terhadap penyadapan dan serangan *Distributed Denial of Service* (DDoS) yang dapat memenuhi server dengan lalu lintas palsu ^[2].

1.2.2 Aspek Teknis

Pada sebuah server, penting untuk memastikan server tersebut bebas dari celah keamanan yang dapat dimanfaatkan oleh penyerang. Dengan melakukan evaluasi keamanan secara berkala dan menyeluruh maka keamanan data pengguna, mekanisme enkripsi data, kelemahan teknis dan fitur-fitur keamanan pada *Website* dapat diidentifikasi dan diperbaiki keamanannya sehingga membantu aplikasi tetap berjalan dengan lancar^[11].

1.2.3 Aspek Lingkungan

Keamanan pada server tidak hanya berdampak terhadap kualitas layanan dari server tersebut tetapi juga berdampak pada para pengguna. Server yang aman dan terpercaya memberikan kenyamanan pada pengguna, mengurangi adanya risiko kebocoran data yang akan meningkatkan kepercayaan pengguna^[5]. Selain itu, adanya evaluasi keamanan yang dilakukan secara berkala juga turut berkontribusi untuk menangani insiden pada keamanan sehingga mendukung teknologi yang semakin ramah lingkungan.

1.3 Analisis Solusi yang Ada

Dalam konteks keamanan pada server dengan adanya tantangan serangan *cyber* berupa peretasan, pencurian data dan serangan *malware*. Maka, penyedia layanan diharapkan untuk mendeteksi, mencegah dan mengurangi risiko keamanan seperti menerapkan teknik autentikasi dan enkripsi yang baik serta melakukan pengecekan secara berkala guna memastikan bahwa fitur-fitur keamanan yang ada di penyedia layanan telah berfungsi dengan baik sehingga tidak ada celah yang dapat dimanfaatkan oleh penyerang.

1.4 Tujuan Tugas Akhir

Tujuan dari *capstone design* ini adalah untuk merancang dan mengembangkan solusi yang mampu mengatasi masalah keamanan *cyber* yang semakin meningkat. Maka, pada *capstone design* ini menawarkan sebuah *platform* yang berisi *tools* yang dapat digunakan untuk pengujian keamanan server. *Platform* ini bertujuan untuk mengetahui celah keamanan pada suatu server sehingga *administrator* server dapat melakukan perbaikan terhadap temuan temuan celah keamanan sebelum dimanfaatkan oleh pihak yang tidak berwenang. *Platform* ini dikembangkan sebagai solusi keamanan server berbasis *Website* yang dapat diakses dengan mudah, sehingga mampu melayani berbagai kalangan, mulai dari pemilik bisnis kecil hingga perusahaan besar.

1.5 Batasan Tugas Akhir

Berikut merupakan batasan – batasan yang perlu diperhatikan dalam pengembangan *platform* ini :

- Solusi yang dikembangkan tidak mencakup pembuatan *tools* pengujian keamanan dari awal, melainkan mengembangkan sebuah *platform* berbasis *Website* yang mengintegrasikan *tools open source* yang sudah ada, dengan fokus utamanya adalah *tools* Nmap dan Nikto.
- Fitur pemindaian kerentanan yang disediakan *platform* ini terbatas pada identifikasi sistem operasi, pemindaian *port*, dan deteksi layanan atau aplikasi spesifik pada server target.
- *Platform* hanya berfungsi untuk mendeteksi, melaporkan temuan, dan memberikan rekomendasi perbaikan berbasis *generative AI* terhadap celah keamanan. Tindakan perbaikan atau mitigasi kerentanan tidak termasuk dalam ruang lingkup tugas akhir ini.
- Pengujian keamanan pada *platform* ini hanya terbatas pada keamanan server sebagai target utama. *Platform* ini tidak memeriksa keamanan seluruh perangkat dalam jaringan seperti router, *firewall*, atau komputer lainnya.
- Interaksi dengan sistem dibatasi hanya pada dua peran pengguna, yaitu “*user*” yang dapat menggunakan fitur pemindaian dan “*admin*” yang dapat mengelola data hasil pemindaian dan profil pengguna.

BAB 2

TINJAUAN PUSTAKA

2.1 *Vulnerability Scanning*

Vulnerability scanning merupakan pemindaian kerentanan yang dapat mengidentifikasi kerentanan atau celah keamanan yang dieksploitasi penyerang pada server. Tujuan dari *vulnerability scanning* ini adalah untuk mendeteksi potensi masalah keamanan sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, *vulnerability scanning* ini dapat memberikan hasil temuan kerentanan serta memberikan rekomendasi perbaikan untuk menutup celah keamanan yang ditemukan^[14] Pemindaian keamanan ini dilakukan dengan menggunakan *tools* khusus yang dapat digunakan untuk mendeteksi celah keamanan pada server.

2.2 OWASP

OWASP (*Open Web Application Security Project*) adalah organisasi nirlaba internasional yang fokus pada keamanan aplikasi *web*. Prinsip utama OWASP adalah menyediakan semua materi secara gratis dan mudah diakses melalui *Website* organisasi tersebut, sehingga pengembang dan administrator dapat meningkatkan keamanan aplikasi *web* yang dimiliki. Dalam konteks pengujian keamanan server, OWASP Top 10 memberikan panduan yang sangat berharga untuk mengidentifikasi celah keamanan yang umum ditemukan pada aplikasi *web*. Hal ini menjadikan OWASP sebagai referensi penting bagi *administrator* sistem dan profesional keamanan dalam melakukan *assessment* keamanan server^[7].

OWASP telah menjadi standar industri dalam mengidentifikasi risiko keamanan aplikasi *web* yang paling kritis. Salah satu kontribusi terpenting OWASP adalah daftar "OWASP Top 10" yang berisi sepuluh kerentanan keamanan aplikasi *web* paling berbahaya. Daftar ini diperbarui secara berkala setiap 3-4 tahun untuk mengikuti perkembangan ancaman keamanan terbaru^[22]. Berikut merupakan TOP 10 daftar risiko keamanan paling kritis menurut OWASP tahun 2021 :

Tabel 1. 1 OWASP Top 10 *Vulnerability*

No	OWASP Top 10 <i>Vulnerability</i> <i>Types</i> 2021	Deskripsi
1	<i>Broken Access Control</i>	Kerentanan yang terjadi karena penerapan kontrol akses situs <i>web</i> yang tidak tepat. Hal ini memungkinkan penyerang masuk ke dalam sistem untuk mencuri informasi [22].
2	<i>Cryptographic Failures</i>	Kerentanan yang terjadi ketika sistem kriptografi rusak dan tidak dapat melindungi informasi sensitif [22].
3	<i>Injection</i>	Kerentanan pada server yang memungkinkan data masukan <i>user</i> dianggap sebagai perintah sehingga sistem dapat menjalankan perintah yang tidak diizinkan yang menyebabkan kebocoran data [22].
4	<i>Insecure Design</i>	Kerentanan yang disebabkan oleh desain yang tidak aman atau kelemahan pada desain [22].
5	<i>Security Misconfiguration</i>	Sistem yang tidak dikonfigurasi dengan benar sehingga penyerang dapat mengeksploitasi sistem [22].
6	<i>Vulnerable and Outdated Components</i>	Kerentanan yang disebabkan oleh perangkat lunak yang usang, rentan dan sudah tidak didukung [22].
7	<i>Identification and Authentication Failures</i>	Risiko keamanan terjadi ketika identitas, otentikasi, atau manajemen sesi pengguna

		tidak ditangani dengan hati-hati, yang dapat memungkinkan penyerang untuk memanfaatkan kata sandi, kunci, token sesi, atau kelemahan dalam perangkat lunak untuk mengambil alih identitas pengguna [22] .
8	<i>Software and Data Integrity Failures</i>	Disebabkan oleh infrastruktur dan kode yang gagal melindungi dari serangan. Pembaruan perangkat lunak, data penting, dan <i>pipeline</i> CI/CD yang diterapkan tanpa verifikasi termasuk di dalamnya [22] .
9	<i>Security Logging and Monitoring Failures</i>	Kerentanan yang terjadi ketika aktivitas sistem tidak diawasi secara aktif yang menyebabkan hilangnya kemampuan untuk serangan, menerima peringatan dini, dan melakukan investigasi [22] .
10	<i>Server-Side Request Forgery</i>	Serangan SSRF dibuat untuk memanfaatkan cara server menangani informasi eksternal. Tujuan utama serangan ini adalah untuk mencuri informasi sensitif di server atau memanfaatkan kerentanan lain dengan menggunakan tindakan penanggulangan validasi <i>input</i> SSRF [22] .

2.3 Nmap scanner

Nmap ("*Network Mapper*") adalah utilitas sumber terbuka dan gratis untuk penemuan jaringan dan audit keamanan. Banyak sistem dan administrator jaringan juga menganggapnya berguna untuk tugas-tugas seperti inventaris jaringan, mengelola jadwal pemutakhiran layanan, dan memantau waktu aktif host atau layanan [\[17\]](#). Nmap mampu mengumpulkan beragam

informasi esensial mengenai topologi dan konfigurasi keamanan sebuah jaringan. Kemampuan utamanya meliputi proses enumerasi untuk menentukan *host* mana saja yang aktif, identifikasi layanan yang berjalan pada setiap *host* beserta nama dan versi aplikasinya, serta deteksi sistem operasi (*OS fingerprinting*) untuk mengetahui jenis dan versi OS yang digunakan. Lebih lanjut, Nmap dapat memberikan indikasi mengenai keberadaan dan jenis *firewall* atau filter paket yang melindungi *host*.

Nmap dirancang untuk memindai jaringan besar dengan cepat, tetapi juga berfungsi dengan baik terhadap *host* tunggal. Fleksibilitas ini menjadikan Nmap sebagai alat yang sangat berguna dalam berbagai skenario audit keamanan jaringan. Nmap berjalan pada semua sistem operasi komputer utama, dengan paket *biner* resmi yang tersedia untuk *windows*, *linux* dan *macOSx*.

Dalam konteks pemindaian keamanan jaringan, Nmap berperan sebagai alat utama untuk identifikasi aset jaringan, pemetaan topologi jaringan, deteksi layanan yang berjalan, identifikasi potensi kerentanan dan monitoring perubahan konfigurasi jaringan.

2.4 Nikto Scanner

Nikto adalah pemindai server *web Open Source GPL (General Public License)* yang melakukan pengujian menyeluruh terhadap server *web* untuk berbagai item, termasuk lebih dari 7.000 file/program yang berpotensi berbahaya, memeriksa versi lama dari lebih dari 1250 server, dan masalah khusus versi pada lebih dari 270 server [\[23\]](#). Nikto juga memeriksa item konfigurasi server seperti keberadaan beberapa file indeks, opsi server HTTP, dan akan mencoba mengidentifikasi server *web* dan perangkat lunak yang terpasang.

Dalam menjalankan pemindaian, nikto melakukan pendekatan yang mengutamakan kecepatan dan kelengkapan analisis daripada beroperasi secara tersembunyi. Namun, setiap pengujian yang dilakukan menghasilkan aktivitas jaringan yang intensif sehingga jejaknya sangat mudah teridentifikasi.

Laporan yang dihasilkan oleh nikto tidak hanya sebatas pada celah keamanan yang bersifat kritis saja, nikto juga memberikan serangkaian temuan informatif yang berfungsi untuk memberi tahu administrator mengenai keberadaan direktori, berkas, atau konfigurasi server tertentu yang mungkin belum terdata, sekalipun tidak menimbulkan risiko keamanan secara langsung.

Nikto memiliki beberapa fungsi utama diantaranya kesalahan konfigurasi server dan perangkat lunak, deteksi file standar yang mungkin tidak dihapus setelah instalasi, pencarian file dan program yang tidak aman, identifikasi versi *software* yang memerlukan pembaruan

dan memberikan rekomendasi untuk melakukan pengujian manual yang lebih mendalam. Dalam pengujian keamanan *web*, nikto berperan sebagai *scanner* kerentanan otomatis, Mengidentifikasi teknologi dan versi *software* yang digunakan, Memberikan penilaian awal terhadap kondisi keamanan *web* server, dan Menjadi bagian dari *toolkit penetration testing* untuk *web applications*.

Item pemindaian dan *plugin* nikto sering diperbarui dan dapat diperbarui secara otomatis dari <https://www.cirt.net> , memastikan bahwa *tool* ini selalu memiliki informasi kerentanan terbaru untuk melakukan *scanning* yang efektif.

2.5 CVSS

Common Vulnerability Scoring System (CVSS) merupakan sebuah kerangka kerja standar global yang dirancang untuk mengkomunikasikan karakteristik dan mengukur tingkat keparahan kerentanan keamanan perangkat lunak. Versi terbarunya, CVSS 4.0, menyempurnakan metodologi penilaian dengan memperkenalkan nomenklatur metrik *Base*, *Threat*, dan *Environmental* (CVSS-BTE) untuk memberikan gambaran risiko yang lebih komprehensif [20]. Metrik Dasar (*Base Metrics*) mengevaluasi karakteristik fundamental kerentanan, seperti Vektor Serangan, Persyaratan Serangan (*Attack Requirements*), serta dampak terhadap kerahasiaan, integritas, dan ketersediaan, baik pada sistem yang rentan (*Vulnerable System*) maupun sistem selanjutnya (*Subsequent Systems*) [20].

Metrik Ancaman (*Threat Metrics*) menyesuaikan skor dasar dengan mempertimbangkan faktor-faktor temporal seperti ketersediaan bukti konsep eksploitasi. Sementara itu, Metrik Lingkungan (*Environmental Metrics*) memungkinkan organisasi untuk mengontekstualisasikan tingkat keparahan dengan memodifikasi metrik dasar sesuai dengan lingkungan spesifik dan kontrol keamanan yang ada. Penerapan kerangka kerja CVSS yang sistematis ini menjadi krusial dalam program manajemen kerentanan modern [3].

2.6 Django

Django adalah sebuah kerangka kerja pengembangan aplikasi *web* tingkat tinggi (*high-level*) berbasis *Python* yang dirancang untuk memfasilitasi pengembangan yang cepat dan pragmatis. Django menerapkan variasi dari pola arsitektur *Model-View-Controller* (MVC) yang dikenal sebagai *Model-View-Template* (MVT), yang secara tegas memisahkan antara logika bisnis (*Model*), logika presentasi (*View*), dan antarmuka pengguna (*Template*) [24]. Filosofi desain utamanya adalah "*batteries-included*", yang mengindikasikan bahwa Django menyediakan serangkaian fungsionalitas inti yang luas dan terintegrasi, siap pakai untuk

menangani kebutuhan pengembangan *web* yang umum [13].

Komponen-komponen fundamental ini mencakup *Object-Relational Mapper* (ORM) untuk interaksi basis data yang aman dan intuitif, sistem perutean URL, mesin *template*, serta berbagai mekanisme perlindungan keamanan bawaan terhadap vektor serangan umum. Dengan menyediakan fondasi yang kokoh dan komponen yang dapat digunakan kembali, Django memungkinkan pengembang untuk lebih fokus pada aspek unik dari aplikasi mereka daripada membangun fungsionalitas dasar dari awal, sehingga secara signifikan mempercepat siklus hidup pengembangan (*development lifecycle*) untuk aplikasi yang kompleks dan berskala produksi [24].

2.7 Docker

Docker adalah sebuah *platform* terkemuka yang mengimplementasikan teknologi kontainerisasi untuk mengemas aplikasi dan seluruh dependensinya ke dalam unit-unit *portabel* yang terisolasi. Teknologi ini memanfaatkan virtualisasi pada tingkat sistem operasi (*OS-level virtualization*) untuk memungkinkan beberapa kontainer berjalan secara simultan pada satu *host* tanpa memerlukan *hypervisor* atau sistem operasi tamu (*guest OS*) penuh untuk setiap aplikasi [16]. Setiap kontainer mencakup semua yang dibutuhkan aplikasi untuk berjalan—kode, *runtime*, *tools*, pustaka, dan pengaturan sehingga menjamin konsistensi perilaku aplikasi di berbagai lingkungan komputasi.

Konsistensi ini didefinisikan secara deklaratif melalui sebuah *Dockerfile*, yang berisi instruksi untuk membangun sebuah *image* kontainer yang spesifik dan dapat direproduksi [16]. Dengan menghilangkan variabilitas lingkungan antara mesin pengembang dan server produksi, docker secara efektif memecahkan tantangan klasik dalam pengembangan perangkat lunak terkait aplikasi berjalan yang berjalan lancar di komputer pengembang, tetapi gagal berfungsi saat dipindahkan ke server produksi. Efisiensi sumber daya, *portabilitas*, dan skalabilitas yang ditawarkan oleh docker menjadikannya sebagai teknologi fondasional dalam paradigma rekayasa perangkat lunak modern, termasuk arsitektur *microservices*, serta alur kerja *Continuous Integration/Continuous Deployment* (CI/CD) dalam ekosistem *cloud-native* [16].

BAB 3

SPESIFIKASI DAN DESAIN SISTEM

3.1 Spesifikasi Sistem

Pengujian keamanan server bertujuan untuk meminimalisir celah keamanan yang dapat dimanfaatkan oleh *hacker* untuk merugikan pihak *administrator* server. Keamanan server harus mencakup perlindungan data sensitif, mencegah akses yang tidak sah, menjamin ketersediaan layanan, dan mencegah penyalahgunaan server^[1]. Maka, terdapat beberapa spesifikasi dari *platform* pengujian keamanan server berbasis *Website* ini memenuhi standar yang telah ditentukan dan sesuai dengan kebutuhan pengguna. Berikut merupakan tabel yang dilampirkan mengenai spesifikasi yang menjadi fokus utama dalam pengembangan *platform* ini :

Tabel 3. 1 Spesifikasi Sistem

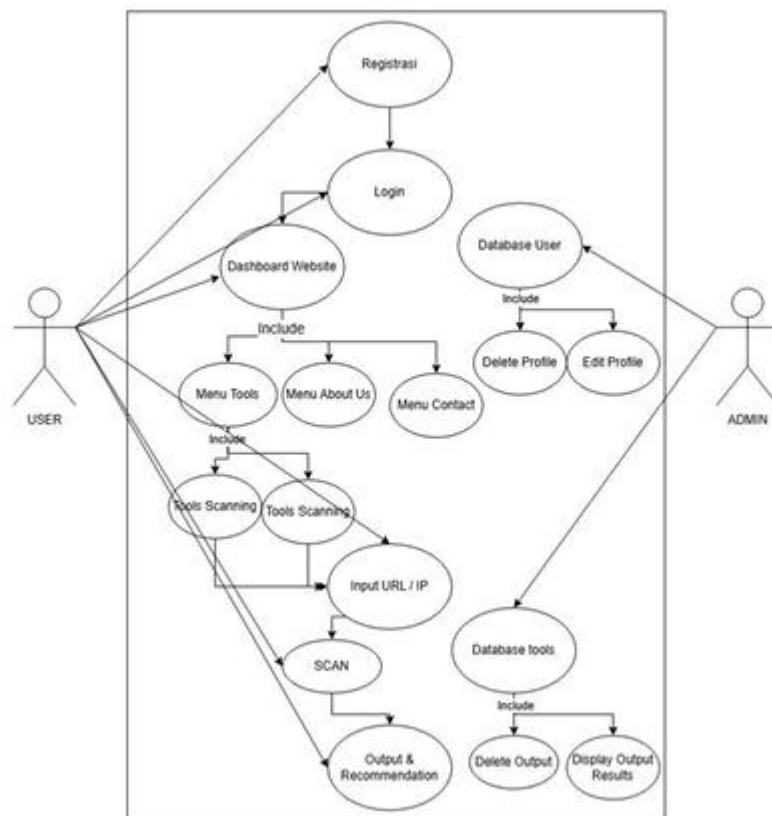
No	Aspek/Fitur	Keterangan
1.	<i>Scanning</i>	<i>Scanning</i> dalam pengujian keamanan server ini merupakan proses mendeteksi, mengidentifikasi, dan menganalisis kerentanan, konfigurasi salah, atau potensi ancaman keamanan pada server ^[4] .
2.	<i>Reporting</i>	<i>Reporting</i> merupakan proses dokumentasi dan pelaporan hasil - hasil pengujian keamanan yang telah dilakukan terhadap sistem, jaringan, atau server. Tujuan dari <i>reporting</i> adalah untuk menyampaikan temuan dan menganalisis risiko. <i>Reporting</i> ini memberikan informasi yang jelas kepada pengguna untuk memahami kondisi keamanan dalam server tersebut ^[12] .

3.	Saran/Rekomendasi	Saran atau rekomendasi dalam konteks pengujian keamanan server atau sistem adalah tindakan atau strategi yang diusulkan untuk mengatasi atau memitigasi kerentanan, ancaman, atau masalah yang ditemukan selama pengujian keamanan [6] .
----	-------------------	--

3.2 Desain Sistem

Desain sistem yang akan digunakan adalah pengembangan sebuah *platform* pengujian keamanan server berbasis *Website* yang mengintegrasikan beberapa *tools* pengujian keamanan, dengan fokus utamanya pada *tools* nmap dan nikto. Dengan adanya penggabungan beberapa *tools* pada *platform* pengujian keamanan ini dapat mempermudah pengguna untuk mendapatkan kemampuan beberapa *tools* secara bersamaan. Dalam satu *platform*, pengguna dapat menjalankan pemindaian nmap untuk mengidentifikasi perangkat dalam jaringan, menentukan layanan yang berjalan, serta menemukan kerentanan pada *port* server tersebut [\[8\]](#). Pengguna juga dapat menggunakan Nikto untuk menganalisis kerentanan pada server *web* seperti file sensitif, konfigurasi lemah, dan kelemahan plugin [\[25\]](#). *Platform* ini juga mendukung kemampuan *reporting* berupa informasi umum *scan*, daftar kerentanan serta ringkasan kerentanan dalam bentuk *chart* dan file PDF yang dapat pengguna unduh, serta terdapat saran yang didukung oleh rekomendasi AI. Fitur ini memastikan laporan yang dihasilkan lebih akurat dan relevan, dengan meminimalkan risiko pelaporan palsu.

3.2.1 Usecase Diagram

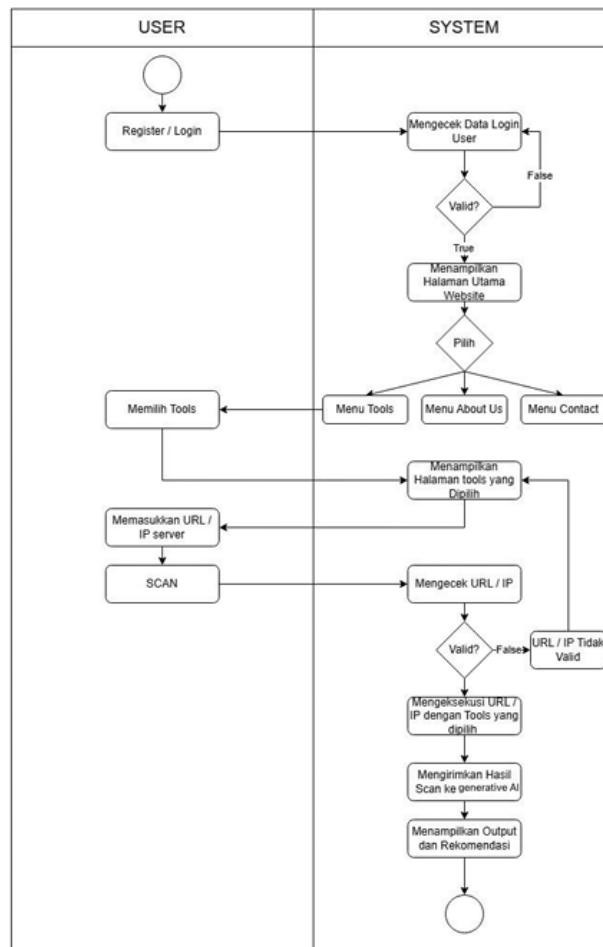


Gambar 3. 1 Usecase Diagram

Gambar 3.1 merupakan *Usecase* diagram yang menggambarkan sistem pengujian keamanan berbasis *Website* yang melibatkan dua pihak utama yaitu *user* dan *admin*. Pada sisi *user* dapat mulai menjalankan *Website* melalui tahap awal yaitu registrasi. Setelah berhasil melakukan registrasi, *user* dapat melakukan *login* untuk masuk ke *dashboard Website* yang terdiri dari *menu tools*, *menu about us*, *menu contact*. Pada *menu tools*, *user* dapat memulai pengujian keamanan dengan menggunakan *tools scanning* dan memasukkan URL/IP yang akan menjadi target pengujian. Setelah itu, proses *scanning* dilakukan dan akan menghasilkan *output reporting* serta rekomendasi yang berisi hasil analisis dan rekomendasi perbaikan.

Pada sisi *admin* berfokus pada pengelolaan data. Dengan adanya *database user*, *admin* dapat mengelola informasi *user* seperti *delete* profil dan *edit* profil. *Admin* juga memiliki akses ke *database tools* untuk mengelola hasil *scanning* seperti menampilkan hasil *scanning* pada *display output result* dan menghapus hasil *scanning* melalui *delete output*.

3.2.2 Activity Diagram



Gambar 3. 2 Activity Diagram

Gambar 3.2 merupakan *activity* diagram yang menggambarkan mengenai alur kerja antara *user* dan sistem. Dimulai dari *user* melakukan proses registrasi/*login* lalu diverifikasi oleh sistem pada langkah memeriksa data *login user*. Jika *login* dinyatakan *valid* maka sistem akan mengarahkan *user* ke halaman utama *Website*, namun jika gagal maka sistem akan mengecek kembali data *login user*. Di dalam halaman utama *Website* terdapat 3 *menu* yang dapat dipilih oleh *user* yaitu *menu tools*, *about us* dan *contact*.

Jika *user* memilih *menu tools*, sistem akan menampilkan halaman sesuai dengan *tools* yang dipilih. Pada halaman tersebut *user* dapat memasukkan URL/IP. Lalu, sistem akan mengecek URL/IP yang dimasukan *valid* atau tidak. Jika URL/IP tidak *valid* maka sistem akan kembali ke *menu tools*. Namun, jika URL/IP *valid* maka sistem akan mengeksekusi URL/IP menggunakan *tools* yang sebelumnya sudah dipilih oleh *user*. Lalu, sistem akan mengirimkan hasil *scanning* ke AI. setelah itu, sistem menampilkan *output* serta rekomendasi perbaikan di *Website*.

3.3 Metode Pengukuran yang Sesuai dengan Solusi Terpilih

Pada bagian ini merupakan metode pengukuran yang digunakan untuk mendukung implementasi solusi terpilih. Metode pengukuran ini mencakup proses *scanning*, *reporting* dan rekomendasi perbaikan. Berikut merupakan mekanisme pengukuran *scanning* yang tercantum pada Tabel 3.2 Pengukuran *Scanning*

Tabel 3. 2 Pengukuran *Scanning*

Keterangan	<i>Scanning</i>
Rincian	Memindai kerentanan target dengan menggunakan dua pilihan <i>tools</i> yaitu nmap dan nikto dengan fitur sebagai berikut : 1. Nmap <i>scanner</i> : OS <i>Detection</i>, Port <i>scan</i>, <i>Vulnerability</i>, dan <i>comprehensive</i>. 2. Nikto <i>Scanner</i> : <i>Basic scan</i>, <i>Full scan</i>, <i>SSL/TSL scan</i>, dan <i>custom scan</i> (menyesuaikan parameter lanjutan).
Mekanisme Pengukuran	Menguji fungsi <i>tools</i> untuk mengidentifikasi kerentanan pada sebuah target dengan menggunakan salah satu <i>tools</i> yang tersedia (nmap atau nikto)
Prosedur Pengukuran	- Pilih salah satu opsi <i>tools</i> (nmap atau nikto) - Masukkan URL/IP target yang akan diuji kerentanannya - Memilih fitur <i>scan</i> yang tersedia pada masing – masing <i>tools</i> sesuai kebutuhan. - Pengecekan status terhadap URL/IP target - Status target dapat di akses maka <i>scanning</i> dilanjutkan

Berikut merupakan mekanisme pengukuran proses *reporting* yang tercantum pada **Tabel 3.3 Reporting**.

Tabel 3. 3 Reporting

Keterangan	Reporting
Rincian	Menyediakan pelaporan berupa ringkasan pemindaian, skor keamanan, analisis keamanan detail dengan kategori tingkat kerentanan <i>Critical, High, Medium, Low, Info.</i> dan menyediakan pelaporan data hasil <i>security scan</i> .
Mekanisme Pengukuran	- Menampilkan ringkasan pemindaian secara umum diantaranya target yang di uji, <i>tools</i> yang digunakan, tipe fitur scan yang digunakan, total kerentanan yang ditemukan. - Pengecekan nilai keamanan berdasarkan kerentanan yang ditemukan dan ditampilkan dalam angka pada skor keamanan sesuai dengan standar perhitungan CVSS. - Menjelaskan temuan kerentanan secara detail dan mengelompokannya sesuai dengan kategori tingkat kerentanan berdasarkan standar OWASP. - Menampilkan ringkasan hasil <i>reporting</i> dalam bentuk point – point utama.
Prosedur Pengukuran	- Sistem menemukan kerentanan pada url/ip target. - Sistem mengelompokan kerentanan sesuai dengan level kategori kerentanan. - Menghitung skor kemanan berdasarkan standar perhitungan CVSS. - Menentukan skor keamanan url/ip secara keseluruhan dengan rentang 0-100. - Menampilkan seluruh data <i>reporting</i> ke halaman riwayat.

Berikut merupakan mekanisme pengukuran pada bagian rekomendasi perbaikan yang tercantum pada Tabel 3.4 Rekomendasi Perbaikan

Tabel 3. 4 Rekomendasi Perbaikan

Keterangan	Rekomendasi Perbaikan
Rincian	Menyediakan rekomendasi perbaikan berbasis <i>generative</i> AI.
Mekanisme Pengukuran	Menampilkan rekomendasi perbaikan dari kerentanan ditemukan dan dapat diunduh dalam format PDF.
Prosedur Pengukuran	- Menyimpan hasil <i>scanning</i> ke <i>database</i>. - Hasil <i>scanning</i> dikirim ke <i>generative</i> AI. - AI mengolah data hasil <i>scanning</i>. - <i>Generative</i> AI menghasilkan rekomendasi dari data tersebut. - Hasil rekomendasi dari <i>generative</i> AI disimpan di <i>database</i>. - Hasil rekomendasi perbaikan ditampilkan pada halaman riwayat.

BAB 4

IMPLEMENTASI

4.1 Deskripsi umum implementasi

Pada implementasi *platform* Pengujian Keamanan Server Berbasis *Website* dirancang sesuai dengan desain solusi terpilih sebelumnya yaitu dengan mengintegrasikan beberapa *tools* pengujian keamanan yang dibuat dalam bentuk *Website*. Sistem implementasi dirancang sesuai dengan desain solusi terpilih pada CD-3. Proses perancangan dimulai dengan melakukan *Focus Group Discussion* (FGD), FGD ini mendiskusikan *tools* yang akan digunakan untuk memindai ancaman atau kerentanan pada suatu server dan belajar untuk memahami serta mengetahui proses ancaman yang sering terjadi pada suatu server saat ini.

Pada platform ini, *tools* yang ditentukan berfokus pada dua *tools* utama yang akan digunakan yaitu Nmap dan Nikto. Nmap berfungsi untuk mengidentifikasi perangkat dalam jaringan, menentukan layanan yang berjalan, serta memetakan topologi jaringan. Sementara itu, Nikto dapat digunakan untuk menganalisis server *web* yang terdeteksi, mengevaluasi kerentanan umum seperti file sensitif yang dapat diakses, konfigurasi server yang lemah, atau kelemahan pada *plugin* yang digunakan.

Dalam pengembangan implementasi *platform* pengujian keamanan server berbasis *Website* ini terdapat tiga bagian utama yaitu *frontend*, *backend*, dan *docker*. Pada bagian *frontend* menggunakan HTM, CSS, dan JavaScript sebagai bahasa pemrogramannya, sedangkan untuk *framework* dan *library frontend* menggunakan bootstrap, jQuery, *Font Awsome*, dan untuk *engine*-nya menggunakan *template* dari Django. Pada bagian *backend* menggunakan *framework* Django dengan bahasa pemrograman Python, serta integrasi *tools* Nmap dan Nikto sebagai inti dari aplikasi. Dan pada bagian Docker, platform ini menggunakan Docker untuk *containerization* seluruh komponen sistem (backend Django, Nmap, Nikto, dan server web) ke dalam microservice terpisah.

4.2 Detail Implementasi

Pada bagian detail implementasi ini merupakan paparan dari sistem yang telah dirancang sebelumnya. Terdapat 2 bagian pada detail implementasi ini yaitu *backend* dan *frontend*.

4.2.1 Backend

Backend merupakan bagian dari sistem aplikasi atau *Website* yang tidak terlihat oleh pengguna akhir (*end user*), yang berfungsi sebagai "mesin" di balik layar untuk memproses data, mengelola *database*, dan menangani logika aplikasi^[15].

Berikut merupakan struktur *backend*, terdapat beberapa folder diantaranya *core*, *nikto scanner*, *nmap scanner*, *scan history*, *scanner project*. Pada folder tersebut terdapat file bawaan dari django diantaranya adalah:

File *init.py*, file ini khusus dalam python yang berfungsi sebagai "penanda" bahwa direktori tersebut adalah python *package*^[9].

File *admin.py* adalah jantung dari Django *admin interface*, file ini berfungsi untuk mengelola data aplikasi. File ini berisi konfigurasi dan *customization* untuk Django *Admin panel*, yang secara otomatis menghasilkan *interface* CRUD (*Create, Read, Update, Delete*) berdasarkan model yang didefinisikan^[9].

File *apps.py*, file ini berisi *class* konfigurasi aplikasi dan berfungsi sebagai pusat konfigurasi metadata aplikasi. Django menggunakan file ini untuk mengenali dan mengatur aplikasi dalam *registry* aplikasi global^[9].

File *models.py*, file ini merupakan inti dari aplikasi django yang mendefinisikan struktur data dan kerangka kerja utama aplikasi melalui Django ORM (*Object-Relational Mapping*), file ini berisi definisi model-model yang mempresentasikan tabel *database* dan relasi antar tabel^[9].

File *test.py*, file ini berfungsi untuk memastikan aplikasi berfungsi dengan benar. File ini menguji *models*, *views*, *forms*, dan berbagai komponen aplikasi secara otomatis^[9].

File *views.py*, file yang berisikan *view function* atau *view classes* yang menangani HTTP *request* dan menghasilkan HTTP *response*. *Views* bertanggung jawab untuk memproses *request* data, berinteraksi dengan *models*, menjalankan cara kerja utama, dan mempersiapkan *context* data untuk *template* atau API *response*^[9].

Ada beberapa aplikasi yang dibuat manual oleh penulis untuk menyesuaikan kebutuhan dalam pengembangan *platform*. Aplikasi tersebut dibuatkan di dalam

folder *platform*. Berikut beberapa *source code* tambahan yang disimpan dalam beberapa folder.

Bagian ini merupakan *source code* pada file *scoring.py* yang terletak di folder *core*. File ini merupakan file khusus yang dibuat untuk menangani logika perhitungan skor dalam penemuan kerentanan.

Folder *core*:

```
def calculate_security_score(scan_result):  
def get_security_rating(score):  
def get_score_color(score):
```

Berikut merupakan *source code* pada file *urls.py* yang terdapat di folder *core*, folder *nikto_scanner* dan *nmap_scanner*. File ini berisi *URLconf* (*URL configuration*) yang mendefinisikan pola URL dan *Mapping* ke *view function* atau *classes*. File ini mencocokkan URL dengan *regex* atau *path patterns*.

Folder *core* :

```
from django.urls import path  
from . import views  
urlpatterns = [  
    # URL yang sudah ada - PERTAHANKAN  
    path('', views.home_view, name='home'),  
    path('about/', views.about_view, name='about'),  
    path('contact/', views.contact_view, name='contact'),  
    # URL UNTUK AUTHENTICATION  
    path('dashboard/',  
views.dashboard_view, name='dashboard'),  
    path('profile/', views.profile_view,  
name='profile'),  
    path('logout/', views.custom_logout_view,  
name='custom_logout'),  
    # API URL  
    path('api/save-scan/', views.save_scan_result,  
name='save_scan_result'),  
]
```

Folder *nikto_scanner* :

```
from django.urls import path
from . import views

urlpatterns = [
    path('', views.nikto_scan_view, name='nikto_scan'),
]
```

Folder *Nmap_scanner* :

```
from django.urls import path
from . import views
urlpatterns = [
    path('', views.nmap_scan_view, name='nmap_scan'),
]
```

Folder *Scan history* :

```
from django.urls import path
from . import views
```

```
urlpatterns = [
```

Berikut ini merupakan file *context_processors.py* berisikan fungsi – fungsi *context processor* yang merupakan fitur *powerful* Django untuk menyediakan data yang tersedia di semua *template*. File ini merupakan fungsi python yang menerima *HttpRequest object* dan mengembalikan *dictionary* berisi variabel – variabel yang akan ditambahkan ke *context* setiap *template*.

Folder *core* :

```
def navigation(request):
    """
    Context processor untuk menentukan item navigasi
    aktif
    """
    path = request.path.strip('/')

    # Default active state
    nav_active = {
    if path == '':
```

```

elif path.startswith('nmap'):
elif path.startswith('nikto'):
elif path.startswith('history'):
elif path.startswith('about'):
elif path.startswith('contact'):
return {'nav_active': nav_active}

```

Pada file `forms.py` ini merupakan file yang berfungsi untuk menangani semua aspek *form handling*, dari *rendering* HTML form hingga validasi data *server-side*.

Folder *core* :

```

# forms.py

from django import forms

from django.contrib.auth.models import User

from .models import UserProfile

class UserProfileForm(forms.ModelForm):

```

File `utils.py` merupakan modul utilitas dalam aplikasi ini yang terdapat pada folder `nikto_scanner` dan `nmap_scanner` yang berfungsi sebagai *layer* abstraksi antara aplikasi *web* Django dan *command-line security tools*. File ini berperan sebagai penghubung yang menghubungkan *interface* dengan *user* dengan *tools* yang dimiliki `nmap` dan `nikto`.

Pada Folder `Nikto_scanner` :

```

import subprocess
import json
import re

from core.models import ScanResult

def run_nikto_scan(target, scan_type, user):
def parse_nikto_output(output):
def aggressive_parse_nikto_output(output):
def classify_severity(description):
# Legacy functions kept for compatibility
def alternative_parse_nikto_output(output):

```

Pada folder *nmap_scanner* :

```
import nmap
import json
from core.models import ScanResult
def run_nmap_scan(target, scan_type, user):
    def classify_vulnerability_severity(script_name,
output):
```

File *scan_extras.py* adalah custom *templatetags* dan *filters* dalam django yang berfungsi untuk memperluas kemampuan *template engine* Django. File ini berisi *utility functions* yang dapat digunakan langsung di dalam *template* HTML untuk melakukan operasi data *processing*, *mathematical calculations*, dan data *formatting* yang tidak tersedia secara *default* di Django.

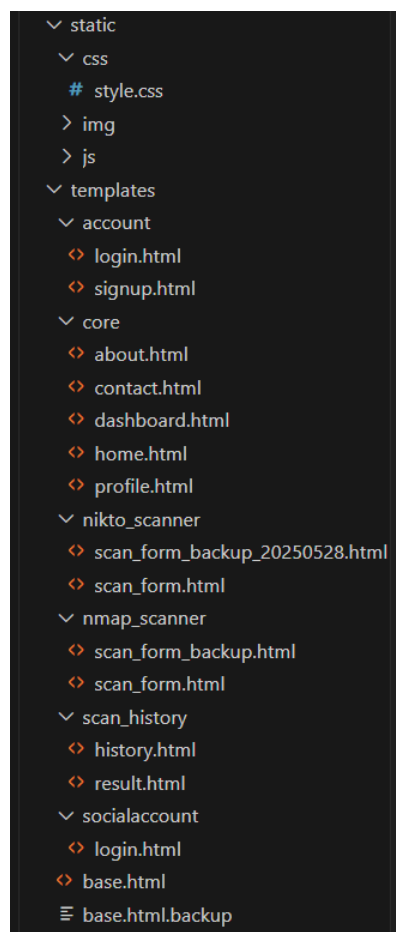
Folder *templatetags* :

```
from django import template
from django.utils.safestring import mark_safe
import json
register = template.Library()
@register.filter
def jsonify(value):
@register.filter
def get_item(dictionary, key):
@register.filter
def mul(value, arg):
@register.filter
def div(value, arg):
@register.filter
def safe_div(value, arg):
```

4.2.2 Frontend

Frontend merupakan salah satu bagian dari sistem aplikasi atau *web* yang berperan untuk pengembangan bagian *Website* diantaranya desain *Website*, animasi *Website*, dan konten yang ditampilkan pada *Website* yang dapat dilihat dan berinteraksi langsung dengan pengguna^[21].

Gambar 4.1 Struktur *Frontend* merupakan struktur file *frontend*, dimana pada folder *templates* menyimpan kode HTML untuk tampilan *Website* seperti struktur dasar halaman, tampilan seperti *heading*, dan *font default Website*. HTML hanya bisa menghasilkan tampilan yang *basic* tanpa warna, terdapat juga folder CSS yang berisi *style.css* untuk mengatur tampilan *Website* seperti *font*, *layout*, *style*, dan mengatur urutan pada *Website* yang dapat yang dilihat *user*. Sedangkan folder *js* atau JavaScript didalamnya terdapat *source code* yang berfungsi untuk membuat *Website* dinamis dan interaktif, menangani interaksi *user* seperti klik, berpindah, dan mengetik, dan Mengubah halaman *Website* secara *realtime* sesuai dengan hasil temuan kerentanan.



Gambar 4. 1 Struktur *Frontend*

Berikut merupakan *source code* HTML *Structure* dan *Head Section* yang merupakan bagian awal dari file HTML menggunakan *framework* Django digunakan untuk membuat antarmuka *Website*. Pada *source code* tersebut memuat file CSS dan JavaScript. Selain itu, pada *source code* ini menggunakan bootstrap untuk *styling*, *font awesome* untuk *icon* dan AOS (*Animate On Scroll*) untuk animasi pada halaman.

```
<!DOCTYPE html>
{% load static %}
<html lang="id">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width,
initial-scale=1.0">
    <title>{% block title %}Vulnerability Scanner{%
endblock %}</title>
    <!-- Bootstrap CSS -->
    <link
href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0-
alpha1/dist/css/bootstrap.min.css" rel="stylesheet">
    <!-- Font Awesome -->
    <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/6.1.1/css/all.min.css">
    <!-- AOS - Animate On Scroll -->
    <link href="https://unpkg.com/aos@2.3.1/dist/aos.css"
rel="stylesheet">
    <!-- Custom CSS -->
    <link rel="stylesheet" href="{% static 'css/style.css'
%
```

Berikut merupakan *source code* struktur navigasi utama yang menggunakan bootstrap sebagai *framework* CSS. Navbar ini berfungsi sebagai navigasi utama yang memungkinkan pengguna untuk berpindah antar halaman dengan mudah.

```
<!-- Navbar -->
<nav class="navbar navbar-expand-lg navbar-dark fixed-
top">
    <div class="container">
        <a class="navbar-brand" href="{% url 'home'
%}">
```

```

        <i class="fas fa-shield-alt"></i>
        Vulnerability Scanner
    </a>

    <button class="navbar-toggler" type="button" data-bs-
toggle="collapse" data-bs-target="#navbarNav">
        <span class="navbar-toggler-icon"></span>
    </button>

    <div class="collapse navbar-collapse" id="navbarNav">
        <ul class="navbar-nav me-auto">
            {% if user.is_authenticated %}
                <li class="nav-item">

<li class="nav-item dropdown">
<li class="nav-item">
</li>

                {% endif %}
            <li class="nav-item">
</li>
</ul>
<!-- User Authentication Menu -->
<ul class="navbar-nav">

```

Berikut merupakan *source code* pada bagian dari file CSS yang berfungsi untuk mengatur tampilan pada *platform* ini. Pada *source code* bagian *root* terdapat sejumlah variabel CSS seperti `--primary-color`, `--detikary-color`, dan `--danger-color` yang berfungsi untuk menetapkan warna warna utama yang digunakan pada *platform*. Terdapat juga *source code* bagian *body* diantaranya `padding-top: 56px;` yang berfungsi untuk memberikan jarak pada halaman. Terdapat juga *source code font* dan *color* untuk mengatur warna dan *font* yang digunakan.

```

root {
    --primary-color: #2c3e50;
    --detikary-color: #1abc9c;
    --danger-color: #e74c3c;
    --warning-color: #f39c12;
    --success-color: #2ecc71;
    --info-color: #3498db;

```



```

        --light-color: #ecf0f1;
        --dark-color: #34495e;
    }
    body {
        padding-top: 56px;
        font-family: 'Poppins', sans-serif;
        background-color: #f8f9fa;
        color: #333;
    }

```

Pada bagian ini merupakan *source code* *setupScanningForms* pada file Javascript yang berfungsi untuk melakukan proses validasi dan animasi saat pengguna melakukan pemindaian (*scanning*). Dengan adanya fungsi *setupScanningForms()* maka aplikasi akan mencari semua elemen yang memiliki kelas *.scan-form* dan melakukan validasi. Jika validasi berhasil maka akan ditampilkan animasi *loading* dengan menggunakan fungsi *showLoadingSpinner()* dengan keterangan bahwa proses *scanning* sedang berlangsung.

```

function setupScanningForms() {
    const scanForms =
document.querySelectorAll('.scan-form');

    scanForms.forEach(form => {
        form.addEventListener('submit', function(e) {
            // Validasi input
            const targetInput =
form.querySelector('input[name="target"]');
            if (!targetInput.value.trim()) {
                e.preventDefault();
                showAlert('Target tidak boleh
kosong!', 'danger');
                return;
            }

            // Tampilkan animasi loading
            showLoadingSpinner('Scanning in
progress... This may take a few minutes.');
```

4.2.3 Docker

Berikut merupakan konfigurasi `docker-compose.yml` terbaru yang mendefinisikan beberapa service utama dalam sistem *Vulnerability Scanner*, yaitu: redis, web, nikto-scanner, dan nmap-scanner. Setiap service memiliki peran tersendiri yang saling terhubung melalui network `vulnscanner_network`.

```
redis:

  image: redis:7-alpine

  container_name: vulnscanner_redis

  volumes:

    - redis_data:/data

  healthcheck:

    test: ["CMD", "redis-cli", "ping"]

    interval: 30s

    timeout: 10s

    retries: 5

  restart: unless-stopped

  networks:

    - vulnscanner_network
```

Service redis berfungsi sebagai sistem caching dan task queue untuk aplikasi scanner. Redis digunakan untuk menyimpan data sementara secara efisien dan mengatur antrian tugas antar komponen. Service ini menggunakan image ringan `redis:7-alpine`, dengan volume `redis_data` untuk menyimpan data secara persisten. Terdapat juga konfigurasi `healthcheck` yang memastikan Redis berjalan dengan baik, serta network `vulnscanner_network` agar dapat berkomunikasi dengan container lain.

```

web:
  build: .
  container_name: vulnscanner_web
  environment:
  volumes:
    - ./media:/app/media
    - ./static:/app/static
  ports:
    - "8000:8000"
  depends_on:
    redis:
      condition: service_healthy
  healthcheck:
    test: ["CMD", "curl", "-f",
"http://localhost:8000/"]
    interval: 30s
    timeout: 10s
    retries: 3
  restart: unless-stopped
  networks:
    - vulnscanner_network

```

Service web merupakan *core* aplikasi berbasis Django yang dibangun langsung dari direktori proyek (build: .). Service ini mengatur berbagai environment variables penting seperti DATABASE_URL, REDIS_URL, dan DJANGO_SUPERUSER untuk pengaturan admin aplikasi. web terhubung dengan Redis, menyajikan web app melalui port 8000, dan menyimpan media serta file statis menggunakan volume lokal. Healthcheck digunakan untuk memastikan service aktif dengan mengakses URL lokal http://localhost:8000/.

```

nikto-scanner:
  build: ./monitoring/nikto-worker
  container_name: nikto_scanner
  environment:
    - REDIS_URL=redis://redis:6379/0
    - WEBAPP_URL=http://vulnscanner_web:8000
    - WORKER_MODE=standby
  restart: unless-stopped
  depends_on:
    redis:
      condition: service_healthy
  networks:
    - vulnscanner_network
  healthcheck:
    test: ["CMD", "python", "-c", "import redis;
redis.Redis.from_url('redis://redis:6379/0').ping()"]
    interval: 30s
    timeout: 10s
    retries: 3

```

Service `nikto-scanner` merupakan *worker container* untuk menjalankan pemindaian keamanan berbasis Nikto. Service ini dibangun dari direktori `./monitoring/nikto-worker` dan berjalan dalam mode siaga (*standby*) untuk menunggu tugas dari sistem. Komunikasi dilakukan melalui redis dan web app, tanpa membuka port publik karena hanya digunakan secara internal. Healthcheck memastikan koneksi redis aktif sebelum tugas dijalankan.

```

nmap-scanner:
  build: ./monitoring/nmap-worker
  container_name: nmap_scanner
  environment:
    - REDIS_URL=redis://redis:6379/0
    - WEBAPP_URL=http://vulnscanner_web:8000
    - WORKER_MODE=standby
  restart: unless-stopped
  depends_on:
    redis:
      condition: service_healthy
  networks:
    - vulnscanner_network
  healthcheck:
    test: ["CMD", "python", "-c", "import redis;
redis.Redis.from_url('redis://redis:6379/0').ping()"]
    interval: 30s
    timeout: 10s
    retries: 3

```

Service `nmap-scanner` berfungsi serupa dengan `nikto-scanner`, namun menggunakan tool Nmap untuk melakukan pemindaian jaringan. Service ini dibangun dari direktori `./monitoring/nmap-worker` dan juga berjalan dalam mode stand by. Konfigurasi `depends_on` memastikan bahwa Redis telah sehat sebelum container ini aktif, dan `healthcheck` memastikan konektivitas redis tersedia.

```

volumes:
  redis_data:

```

Volume `redis_data` digunakan untuk menyimpan data Redis secara persisten agar tetap tersedia meskipun container dimatikan atau di-*restart*. Hal ini menjaga stabilitas sistem caching dan task queue.

```

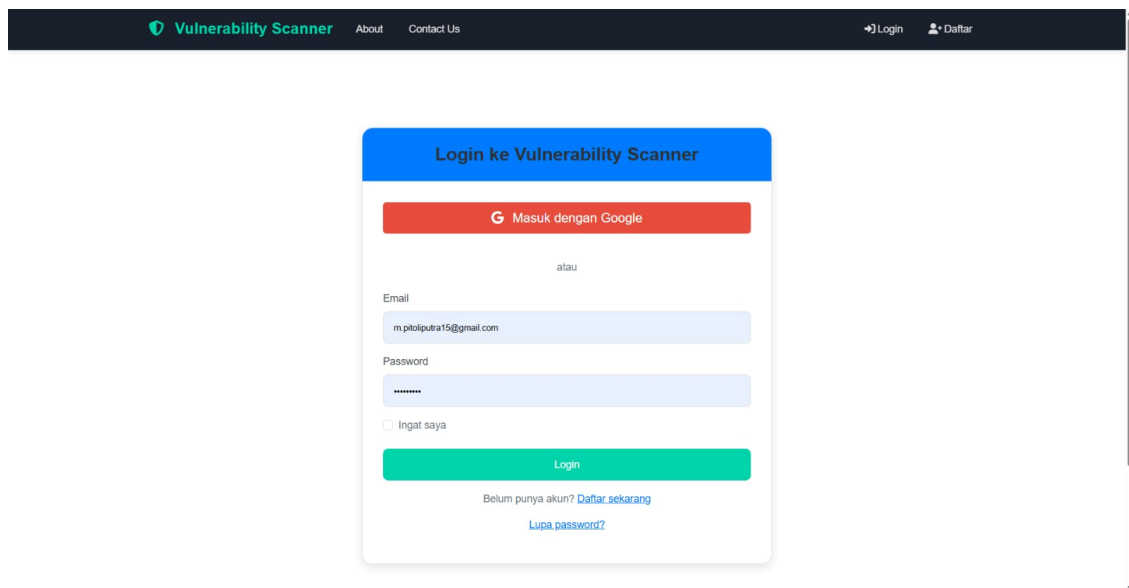
networks:
  vulnscanner_network:
    driver: bridge

```

Network vulnscanner_network menggunakan driver bridge untuk menghubungkan semua service dalam jaringan internal Docker. Konfigurasi ini memungkinkan setiap container saling berkomunikasi menggunakan nama servicenya sebagai hostname.

4.3 Prosedur Pengoperasian Solusi

Platform ini dapat diakses oleh pengguna melalui *browser* tanpa memerlukan instalasi tambahan, sehingga memudahkan pengguna dalam melakukan pengujian terhadap keamanan server secara mandiri.



Gambar 4.2 *Login Page*

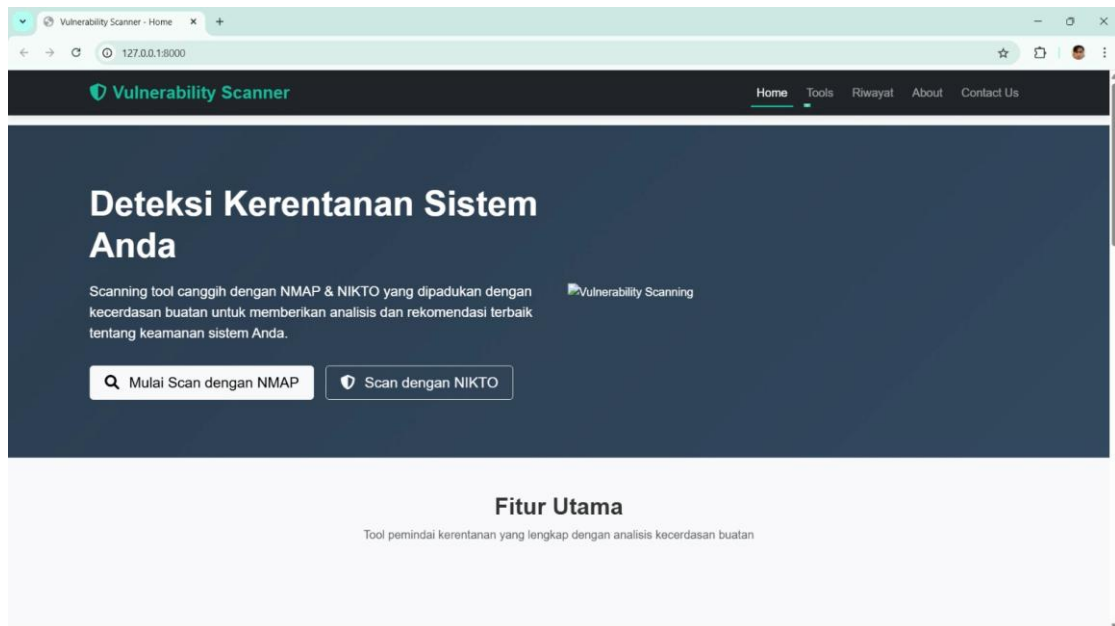
Setelah *platform* dapat diakses, langkah selanjutnya pengguna dapat melakukan *login* terlebih dahulu pada halaman *login page* apabila pengguna telah memiliki akun. Namun, apabila pengguna belum memiliki akun maka terlebih dahulu melakukan pendaftaran pada menu “Daftar Sekarang”.



Gambar 4.3 *Menu Bar*

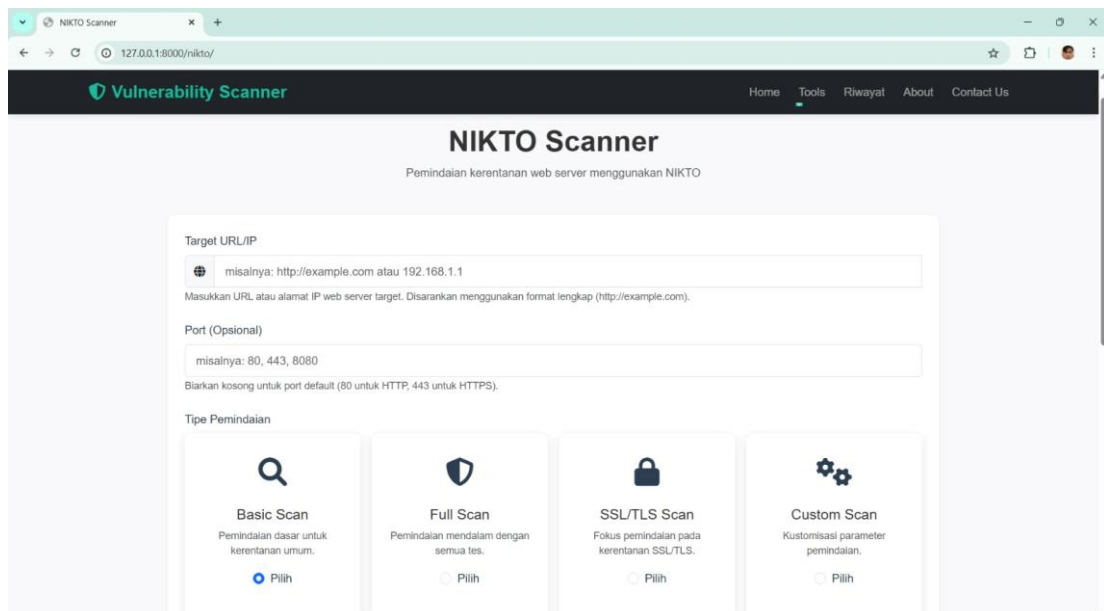
Gambar 4.3 Menu Bar merupakan tampilan menu bar pada *platform* ini, terdapat beberapa *menu* yang dapat diakses diantaranya “*Home*” yang mengarahkan pengguna ke halaman utama, *menu* “*Tools*” yang dapat digunakan oleh pengguna untuk mengakses berbagai fitur *scanning* dalam *platform*, *menu* “*Riwayat*” yang menampilkan catatan hasil pemindaian yang telah dilakukan, *menu* “*About*” yang memberikan informasi mengenai

platform ini dan menu “*Contact Us*” yang dapat digunakan oleh pengguna untuk menghubungi tim layanan pelanggan.



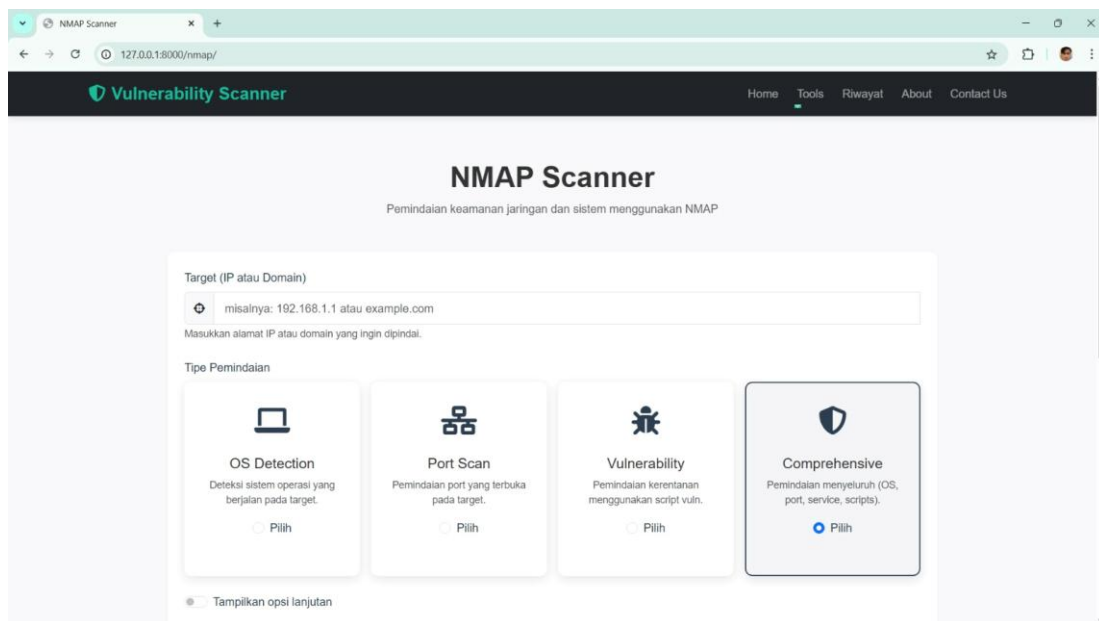
Gambar 4.4 *Home Page*

Gambar 4.4 *Home Page* merupakan halaman “*Home*” yang merupakan fitur utama dari *platform* ini. Pada menu “*home*” tersebut pengguna dapat memilih melakukan *scanning* menggunakan nikto atau nmap.



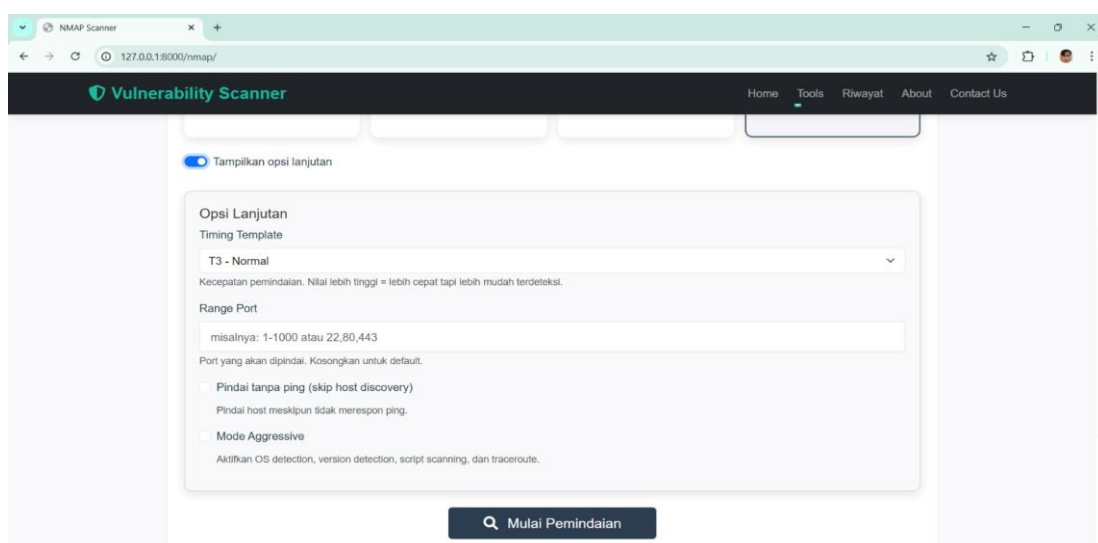
Gambar 4.5 *Fitur-fitur Nikto Scanner*

Gambar 4.5 Fitur-fitur Nikto Scanner merupakan *page* dari fitur Nikto Scanner, pada *page* ini pengguna dapat memasukkan target URL/IP dan *Port*. Pengguna dapat memilih tipe pemindaian yang ingin dilakukan, terdapat beberapa tipe diantaranya *Basic Scan*, *Full Scan*, *SSL/TLS scan* dan *custom scan*.



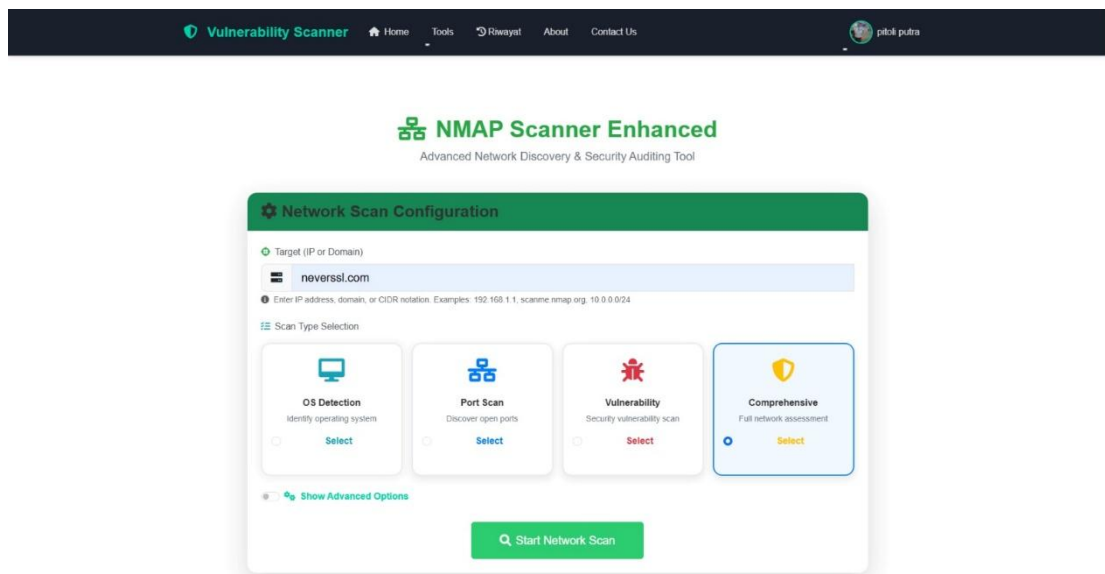
Gambar 4.6 Fitur-fitur Nmap Scanner

Gambar 4.6 Fitur-fitur Nmap Scanner merupakan *page* dari fitur Nmap Scanner pada *platform* pengujian ini. Pada *page* ini pengguna dapat memasukkan target IP atau *domain* lalu memilih tipe pemindaian yang ingin dilakukan, terdapat beberapa tipe diantaranya *OS Detection*, *Port Scan*, *Vulnerability* dan *Comperhensive*.



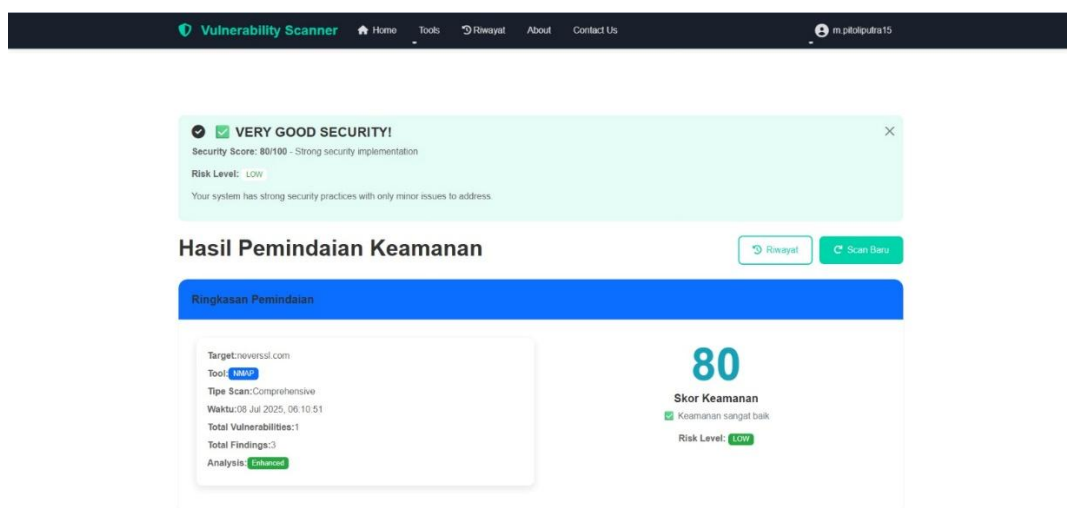
Gambar 4.7 Opsi Lanjutan Nmap Scanner

Pada Nmap *scanner* ini pengguna juga dapat menggunakan opsi lanjutan yang berisi pilihan waktu pemindaian, terdapat juga pilihan *range port* yang akan dipindai apabila pengguna hanya ingin memindai salah satu *port* saja, terdapat juga pilihan “pindai tanpa *ping*” serta pilihan “mode *aggressive*”.



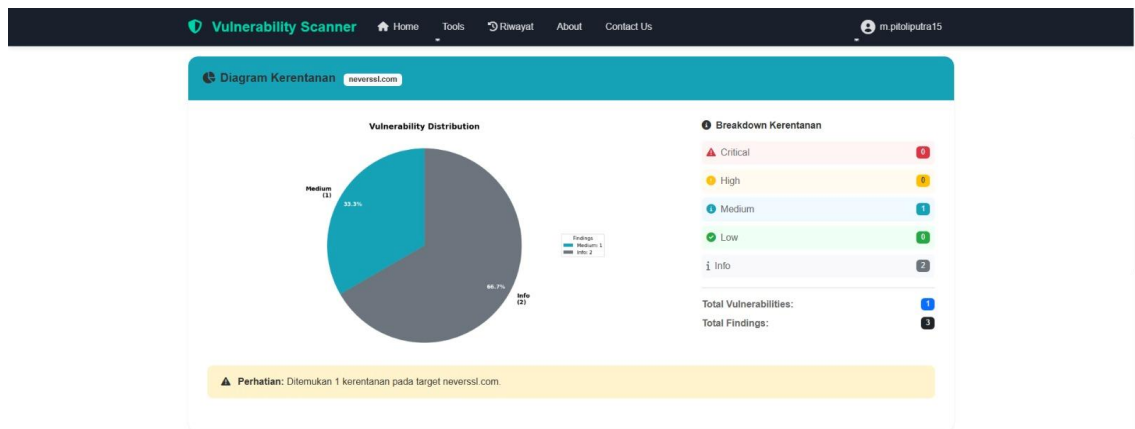
Gambar 4.8 Fitur *Port Scan*

Gambar 4.8 Fitur *Port scan* merupakan contoh cara menggunakan *Comperhensive Scan* pada Nmap *Scanner*. Pengguna dapat memasukan IP pada *menu Target (IP atau Domain)* dan memilih opsi *Comperhensive Scan* dan dapat mengklik tombol mulai pemindaian untuk memulai pengujian keamanan.



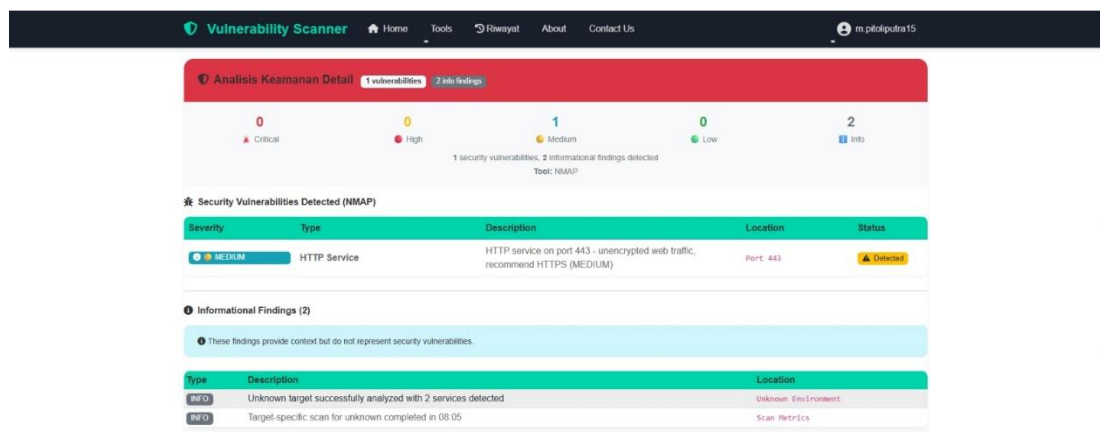
Gambar 4.9 Hasil Pemindaian

Setelah pemindaian selesai dilakukan, *platform* akan memunculkan halaman hasil pemindaian seperti pada Gambar 4.9 Hasil Pemindaian Pada halaman hasil pemindaian ini pengguna dapat melihat ringkasan pemindaian dan skor keamanan.



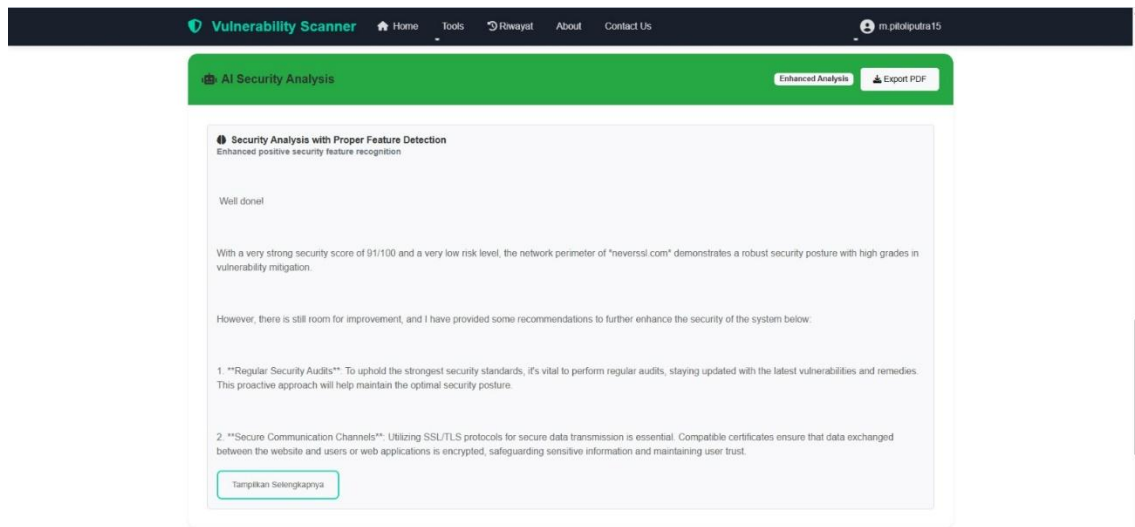
Gambar 4. 10 Diagram Kerentanan

Pada halaman hasil pemindaian juga pengguna dapat melihat diagram kerentanan seperti pada Gambar 4. 10 sesuai dengan kategori temuan kerentanan.



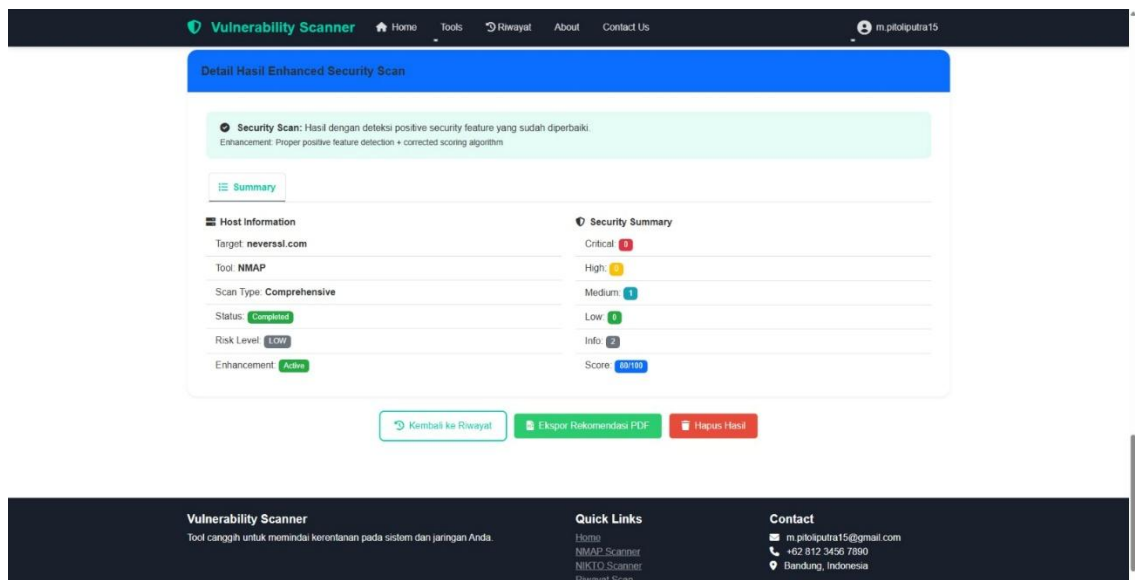
Gambar 4.11 Analisis Keamanan Detail

Pada halaman hasil pemindaian, pengguna dapat melihat analisis keamanan detail seperti pada gambar 4. 11, Terdapat ringkasan temuan kerentanan yang dikelompokkan sesuai dengan kategori temuan yaitu critical, high, medium, low dan info. Pengguna dapat melihat detail type kerentanan apa saja yang ditemukan dan juga terdapat informational finding yang memberikan info konteks namun bukan kerentanan keamanan.



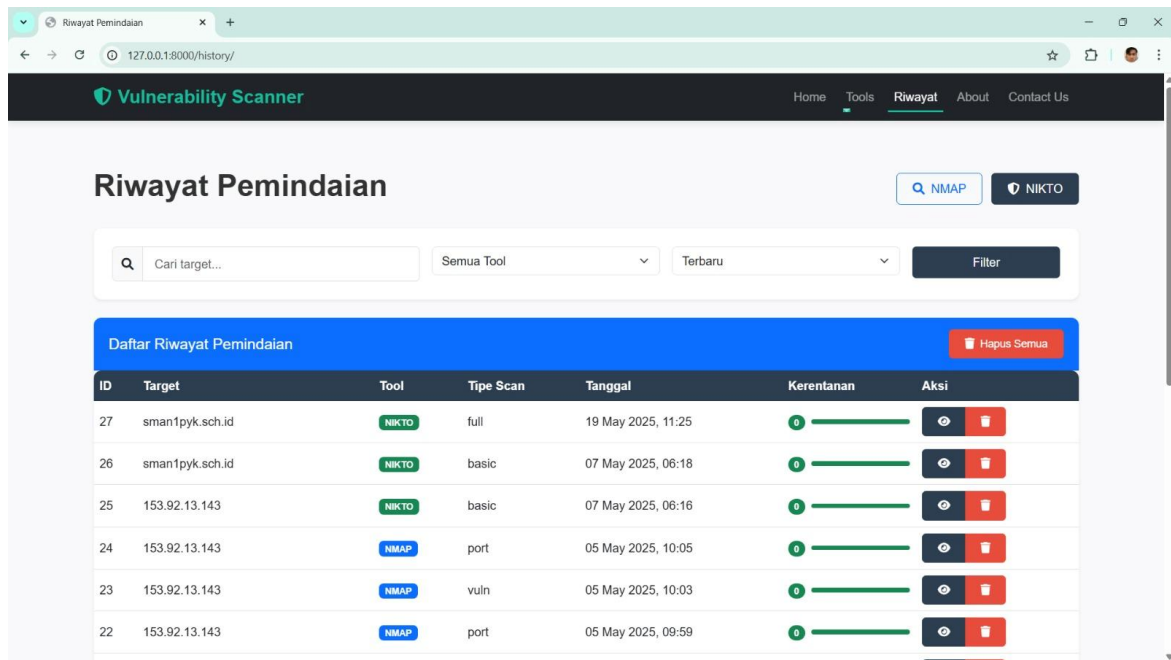
Gambar 4.12 Rekomendasi Perbaikan Berbasis *Generative AI*

Pada halaman hasil pemindaian juga pengguna dapat melihat rekomendasi perbaikan berbasis *generative AI* seperti Gambar 4.10 Rekomendasi Perbaikan Berbasis *Generative AI* sehingga pengguna dapat mengetahui perbaikan seperti apa yang perlu dilakukan terhadap target yang telah dipindai.



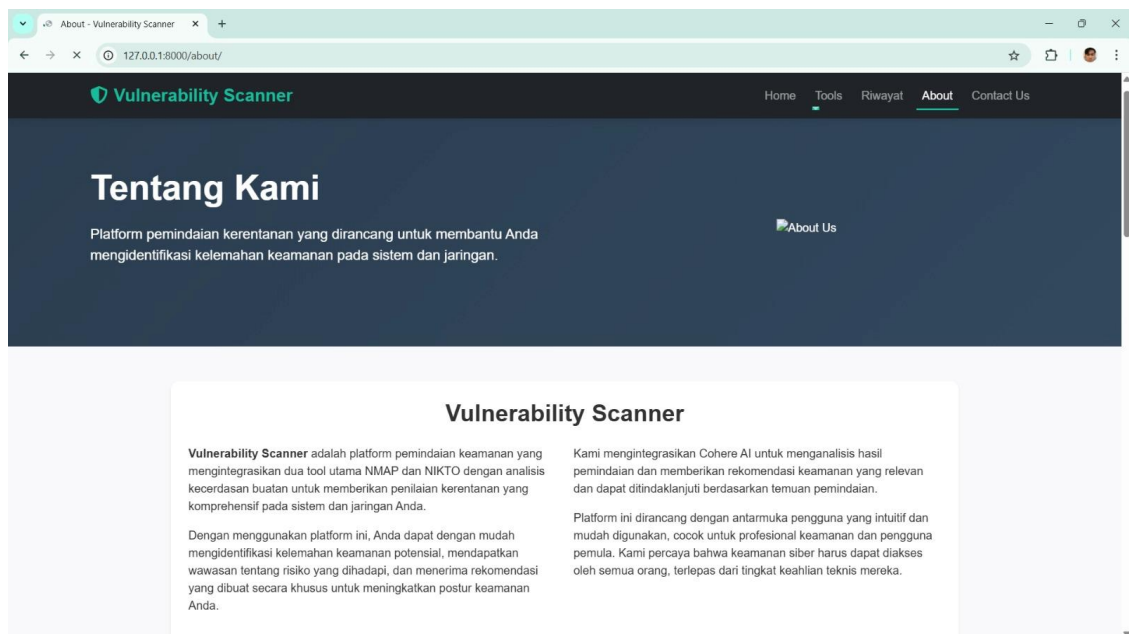
Gambar 4.13 Unduh Ringkasan Pemindaian

Gambar 4.13 merupakan menu detail hasil pemindaian. Pada *menu* ini pengguna dapat mengunduh hasil pemindaian tersebut dalam bentuk file PDF.



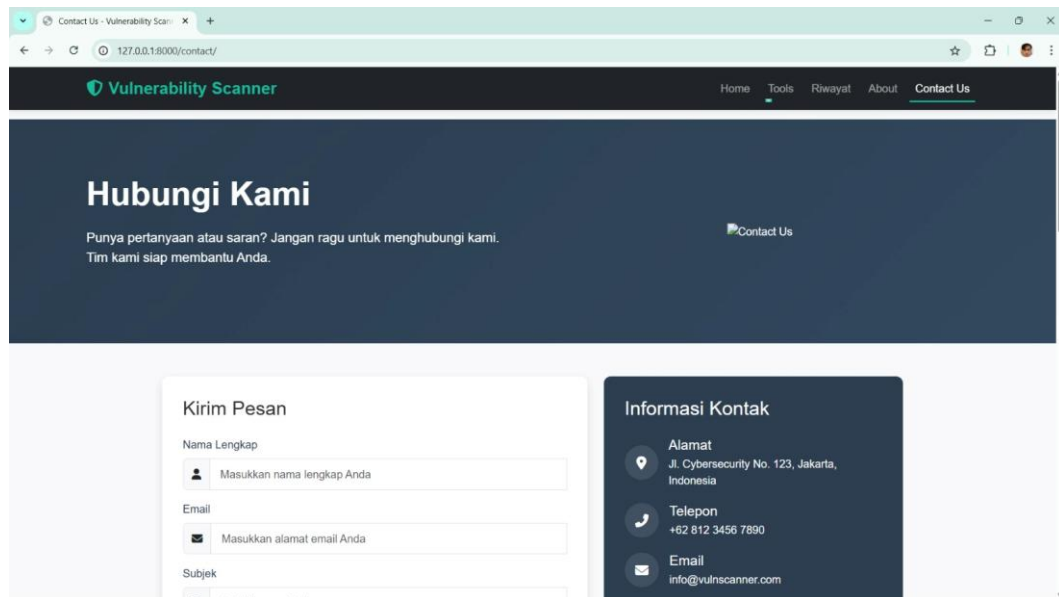
Gambar 4.14 Menu Riwayat Pemindaian

Gambar 4.12 *Menu Riwayat Pemindaian* Menampilkan *menu* “Riwayat pemindaian”, pada halaman ini pengguna dapat mengakses pemindaian yang telah dilakukan dan melihat riwayat hasil pemindaian pada *menu* aksi. Pengguna juga dapat menghapus riwayat pemindaian apabila sudah tidak diperlukan lagi.



Gambar 4.15 Menu About US

Gambar 4.13 *Menu About US* menjelaskan bahwa *platform* ini dirancang untuk membantu pengguna dalam mengidentifikasi kelemahan keamanan pada sistem dan jaringan.



Gambar 4.16 *Menu Contact Us*

Gambar 4.14 *Menu Contact Us* merupakan yang dapat digunakan oleh pengguna dalam menyampaikan pertanyaan, saran, maupun kendala yang pengguna alami.

BAB 5

PENGUJIAN

5.1 Skema Pengujian Sistem

Pengujian ini bertujuan untuk mengumpulkan data tentang kondisi keamanan server melalui proses *scanning*. Pengujian ini dilakukan untuk mengidentifikasi dan mendokumentasikan celah keamanan pada server yang memungkinkan untuk dieksploitasi oleh penyerang. Selain itu, pengujian ini juga bertujuan untuk memvalidasi efektivitas *Website* yang sudah dibuat dalam mendeteksi kerentanan yang ada. Lokasi pengujian dilakukan di Laboratorium Elektronika Komunikasi, Telkom University dan waktu pengujian dilakukan pada hari Senin, 7 Juli 2025.

5.1.1 Daftar Pengujian

Pengujian yang akan dilakukan berfokus pada beberapa aspek penting yang diperlukan untuk mendapatkan hasil maksimal. Maka, aspek aspek yang akan diuji adalah sebagai berikut:

- Waktu Proses *Scanning*,
- Konsistensi hasil temuan kerentanan,
- Pengujian Komparasi Nmap dan Nikto,
- Validasi hasil rekomendasi perbaikan,
- Pengujian performa backend, frontend dan platform pengujian keamanan server menggunakan apache Jmeter,
- monitoring penggunaan CPU dan memori pada sistem backend menggunakan *tools* HTOP, dan
- Pengujian performa docker *container*

5.1.2 Skenario Pengujian

Dalam skenario pengujian ini, dilakukan pengujian menggunakan dua *tools* utama yang ada pada *website* vulnerability scanning yaitu *tools* Nikto dan *tools* Nmap. Pada masing – masing *tools* disediakan 3 jenis *website* untuk dijadikan target pengujian yaitu *website* localhost 1 device, *website* localhost dari device lain, dan pengujian *website* dari internet. Pada ketiga *website* tersebut dilakukan masing – masing 3 kali percobaan untuk melihat konsistensi dari hasil temuan kerentanan *website* tersebut. Pengujian performa dilakukan terhadap backend, frontend, dan platform pengujian

keamanan server menggunakan Apache JMeter. Selain itu, pemantauan performa sistem backend dilakukan menggunakan tools HTOP, dengan metode observasi selama 5 menit dan pencatatan lima data dari kondisi minimum hingga maksimum. Monitoring ini mencakup tiga kondisi: website dalam keadaan normal, saat proses pemindaian dengan Nikto, dan saat pemindaian dengan Nmap. Untuk menguji performa container, dilakukan pula pemantauan melalui Docker Desktop guna melihat penggunaan CPU dan memori dari masing-masing layanan Docker saat proses berjalan.

5.2 Proses Pengujian dan Analisis Hasil

Bagian ini merupakan detail proses pengujian dan hasil analisis yang akan dijabarkan pada bagian-bagian berikut.

5.2.1 Pengujian Menggunakan Nikto Scanner

Pengujian menggunakan Nikto *scanner* ini mencakup 3 metode dengan menggunakan 3 *Website* per masing – masing metodenya.

5.2.1.1 Pengujian *Website Localhost 1 Device*

Pada pengujian *Website localhost 1 device* menggunakan 3 buah *Website* sebagai berikut :

a. *Website 1 (localhost:5001)*

- Pengujian Pertama :

Gambar 5.1 merupakan hasil pengujian ketiga *Website localhost:5001* dengan durasi *scanning* selama 1.92 Detik yang menunjukkan hasil analisis temuan celah keamanan detail yaitu 3 kerentanan kategori *critical* adalah *SQL Injection*, *Command Injection* dan *Unrestricted File Upload*. 1 kerentanan kategori *high* yaitu XSS (*Cross-Site Scripting*). 1 kerentanan kategori *medium* yaitu *Missing Security Headers*, 0 kerentanan kategori *low* dan 4 kategori info. Berdasarkan temuan kerentanan tersebut skor keamanan *Website localhost:5001* adalah 0 yang berarti bahwa *Website* ini sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at /login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
MEDIUM	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/3.1.1.3
INFO	The anti-clickjacking X-Frame-Options header is not present.	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Gambar 5.1 Pengujian Pertama *Website 1 Device* (Localhost:5001) dengan Nikto scanner

• Pengujian Kedua :

Gambar 5.2 merupakan hasil pengujian ketiga *Website* localhost:5001 dengan durasi *scanning* selama 1.73 Detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 3 kerentanan kategori *critical* adalah *SQL Injection*, *Command Injection* dan *Unrestricted File Upload*. 1 kerentanan kategori *high* yaitu XSS (*Cross-Site Scripting*). 1 kerentanan kategori *medium* yaitu *Missing Security Headers*, 0 kerentanan kategori *low* dan 4 kategori info. Berdasarkan temuan kerentanan tersebut skor keamanan *Website* localhost:5001 adalah 0 yang berarti bahwa *Website* ini sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at /login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
MEDIUM	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/3.1.1.3
INFO	The anti-clickjacking X-Frame-Options header is not present.	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Gambar 5.2 Pengujian kedua *Website 1 device* (Localhost:5001) dengan Nikto Scanner

- Pengujian Ketiga :

Gambar 5.3 merupakan hasil pengujian ketiga *Website* localhost:5001 dengan durasi *scanning* selama 1.67 Detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 3 kerentanan kategori *critical* adalah SQL Injection, Command Injection dan Unrestricted File Upload. 1 kerentanan kategori *high* yaitu XSS (Cross-Site Scripting). 1 kerentanan kategori *medium* yaitu Missing *Security* Headers, 0 kerentanan kategori *low* dan 4 kategori info. Berdasarkan temuan kerentanan tersebut skor keamanan *Website* localhost:5001 adalah 0 yang berarti bahwa *Website* ini sangat rentan terhadap serangan.

Security	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at /login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
HIGH	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/index
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

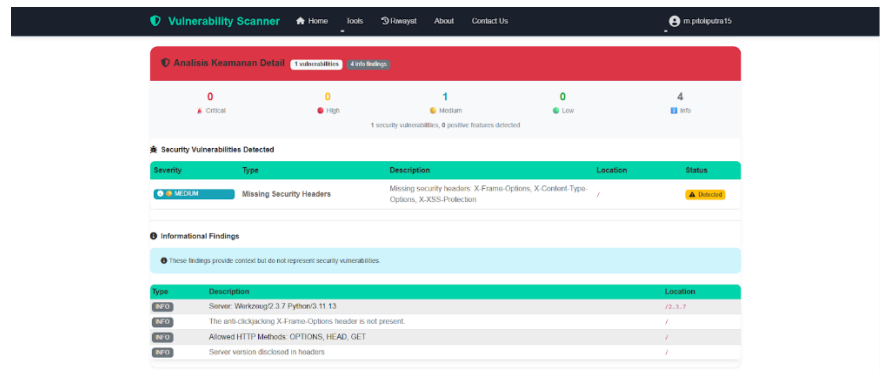
Gambar 5.3 Pengujian ketiga *Website* 1 device (Localhost:5001) dengan Nikto Scanner

b. *Website* 2(localhost:5002)

- Pengujian Pertama :

Gambar 5.4 merupakan hasil pengujian pertama pada *Website* localhost:5002 dengan durasi *scanning* selama 1.03 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 0 kategori *critical*, 0 kategori *high*, 1 kategori *medium* yaitu Missing *Security* Headers, 0 kategori *low* dan 4 kategori info. Berdasarkan temuan kerentanan tersebut skor keamanan *Website* localhost:5002 adalah 80 yang berarti

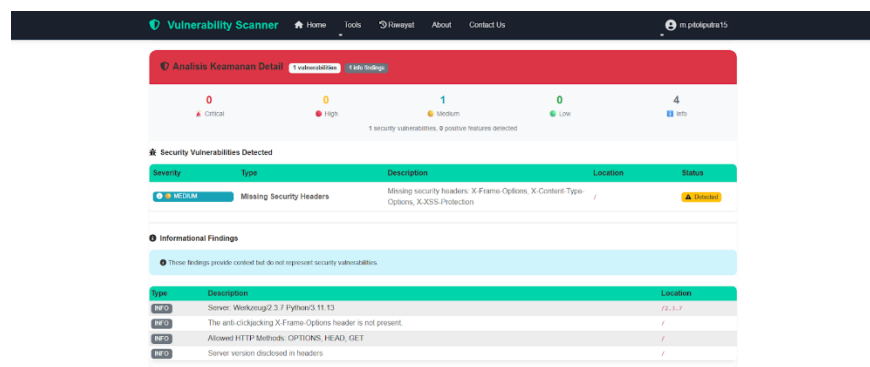
bahwa *Website* ini cukup aman dari serangan namun perlu adanya perbaikan.



Gambar 5.4 Pengujian pertama *Website 1 device* (Localhost:5002) dengan *Nikto Scanner*

- Pengujian Kedua :

Gambar 5.5 merupakan hasil pengujian kedua pada *Website* localhost:5002 dengan durasi *scanning* selama 1.08 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 0 kategori *critical*, 0 kategori *high*, 1 kategori *medium* yaitu *Missing Security Headers*, 0 kategori *low* dan 4 kategori *info*. Berdasarkan temuan kerentanan tersebut skor keamanan *Website* localhost:5002 adalah 80 yang berarti bahwa *Website* ini cukup aman dari serangan namun perlu adanya perbaikan.



Gambar 5.5 Pengujian kedua *Website 1 device* (Localhost:5002) dengan *Nikto Scanner*

- Pengujian Ketiga :

Gambar 5.6 merupakan Hasil pengujian ketiga pada *Website* localhost:5002 dengan durasi *scanning* selama 0.85 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 0 kategori *critical*, 0 kategori *high*, 1 kategori *medium* yaitu Missing Security Headers, 0 kategori *low* dan 4 kategori info. Berdasarkan temuan kerentanan tersebut skor keamanan *Website* localhost:5002 adalah 80 yang berarti bahwa *Website* ini cukup aman dari serangan namun perlu adanya perbaikan.

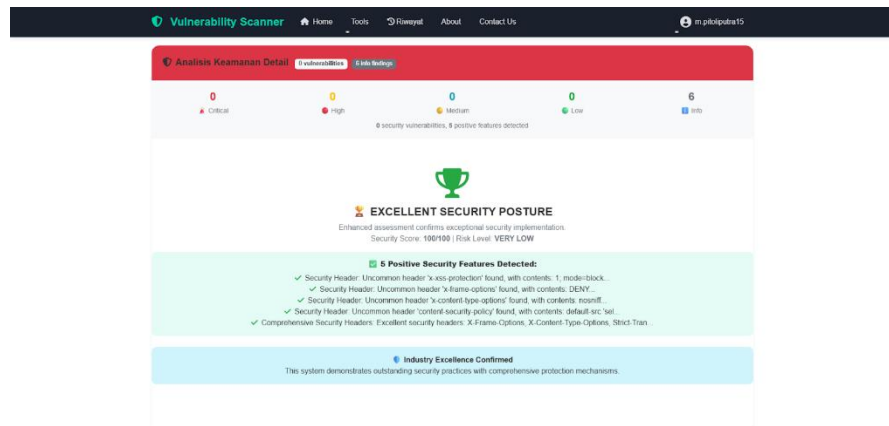
Severity	Type	Description	Location	Status
Medium	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Unfixed
Informational Findings				
These findings provide context but do not represent security vulnerabilities.				
Type	Description	Location		
INFO	Server: Werkzeug/2.3.7 Python/3.11.13	/2.3.7		
INFO	The anti-clickjacking X-Frame-Options header is not present.	/		
INFO	Allowed HTTP Methods: OPTIONS, HEAD, GET	/		
INFO	Server version disclosed in headers	/		

Gambar 5.6 Pengujian ketiga *Website* 1 device (Localhost:5002) dengan Nikto Scanner

c. *Website* 3 (localhost:5003)

- Pengujian pertama :

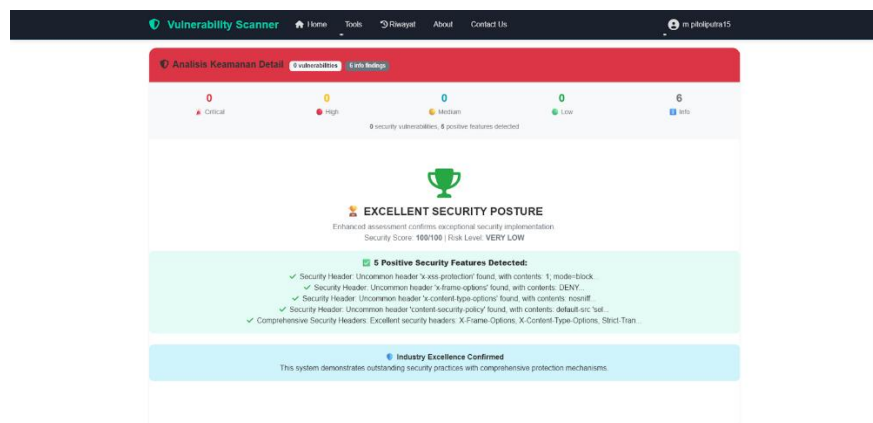
Gambar 5.7 merupakan Hasil dari pengujian pertama pada *Website* localhost:5003 dengan durasi *scanning* selama 0.94 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 0 kategori *critical*, 0 kategori *high*, 0 kategori meidum, 0 kategori *low* dan 6 kategori info. Berdasarkan hasil temuan tersebut didapatkan *security score Website* localhost:5003 adalah 100 yang menunjukkan tingkat risiko serangan sangat rendah.



Gambar 5.7 Pengujian pertama *Website 1 device* (Localhost:5003) dengan Nikto Scanner

• Pengujian kedua :

Gambar 5.8 merupakan merupakan hasil pengujian kedua pada *Website* localhost:5003 dengan durasi *scanning* selama 1.25 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 0 kategori *critical*, 0 kategori *high*, 0 kategori meidum, 0 kategori *low* dan 6 kategori info. Berdasarkan hasil temuan tersebut didapatkan *security score Website* localhost:5003 adalah 100 yang menunjukkan tingkat risiko serangan sangat rendah.

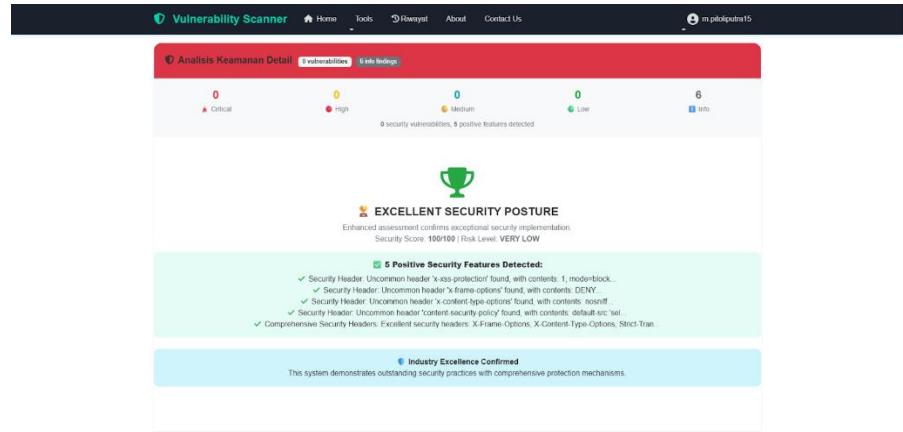


Gambar 5.8 Pengujian kedua *Website 1 device* (Localhost:5003) dengan Nikto Scanner

• Pengujian ketiga :

Gambar 5.9 merupakan merupakan hasil pengujian kedua pada *Website* localhost:5003 dengan durasi *scanning* selama 1.46 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 0 kategori *critical*, 0

kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori *info*. Berdasarkan hasil temuan tersebut didapatkan *security score Website localhost:5003* adalah 100 yang menunjukkan tingkat risiko serangan sangat rendah.



Gambar 5.9 Pengujian ketiga *Website 1 device (Localhost:5003)* dengan *Nikto Scanner*

Tabel 5.1 Pengujian *Website Localhost 1 Device* Menggunakan *Nikto Scanner*

No.	Waktu Pengujian			Konsistensi Hasil Temuan			Keterangan
	P1	P 2	P 3	P 1	P 2	P 3	
<i>Website 1</i>	1.92 detik	1.73 detik	1.67 detik	Skor kerentanan 0	Skor kerentanan 0	Skor kerentanan 0	Hasil konsisten
<i>Website 2</i>	1.03 detik	1.08 detik	0.85 detik	Skor kerentanan 80	Skor kerentanan 80	Skor kerentanan 80	Hasil konsisten
<i>Website 3</i>	0.94 detik	1.25 detik	1.46 detik	Skor kerentanan 100	Skor kerentanan 100	Skor kerentanan 100	Hasil konsisten

5.2.1.2 Pengujian *Website Localhost* dari *Device* yang Berbeda

Pengujian *Website localhost* dari *device* yang berbeda menggunakan 3 jenis *Website* sebagai berikut :

a. *Website 1 (localhost:5001)*

- Pengujian Pertama :

Gambar 5.10 merupakan merupakan hasil pengujian pertama pada *Website localhost:5001* dengan durasi *scanning* selama 10.51 detik

menunjukkan hasil analisis temuan celah keamanan detail yaitu 3 kategori *critical* diantaranya SQL Injection, command Injection dan Unrestricted File Upload. 1 kategori *high* yaitu Cross-Site Scripting (XSS). 1 kategori *medium* yaitu missing *security* headers. 0 kategori *low* dan 4 kategori info. Dari hasil temuan tersebut didapatkan *security score Website* localhost:5001 adalah 0 yang menandakan *Website* tersebut sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at /login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
HIGH	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/3.1.3
INFO	The anti-clickjacking X-Frame-Options header is not present.	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Gambar 5.10 Pengujian pertama *Website* beda *device* (Localhost:5001) dengan Nikto *Scanner*

- Pengujian Kedua :

Gambar 5.11 merupakan hasil pengujian kedua pada *Website* localhost:5001 dengan durasi *scanning* selama 9.71 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 3 kategori *critical* diantaranya SQL Injection, command Injection dan Unrestricted File Upload. 1 kategori *high* yaitu Cross-Site Scripting (XSS). 1 kategori *medium* yaitu missing *security* headers. 0 kategori *low* dan 4 kategori info. Dari hasil temuan tersebut didapatkan *security score Website* localhost:5001 adalah 0 yang menandakan *Website* tersebut sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at /login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
HIGH	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/vuln-3
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Gambar 5.11 Pengujian kedua *Website* beda *device* (Localhost:5001) dengan Nikto Scanner

• Pengujian Ketiga :

Gambar 5.12 merupakan hasil pengujian ketiga pada *Website* localhost:5001 dengan durasi *scanning* selama 10.14 detik menunjukkan hasil analisis temuan celah keamanan detail yaitu 3 kategori *critical* diantaranya SQL Injection, command Injection dan Unrestricted File Upload. 1 kategori *high* yaitu Cross-Site Scripting (XSS). 1 kategori *medium* yaitu missing *security* headers. 0 kategori *low* dan 4 kategori *info*. Dari hasil termuan tersebut didapatkan *security score Website* localhost:5001 adalah 0 yang menandakan *Website* tersebut sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at /login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
HIGH	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

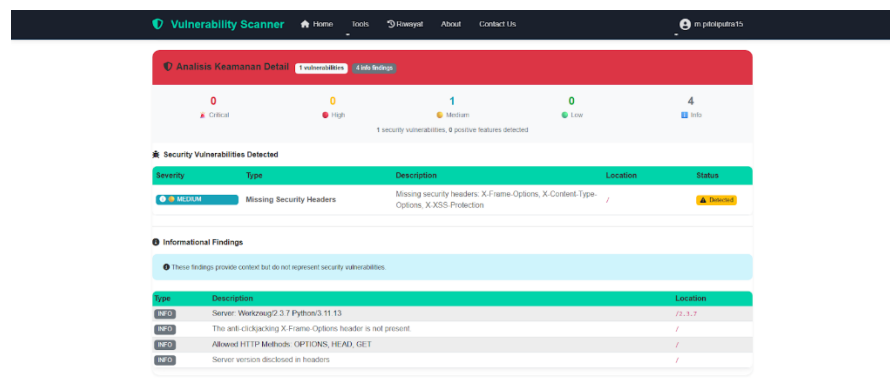
Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/vuln-3
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Gambar 5.12 Pengujian ketiga *Website* beda *device* (Localhost:5001) dengan Nikto Scanner

b. *Website 2* (localhost:5002)

- Pengujian pertama :

Gambar 5.13 merupakan Hasil pengujian pertama pada *Website* localhost:5002 dengan durasi *scanning* selama 8.23 detik, menunjukkan hasil temuan celah keamanan berupa 0 kategori *critical*, 0 kategori *high*, 1 kategori *medium* yaitu missing *security* header, 0 kategori *low* dan 4 kategori *info*. Dari hasil temuan tersebut didapatkan *security score* *Website* ini adalah 80 yang menunjukkan bahwa *Website* ini sudah cukup aman namun perlu dilakukan perbaikan untuk memaksimalkan *Website* tersebut.



Security	Type	Description	Location	Status
0	Critical			
0	High			
1	Medium	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Failed
0	Low			
4	Info			

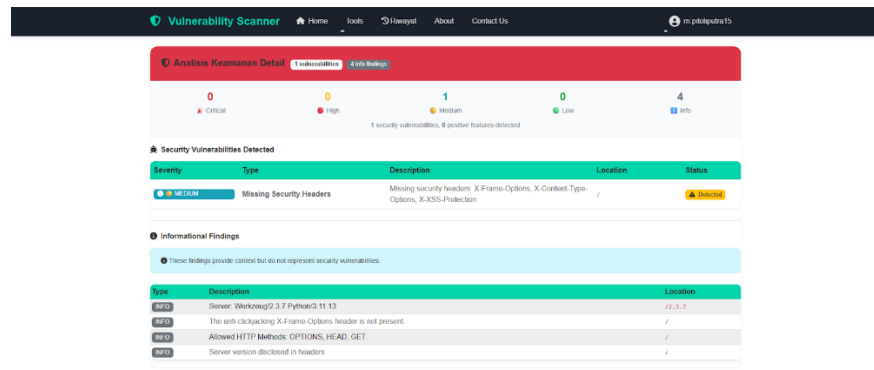
Type	Description	Location
INFO	Server: Werkzeug/2.3.7 Python/3.11.13	/2.3.7
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: OPTIONS, HEAD, GET	/
INFO	Server version disclosed in headers	/

Gambar 5.13 Pengujian pertama *Website* beda *device* (Localhost:5002) dengan Nikto *Scanner*

- Pengujian kedua :

Gambar 5.14 merupakan hasil pengujian kedua pada *Website* localhost:5002 dengan durasi *scanning* selama 6.12 detik, menunjukkan hasil temuan celah keamanan berupa 0 kategori *critical*, 0 kategori *high*, 1 kategori *medium* yaitu missing *security* header, 0 kategori *low* dan 4 kategori *info*. Dari hasil temuan tersebut didapatkan *security score* *Website* ini adalah 80 yang menunjukkan bahwa *Website* ini sudah cukup

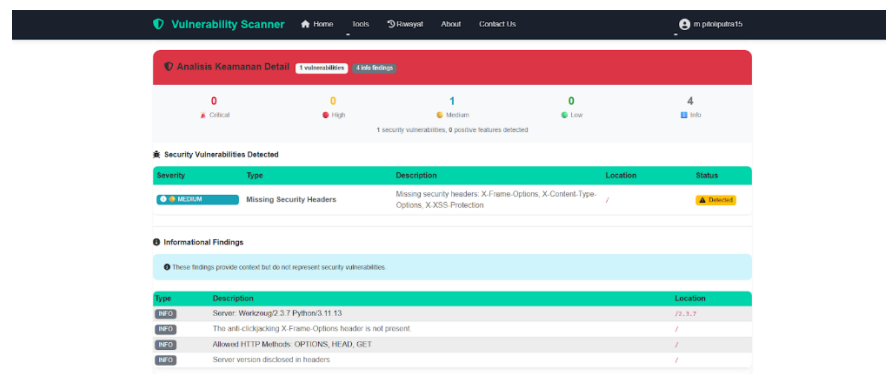
aman namun perlu dilakukan perbaikan untuk memaksimalkan *Website* tersebut.



Gambar 5.14 Pengujian kedua *Website* beda *device* (Localhost:5002) dengan Nikto Scanner

- Pengujian ketiga :

Gambar 5.15 merupakan hasil pengujian ketiga pada *Website* localhost:5002 dengan durasi *scanning* selama 11.82 detik, menunjukkan hasil temuan celah keamanan berupa 0 kategori *critical*, 0 kategori *high*, 1 kategori *medium* yaitu missing *security* header, 0 kategori *low* dan 4 kategori info. Dari hasil temuan tersebut didapatkan *security score Website* ini adalah 80 yang menunjukkan bahwa *Website* ini sudah cukup aman namun perlu dilakukan perbaikan untuk memaksimalkan *Website* tersebut.

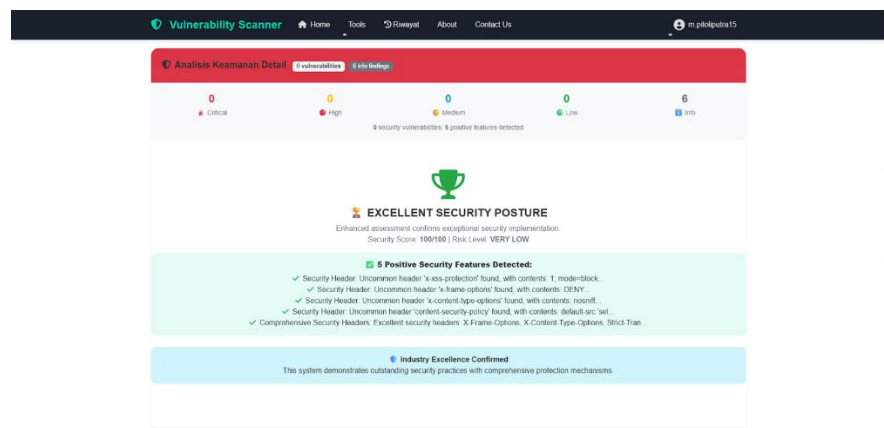


Gambar 5.15 Pengujian ketiga *Website* beda *device* (Localhost:5002) dengan Nikto Scanner

c. *Website 3* (localhost:5003)

- Pengujian pertama :

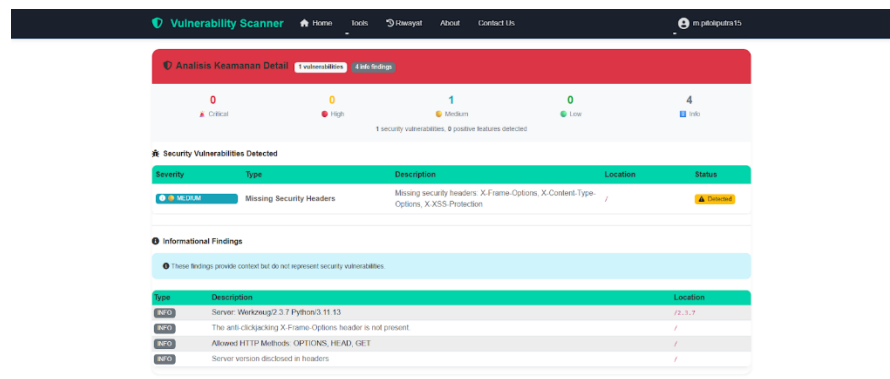
Gambar 5.16 merupakan hasil pengujian ketiga pada *Website* localhost:5003 dengan durasi scan selama 4.15 detik, menunjukan hasil temuan kerentanan celah keamanan berupa 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori info. Dari hasil yang didapatkan maka *security score Website* localhost:5003 adalah 100 yang menunjukkan *Website* ini aman dan tingkat risiko serangan sangat rendah.



Gambar 5.16 Pengujian pertama *Website* beda *device* (Localhost:5003) dengan Nikto Scanner

- Pengujian kedua :

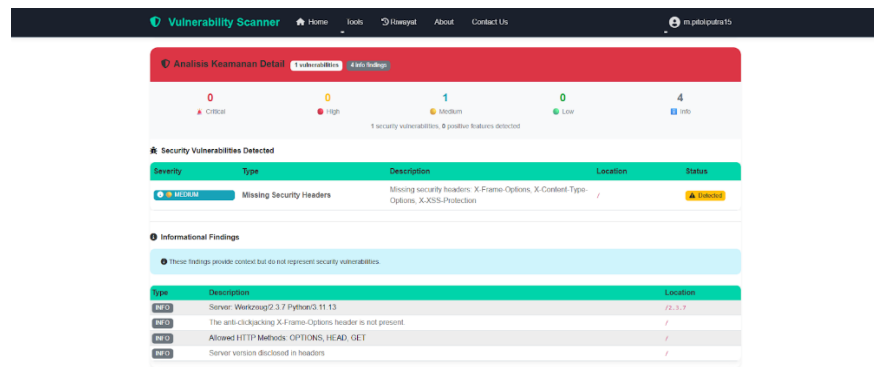
Gambar 5.17 merupakan hasil pengujian ketiga pada *Website* localhost:5003 dengan durasi scan selama 5.35 detik, menunjukan hasil temuan kerentanan celah keamanan berupa 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori info. Dari hasil yang didapatkan maka *security score Website* localhost:5003 adalah 100 yang menunjukkan *Website* ini aman dan tingkat risiko serangan sangat rendah.



Gambar 5.17 Pengujian kedua *Website* beda *device* (Localhost:5003) dengan Nikto *Scanner*

- Pengujian ketiga :

Gambar 5.18 merupakan hasil pengujian ketiga pada *Website* localhost:5003 dengan durasi scan selama 4.03 detik, menunjukan hasil temuan kerentanan celah keamanan berupa 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori info. Dari hasil yang didapatkan maka *security score Website* localhost:5003 adalah 100 yang menunjukkan *Website* ini aman dan tingkat risiko serangan sangat rendah.



Gambar 5.18 Pengujian ketiga *Website* beda *device*

Tabel 5.2 Pengujian *Website* Localhost Beda *Device* Menggunakan Nikto Scanner

No.	Waktu Pengujian			Konsistensi Hasil Temuan			Keterangan
	P1	P 2	P 3	P 1	P 2	P 3	
<i>Website</i> 1	10.51 detik	9.71 detik	10.14 detik	Skor kerentanan 0	Skor kerentanan 0	Skor kerentanan 0	Hasil konsisten
<i>Website</i> 2	8.23 detik	6.12 detik	11.82 detik	Skor kerentanan 80	Skor kerentanan 80	Skor kerentanan 80	Hasil konsisten
<i>Website</i> 3	4.15 detik	5.35 detik	4.03 detik	Skor kerentanan 100	Skor kerentanan 100	Skor kerentanan 100	Hasil konsisten

5.2.1.3 Pengujian *Website* dari Internet

Pengujian *Website* dari internet menggunakan 3 buah *Website* sebagai berikut :

a. *Website* 1 (<https://www.pln.co.id>)

- Pengujian pertama :

Gambar 5.19 merupakan hasil pengujian pertama pada *Website* <https://www.pln.co.id> dengan durasi scan 20.53 detik, menunjukkan hasil temuan kerentanan berupa 1 kategori *critical* yaitu command injection, 0 kategori *high*, 0 kategori *medium*, 1 kategori *low* yaitu infrastructure finding, dan 5 kategori info. Dari hasil temuan kerentanan tersebut didapatkan *security score Website* <https://www.pln.co.id> adalah 16 yang menunjukan bahwa *Website* ini sangat rentan terhadap serangan.

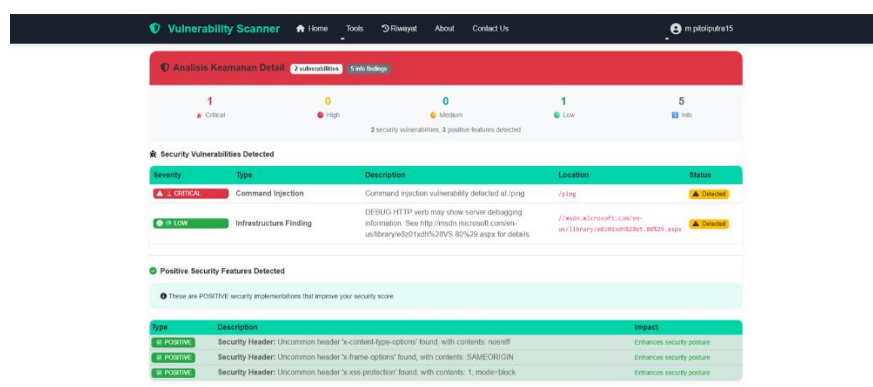
Severity	Type	Description	Location	Status
CRITICAL	Command Injection	Command injection vulnerability detected at /jmg	/jmg	Detected
LOW	Infrastructure Finding	DEBUG HTTP web may show server debugging information. See http://msdn.microsoft.com/en-us/library/ee563028.aspx for details.	https://www.pln.co.id/_layouts/15/default.aspx	Detected

Type	Description	Impact
POSITIVE	Security Header: Uncommon header "x-content-type-options" found, with contents: nosniff	Enhances security posture
POSITIVE	Security Header: Uncommon header "x-frame-options" found, with contents: SAMEORIGIN	Enhances security posture
POSITIVE	Security Header: Uncommon header "x-xss-protection" found, with contents: 1; mode=block	Enhances security posture

Gambar 5.19 Pengujian pertama *Website* internet (<https://www.pln.co.id>) dengan Nikto Scanner

- Pengujian kedua :

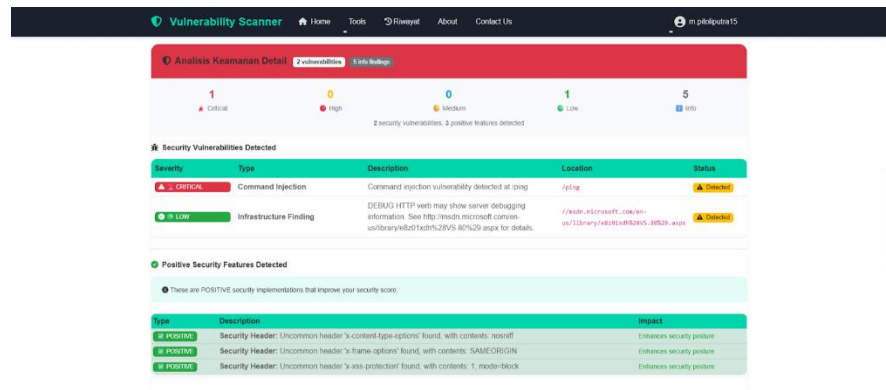
Gambar 5.20 merupakan hasil pengujian kedua pada *Website* <https://www.pln.co.id> dengan durasi scan 19.78 detik, menunjukkan hasil temuan kerentanan berupa 1 kategori *critical* yaitu command injection, 0 kategori *high*, 0 kategori *medium*, 1 kategori *low* yaitu infrastructure finding, dan 5 kategori info. Dari hasil temuan kerentanan tersebut didapatkan *security score Website* <https://www.pln.co.id> adalah 16 yang menunjukan bahwa *Website* ini sangat rentan terhadap serangan.



Gambar 5.20 Pengujian kedua *Website* internet (<https://www.pln.co.id>) dengan Nikto Scanner

- Pengujian ketiga :

Gambar 5.21 merupakan hasil pengujian ketiga pada *Website* <https://www.pln.co.id> dengan durasi scan 20.22 detik, menunjukkan hasil temuan kerentanan berupa 1 kategori *critical* yaitu command injection, 0 kategori *high*, 0 kategori *medium*, 1 kategori *low* yaitu infrastructure finding, dan 5 kategori info. Dari hasil temuan kerentanan tersebut didapatkan *security score Website* <https://www.pln.co.id> adalah 16 yang menunjukan bahwa *Website* ini sangat rentan terhadap serangan.

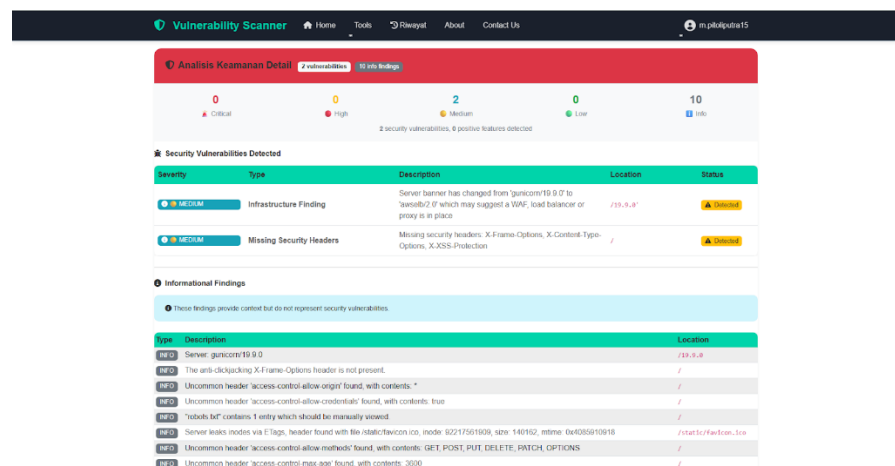


Gambar 5.21 Pengujian ketiga *Website* internet (<https://www.pln.co.id>) dengan Nikto Scanner

b. *Website 2* (<http://httpbin.org>)

- Pengujian pertama :

Gambar 5.22 merupakan hasil pengujian pertama pada *Website* <http://httpbin.org> dengan durasi scan selama 83.10 detik, menunjukkan hasil temuan kerentanan berupa 0 kategori *critical*, 0 kategori *high*, 2 kategori *medium* yaitu infrastructure Finding dan missing security headers, 0 kategori *low* dan 10 kategori info. Berdasarkan hasil temuan kerentanan tersebut, maka didapatkan *security score Website* <http://httpbin.org> adalah 60 yang menunjukkan bahwa *Website* ini cukup aman dari serangan namun perlu dilakukan perbaikan.



Gambar 5.22 Pengujian pertama *Website* internet (<http://httpbin.org>) dengan Nikto Scanner

- Pengujian kedua :

Gambar 5.23 merupakan hasil pengujian kedua pada *Website* <http://httpbin.org> dengan durasi scan selama 83.97 detik, menunjukkan hasil temuan kerentanan berupa 0 kategori *critical*, 0 kategori *high*, 2 kategori *medium* yaitu *infrastructure Finding* dan *missing security headers*, 0 kategori *low* dan 10 kategori *info*. Berdasarkan hasil temuan kerentanan tersebut, maka didapatkan *security score Website* <http://httpbin.org> adalah 60 yang menunjukkan bahwa *Website* ini cukup aman dari serangan namun perlu dilakukan perbaikan.

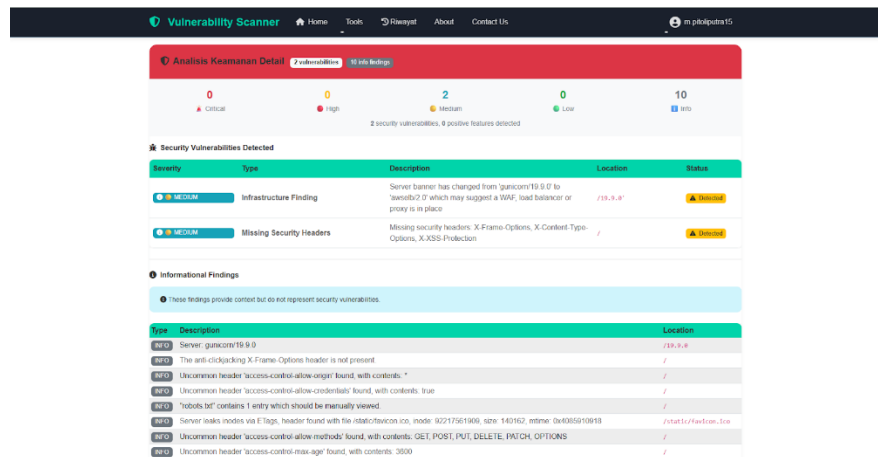
Severity	Type	Description	Location	Status
Medium	Infrastructure Finding	Server banner has changed from 'gunicorn/19.0.0' to 'awscli/2.0' which may suggest a WAN, load balancer or proxy is in place	/19.0.0	Detected
Medium	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Type	Description	Location
Info	Server: gunicorn/19.0.0	/19.0.0
Info	The anti-clickjacking X-Frame-Options header is not present.	/
Info	Uncommon header 'access-control-allow-origin' found, with contents: *	/
Info	Uncommon header 'access-control-allow-credentials' found, with contents: true	/
Info	'robots.txt' contains 1 entry which should be manually viewed.	/
Info	Server leaks nodes via ETags, header found with file: /static/favicon.ico, mode: 82217361809, size: 140912, mime: 0x9865910918	/static/favicon.ico
Info	Uncommon header 'access-control-allow-methods' found, with contents: GET, POST, PUT, DELETE, PATCH, OPTIONS	/
Info	Uncommon header 'access-control-expose-headers' found, with contents: 3800	/

Gambar 5.23 Pengujian kedua *Website* internet (<http://httpbin.org>) dengan Nikto Scanner

- Pengujian ketiga :

Gambar 5.24 merupakan hasil pengujian ketiga pada *Website* <http://httpbin.org> dengan durasi scan selama 81.21 detik, menunjukkan hasil temuan kerentanan berupa 0 kategori *critical*, 0 kategori *high*, 2 kategori *medium* yaitu *infrastructure Finding* dan *missing security headers*, 0 kategori *low* dan 10 kategori *info*. Berdasarkan hasil temuan kerentanan tersebut, maka didapatkan *security score Website* <http://httpbin.org> adalah 60 yang menunjukkan bahwa *Website* ini cukup aman dari serangan namun perlu dilakukan perbaikan.

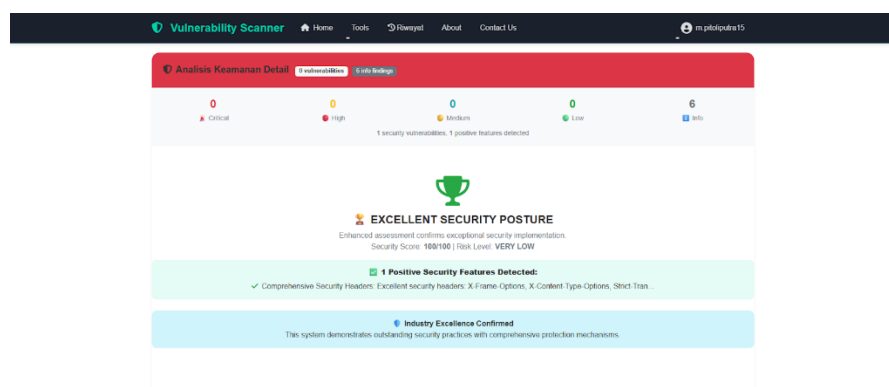


Gambar 5.24 Pengujian ketiga *Website* internet (<http://httpbin.org>) dengan Nikto Scanner

c. *Website* 3 (<https://www.komdigi.go.id/>)

- Pengujian pertama :

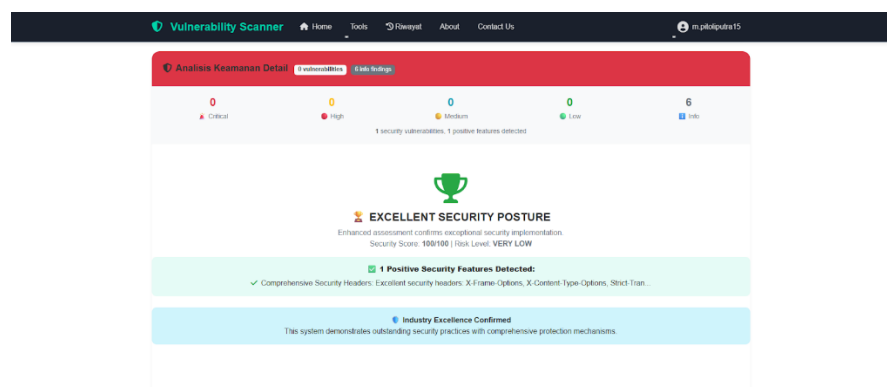
Gambar 5.25 merupakan hasil pengujian pertama pada *Website* <https://www.komdigi.go.id/> dengan durasi scan selama 22.52 detik, menunjukkan hasil temuan kerentanan berupa 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori *info*. Berdasarkan hasil temuan kerentanan tersebut, maka didapatkan *security score Website* <https://www.komdigi.go.id/> adalah 100 yang menunjukkan bahwa *Website* sangat aman dan sangat minim terhadap risiko serangan.



Gambar 5.25 Pengujian pertama *Website* internet (<https://www.komdigi.go.id/>) dengan Nikto Scanner

- Pengujian kedua :

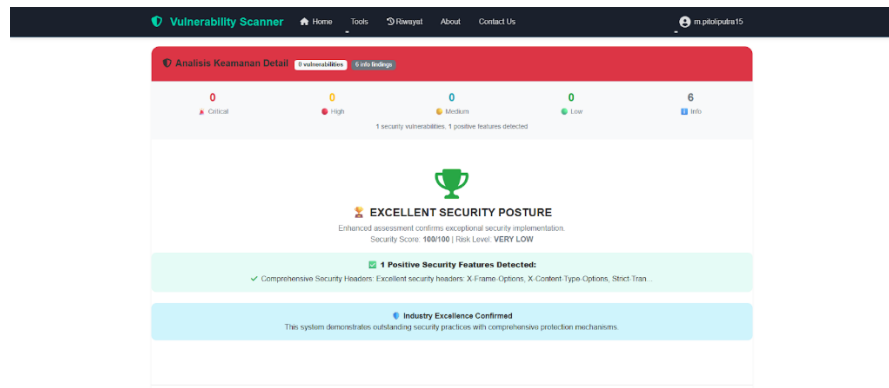
Gambar 5.26 merupakan hasil pengujian kedua pada *Website* <https://www.komdigi.go.id/> dengan durasi scan selama 24.12 detik, menunjukkan hasil temuan kerentanan berupa 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori *info*. Berdasarkan hasil temuan kerentanan tersebut, maka didapatkan *security score* *Website* <https://www.komdigi.go.id/> adalah 100 yang menunjukkan bahwa *Website* sangat aman dan sangat minim terhadap risiko serangan.



Gambar 5.26 Pengujian kedua *Website* internet
(<https://www.komdigi.go.id/>) dengan Nikto Scanner

- Pengujian ketiga :

Gambar 5.27 merupakan hasil pengujian ketiga pada *Website* <https://www.komdigi.go.id/> dengan durasi scan selama 23.88 detik, menunjukkan hasil temuan kerentanan berupa 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 6 kategori *info*. Berdasarkan hasil temuan kerentanan tersebut, maka didapatkan *security score* *Website* <https://www.komdigi.go.id/> adalah 100 yang menunjukkan bahwa *Website* sangat aman dan sangat minim terhadap risiko serangan.



Gambar 5.27 Pengujian ketiga *Website* internet
(<https://www.komdigi.go.id/>) dengan Nikto Scanner

Tabel 5. 3 Pengujian *Website* Internet Menggunakan Nikto Scanner

No.	Waktu Pengujian			Konsistensi Hasil Temuan			Keterangan
	P1	P 2	P 3	P 1	P 2	P 3	
<i>Website</i> 1	20.53 detik	19.78 detik	20.22 detik	Skor kerentanan 16	Skor kerentanan 16	Skor kerentanan 16	Hasil konsisten
<i>Website</i> 2	83.10 detik	83.97 detik	81.21 detik	Skor kerentanan 60	Skor kerentanan 60	Skor kerentanan 60	Hasil konsisten
<i>Website</i> 3	22.52 detik	24.12 detik	23.88 detik	Skor kerentanan 100	Skor kerentanan 100	Skor kerentanan 100	Hasil konsisten

5.2.2 Pengujian Menggunakan Nmap Scanner

Pengujian menggunakan Nmap scanner ini mencakup 3 metode dengan menggunakan 3 *Website* per masing – masing metodenya.

5.2.2.1 Pengujian *Website* Localhost 1 Device

Pada pengujian *Website* localhost 1 device menggunakan 3 buah *Website* sebagai berikut :

a. *Website* 1 (localhost:8081)

- Pengujian pertama :

Gambar 5.28 dan Gambar 5.29 merupakan hasil pengujian pertama pada *Website* target localhost:8081 dengan durasi scan selama 840.91 detik, didapatkan hasil temuan kerentanan dengan 4 kategori *critical*

diantaranya *FTP service*, *TELNET service*, dan *TCPWRAPPED service*. Terdapat 3 kategori *high* yaitu *http-title script* dan *TCPWRAPPED services*. Terdapat 6 kategori *medium* yaitu *SMTP service*, *HTTP Service*, dan *POP3 Service* *IMAP service*. Terdapat 2 kategori *low* yaitu *http-cookie-flags script* dan 4 kategori *info*. Dari hasil temuan kerentanan tersebut, *Website localhost:8081* mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* ini sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8512	Port: 8512	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8513	Port: 8513	Detected
HIGH	http-title Script	Script http-title found high severity issue	Port: 8080 - http://131a	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8161	Port: 8161	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http://131a	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http://131a	Detected

Gambar 5.28 Pengujian pertama *Website 1 device* (Localhost:8081) dengan *nmap Scanner*

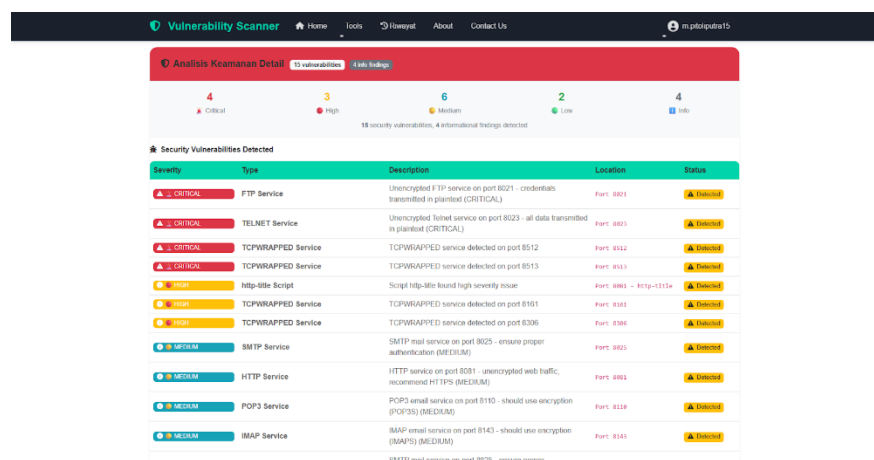
Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8512	Port: 8512	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8513	Port: 8513	Detected
HIGH	http-title Script	Script http-title found high severity issue	Port: 8080 - http://131a	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8161	Port: 8161	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http://131a	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http://131a	Detected

Gambar 5.29 Pengujian pertama *Website 1 device* (Localhost:8081) dengan *nmap Scanner*

- Pengujian kedua :

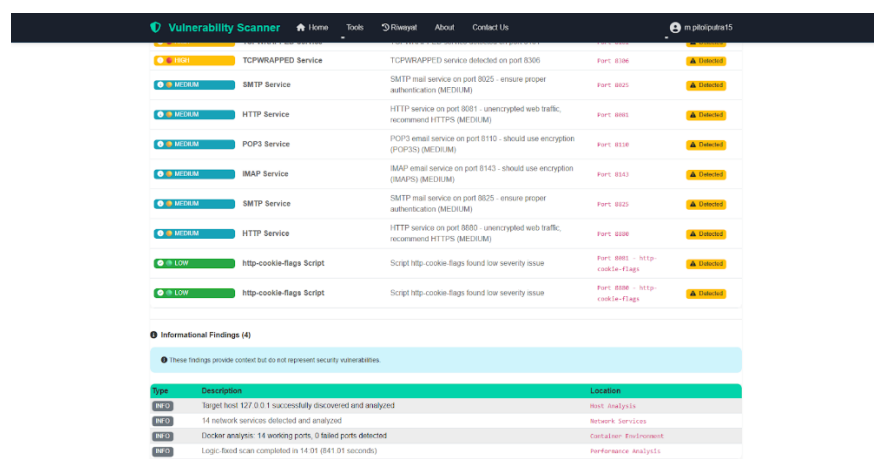
Gambar 5.30 dan Gambar 5.31 merupakan hasil pengujian kedua pada *Website* target localhost:8081 dengan durasi scan selama 851.11

detik, didapatkan hasil temuan kerentanan dengan 4 kategori *critical* diantaranya FTP service, TELNET service, dan TCPWRAPPED service. Terdapat 3 kategori *high* yaitu http-title script dan TCPWRAPPED services. Terdapat 6 kategori *medium* yaitu SMTP service, HTTP Service, dan POP3 Service IMAP service. Terdapat 2 kategori *low* yaitu http-cookiep-flags script dan 4 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8081 mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* ini sangat rentan terhadap serangan.



Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted Telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8512	Port: 8512	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8513	Port: 8513	Detected
HIGH	http-title Script	Script http-title found high severity issue	Port: 8080 - http-8080	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8161	Port: 8161	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper		Detected

Gambar 5.30 Pengujian kedua *Website* 1 device (Localhost:8081) dengan nmap Scanner



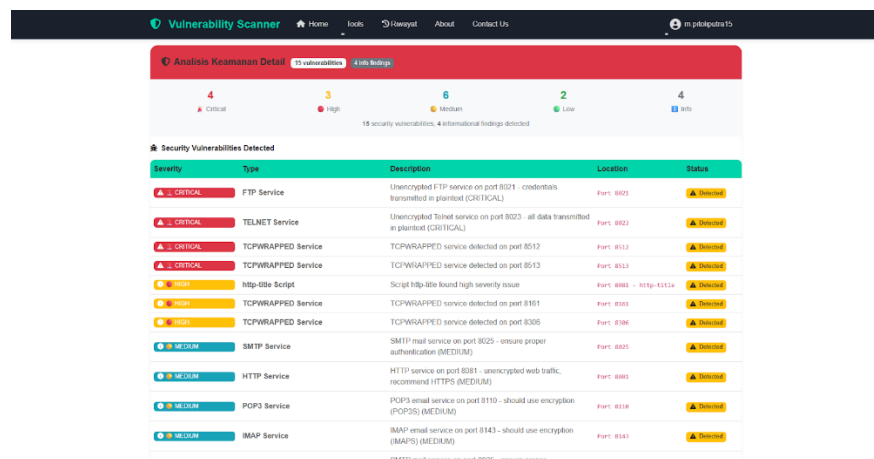
Severity	Type	Description	Location	Status
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected

Type	Description	Location
INFO	Target host 127.0.0.1 successfully discovered and analyzed	Host Analysis
INFO	14 network services detected and analyzed	Network Services
INFO	Docker analysis: 14 working ports, 0 failed ports detected	Container Environment
INFO	Logic based scan completed in 14.01 (841.01 seconds)	Performance Analysis

Gambar 5.31 Pengujian kedua *Website* 1 device (Localhost:8081) dengan nmap Scanner

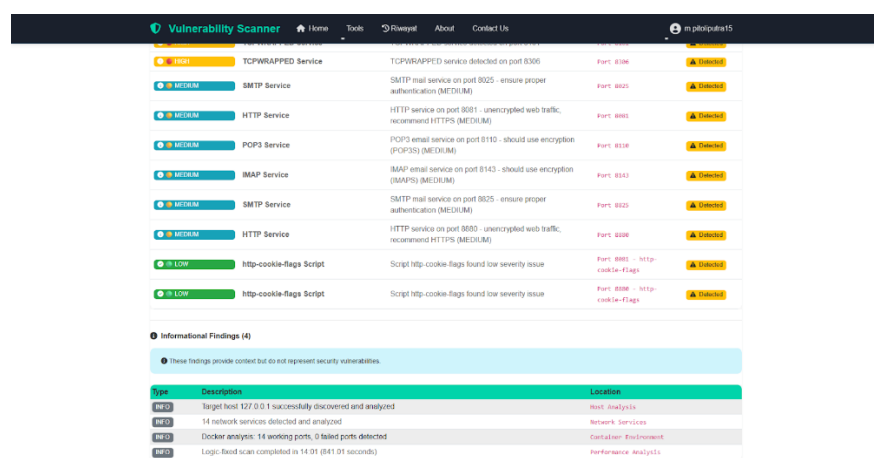
- Pengujian ketiga :

Gambar 5.32 dan Gambar 5.33 merupakan hasil pengujian ketiga pada *Website* target localhost:8081 dengan durasi scan selama 849.41 detik, didapatkan hasil temuan kerentanan dengan 4 kategori *critical* diantaranya FTP *service*, TELNET *service*, dan TCPWRAPPED *service*. Terdapat 3 kategori *high* yaitu http-title script dan TCPWRAPPED *services*. Terdapat 6 kategori *medium* yaitu SMTP *service*, HTTP *Service*, dan POP3 *Service* IMAP *service*. Terdapat 2 kategori *low* yaitu http-cookie-flags script dan 4 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8081 mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* ini sangat rentan terhadap serangan.



Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted Telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8012	Port: 8012	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8013	Port: 8013	Detected
HIGH	http-title Script	Script http-title found high severity issue	Port: 8080 - http-title	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8161	Port: 8161	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected

Gambar 5.32 Pengujian ketiga *Website* 1 device (Localhost:8081) dengan nmap Scanner



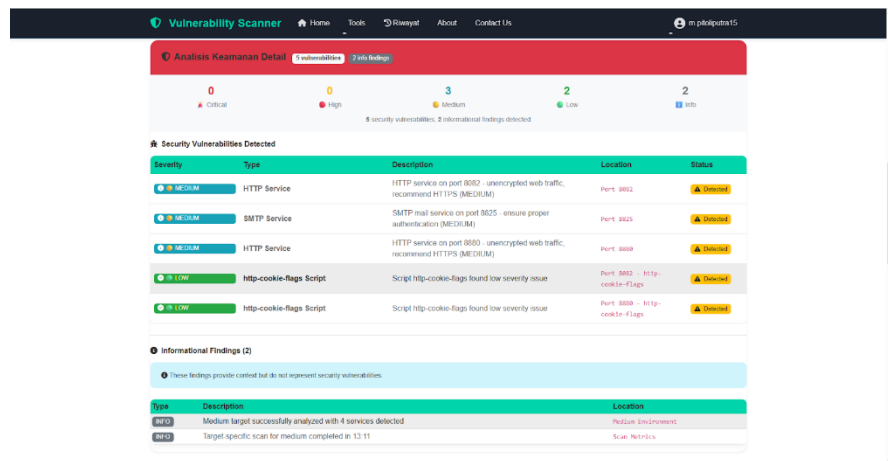
Severity	Type	Description	Location	Status
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected
LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected

Gambar 5.33 Pengujian ketiga *Website* 1 device (Localhost:8081) dengan nmap Scanner

b. *Website 2* (localhost:8082)

- Pengujian pertama :

Gambar 5.34 merupakan hasil pengujian pertama pada *Website* target localhost:8082 dengan durasi scan selama 791.64 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP service, HTTP Service, 2 kategori *low* yaitu http-cookie-flags script dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8082 mendapatkan *security score* sebesar 57 yang menunjukkan bahwa *Website* ini cukup aman namun perlu dilakukan perbaikan.



Severity	Type	Description	Location	Status
Medium	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8082	Detected
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
Medium	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8082 - http-cookie-flags	Detected
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected

Type	Description	Location
Info	Medium target successfully analyzed with 4 services detected	Medium Environment
Info	Target specific scan for medium completed in 13.11	Scan Metrics

Gambar 5.34 Pengujian pertama *Website 1 device* (Localhost:8082) dengan nmap Scanner

- Pengujian kedua :

Gambar 5.35 merupakan hasil pengujian kedua pada *Website* target localhost:8082 dengan durasi scan selama 801.13 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP service, HTTP Service, 2 kategori *low* yaitu http-cookie-flags script dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8082 mendapatkan *security score* sebesar 57 yang menunjukkan bahwa *Website* ini cukup aman namun perlu dilakukan perbaikan.

Severity	Type	Description	Location	Status
0 MEDIUM	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8082	Unpatched
0 MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Unpatched
0 MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Unpatched
0 LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8082 - http-cookie-flags	Unpatched
0 LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Unpatched

Type	Description	Location
INFO	Medium target successfully analyzed with 4 services detected	Medium Environment
INFO	Target-specific scan for medium completed in 13:11	Scan Metrics

Gambar 5. 35 Pengujian kedua *Website 1 device* (Localhost:8082) dengan nmap *Scanner*

- Pengujian ketiga :

Gambar 5.36 merupakan hasil pengujian ketiga pada *Website* target localhost:8082 dengan durasi scan selama 782.34 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP *service*, HTTP *Service*, 2 kategori *low* yaitu http-cookie-flags script dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8082 mendapatkan *security score* sebesar 57 yang menunjukkan bahwa *Website* ini cukup aman namun perlu dilakukan perbaikan.

Severity	Type	Description	Location	Status
0 MEDIUM	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8082	Unpatched
0 MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Unpatched
0 MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Unpatched
0 LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8082 - http-cookie-flags	Unpatched
0 LOW	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Unpatched

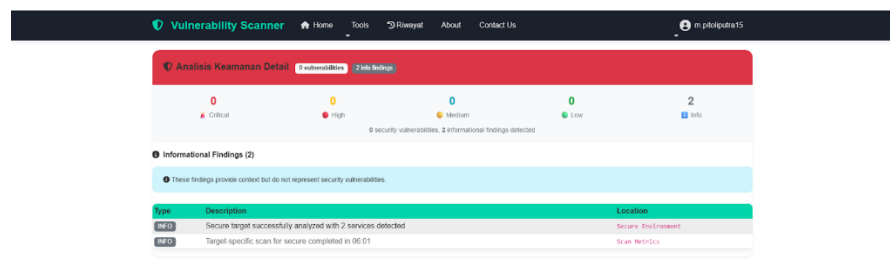
Type	Description	Location
INFO	Medium target successfully analyzed with 4 services detected	Medium Environment
INFO	Target-specific scan for medium completed in 13:11	Scan Metrics

Gambar 5.36 Pengujian ketiga *Website 1 device* (Localhost:8082) dengan nmap *Scanner*

c. *Website 3* (localhost:8083)

- Pengujian pertama :

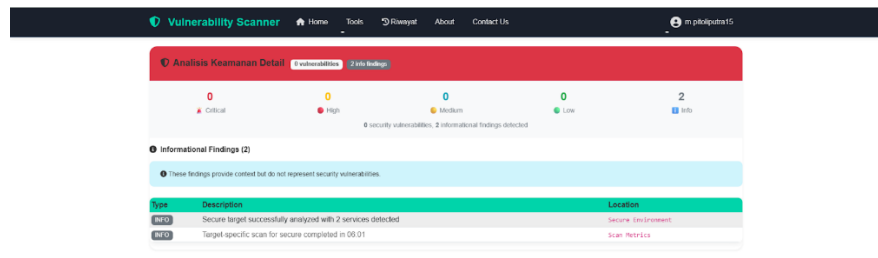
Gambar 5.37 merupakan hasil pengujian pertama pada *Website* target localhost:8083 dengan durasi scan selama 361.34 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP service, HTTP Service, 0 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8083 mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.37 Pengujian pertama *Website 1 device* (Localhost:8083) dengan nmap Scanner

- Pengujian kedua :

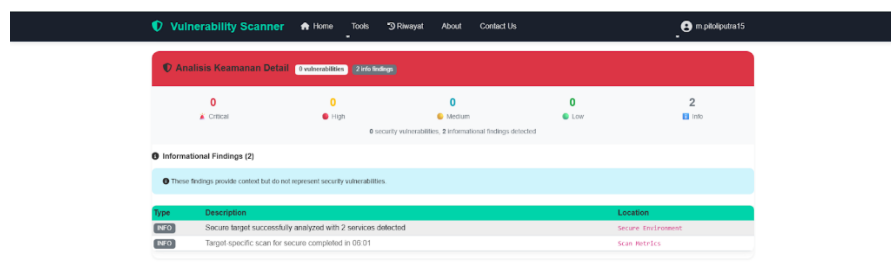
Gambar 5.38 merupakan hasil pengujian kedua pada *Website* target localhost:8083 dengan durasi scan selama 354.09 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP service, HTTP Service, 0 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8083 mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.38 Pengujian kedua *Website 1 device* (Localhost:8083) dengan nmap Scanner

- Pengujian ketiga :

Gambar 5.39 merupakan hasil pengujian ketiga pada *Website* target localhost:8083 dengan durasi scan selama 359.03 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP service, HTTP Service, 0 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8083 mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.39 Pengujian ketiga *Website 1 device* (Localhost:8083) dengan nmap Scanner

Tabel 5.4 Tabel Pengujian *Website 1 Device* Menggunakan Nmap Scanner

No.	Waktu Pengujian			Konsistensi Hasil Temuan			Keterangan
	P1	P 2	P 3	P 1	P 2	P 3	
<i>Website 1</i>	840.91 detik	851.11 detik	849.41 detik	Skor kerentanan 0	Skor kerentanan 0	Skor kerentanan 0	Hasil konsisten
<i>Website 2</i>	791.64 detik	801.13 detik	782.34 detik	Skor kerentanan 57	Skor kerentanan 57	Skor kerentanan 57	Hasil konsisten
<i>Website 3</i>	361.43 detik	354.09 detik	359.03 detik	Skor kerentanan 100	Skor kerentanan 100	Skor kerentanan 100	Hasil konsisten

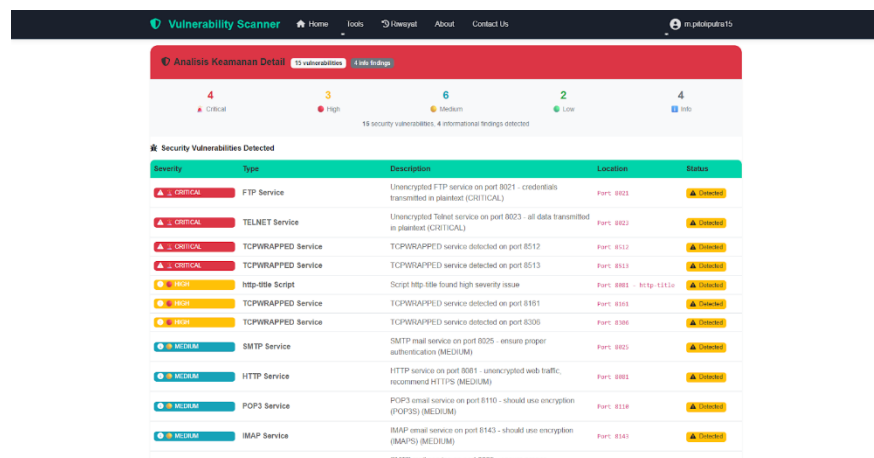
5.2.2.2 Pengujian *Website* Localhost dari *Device* yang Berbeda

Pada pengujian *Website* localhost dari *device* yang berbeda menggunakan 3 buah *Website* sebagai berikut :

a. *Website* 1 (localhost:8081)

- Pengujian pertama :

Gambar 5.40 dan Gambar 5.41 merupakan hasil pengujian pertama pada *Website* target localhost:8081 dari *device* lain dengan durasi scan selama 982.12 detik, didapatkan hasil temuan kerentanan dengan 4 kategori *critical* diantaranya FTP *service*, TELNET *service*, dan TCPWRAPPED *service*. Terdapat 3 kategori *high* yaitu http-title script dan TCPWRAPPED *services*. Terdapat 6 kategori *medium* yaitu SMTP *service*, HTTP *Service*, dan POP3 *Service* IMAP *service*. Terdapat 2 kategori *low* yaitu http-cookiep-flags script dan 4 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8081 mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* ini sangat rentan terhadap serangan.



Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted Telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8512	Port: 8512	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8513	Port: 8513	Detected
HIGH	http-title Script	Script http title found high severity issue	Port: 8081 - http://11111	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8191	Port: 8191	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
	SMTP mail service on port 8025 - ensure proper			

Gambar 5.40 Pengujian pertama *Website* beda *device*
(Localhost:8081) dengan nmap *Scanner*

Severity	Service	Description	Port	Action
High	TCPWRAPPED Service	TCPWRAPPED service detected on port 8086	Port: 8086	Blocked
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Blocked
Medium	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Blocked
Medium	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Blocked
Medium	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Blocked
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Blocked
Medium	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Blocked
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8081 - http-cookie-flags	Blocked
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Blocked

Type	Description	Location
INFO	Target host 127.0.0.1 successfully discovered and analyzed	Host Analysis
INFO	14 network services detected and analyzed	Network Services
INFO	Checker analysis: 14 working ports, 0 failed ports detected	Container Environment
INFO	Logic-based scan completed in 14.01 (841.01 seconds)	Performance Analysis

Gambar 5.41 Pengujian pertama *Website* beda *device*
(Localhost:8081) dengan nmap *Scanner*

- Pengujian kedua :

Gambar 5.42 dan Gambar 5.43 merupakan hasil pengujian kedua pada *Website* target localhost:8081 dari *device* lain dengan durasi scan selama 993.42 detik, didapatkan hasil temuan kerentanan dengan 4 kategori *critical* diantaranya *FTP service*, *TELNET service*, dan *TCPWRAPPED service*. Terdapat 3 kategori *high* yaitu *http-title script* dan *TCPWRAPPED services*. Terdapat 6 kategori *medium* yaitu *SMTP service*, *HTTP Service*, dan *POP3 Service* *IMAP service*. Terdapat 2 kategori *low* yaitu *http-cookie-flags script* dan 4 kategori *info*. Dari hasil temuan kerentanan tersebut, *Website* localhost:8081 mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* ini sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted Telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8012	Port: 8012	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8013	Port: 8013	Detected
HIGH	Http-Title Script	Script http-title found high severity issue	Port: 8080 - http://011a	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8161	Port: 8161	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected

Gambar 5.42 Pengujian kedua *Website* beda *device* (Localhost:8081) dengan *nmap Scanner*

Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted Telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8012	Port: 8012	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8013	Port: 8013	Detected
HIGH	Http-Title Script	Script http-title found high severity issue	Port: 8080 - http://011a	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8161	Port: 8161	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
LOW	Http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http://cookie-flags	Detected
LOW	Http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http://cookie-flags	Detected

Gambar 5.43 Pengujian kedua *Website* beda *device* (Localhost:8081) dengan *nmap Scanner*

• Pengujian ketiga :

Gambar 5.44 dan Gambar 5.45 merupakan hasil pengujian ketiga pada *Website* target localhost:8081 dari *device* lain dengan durasi scan selama 992.22 detik, didapatkan hasil temuan kerentanan dengan 4 kategori *critical* diantaranya *FTP service*, *TELNET service*, dan *TCPWRAPPED service*. Terdapat 3 kategori *high* yaitu *http-title script* dan *TCPWRAPPED services*. Terdapat 6 kategori *medium* yaitu *SMTP service*, *HTTP Service*, dan *POP3 Service* *IMAP service*. Terdapat 2 kategori *low* yaitu *http-cookie-flags script* dan 4 kategori *info*. Dari hasil temuan kerentanan tersebut, *Website* localhost:8081 mendapatkan

security score sebesar 0 yang menunjukkan bahwa *Website* ini sangat rentan terhadap serangan.

The screenshot shows the 'Vulnerability Scanner' interface with a summary of findings: 4 Critical, 3 High, 6 Medium, 2 Low, and 4 Info. Below this, a table lists the detected security vulnerabilities.

Severity	Type	Description	Location	Status
Critical	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
Critical	TELNET Service	Unencrypted Telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
Critical	TCPWRAPPED Service	TCPWRAPPED service detected on port 8012	Port: 8012	Detected
Critical	TCPWRAPPED Service	TCPWRAPPED service detected on port 8013	Port: 8013	Detected
High	http-title Script	Script http-title found high severity issue	Port: 8081 - http-8081	Detected
High	TCPWRAPPED Service	TCPWRAPPED service detected on port 8061	Port: 8061	Detected
High	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
Medium	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
Medium	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
Medium	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected

Gambar 5.44 Pengujian ketiga *Website* beda *device* (Localhost:8081) dengan nmap *Scanner*

The screenshot shows the 'Vulnerability Scanner' interface with a summary of findings: 1 High, 5 Medium, 2 Low, and 4 Info. Below this, a table lists the detected security vulnerabilities.

Severity	Type	Description	Location	Status
High	TCPWRAPPED Service	TCPWRAPPED service detected on port 8306	Port: 8306	Detected
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
Medium	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
Medium	POP3 Service	POP3 email service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
Medium	IMAP Service	IMAP email service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
Medium	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8081 - http-cookie-flags	Detected
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected

Informational Findings (4)

Type	Description	Location
INFO	Target host 127.0.0.1 successfully discovered and analyzed	Host Analysis
INFO	14 network services detected and analyzed	Network Services
INFO	Docker analysis: 14 working ports, 0 failed ports detected	Container Environment
INFO	Logic based scan completed in 14.01 (841.01 seconds)	Performance Analysis

Gambar 5.45 Pengujian ketiga *Website* beda *device* (Localhost:8081) dengan nmap *Scanner*

b. *Website* 2 (localhost:8082)

- Pengujian pertama :

Gambar 5.46 merupakan hasil pengujian pertama pada *Website* target localhost:8082 dengan durasi scan selama 850.21 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP *service*, HTTP *Service*, 2 kategori *low* yaitu http-cookie-flags script dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8082 mendapatkan *security score* sebesar 57

yang menunjukkan bahwa *Website* ini cukup aman namun perlu dilakukan perbaikan.

Severity	Type	Description	Location	Status
Medium	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8082	Unfixed
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Unfixed
Medium	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Unfixed
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8082 - http-cookie-flags	Unfixed
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Unfixed

Type	Description	Location
Info	Medium target successfully analyzed with 4 services detected	Medium Environment
Info	Target-specific scan for medium completed in 13:11	Scan Metrics

Gambar 5.46 Pengujian pertama *Website* beda device
(Localhost:8082) dengan nmap Scanner

- Pengujian kedua :

Gambar 5.47 merupakan hasil pengujian kedua pada *Website* target localhost:8082 dari *device* lain dengan durasi scan selama 862.12 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP service, HTTP Service, 2 kategori *low* yaitu http-cookie-flags script dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8082 mendapatkan *security score* sebesar 57 yang menunjukkan bahwa *Website* ini cukup aman namun perlu dilakukan perbaikan.

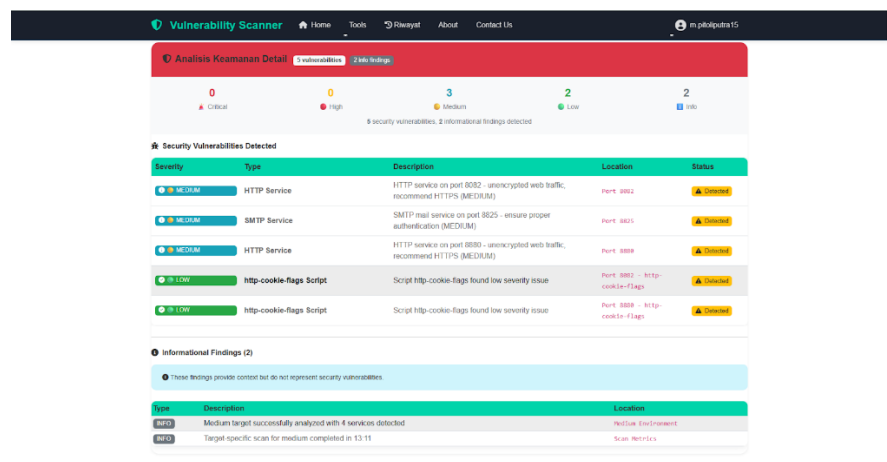
Severity	Type	Description	Location	Status
Medium	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8082	Unfixed
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Unfixed
Medium	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Unfixed
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8082 - http-cookie-flags	Unfixed
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Unfixed

Type	Description	Location
Info	Medium target successfully analyzed with 4 services detected	Medium Environment
Info	Target-specific scan for medium completed in 13:11	Scan Metrics

Gambar 5.47 Pengujian kedua *Website* beda device (Localhost:8082)
dengan nmap Scanner

- Pengujian ketiga :

Gambar 5.48 merupakan hasil pengujian ketiga pada *Website* target localhost:8082 dari *device* lain dengan durasi scan selama 859.33 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP *service*, HTTP *Service*, 2 kategori *low* yaitu http-cookiep-flags script dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8082 mendapatkan *security score* sebesar 57 yang menunjukkan bahwa *Website* ini cukup aman namun perlu dilakukan perbaikan.



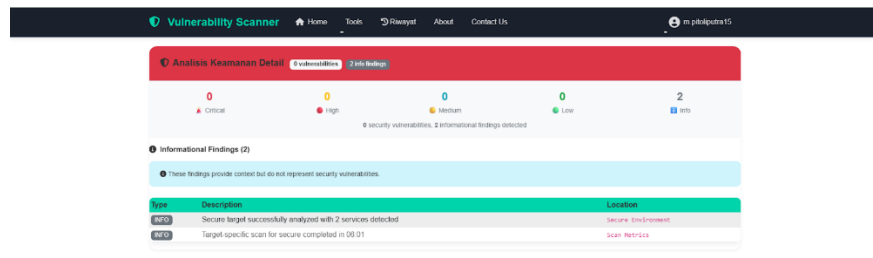
Severity	Type	Description	Location	Status
Medium	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 8082	Detected
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port 8025	Detected
Medium	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 8080	Detected
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port 8082 - http-cookie-flags	Detected
Low	http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port 8080 - http-cookie-flags	Detected

Gambar 5.48 Pengujian ketiga *Website* beda *device* (Localhost:8082) dengan nmap *Scanner*

c. *Website* 3 (localhost:8083)

- Pengujian pertama :

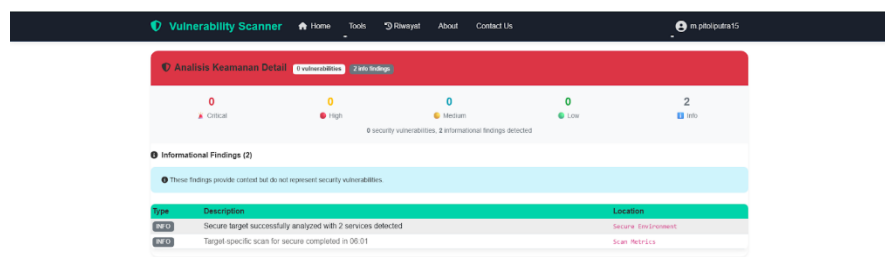
Gambar 5.49 merupakan hasil pengujian pertama pada *Website* target localhost:8083 dengan durasi scan selama 442.76 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP *service*, HTTP *Service*, 0 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* localhost:8083 mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.49 Pengujian pertama *Website* beda *device* (Localhost:8083) dengan nmap *Scanner*

- Pengujian kedua :

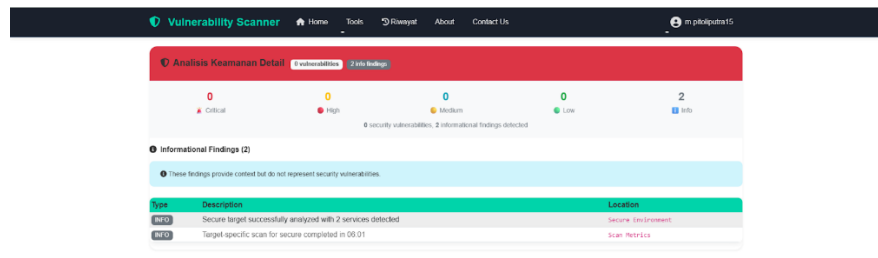
Gambar 5.50 merupakan hasil pengujian kedua pada *Website* target localhost:8083 dengan durasi scan selama 437.21 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP *service*, HTTP *Service*, 0 kategori *low* dan 2 kategori *info*. Dari hasil temuan kerentanan tersebut, *Website* localhost:8083 mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.50 Pengujian kedua *Website* beda *device* (Localhost:8083) dengan nmap *Scanner*

- Pengujian ketiga :

Gambar 5.51 merupakan hasil pengujian ketiga pada *Website* target localhost:8083 dengan durasi scan selama 459.45 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 3 kategori *medium* yaitu SMTP *service*, HTTP *Service*, 0 kategori *low* dan 2 kategori *info*. Dari hasil temuan kerentanan tersebut, *Website* localhost:8083 mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.51 Pengujian ketiga *Website* beda *device* (Localhost:8083) dengan nmap *Scanner*

Tabel 5.5 Pengujian *Website* Beda *Device* Menggunakan Nmap *Scanner*

No.	Waktu Pengujian			Konsistensi Hasil Temuan			Keterangan
	P 1	P 2	P 3	P 1	P 2	P 3	
<i>Website</i> 1	982.12 detik	993.42 detik	992.22 detik	Skor kerentanan 0	Skor kerentanan 0	Skor kerentanan 0	Hasil konsisten
<i>Website</i> 2	850.12 detik	862.12 detik	859.33 detik	Skor kerentanan 57	Skor kerentanan 57	Skor kerentanan 57	Hasil konsisten
<i>Website</i> 3	422.76 detik	437.21 detik	459.45 detik	Skor kerentanan 100	Skor kerentanan 100	Skor kerentanan 100	Hasil konsisten

5.2.2.3 Pengujian *Website* dari Internet

Pada pengujian *Website* dari internet menggunakan 3 buah *Website* sebagai berikut :

a. *Website* 1 (scanme.nmap.org)

- Pengujian pertama :

Gambar 5.52 merupakan hasil pengujian pertama pada *Website* target scanme.nmap.org dengan durasi scan selama 176.18 detik, didapatkan hasil temuan kerentanan dengan 2 kategori *critical* yaitu vulners script, 0 kategori *high*, 2 kategori *medium* yaitu HTTP *Service* dan http-comments-displayer script, 3 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* scanme.nmap.org mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 22 - vulners	Detected
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 80 - vulners	Detected
MEDIUM	http-comments-displayer Script	Script http-comments-displayer found medium severity issue	Port 80 - http-comments-displayer	Detected
MEDIUM	HTTP Service	HTTP service - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 80	Detected
LOW	http-sitemap-generator Script	Script http-sitemap-generator found low severity issue	Port 80 - http-sitemap-generator	Detected
LOW	http-security-headers Script	Script http-security-headers found low severity issue	Port 80 - http-security-headers	Detected
LOW	http-headers Script	Script http-headers found low severity issue	Port 80 - http-headers	Detected

Gambar 5.52 Pengujian pertama *Website* internet (scanme.nmap.org) dengan nmap Scanner

- Pengujian kedua :

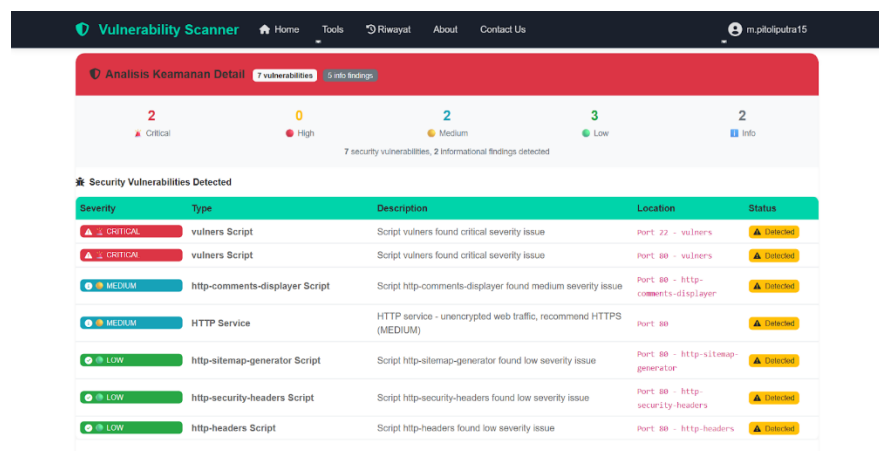
Gambar 5.53 merupakan hasil pengujian kedua pada *Website* target scanme.nmap.org dengan durasi scan selama 180.01 detik, didapatkan hasil temuan kerentanan dengan 2 kategori *critical* yaitu vulners script, 0 kategori *high*, 2 kategori *medium* yaitu HTTP Service dan http-comments-displayer script, 3 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* scanme.nmap.org mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* sangat rentan terhadap serangan.

Severity	Type	Description	Location	Status
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 22 - vulners	Detected
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 80 - vulners	Detected
MEDIUM	http-comments-displayer Script	Script http-comments-displayer found medium severity issue	Port 80 - http-comments-displayer	Detected
MEDIUM	HTTP Service	HTTP service - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 80	Detected
LOW	http-sitemap-generator Script	Script http-sitemap-generator found low severity issue	Port 80 - http-sitemap-generator	Detected
LOW	http-security-headers Script	Script http-security-headers found low severity issue	Port 80 - http-security-headers	Detected
LOW	http-headers Script	Script http-headers found low severity issue	Port 80 - http-headers	Detected

Gambar 5.53 Pengujian kedua *Website* internet (scanme.nmap.org) dengan nmap Scanner

- Pengujian ketiga :

Gambar 5.54 merupakan hasil pengujian ketigas pada *Website* target scanme.nmap.org dengan durasi scan selama 166.12 detik, didapatkan hasil temuan kerentanan dengan 2 kategori *critical* yaitu vulners script, 0 kategori *high*, 2 kategori *medium* yaitu HTTP Service dan http-comments-displayer script, 3 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* scanme.nmap.org mendapatkan *security score* sebesar 0 yang menunjukkan bahwa *Website* sangat rentan terhadap serangan.



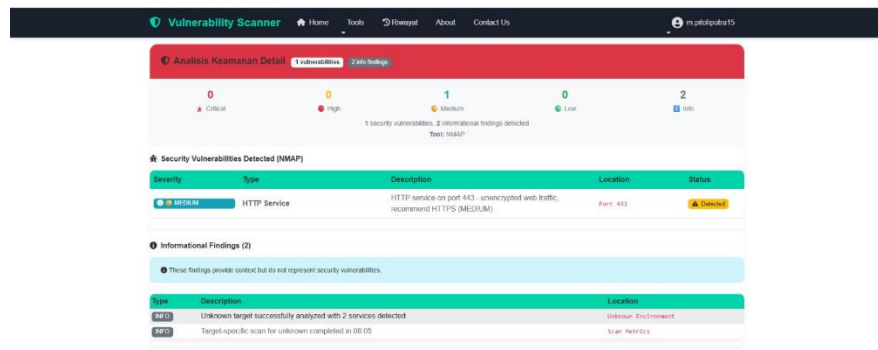
Severity	Type	Description	Location	Status
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 22 - vulners	Detected
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 80 - vulners	Detected
MEDIUM	http-comments-displayer Script	Script http-comments-displayer found medium severity issue	Port 80 - http-comments-displayer	Detected
MEDIUM	HTTP Service	HTTP service - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 80	Detected
LOW	http-sitemap-generator Script	Script http-sitemap-generator found low severity issue	Port 80 - http-sitemap-generator	Detected
LOW	http-security-headers Script	Script http-security-headers found low severity issue	Port 80 - http-security-headers	Detected
LOW	http-headers Script	Script http-headers found low severity issue	Port 80 - http-headers	Detected

Gambar 5.54 Pengujian ketiga *Website* internet (scanme.nmap.org) dengan nmap Scanner

b. *Website* 2 (neverssl.com)

- Pengujian pertama :

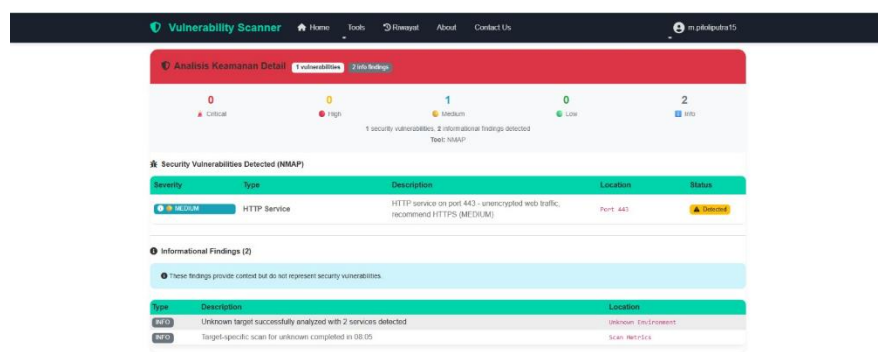
Gambar 5.55 merupakan hasil pengujian pertama pada *Website* target neverssl.com dengan durasi scan selama 481.57 detik, didapatkan hasil temuan kerentanan dengan 1 kategori *medium* yaitu HTTP Service dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* neverssl.com mendapatkan *security score* sebesar 80 yang menunjukkan bahwa *Website* sangat rentan terhadap serangan.



Gambar 5.55 Pengujian pertama *Website* internet (neverssl.com) dengan nmap *Scanner*

- Pengujian kedua :

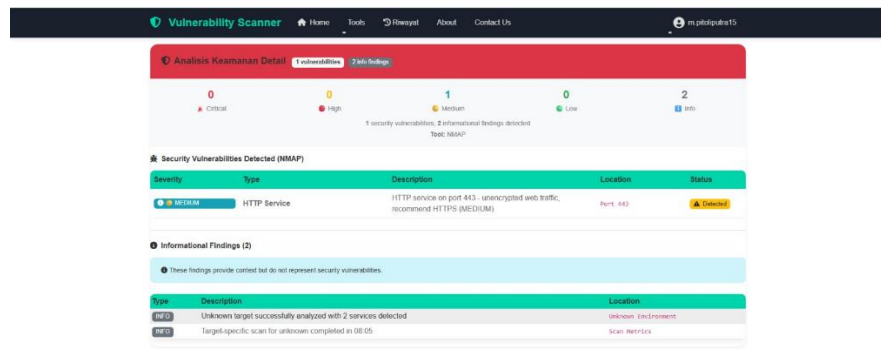
Gambar 5.56 merupakan hasil pengujian pertama pada *Website* target neverssl.com dengan durasi scan selama 485.81 detik, didapatkan hasil temuan kerentanan dengan 1 kategori *medium* yaitu *HTTP Service* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* neverssl.com mendapatkan *security score* sebesar 80 yang menunjukkan bahwa *Website* sangat rentan terhadap serangan.



Gambar 5.56 Pengujian kedua *Website* internet (neverssl.com) dengan nmap *Scanner*

- Pengujian ketiga :

Gambar 5.57 merupakan hasil pengujian pertama pada *Website* target neverssl.com dengan durasi scan selama 477.32 detik, didapatkan hasil temuan kerentanan dengan 1 kategori *medium* yaitu *HTTP Service* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* neverssl.com mendapatkan *security score* sebesar 80 yang menunjukkan bahwa *Website* sangat rentan terhadap serangan.

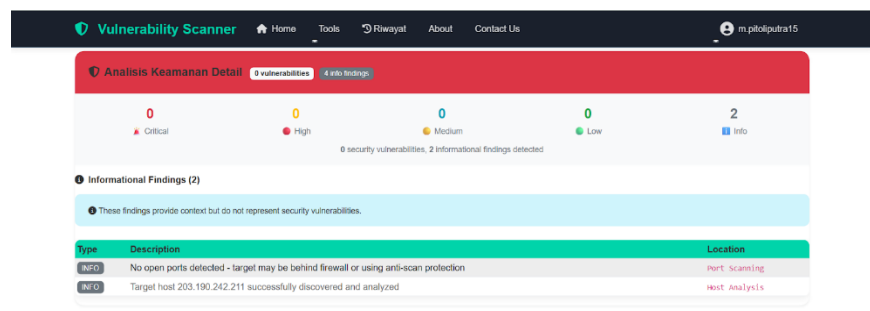


Gambar 5.57 Pengujian ketiga *Website* internet (neverssl.com) dengan *nmap Scanner*

c. *Website* 3 (www.detik.com)

- Pengujian pertama :

Gambar 5.58 merupakan hasil pengujian pertama pada *Website* target www.detik.com dengan durasi scan selama 513.35 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* www.detik.com mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.

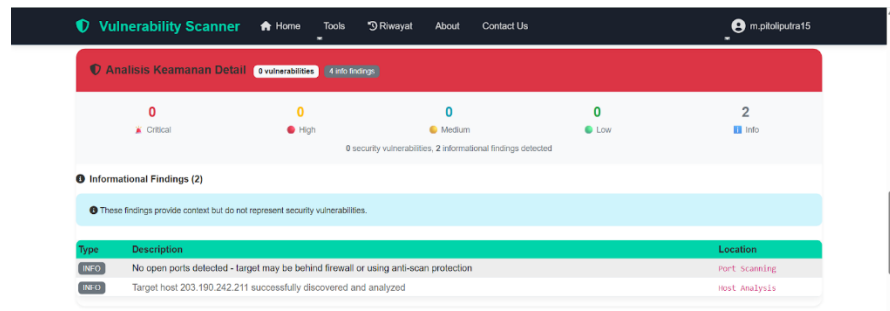


Gambar 5.58 Pengujian pertama *Website* internet (www.detik.com) dengan *nmap Scanner*

- Pengujian kedua :

Gambar 5.59 merupakan hasil pengujian kedua pada *Website* target www.detik.com dengan durasi scan selama 502.01 detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 2 kategori info. Dari hasil temuan kerentanan tersebut, *Website* www.detik.com mendapatkan *security*

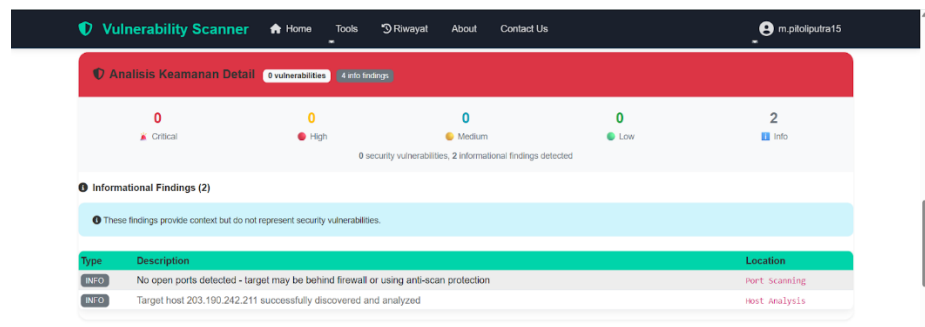
score sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5.59 Pengujian kedua *Website internet* (www.detik.com) dengan nmap Scanner

- Pengujian ketiga :

Gambar 5.60 merupakan hasil pengujian ketiga pada *Website* target www.detik.com dengan durasi scan selama **521.33** detik, didapatkan hasil temuan kerentanan dengan 0 kategori *critical*, 0 kategori *high*, 0 kategori *medium*, 0 kategori *low* dan 2 kategori *info*. Dari hasil temuan kerentanan tersebut, *Website* www.detik.com mendapatkan *security score* sebesar 100 yang menunjukkan bahwa *Website* sangat aman dan kemungkinan mendapat serangan sangat rendah.



Gambar 5. 60 Pengujian ketiga *Website internet* (www.detik.com) dengan nmap Scanner

Tabel 5. 6 Pengujian *Website* Internet Menggunakan Nmap Scanner

No.	Waktu Pengujian			Konsistensi Hasil Temuan			Keterangan
	P1	P 2	P 3	P 1	P 2	P 3	
<i>Website</i> 1	176.18 detik	180.01 detik	166.12 detik	Skor kerentanan 0	Skor kerentanan 0	Skor kerentanan 0	Hasil konsisten
<i>Website</i> 2	481.57 detik	485.81 detik	477.32 detik	Skor kerentanan 80	Skor kerentanan 80	Skor kerentanan 80	Hasil konsisten
<i>Website</i> 3	513.35 detik	502.01 detik	521.33 detik	Skor kerentanan 100	Skor kerentanan 100	Skor kerentanan 100	Hasil konsisten

Berdasarkan semua pengujian di atas, didapatkan data hasil analisis rangkuman seperti yang tertera pada **Tabel 5.7** Rekap Hasil Analisis Pengujian *Website*

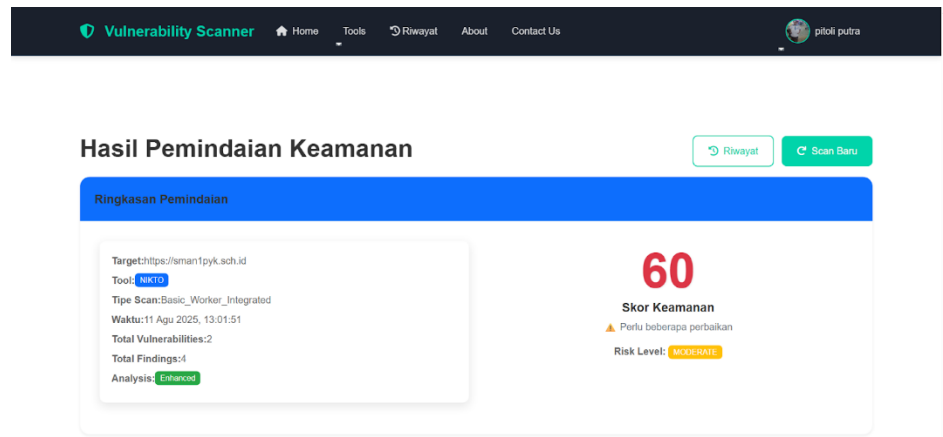
Tabel 5. 7 Rekap Hasil Analisis Pengujian *Website*

Jenis Pengujian	TOOLS		Hasil Pengukuran		
	NIKTO	NMAP	Rata-Rata Durasi Scan Nikto	Rata-Rata Durasi Scan Nmap	Konsistensi Temuan
Local Host 1 Device	<i>Website</i> 1 (5001)	<i>Website</i> 1 (8081)	1.77 detik	174.10 detik	Konsisten
	<i>Website</i> 2 (5002)	<i>Website</i> 2 (8082)	0.99 detik	481.57 detik	Konsisten
	<i>Website</i> 3 (5003)	<i>Website</i> 3 (8083)	1.22 detik	512.23 detik	Konsisten
Local Host Beda Device	<i>Website</i> 1 (5001)	<i>Website</i> 1 (8081)	10.12 detik	989.25 detik	Konsisten
	<i>Website</i> 2 (5002)	<i>Website</i> 2 (8082)	8.72 detik	857.19 detik	Konsisten
	<i>Website</i> 3 (5003)	<i>Website</i> 3 (8083)	4.51 detik	439.81 detik	Konsisten
Internet	www.pln.co.id	scanme.nmap	20.18 detik	847.14 detik	Konsisten
	httpbin.org	neverssl.com	82.76 detik	791.70 detik	Konsisten
	www.komdigi.go.id	www.detik.com	23.51 detik	358.18 detik	Konsisten

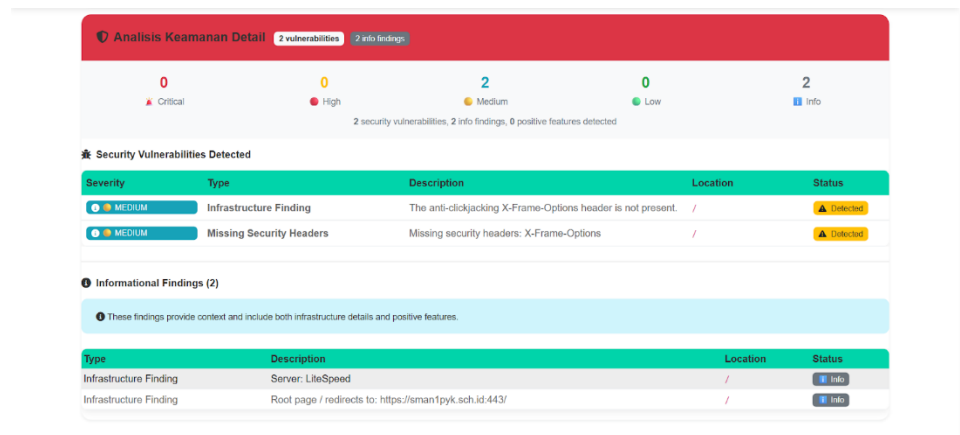
5.2.3 Pengujian Komparasi Nmap dan Nikto

5.2.3.1 Website <https://sman1pyk.sch.id/>

a. Menggunakan Tools Nikto



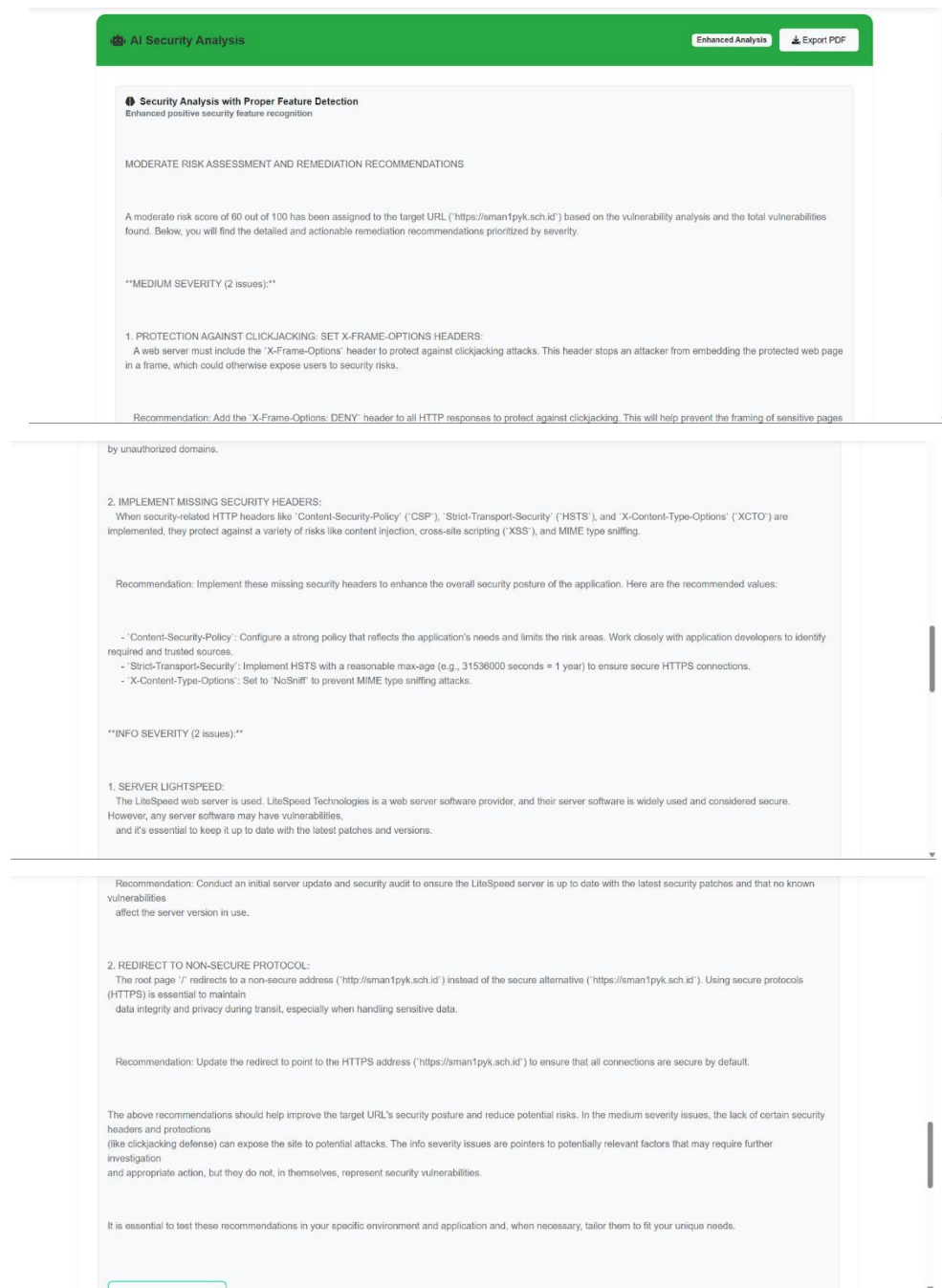
Gambar 5. 61 Skor Keamanan Website <https://sman1pyk.sch.id/>
Berdasarkan Hasil Pemindaian Nikto



Gambar 5. 62 Hasil Temuan Kerentanan Website
<https://Sman1pyk.Sch.Id/> Berdasarkan Hasil Pemindaian Nikto

Gambar 5.61 dan Gambar 5.62 menampilkan hasil pengujian terhadap website target <https://sman1pyk.sch.id/> menggunakan tools Nikto. Pengujian ini menghasilkan dua temuan dengan tingkat *medium*. Temuan pertama diidentifikasi sebagai tipe *Infrastructure Finding*, yaitu tidak adanya *header* anti-clickjacking X-Frame-Options. Temuan kedua diidentifikasi sebagai tipe *Missing Security Headers* dengan deskripsi yang sama, yakni ketiadaan *header* X-Frame-Options. Selain itu, ditemukan dua informasi pendukung (*informational findings*), yaitu penggunaan server LiteSpeed serta adanya pengalihan (*redirect*) dari halaman utama menuju

<https://sman1pyk.sch.id:443/>. Berdasarkan keseluruhan temuan, *website* ini memperoleh nilai keamanan (*security score*) sebesar 60, yang menunjukkan tingkat kerentanan yang cukup signifikan terhadap potensi serangan.

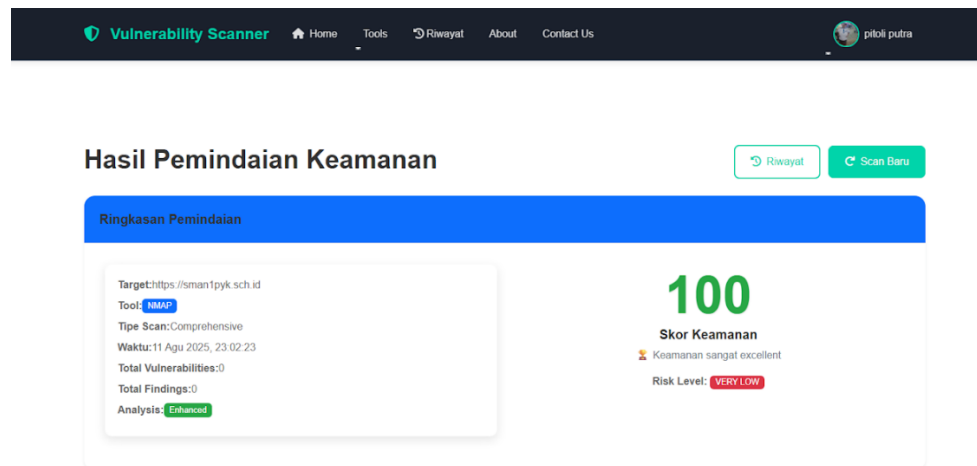


Gambar 5. 63 Hasil Rekomendasi AI *Website* <https://sman1pyk.sch.id/>
Berdasarkan Hasil Pemindaian Nikto

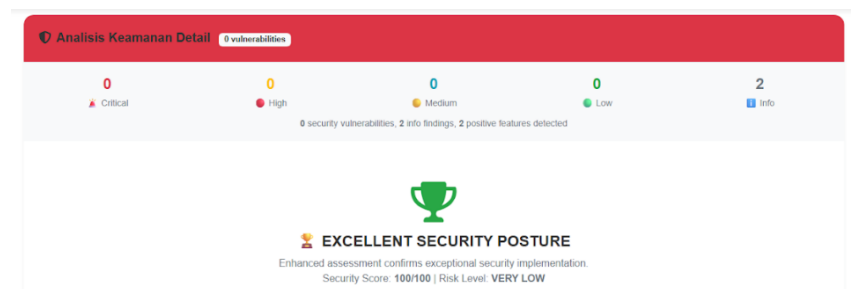
Gambar 5. 63 menampilkan rekomendasi perbaikan yang selaras dengan temuan kerentanan pada *website* target. Ketiadaan *header* keamanan X-Frame-Options direspons dengan saran untuk menambahkan X-Frame-

Options: DENY pada seluruh respons HTTP, sehingga dapat mencegah potensi serangan *clickjacking*. Temuan serupa pada tipe *Missing Security Headers* diikuti dengan rekomendasi untuk mengimplementasikan *security headers* yang hilang, guna memperkuat perlindungan aplikasi. Penggunaan server LiteSpeed diantisipasi melalui anjuran pembaruan dan audit keamanan, memastikan versi server telah mendapatkan *security patch* terbaru. Sementara itu, pengalihan dari halaman utama menuju <https://sman1pyk.sch.id:443/> diatasi dengan saran memperbarui tujuan pengalihan agar langsung mengarah ke <https://sman1pyk.sch.id>, menjamin koneksi aman secara default melalui HTTPS.

b. Menggunakan Tools Nmap



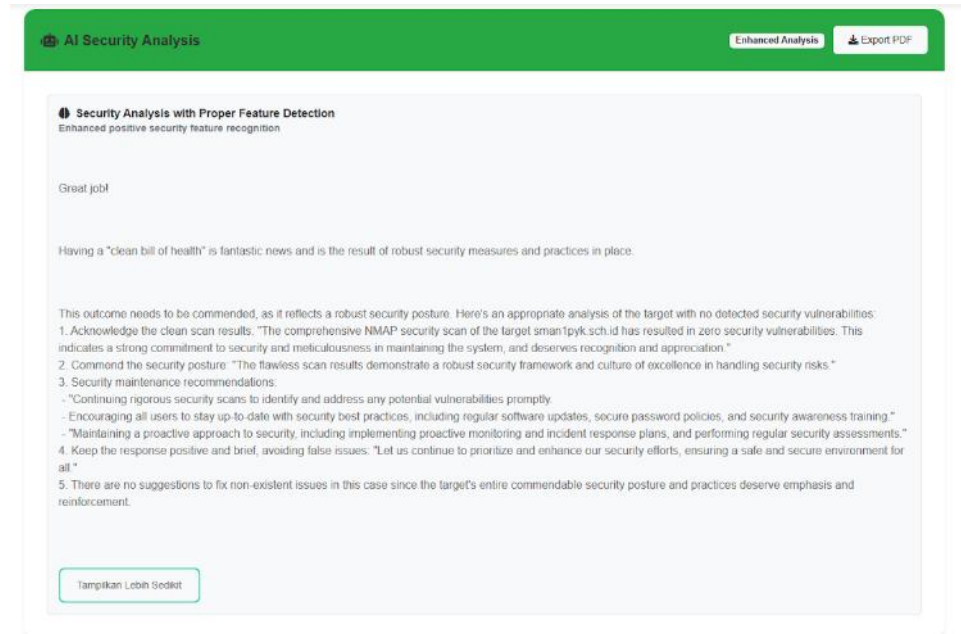
Gambar 5. 64 Skor Keamanan Website <https://sman1pyk.sch.id/>
Berdasarkan Hasil Pemindaian Nmap



Gambar 5. 65 Hasil Temuan Kerentanan Website
<https://Sman1pyk.Sch.Id/> Berdasarkan Hasil Pemindaian Nmap

Gambar 5. 64 dan Gambar 5. 65 menampilkan hasil pengujian terhadap website target <https://sman1pyk.sch.id/> menggunakan tools Nmap.

Pengujian ini tidak menemukan adanya kerentanan pada *website*. Berdasarkan hasil tersebut, *website* ini memperoleh nilai keamanan (*security score*) sebesar 100, yang menunjukkan bahwa *website* berada dalam kondisi sangat aman dan minim risiko serangan.

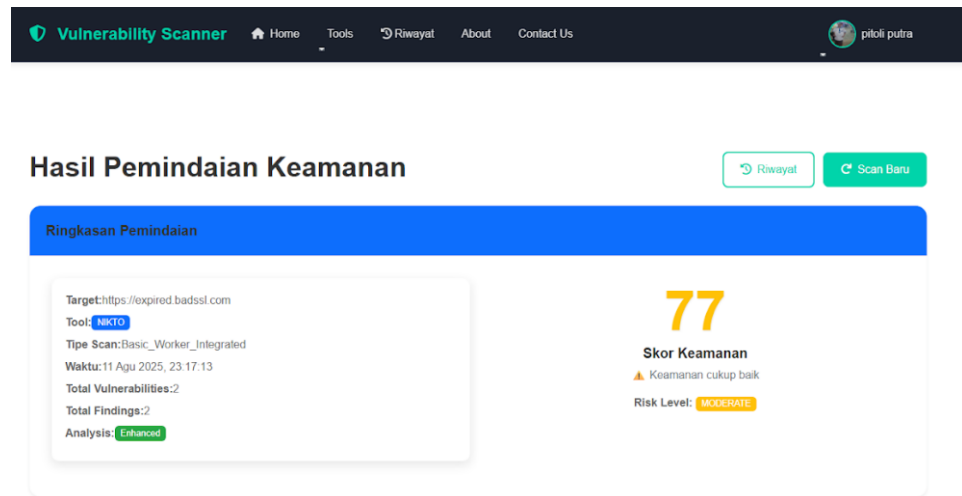


Gambar 5. 66 Hasil Rekomendasi AI *Website* <https://sman1pyk.sch.id/>
Berdasarkan Hasil Pemindaian Nmap

Gambar 5. 66 merupakan hasil rekomendasi dari AI untuk *website* target <https://sman1pyk.sch.id/>. Berdasarkan hasil pengujian, nilai kerentanan tercatat 0 atau tidak ditemukan kerentanan pada *website* ini. Meskipun demikian, rekomendasi yang diberikan tetap relevan untuk menjaga keamanan jangka panjang. Saran yang disampaikan meliputi pelaksanaan *security scan* secara ketat dan berkelanjutan untuk mengidentifikasi serta menangani potensi kerentanan secara cepat, memastikan seluruh pengguna selalu mengikuti praktik keamanan terbaik seperti pembaruan perangkat lunak secara rutin, kebijakan kata sandi yang kuat, dan pelatihan kesadaran keamanan, serta mempertahankan pendekatan keamanan proaktif melalui penerapan pemantauan berkelanjutan, rencana respons insiden, dan penilaian keamanan secara berkala.

5.2.3.2 Website <https://expired.badssl.com>

a. Menggunakan Tools Nikto



Gambar 5. 67 Skor Keamanan *Website* <https://expired.badssl.com>
Berdasarkan Hasil Pemindaian Nikto

Analisis Keamanan Detail 2 vulnerabilities

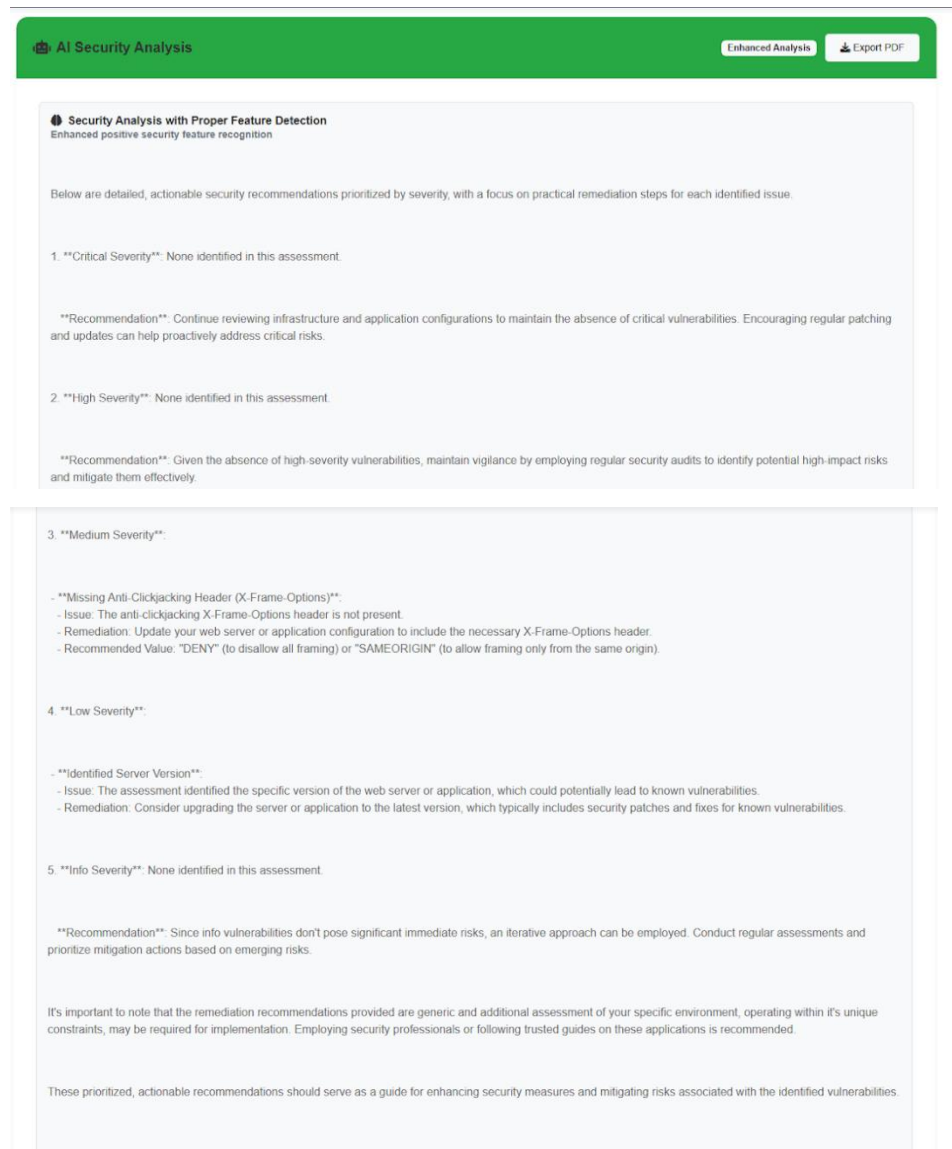
0 Critical 0 High 1 Medium 1 Low 0 Info
2 security vulnerabilities, 0 info findings, 0 positive features detected

★ Security Vulnerabilities Detected

Severity	Type	Description	Location	Status
MEDIUM	Infrastructure Finding	The anti-clickjacking X-Frame-Options header is not present.	/	Detected
LOW	Infrastructure Finding	Server: nginx/1.10.3 (Ubuntu)	/1.10.3	Detected

Gambar 5. 68 Hasil Temuan Kerentanan *Website* <https://expired.badssl.com>
Berdasarkan Hasil Pemindaian Nikto

Gambar 5.67 dan Gambar 5.68 menampilkan hasil pengujian terhadap *website* target <https://expired.badssl.com> menggunakan *tools* Nikto. Pengujian ini menghasilkan dua temuan kerentanan. Temuan pertama memiliki kategori *medium* dan dikategorikan sebagai tipe *Infrastructure Finding*, yaitu tidak adanya header anti-clickjacking X-Frame-Options. Temuan kedua memiliki kategori *low* dengan tipe *Infrastructure Finding*, yang menunjukkan bahwa server menggunakan nginx/1.10.3 (Ubuntu). Berdasarkan keseluruhan temuan, *website* ini memperoleh nilai keamanan (*security score*) sebesar 77, yang menunjukkan tingkat risiko sedang (*moderate risk level*).



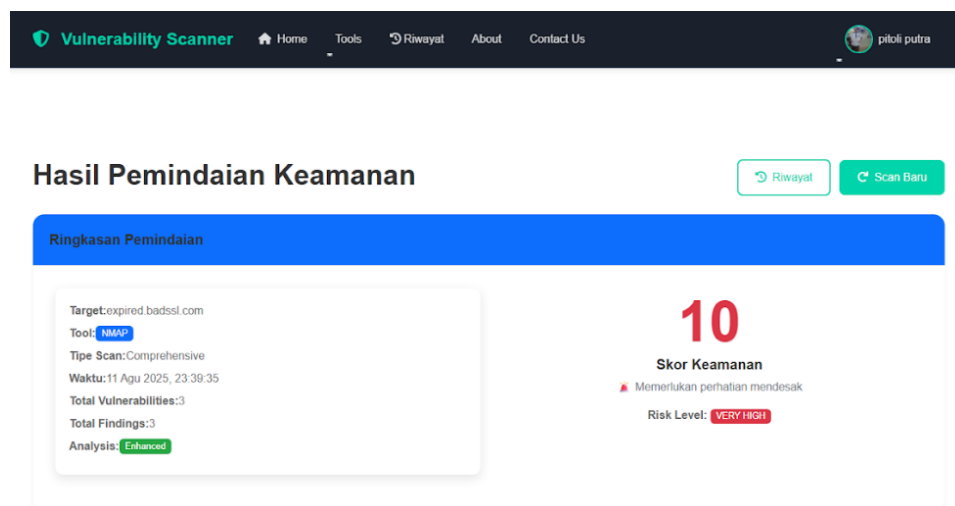
Gambar 5. 69 Hasil Rekomendasi AI *Website*

<https://Expired.Badssl.Com> Berdasarkan Hasil Pemindaian Nikto

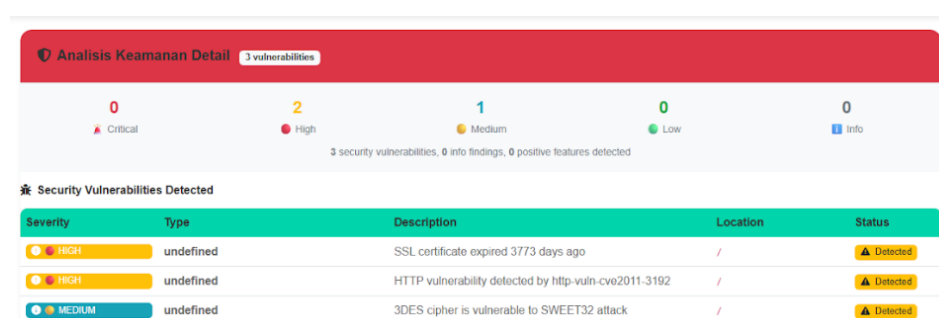
Gambar 5. 69 menampilkan hasil rekomendasi perbaikan yang sesuai dengan temuan kerentanan pada website target <https://expired.badssl.com> . Untuk kerentanan dengan tingkat medium, yaitu ketiadaan header anti-clickjacking X-Frame-Options, rekomendasi yang diberikan adalah memperbarui konfigurasi server atau aplikasi web agar menyertakan header X-Frame-Options dengan nilai yang disarankan, yaitu "DENY" untuk melarang seluruh framing atau "SAMEORIGIN" untuk mengizinkan framing hanya dari sumber yang sama. Untuk temuan dengan tingkat rendah yang berkaitan dengan versi server nginx/1.10.3 (Ubuntu), rekomendasi yang dianjurkan adalah melakukan pembaruan server atau

aplikasi ke versi terbaru guna memastikan penerapan patch keamanan dan perbaikan atas kerentanan yang sudah diketahui.

b. Menggunakan Tools Nmap



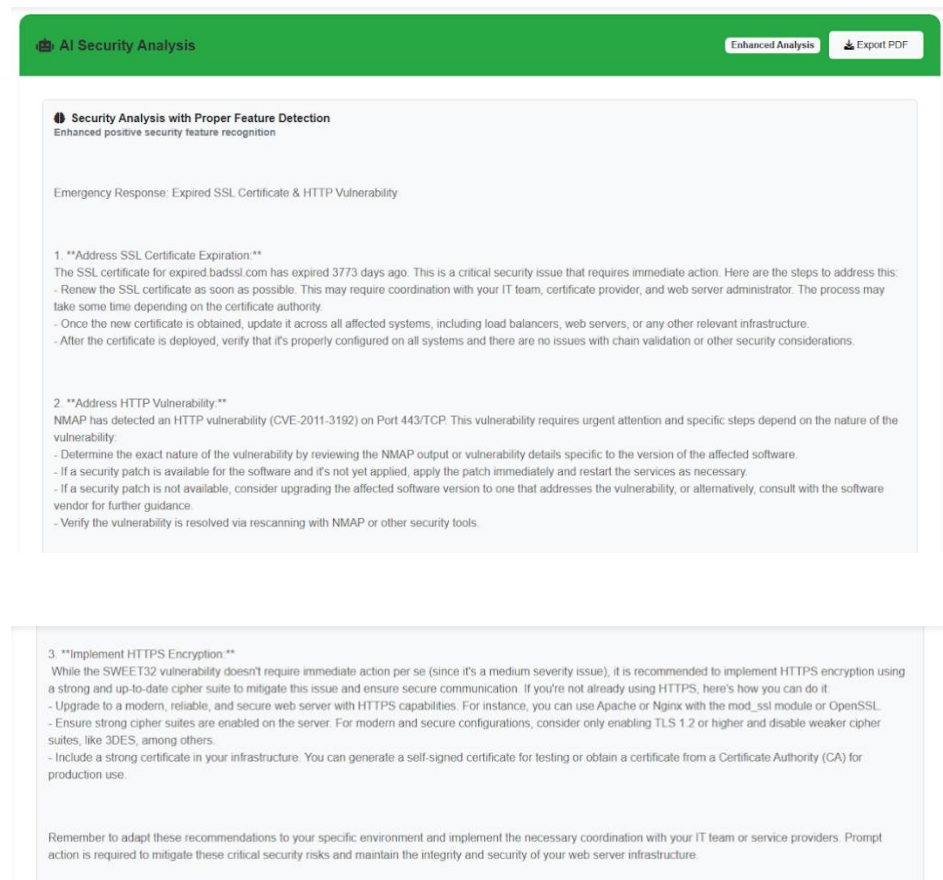
Gambar 5. 70 Skor Keamanan *Website* <https://expired.badssl.com>
Berdasarkan Hasil Pemindaian Nmap



Gambar 5. 71 Hasil Temuan Kerentanan *Website*
<https://Expired.Badssl.Com> Berdasarkan Hasil Pemindaian Nmap

Gambar 5. 70 dan Gambar 5. 71 menampilkan hasil pengujian terhadap *website* target <https://expired.badssl.com> menggunakan *tools* Nmap. Pengujian ini mengidentifikasi tiga temuan kerentanan dengan kategori yang berbeda. Temuan pertama memiliki kategori *high* yaitu sertifikat SSL yang telah kedaluwarsa selama 3773 hari. Temuan kedua memiliki kategori *high* yaitu adanya kerentanan HTTP yang terdeteksi melalui CVE-2011-3192. Sementara itu, temuan ketiga memiliki kategori *medium* yaitu penggunaan cipher 3DES yang rentan terhadap serangan SWEET32.

Berdasarkan hasil keseluruhan, *website* ini memperoleh skor keamanan sebesar 10 dengan tingkat risiko sangat tinggi (*very high risk level*).



Gambar 5. 72 Hasil Rekomendasi AI *Website*

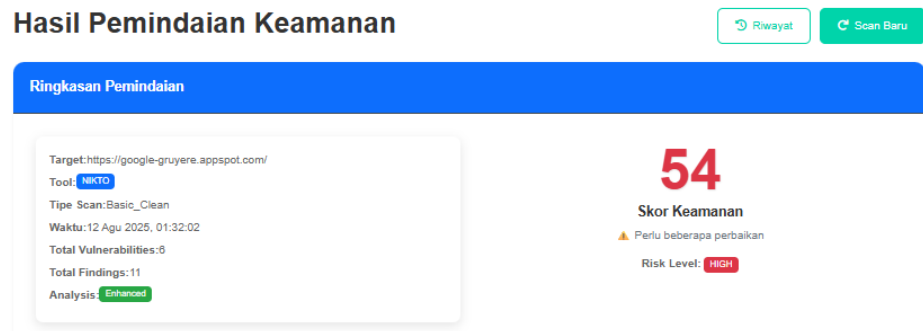
<https://Expired.Badssl.Com> Berdasarkan Hasil Pemindaian Nmap

Gambar 5. 72 menampilkan hasil rekomendasi perbaikan yang sesuai dengan temuan kerentanan pada *website* target <https://expired.badssl.com> . Untuk kerentanan terkait sertifikat SSL yang telah kedaluwarsa selama 3773 hari, rekomendasi yang diberikan meliputi pembaruan sertifikat SSL secara segera, koordinasi dengan tim TI dan penyedia sertifikat, serta verifikasi konfigurasi sertifikat setelah penerapan pada seluruh sistem terkait. Mengenai kerentanan HTTP yang terdeteksi melalui CVE-2011-3192, saran yang disampaikan adalah untuk mengidentifikasi sifat kerentanan secara tepat, menerapkan *patch* keamanan jika tersedia, melakukan pembaruan perangkat lunak jika diperlukan, dan melakukan pemindaian ulang guna memastikan kerentanan telah tertangani. Untuk isu penggunaan cipher 3DES yang rentan terhadap serangan SWEET32, dianjurkan penerapan enkripsi HTTPS dengan konfigurasi *cipher suite*

yang kuat dan mutakhir, seperti penggunaan TLS 1.2 ke atas serta menonaktifkan *cipher* yang lemah, termasuk 3DES, guna memastikan komunikasi yang aman.

5.2.3.3 Website <https://google-gruyere.appspot.com/>

a. Menggunakan Tools Nikto



Gambar 5. 73 Skor Keamanan Website <https://google-gruyere.appspot.com/> Berdasarkan Hasil Pemindaian Nikto

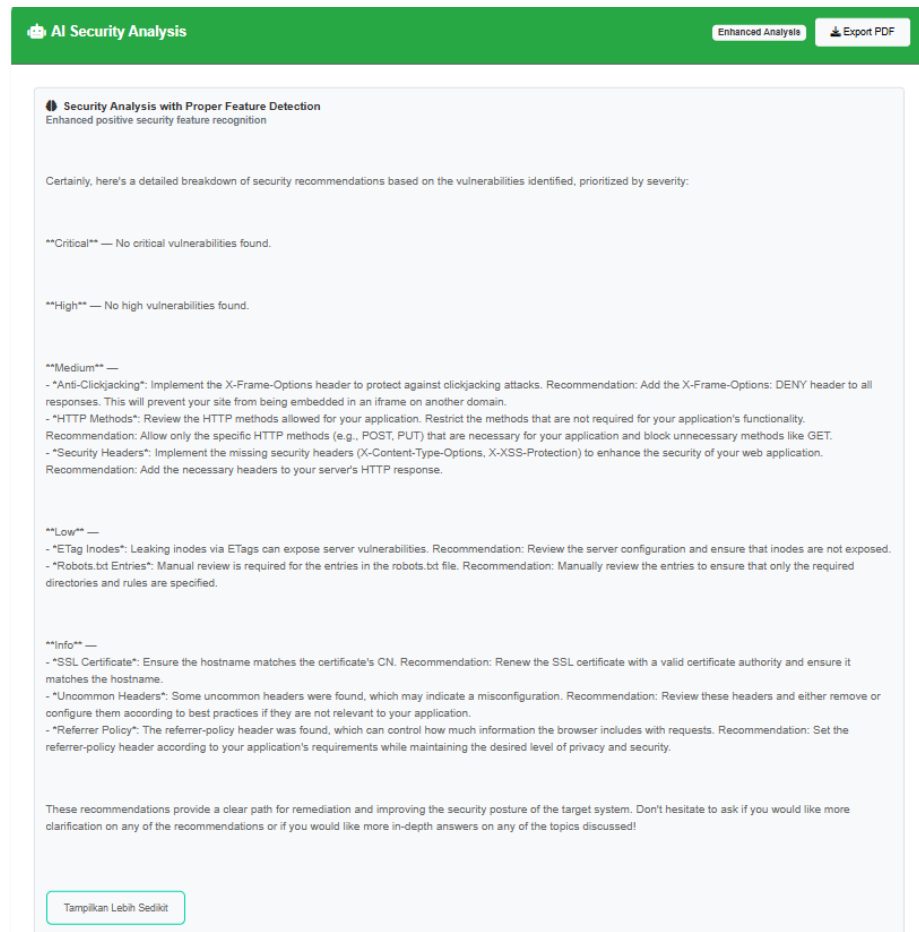
The screenshot shows the 'Analisis Keamanan Detail' (Detailed Security Analysis) page from Nikto. It provides a breakdown of the scan results by severity level: 0 Critical, 0 High, 4 Medium, 2 Low, and 5 Info. Below this, a table lists the detected security vulnerabilities.

Severity	Type	Description	Location	Status
MEDIUM	Infrastructure Finding	The anti-clickjacking X-Frame-Options header is not present.	/	Detected
MEDIUM	Infrastructure Finding	Uncommon header 'x-cloud-trace-context' found, with contents: 97acb333ac09fb83defb02a33642f34d	/	Detected
MEDIUM	Infrastructure Finding	Allowed HTTP Methods: GET	/	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected
LOW	Infrastructure Finding	Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x3m8CBg	/robots.txt	Detected
LOW	Infrastructure Finding	"robots.txt" contains 12 entries which should be manually viewed.	/	Detected

Gambar 5. 74 Hasil Temuan Kerentanan Website <https://google-gruyere.appspot.com/> Berdasarkan Hasil Pemindaian Nikto

Gambar 5. 73 dan Gambar 5 .74 menampilkan hasil pengujian terhadap website target <https://google-gruyere.appspot.com/> menggunakan tools Nikto. Pengujian ini menghasilkan enam temuan kerentanan dengan variasi kategori dan tingkat kerentanan. Terdapat empat temuan dengan kategori *medium*, yaitu ketiadaan *header anti-clickjacking X-Frame-Options*, keberadaan *header* tidak umum 'x-cloud-trace-context' dengan nilai tertentu, metode HTTP yang diizinkan hanya GET, serta ketiadaan

beberapa *header* keamanan penting seperti *X-Frame-Options*, *X-Content-Type-Options*, dan *X-XSS-Protection*. Selain itu, terdapat dua temuan dengan kategori low berupa kebocoran *inode* melalui *header* ETags pada file */robots.txt* dan adanya 12 entri dalam file "*robots.txt*" yang perlu ditinjau secara manual. Berdasarkan keseluruhan temuan, *website* ini memperoleh nilai keamanan (*security score*) sebesar 54 dengan tingkat risiko tinggi (*high risk level*).



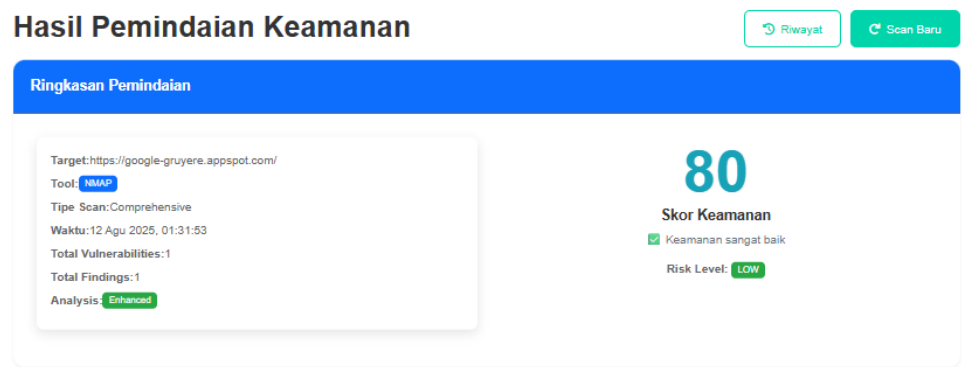
Gambar 5. 75 Hasil Rekomendasi AI *Website* <https://google-gruyere.appspot.com/> Berdasarkan Hasil Pemindaian Nikto

Gambar 5. 75 menunjukkan hasil validasi rekomendasi AI terhadap temuan kerentanan pada *website* target <https://google-gruyere.appspot.com/>. Untuk kerentanan kategori *medium*, seperti ketiadaan *header anti-clickjacking X-Frame-Options*, disarankan penambahan *header X-Frame-Options: DENY* pada seluruh respons HTTP guna mencegah serangan *clickjacking*. Selain itu, metode HTTP

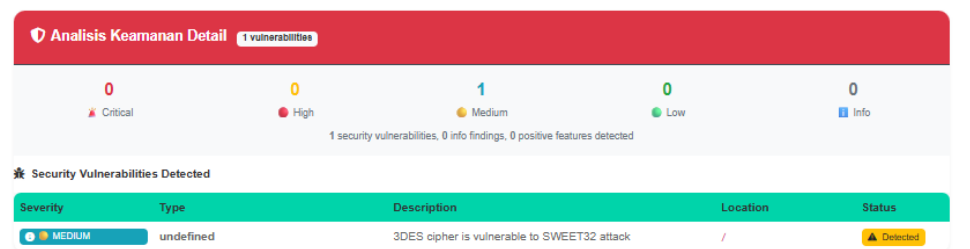
yang diizinkan (misalnya GET) perlu dibatasi hanya pada metode yang relevan dengan fungsi aplikasi, serta memblokir metode yang tidak diperlukan. Implementasi *header* keamanan tambahan seperti *X-Content-Type-Options* dan *X-XSS-Protection* juga direkomendasikan untuk memperkuat perlindungan aplikasi web.

Untuk temuan kategori rendah, seperti kebocoran *inode* melalui ETags, perlu dilakukan peninjauan konfigurasi server agar informasi *inodes* tidak terekspos. *Entry* pada file robots.txt juga harus ditinjau secara manual untuk memastikan hanya direktori dan aturan yang diperlukan yang dicantumkan. Dan temuan tambahan terkait *header* tidak umum dan kebijakan *referrer* disarankan untuk dikaji dan disesuaikan dengan praktik terbaik demi menjaga privasi dan keamanan aplikasi.

b. Menggunakan *Tools* Nmap



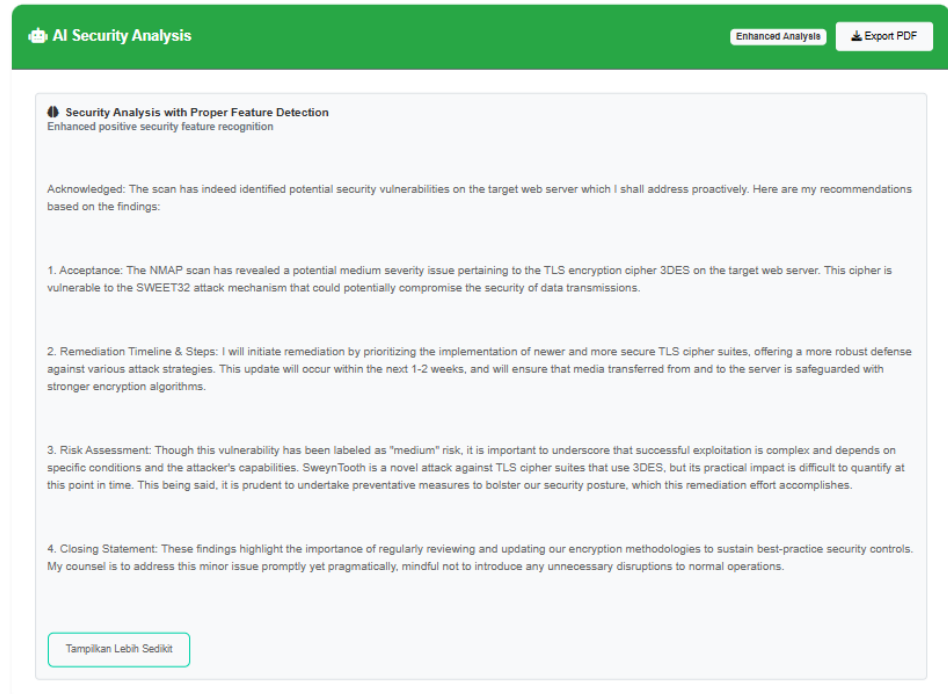
Gambar 5. 76 Skor Keamanan *Website* <https://google-gruyere.appspot.com/> Berdasarkan Hasil Pemindaian Nmap



Gambar 5. 77 Hasil Temuan Kerentanan *Website* <https://google-gruyere.appspot.com/> Berdasarkan Hasil Pemindaian Nmap

Gambar 5. 76 dan Gambar 5. 77 menampilkan hasil pengujian terhadap *website* target <https://google-gruyere.appspot.com/> menggunakan *tools* Nmap. Pengujian ini mengidentifikasi satu temuan kerentanan dengan

kategori *medium*, yaitu penggunaan *cipher* 3DES yang rentan terhadap serangan SWEET32. Berdasarkan hasil keseluruhan, *website* ini memperoleh skor keamanan sebesar 80 dengan tingkat risiko rendah (*low risk level*).



Gambar 5. 78 Hasil Rekomendasi AI *Website* <https://google-gruyere.appspot.com/> Berdasarkan Hasil Pemindaian Nmap

Gambar 5. 78 menampilkan hasil validasi rekomendasi AI yang sesuai dengan temuan kerentanan pada *website* target <https://google-gruyere.appspot.com/>. Temuan kategori *medium* tentang penggunaan *cipher* 3DES yang rentan terhadap serangan SWEET32 merupakan masalah keamanan yang perlu ditangani. Rekomendasi yang diberikan menekankan penerapan *cipher* TLS yang lebih baru dan kuat sebagai langkah mitigasi, dengan rencana perbaikan dalam jangka waktu 1-2 minggu guna memastikan data yang ditransfer ke dan dari server terlindungi dengan algoritma enkripsi yang lebih aman.

5.2.3.4 Hasil Analisis Pengujian Komparasi Nikto dan Nmap

Tabel 5. 8 Rekapitulasi Hasil Pengujian Komparasi Nikto dan Nmap

<i>Website</i>	<i>Security Score</i>				Validasi Rekomendasi AI
	Nikto	<i>Risk Level</i>	Nmap	<i>Risk Level</i>	
https://sman1pyk.sch.id/	60	<i>Moderate</i>	100	<i>Very Low</i>	Sesuai dengan temuan
https://expired.badssl.com	77	<i>Moderate</i>	10	<i>Very High</i>	Sesuai dengan temuan
https://google-gruyere.appspot.com/	54	<i>High</i>	80	<i>Low</i>	Sesuai dengan temuan

Tabel 5.8 menunjukan hasil pengujian yang dilakukan terhadap tiga *website* menggunakan dua *tools* berbeda, yaitu *Nmap* dan *Nikto*, ditemukan bahwa pengujian yang dilakukan pada target yang sama, skor keamanan (*security score*) dan tingkat risiko (*risk level*) yang dihasilkan menunjukkan perbedaan yang cukup signifikan. Misalnya, pada *website* <https://expired.badssl.com>, *Nikto* memberikan skor 77 dengan tingkat risiko *Moderate*, sedangkan *Nmap* memberikan skor 10 dengan tingkat risiko *Very High*. Perbedaan ini juga terlihat pada *website* lainnya, di mana skor dan tingkat risiko yang diberikan oleh masing-masing *tools* berbeda.

Perbedaan ini secara teknis dapat dijelaskan melalui karakteristik dan fokus utama dari kedua *tools* tersebut. *Nmap* berfungsi sebagai *network scanner* yang berfokus pada pemetaan *port*, layanan, dan konfigurasi jaringan. Temuan *Nmap* berfokus pada kerentanan yang terkait dengan *network exposure*, konfigurasi *port*, dan protokol yang digunakan. Sementara itu, *Nikto* adalah *web vulnerability scanner* yang secara spesifik menilai kerentanan pada sisi aplikasi *website*, seperti konfigurasi *server HTTP*, file berbahaya, potensi injeksi, dan masalah keamanan pada halaman *web*. Perbedaan ruang lingkup inilah yang menyebabkan hasil pengujian terhadap target yang sama dapat berbeda secara signifikan baik dari sisi skor maupun tingkat risiko.

Berdasarkan analisis lebih lanjut, hasil temuan kerentanan kemudian dikategorikan sesuai dengan tingkat keparahan berdasarkan *CVSS (Common Vulnerability Scoring System)* yang membagi kerentanan menjadi empat

kategori, yaitu *Critical*, *High*, *Low*, dan *Info*. Penilaian skor keamanan pada tabel ini dihitung menggunakan metode *OWASP Risk Rating Methodology*, yaitu dengan mempertimbangkan seberapa besar peluang celah keamanan tersebut dapat dimanfaatkan dan seberapa besar dampaknya jika terjadi serangan. Perbedaan fokus deteksi kedua *tools* membuat hasil skornya berbeda meskipun diuji pada target yang sama.

Dari ketiga pengujian yang telah dilakukan, rekomendasi perbaikan yang dihasilkan oleh AI terbukti sesuai dan relevan dengan kerentanan yang ditemukan oleh kedua tools. Pada <https://sman1pyk.sch.id>, rekomendasi AI menanggapi temuan seperti ketiadaan *security header* dan pengalihan yang tidak optimal dengan saran implementasi konfigurasi yang tepat, pembaruan *server*, serta praktik keamanan proaktif. Pada <https://expired.badssl.com>, AI secara akurat memberikan langkah mitigasi untuk *SSL certificate* yang kedaluwarsa, kerentanan *HTTP*, dan penggunaan *cipher* lemah, termasuk pembaruan *certificate*, penerapan *security patch*, dan penguatan konfigurasi enkripsi. Sementara itu, pada <https://google-gruyere.appspot.com/>, AI menyesuaikan rekomendasi dengan kelemahan seperti *security header* yang hilang, konfigurasi metode *HTTP* yang berlebihan, kebocoran *inode* melalui *ETags*, serta masalah pada *robots.txt* dan kebijakan *referrer*, dengan memberikan langkah teknis yang tepat untuk mitigasi. Keseluruhan hasil ini menunjukkan bahwa rekomendasi tersebut sesuai dengan temuan yang telah diidentifikasi pada masing-masing *website*.

5.2.4 Pengujian Reliability Menggunakan ApacheJmeter

Pengujian menggunakan apache JMeter pada Platform Pengujian Keamanan Server Berbasis *Website* bertujuan untuk melihat performa platform ini dalam menjalankan tugasnya. Pengujian ini dilakukan sebanyak 6 kali dengan jumlah *request* user yang berbeda beda. Terdapat beberapa hal yang diuji pada pengujian menggunakan apache JMeter ini diantaranya :

- *Stability* = Kemampuan sistem untuk tetap berjalan/online tanpa crash, hang, atau shutdown
- *Reliability* = Kemampuan sistem untuk memberikan hasil yang benar/sukses secara konsisten

- *Scalability* = Kemampuan sistem untuk handle beban yang meningkat dengan menambah kapasitas secara proporsional
- *Performance* = Kecepatan sistem dalam memproses dan merespons

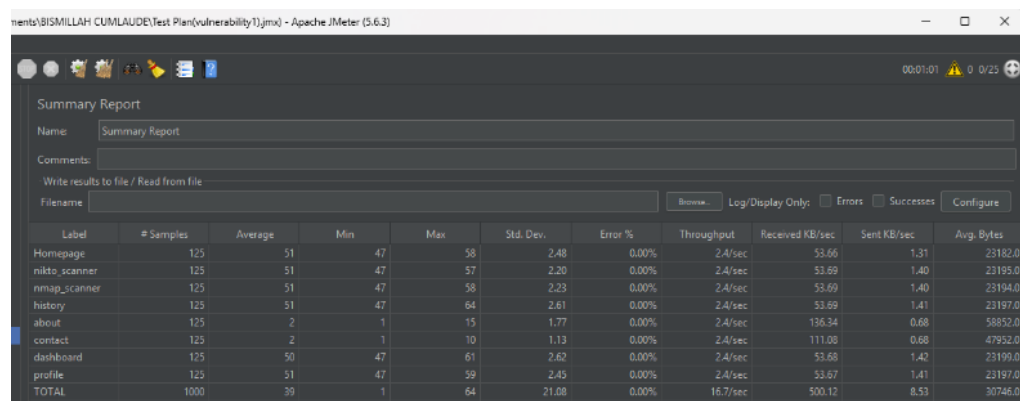
Tabel 5.9 merupakan pengujian menggunakan apache Jmeter yang dilakukan sebanyak 6 kali pengujian dengan data skenario seperti pada tabel.

Tabel 5.9 Rekap Hasil Pengujian Performa Website

Pengujian	Jumlah User	Waktu	Loops
1	25 users	10 detik	5 loops
2	50 users	30 detik	5 loops
3	100 user	60 detik	5 loops
4	200 users	120 detik	5 loops
5	800 users	60 detik	5 loops
6	1200 users	60 detik	5 loops

a. Pengujian 1

pengujian 1 menggunakan 25 *user*, 10 detik dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis *Website* ini.



Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Homepage	125	51	47	58	2.48	0.00%	2.4/sec	53.66	1.31	23182.0
nikto_scanner	125	51	47	57	2.20	0.00%	2.4/sec	53.69	1.40	23195.0
nmap_scanner	125	51	47	58	2.23	0.00%	2.4/sec	53.69	1.40	23194.0
history	125	51	47	64	2.61	0.00%	2.4/sec	53.69	1.41	23197.0
about	125	2	1	15	1.77	0.00%	2.4/sec	136.34	0.68	58852.0
contact	125	2	1	10	1.13	0.00%	2.4/sec	111.08	0.68	47952.0
dashboard	125	50	47	61	2.62	0.00%	2.4/sec	53.68	1.42	23199.0
profile	125	51	47	59	2.45	0.00%	2.4/sec	53.67	1.41	23197.0
TOTAL	1000	39	1	64	21.08	0.00%	16.7/sec	500.12	8.53	30746.0

Gambar 5. 79 Pengujian 1

Gambar 5. 79 merupakan hasil pengujian berupa Total *request* sebanyak 1.000 *Request*, Total error rate sebesar 0.00%, Average Respon Time selama 39 ms dan Throughput sebanyak 16.7 *request*/detik.

b. Pengujian 2

Pengujian 2 menggunakan 50 *user*, 30 detik dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis *Website* ini. Berdasarkan pengujian tersebut didapatkan hasil pengujian berupa Total *request*

sebanyak 2.000 *Request*, Total error rate sebesar 0.00%, Average Respon Time selama 40 ms dan Throughput sebanyak 28.4 *request*/detik.

c. Pengujian 3

Pengujian 3 menggunakan 100 *user*, 60 detik dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis *Website* ini. Berdasarkan pengujian tersebut didapatkan hasil pengujian berupa Total *request* sebanyak 4.000 *Request*, Total error rate sebesar 0.00%, Average Respon Time selama 40 ms dan Throughput sebanyak 39.9 *request*/detik.

d. Pengujian 4

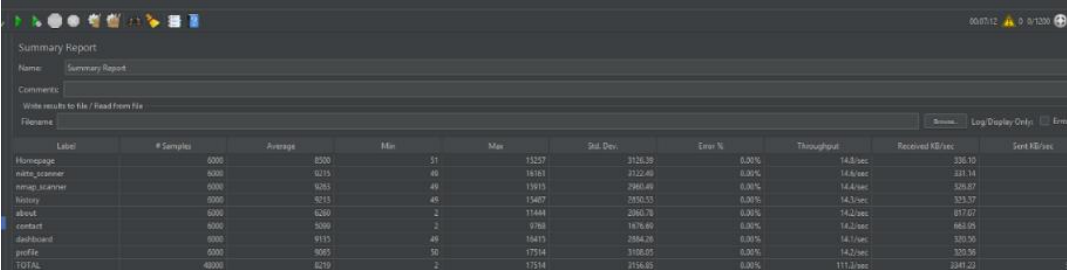
Pengujian 4 menggunakan 200 *user*, 120 detik dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis *Website* ini. Berdasarkan pengujian tersebut didapatkan hasil pengujian berupa Total *request* sebanyak 8.000 *Request*, Total error rate sebesar 0.00%, Average Respon Time selama 42 ms dan Throughput sebanyak 49.9 *request*/detik.

e. Pengujian 5

Pengujian 5 menggunakan 800 *user*, 60 detik dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis *Website* ini. Berdasarkan pengujian tersebut didapatkan hasil pengujian berupa Total *request* sebanyak 32.000 *Request*, Total error rate sebesar 0.00%, Average Respon Time selama 4539 ms dan Throughput sebanyak 114.2 *request*/detik.

f. Pengujian 6

Pengujian 6 menggunakan 1200 *user*, 60 detik dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis *Website* ini.



Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec
Homepage	6000	6000	51	11257	3126.39	0.00%	14.8/sec	328.10	328.10
static_resource	6000	6175	48	14163	3122.46	0.00%	14.8/sec	333.14	333.14
image_resource	6000	6263	49	13915	2960.49	0.00%	14.4/sec	328.87	328.87
history	6000	9113	48	15487	2852.53	0.00%	14.3/sec	323.57	323.57
about	6000	6200	2	11444	2060.79	0.00%	14.2/sec	317.67	317.67
contact	6000	6099	2	13768	1616.89	0.00%	14.2/sec	363.05	363.05
dashboard	6000	6112	48	16613	2654.28	0.00%	14.5/sec	310.56	310.56
profile	6000	6097	50	17714	3108.05	0.00%	14.2/sec	322.95	322.95
TOTAL	40000	6219	2	17534	3116.85	0.00%	111.3/sec	2347.23	2347.23

Gambar 5.80 Pengujian 6

Gambar 5.80 merupakan hasil pengujian berupa Total *request* sebanyak 48.000 *Request*, Total *error rate* sebesar 0.00%, *Average Respon Time* selama 8219 ms dan *Throughput* sebanyak 111.3 *request/detik*.

Berdasarkan 6 pengujian menggunakan apache JMeter di atas, didapatkan data hasil analisis sebagai berikut :

Tabel 5.10 Rekap Hasil Pengujian Menggunakan Apache JMeter

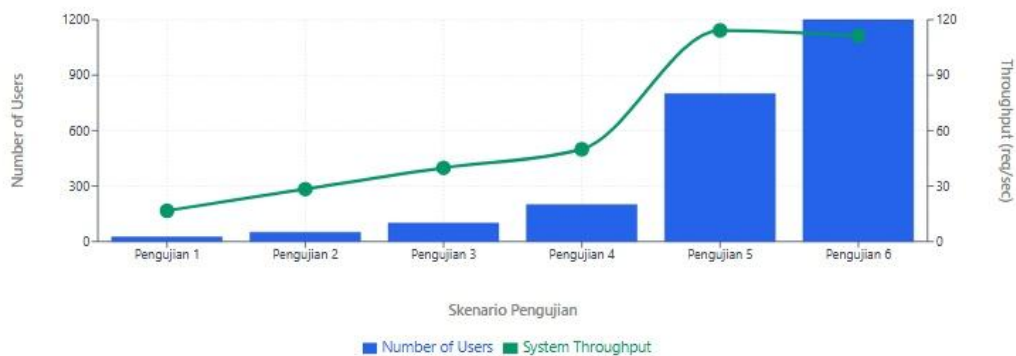
Pengujian	Hasil Pengujian			
	Total Request	Total Error Rate	Average Respon Time	Throughput
1	1.000 Request	0.00%	39 ms	16.7 request/detik
2	2.000 Request	0.00%	40 ms	28.4 request/detik.
3	4.000 Request	0.00%	40 ms	39.9 request/detik
4	8.000 Request	0.00%	42 ms	49.9 request/detik
5	32.000 Request	0.00%	4539 ms	114.2 request/detik
6	48.000 Request	0.00%	8219 ms	111.3 request/detik

Tabel 5.11 Hasil Analisis pengujian menggunakan Apache JMeter

STABILITY	SCALABILITY	RELIABILITY	PERFORMANCE
Stabil (no crashes)	Good (linear throughput)	Perfect (0% error)	Slow response ketika diberi <i>request</i> yang sangat tinggi di 32.000 – 48.000



Gambar 5. 81 Grafik *Average Response Time*



Gambar 5.82 Grafik *System Throughput*

Tabel 5.10, Tabel 5.11, Gambar 5.81, dan Gambar 5.82 menunjukkan bahwa *Platform* Pengujian Keamanan Server Berbasis *Website* ini reliability yang baik karena ketika diuji dengan berbagai input berdasarkan data di atas, *Website* mampu merespons semua permintaan dengan sukses, ditunjukkan oleh tingkat error 0% dan tidak adanya crash, sehingga *Website* berjalan stabil. Selain itu, ketika jumlah *request* ditingkatkan, nilai throughput juga ikut meningkat, yang menandakan kemampuan scalability *Website* cukup bagus. Namun, terdapat sedikit penurunan throughput ketika diberikan 120 *request* dalam 60 detik. Namun, Saat jumlah *request* yang diterima sangat besar, performa *Website* mengalami penurunan yaitu respon menjadi lebih lambat.

5.2.5 Pengujian Backend

Pengujian performa Backend pada *platform* Pengujian Keamanan server Berbasis Website ini dilakukan dengan tujuan memastikan bahwa Backend dari *platform* yang telah dirancang dapat diakses dengan baik sehingga mampu menampung pengguna yang mengakses website ini dengan jumlah banyak secara bersamaan, dan pengujian ini juga dilakukan untuk menganalisa batas kemampuan website ketika di akses pengguna yang banyak. Dalam proses ini menggunakan ApacheJMeter sebagai alat uji peforma (*load testing*) untuk melakukan simulasi aktivitas pengguna yang mengakases website pada waktu yang bersamaan.

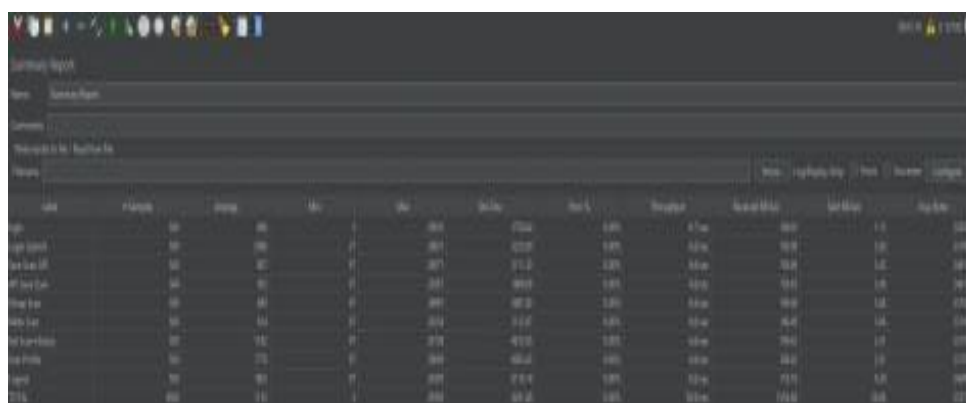
Skenario pengujian dimulai dengan melakukan konfigurasi ApacheJMeter, yaitu menentukan jumlah pengguna yang mengakses website per-30 detik, konfigurasi seperti ini bertujuan untuk melihat bagaimana performa Backend website pada banyak pengguna yang di konfigurasi per-30 detik dan nantinya jumlah pengguna akan ditambah secara terus menerus sampai menemukan titik batas kemampuan Backend website (*breaking point*).

5.2.5.1 Hasil Pengujian *Load Testing*

Pada hasil pengujian performa *backend (load testing)* ini, pengujian dilakukan menggunakan *software* ApacheJMeter. Pengujian dilakukan sebanyak 5 kali dengan level yang berbeda.

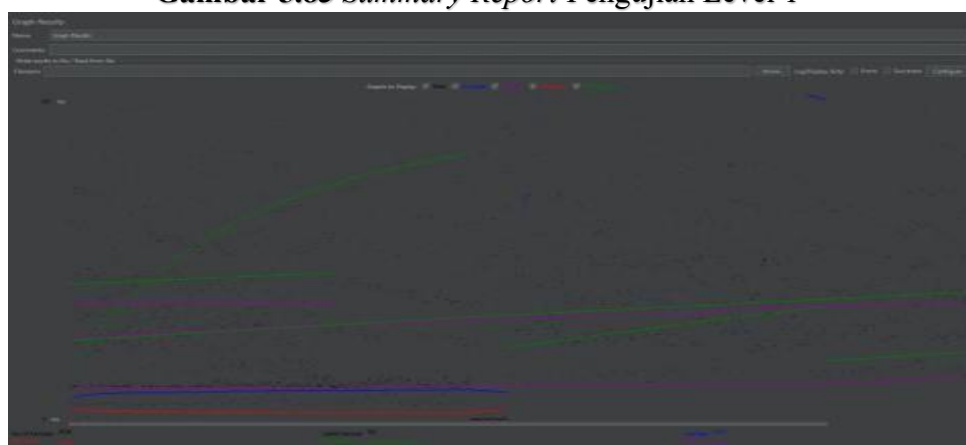
1. Pengujian 1

pengujian 1 ini menggunakan 100 pengguna dalam waktu 30 detik dan 5 kali pengulangan untuk melihat performa backend pada platform pengujian keamanan server berbasis website ini.



Test Element	Sample	Success	Fail	Latency	Min	Max	Avg	StdDev	Min	Max	Avg	StdDev	Min	Max	Avg	StdDev
Test	100	100	0	100	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00
Test 1	100	100	0	100	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00
Test 2	100	100	0	100	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00
Test 3	100	100	0	100	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00
Test 4	100	100	0	100	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00
Test 5	100	100	0	100	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00
Total	500	500	0	500	0.00	100.00	100.00	0.00	0.00	0.00	100.00	0.00	0.00	0.00	100.00	0.00

Gambar 5.83 *Summary Report* Pengujian Level 1



Gambar 5.84 *Graph Result* Pengujian Level 1

2. Pengujian 2

pengujian 2 menggunakan 250 pengguna dalam waktu 30 detik dan 5 kali pengulangan untuk melihat performa backend pada platform pengujian keamanan server berbasis website ini.

3. Pengujian 3

pengujian 3 menggunakan 500 pengguna dalam waktu 30 detik dan 5 kali pengulangan untuk melihat performa backend pada *platform* pengujian keamanan server berbasis website ini.

4. Pengujian 4

pengujian 4 menggunakan 1000 pengguna dalam waktu 30 detik dan 5 kali pengulangan untuk melihat performa backend pada *platform* pengujian keamanan server berbasis website ini.

5. Pengujian 5

pengujian 5 menggunakan 2000 pengguna dalam waktu 30 detik dan 5 kali pengulangan untuk melihat performa *backend* pada platform pengujian keamanan *server* berbasis website ini.

Berdasarkan 5 pengujian di atas didapatkan hasil seperti pada tabel berikut :

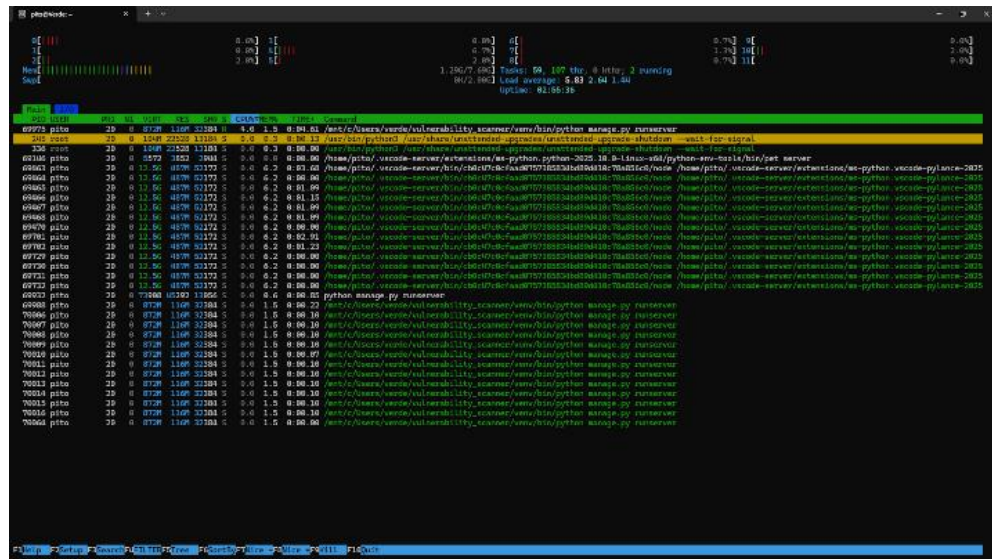
Tabel 5.12 data pengujian *load testing* sistem *backend*

Skenario	Users	Response Time (ms)	Throughput (req/s)	ErrorRate
Pengujian 1	100	1152	58.9	0.00%
Pengujian 2	250	934	154.1	0.00%
Pengujian 3	500	2561	153.3	0.00%
Pengujian 4	1000	6449	140.2	0.00%
Pengujian 5	2000	12716	147.4	13.42%

Tabel 5.12 merupakan hasil pengujian ApacheJMeter, performa backend pada *platform* pengujian keamanan server berbasis website yang sangat baik dan stabil hingga 1000 *concurrent users* dengan *response time* berkisar 696-7022 ms dan *error rate* 0.00%, menandakan sistem dapat menangani beban kerja normal hingga *stress test* tanpa kegagalan. *Throughput* konsisten pada level 140- 154 req/s untuk beban medium hingga *stress test*, menunjukkan sistem memiliki kapasitas optimal sekitar 1000 *users concurrent*. Namun, pada *Extreme Load* (2000 users), terjadi degradasi signifikan dengan *response time* melonjak drastis ke 9184-14,716 ms dan *error rate* mencapai 8.8-19.3%, mengindikasikan *breaking point* sistem berada di sekitar 1500-2000 *users concurrent*. Kesimpulannya, website dapat beroperasi dengan sangat baik untuk penggunaan normal

hingga 1000 *users*, namun memerlukan optimasi infrastruktur atau *load balancing* untuk menangani *traffic* ekstrem di atas 1500 *users concurrent*.

5.2.5.2 Monitoring Penggunaan CPU dan Memori pada Backend



Gambar 5.85 Monitoring Penggunaan CPU dan Memori

Gambar 5.85 merupakan monitoring penggunaan CPU dan memori pada sistem backend ini menggunakan *tools* HTOP pada *command prompt*, untuk mendapatkan hasil yang maksimal, penulis menggunakan metode pengambilan data dengan cara mengamati data HTOP selama 5 menit dan mencatat data sebanyak 5 kali termasuk data penggunaan CPU dan memori minimum sampai data penggunaan CPU dan memori maksimum. Untuk *monitoring* ini dilakukan di 3 kondisi yang berbeda yaitu: website dalam keadaan normal (tidak ada proses yang berjalan), website dalam keadaan proses *scanning* dengan *tools* nikto dan terakhir website dalam keadaan proses *scanning tools* nmap.

Tabel 5.13 Data Penggunaan CPU

Kondisi	CPU Min	CPU Max	CPU AVG
Normal	4.0%	12.0%	7.44%
Scan Nikto	7.3%	11.4%	9.22%
Scan Nmap	6.7%	12.0%	9.84%

Tabel 5.14 Data Penggunaan Memori

Kondisi	Memori Min	Memori	Memori
		Max	AVG
Normal	1.5%	1.5%	1.50%
Scan Nikto	1.6%	1.7%	1.62%
Scan Nmap	1.7%	1.8%	1.76%

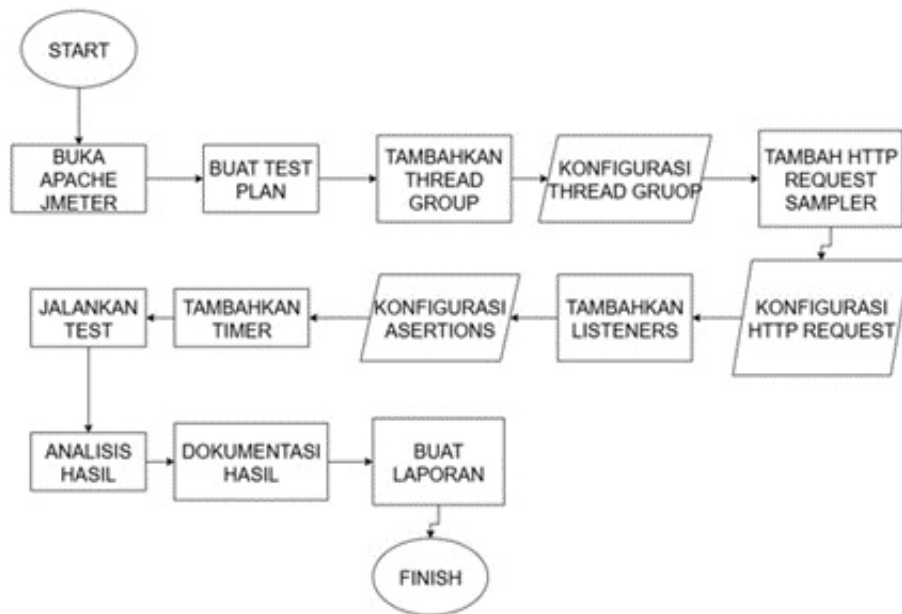
Tabel 5.13 dan Tabel 5.14 merupakan monitoring penggunaan CPU dan memori. Maka, dapat disimpulkan bahwa tentunya penggunaan CPU dan memori paling rendah berada pada kondisi website dalam keadaan normal karena website tidak sedang dalam proses apapun, tetapi jika dibandingkan dalam kondisi proses *scanning*, *scan nmap* lebih banyak menggunakan CPU dan memori dibandingkan *scan nikto*. Penggunaan CPU dan memori *scan nmap* sedikit lebih tinggi karena *nmap* melakukan pekerjaan yang lebih kompleks di level jaringan yang lebih rendah, sementara *nikto* fokus pada level aplikasi yang lebih sederhana dan efisien.

5.2.6 Pengujian Frontend

Pengujian antarmuka *website* dilakukan dengan tujuan memastikan bahwa *platform* pengujian keamanan server yang telah dikembangkan dapat diakses dengan baik dan mampu menangani sejumlah permintaan secara bersamaan. Dalam proses ini, digunakan ApacheJMeter sebagai alat uji performa (*load testing*) untuk melakukan simulasi aktivitas pengguna yang mengakses *website* pada waktu yang bersamaan. Berikut merupakan skenario pengujian dan *flowchart* pengujian yang tertera pada Tabel 5.14 dan Gambar 5.68 *Flowchart* alur pengujian *Frontend*.

Tabel 5. 15 Skenario Pengujian *Interface*

Pengujian	Jumlah User	Waktu	Loops
1	100 users	30 detik	5 loops
2	250 users	30 detik	5 loops
3	500 users	30 detik	5 loops
4	1000 users	30 detik	5 loops
5	2000 users	30 detik	5 loops



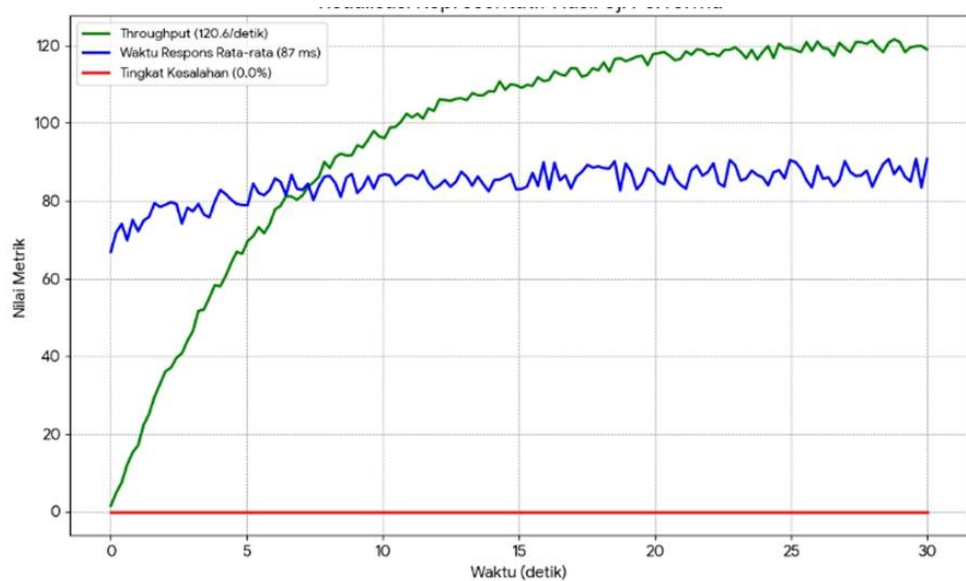
Gambar 5.86 Flowchart Alur Pengujian Frontend

1. Pengujian 1

pengujian 1 menggunakan 100 user, 30 second dan 5 loops untuk melihat performa platform pengujian keamanan server berbasis website ini. Gambar 5.87 dan Gambar 5.88 menunjukkan bahwa dari pengujian ini didapatkan hasil *average respon time* selama 87 ms, *throughput* sebesar 120.6/sec, *error rate* sebesar 0.00%.

Summary Report													
Name:	Summary Report												
Comments:													
Write results to file / Read from file:													
Filename:													
Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes			
Tampilan NMAP	500	92	51	108	17.05	0.00%	15.5/sec	347.58	5.88	23194.0			
Tampilan NBT	500	101	84	121	3.49	0.00%	15.5/sec	347.58	6.39	23192.0			
Tampilan HISTORY	500	101	95	127	5.86	0.00%	15.5/sec	347.11	6.25	23197.0			
Tampilan ABOUT	500	49	47	57	2.23	0.00%	15.5/sec	891.94	2.98	58852.0			
Tampilan CONTACT US	500	49	11	57	2.84	0.00%	15.5/sec	716.80	2.87	47862.0			
Tampilan DATA BOARD	500	101	93	127	5.20	0.00%	15.5/sec	347.14	6.15	23193.0			
Tampilan PROFILE	500	101	84	127	5.88	0.00%	15.5/sec	347.11	6.25	23197.0			
Tampilan HOME	500	101	83	108	5.84	0.00%	15.5/sec	346.89	5.91	23182.0			
TOTAL	4000	87	11	131	23.48	0.00%	120.6/sec	3621.01	41.88	36786.0			

Gambar 5.87 Hasil Pengujian 1



Gambar 5.88 Grafik Hasil Pengujian 1

2. Pengujian 2

Pada pengujian 2 menggunakan 250 *user*, 30 *second* dan 5 *loops* untuk melihat performa *platform* pengujian keamanan server berbasis website ini. Dari pengujian tersebut didapatkan hasil *average respon time* selama 564 ms, *throughput* sebesar 187.6/sec, *error rate* sebesar 0.00%.

3. Pengujian 3

Pada pengujian 3 ini menggunakan 500 *user*, 30 *second* dan 5 *loops* untuk melihat performa *platform* pengujian keamanan server berbasis website ini. Dari pengujian tersebut didapatkan hasil *average respon time* selama 2113 ms, *throughput* sebesar 171.5/sec, *error rate* sebesar 0.00%.

4. Pengujian 4

Pada pengujian 4 ini menggunakan 1000 *user*, 30 *second* dan 5 *loops* untuk melihat performa *platform* pengujian keamanan server berbasis website ini. Dari pengujian tersebut didapatkan hasil *average respon time* selama 5584 ms, *throughput* sebesar 156.3/sec, *error rate* sebesar 0.00%.

5. Pengujian 5

Pada pengujian 3 ini menggunakan 2000 *user*, 30 *second* dan 5 *loops* untuk melihat performa *platform* pengujian keamanan server berbasis website ini. Dari pengujian tersebut didapatkan hasil berupa *average respon time* selama 12644 ms, *throughput* sebesar 146.6/sec, *error rate* sebesar 3.51%.

Berdasarkan Hasil pengujian diatas, didapatkan data tabel rekap sebagai berikut:

Tabel 5.16 Rekapitulasi Data Hasil Pengujian Frontend

<i>users</i>	<i>Avg Response Time</i>	<i>Throughput</i>	<i>Errorrate</i>	<i>status</i>
100	87 ms	120.6/sec	0.00%	sempurna
250	564 ms	187.6/sec	0.00%	bagus
500	2113 ms	171.5/sec	0.00%	layak
1000	5584 ms	156.3/sec	0.00%	Sangat lambat
2000	12644 ms	146.6/sec	3.51%	tidak layak

Tabel 5.15 Rekapitulasi Data Hasil Pengujian Frontend menunjukkan bahwa hasil pengujian performa menunjukkan bahwa waktu respons aplikasi sangat optimal pada 100 pengguna dengan rata-rata 87 milidetik, tetap berada dalam batas wajar pada 250 pengguna dengan 564 milidetik, dan mulai melambat menjadi 2,1 detik pada 500 pengguna. Pada 1000 pengguna, respons mencapai 5,6 detik, sedangkan pada 2000 pengguna menjadi sangat lambat yaitu 12,6 detik, sehingga tidak layak digunakan dalam kondisi produksi. Dari sisi *throughput*, nilai tertinggi tercatat sebesar 187,6 permintaan per detik pada 250 pengguna, kemudian mengalami penurunan seiring bertambahnya jumlah pengguna, dengan tingkat efisiensi terbaik ditemukan pada rentang 250 hingga 500 pengguna. Analisis tingkat kesalahan menunjukkan tidak terdapat *error* hingga pengujian 1000 pengguna, yang menandakan stabilitas aplikasi masih sangat baik, sedangkan pada 2000 pengguna muncul *error rate* sebesar 3,51% akibat beban yang melebihi kapasitas sistem.

Tabel 5. 17 Rekapitulasi Performa Setiap *Endpoint*

<i>endpoint</i>	<i>avg response</i>	<i>error rate</i>	<i>severity</i>
NMAP	14162ms	3.06%	<i>critical</i>
NIKTO	14079ms	3.65%	<i>critical</i>
HISTORY	13914ms	3.36%	<i>critical</i>
HOME	13818ms	4.44%	<i>critical</i>
DASHBOARD	14045ms	4.25%	<i>critical</i>
PROFILE	13818ms	5.16%	<i>critical</i>
ABOUT	9901ms	2.31%	<i>warning</i>
CONTACT	8414ms	1.83%	<i>warning</i>

Tabel 5.16 menunjukkan hasil analisis performa setiap *endpoint* pada *platform* pengujian keamanan server saat diuji dengan beban 2000 pengguna secara bersamaan. Pengujian difokuskan untuk mengidentifikasi *bottleneck* yang memengaruhi kecepatan respon dan stabilitas sistem. Hasil menunjukkan *endpoint* PROFILE dan HOME menjadi yang paling bermasalah dengan *error rate* di atas 5%, sedangkan ABOUT dan CONTACT paling stabil karena menampilkan konten statis. Halaman pemindaian NMAP dan NIKTO mengalami *latency* tinggi. Secara keseluruhan, aplikasi berjalan stabil tanpa *error* hingga 1000 pengguna dan menunjukkan performa sangat baik pada beban normal 100–250 pengguna.

5.2.7 Pengujian Docker

Pengujian ini dilakukan menggunakan Docker *Dekstop*. Pengujian dilakukan dengan tujuan memastikan bahwa setiap layanan *microservice* yang berjalan di dalam docker dapat bekerja dengan baik dan tidak menggunakan sumber daya server secara berlebihan. Dalam proses ini, Docker *Desktop* digunakan untuk memantau penggunaan CPU, memori, jaringan, dan aktivitas disk dari masing-masing *container* secara langsung. Skenario pengujian dimulai dengan menjalankan semua *container* menggunakan Docker *Dekstop*, sehingga seluruh layanan aktif bersamaan. Skenario pengujian dilakukan dengan menjalankan seluruh *container* secara manual melalui Docker *Desktop*, sehingga semua layanan aktif secara bersamaan. Pengujian dibagi menjadi dua kondisi, yaitu:

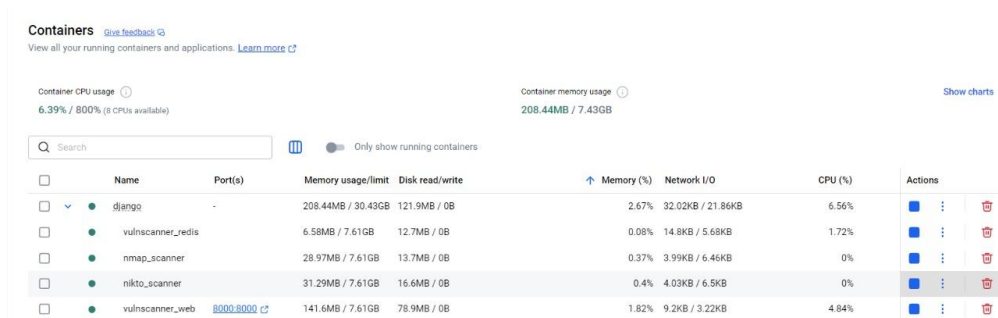
- Docker dalam keadaan aktif tanpa menjalankan proses pemindaian.
- Docker aktif dengan proses pemindaian berjalan.

Pemindaian dilakukan menggunakan tiga metode yaitu Nikto, Nmap, dan kombinasi keduanya secara bersamaan. Data yang dikumpulkan mencakup persentase penggunaan CPU, total penggunaan memori, lalu lintas data jaringan (data terkirim dan diterima), aktivitas baca dan tulis pada disk, serta jumlah proses yang berjalan pada masing-masing *container*.

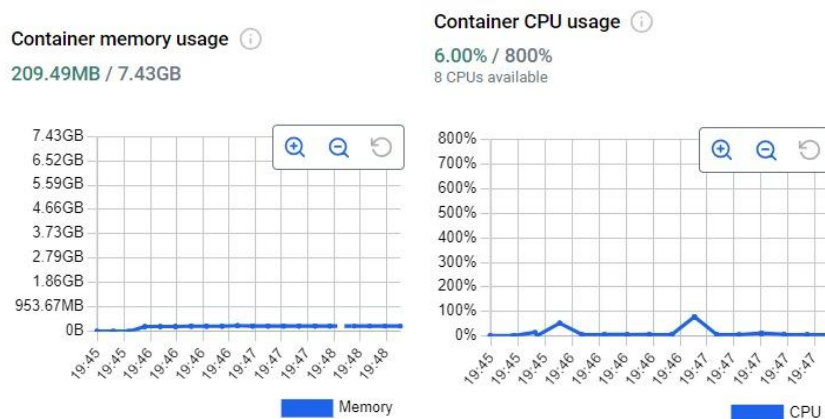
5.2.7.1 Hasil Pengujian Docker

a. Docker Aktif Tanpa Proses Pemindaian

Berikut merupakan hasil pengujian docker aktif tanpa proses pemindaian.



Gambar 5.89 Hasil Pengujian Tanpa Proses Pemindaian 1



Gambar 5.90 Grafik CPU dan Memory

Tabel 5.18 Hasil Pengujian Tanpa Proses Pemindaian 1

Container	CPU	Memory	Network		Disk	
			data sent	data received	data read	data write
vulscanner_web	0 % - 4.61 %	0 B – 114.4 MB	0 B – 3.22 KB	0 B – 9.15 KB	0 B	0 B
nikto_scanner	0%	0 B – 20.36 MB	0 B – 15.3 KB	0 B – 8.09 KB	0 B	0 B
nmap_scanner	0%	0 B – 16.64 MB	0 B – 21 KB	0 B – 10.1 KB	0 B	0 B
vulnscanner_redis	0 % - 2.01 %	0 B – 3.75 MB	0 B – 23.5 KB	0 B – 78.3 KB	0 B – 49.2 KB	0 B

Tabel 5.17 merupakan Hasil pengujian pada kondisi docker aktif tanpa proses pemindaian yang menunjukkan total penggunaan CPU sebesar 0% hingga 19,05% dan total penggunaan memory sebesar 0 B hingga 155,13 MB. Seluruh kontainer menunjukkan efisiensi penggunaan sumber daya dengan konsumsi CPU dan memory yang relatif rendah. Kontainer vulscanner_web memiliki penggunaan CPU tertinggi sebesar 4,61% dan memory sebesar 114,4 MB. Kontainer lainnya seperti nikto_scanner, nmap_scanner, dan

vulscanner_redis mencatat penggunaan CPU di bawah 2,1% dan memory di bawah 21 MB. Aktivitas network dan disk juga sangat minim. Seluruh kontainer mencatat penggunaan data sent tidak lebih dari 23,5 KB dan data received tidak melebihi 78,3 KB. Hanya kontainer vulscanner_redis yang mencatat aktivitas data read pada disk sebesar 49,2 KB, sementara kontainer lainnya tidak menunjukkan aktivitas read maupun write pada disk.

b. Docker Aktif dengan Proses Pemindaian

Pada bagian ini terdapat 3 jenis pemindaian, yaitu pemindaian menggunakan Nikto, pemindaian menggunakan Nmap dan pemindaian menggunakan Nikto dan Nmap secara bersamaan.

1. Nikto

Tabel 5.19 Hasil 1 (Pengujian Docker Aktif dengan Pemindaian Menggunakan Nikto)

Container	CPU	Memory	Network		Disk	
			data sent	data received	data read	data write
vulscanner_web	4.79 % - 63.76 %	122.6 MB – 130.7 MB	276 KB – 510 KB	161 KB – 596 KB	8.65 MB – 13.5 MB	0 B
nikto_scanner	43.61 % - 67.26 %	16.8 MB – 16.81 MB	39.6 KB – 70.4 KB	16.6 KB – 26.9 KB	0 B	0 B
nmap_scanner	0%	16.64 MB – 16.72 MB	39.3 KB – 70.1 KB	16.5 KB – 31 KB	0 B	0 B
vulscanner_redis	1.4 % - 13.01 %	3.48 MB – 3.73 MB	35 KB – 65.8 KB	106 KB – 196 KB	81.9 KB	4.1 KB

Tabel 5.18 Hasil pengujian pada kondisi docker aktif dengan proses pemindaian menggunakan Nikto menunjukkan total penggunaan CPU berada pada rentang 6,23% hingga 125,40%, dan total penggunaan memory sebesar 167,63 MB hingga 176,8 MB. Kontainer dengan penggunaan CPU tertinggi adalah nikto_scanner dengan nilai mencapai 67,26%, diikuti oleh vulscanner_web sebesar 63,76%. Sementara itu, kontainer nmap_scanner tidak mencatat aktivitas CPU, dan vulscanner_redis menggunakan CPU hingga 13,01%. Dari sisi *memory*, kontainer vulscanner_web menunjukkan penggunaan tertinggi, yaitu antara 122,6 MB hingga 130,7 MB, sedangkan kontainer lain berada di bawah 17 MB.

Aktivitas network tercatat cukup signifikan pada kontainer vulscanner_web dan vulscanner_redis. Data sent tertinggi dicatat oleh vulscanner_web sebesar 510 KB, dan data received

mencapai 596 KB. Kontainer vulscanner_redis juga menunjukkan aktivitas network yang cukup tinggi dengan data received hingga 196 KB. Pada aktivitas disk, data read tertinggi tercatat pada vulscanner_web sebesar 13,5 MB, dan vulscanner_redis sebesar 81,9 KB. Satu-satunya aktivitas data write tercatat pada kontainer vulscanner_redis sebesar 4,1 KB, sedangkan kontainer lainnya tidak mencatat aktivitas write pada disk.

2. Nmap

Tabel 5.20 Hasil 1 (Pengujian Docker aktif dengan Pemindaian Menggunakan Nmap)

Container	CPU	Memory	Network		Disk	
			data sent	data received	data read	data write
vulscanner_web	5.93 % - 16.72 %	133.9 MB – 152.3 MB	513 KB – 990 KB	599 KB – 782 KB	13.5 MB – 19.3 MB	0 B
nikto_scanner	0%	16.81 MB	89.4 KB – 106 KB	34.6 KB – 44.7 KB	0 B	0 B
nmap_scanner	18.08 % - 94.02 %	16.64 MB – 16.8 MB	87 KB – 124 KB	35 KB – 47.5 KB	0 B	0 B
vulnscanner_redis	1.41 % - 12.6 %	3.48 MB – 3.77 MB	70.2 KB – 104 KB	203 KB – 314 KB	8.19 KB – 12.3 KB	81.9 KB

Tabel 5.19 Hasil pengujian pada kondisi docker aktif dengan proses pemindaian menggunakan Nmap menunjukkan total penggunaan CPU berada pada rentang 3,76% hingga 129,79%, dan total penggunaan memory sebesar 37,1 MB hingga 189,42 MB. Kontainer dengan penggunaan CPU tertinggi adalah nmap_scanner yang mencapai 94,02%, diikuti oleh vulscanner_web sebesar 16,72%. Kontainer nikto_scanner tidak mencatat aktivitas CPU, dan vulscanner_redis menggunakan CPU hingga 12,6%. Dari sisi memory, vulscanner_web menjadi kontainer dengan penggunaan tertinggi yaitu hingga 152,3 MB, sementara kontainer lainnya tercatat menggunakan memory di bawah 17 MB.

Aktivitas network juga meningkat terutama pada vulscanner_web dan vulscanner_redis. Data sent tertinggi dicatat oleh vulscanner_web sebesar 990 KB dan *data received* mencapai 782 KB. Kontainer vulscanner_redis juga mencatat

data received yang cukup tinggi hingga 314 KB. Untuk aktivitas disk, vulscanner_web mencatat data read tertinggi sebesar 19,3 MB, disusul oleh vulscanner_redis dengan *data read* sebesar 12,3 KB dan satu-satunya aktivitas *data write* sebesar 81,9 KB. Kontainer lainnya tidak mencatat aktivitas read maupun write pada disk.

3. Nikto dan Nmap Secara Bersamaan

Tabel 5.21 Hasil 2 (Pengujian Docker Aktif Dengan Pemindaian Menggunakan Nmap Dan Nikto Bersamaan)

Container	CPU	Memory	Network		Disk	
			data sent	data received	data read	data write
vulscanner_web	12.41 % - 93.74 %	144.7 MB – 162.5 MB	1.02 MB – 1.78 MB	141 KB – 1.71 MB	5.58 MB	28.7 KB
nikto_scanner	46.24 % - 139.52 %	16.78 MB – 31.89 MB	10.1 KB – 48.9 KB	4.93 KB – 18 KB	0 B	0 B
nmap_scanner	25.41 % - 68.22 %	16.77 MB – 16.79 MB	9.9 KB – 51.6 KB	4.83 KB – 20.8 KB	0 B	0 B
vulnscanner_redis	1.72 % - 16.5 %	3.75 MB – 4.02 MB	36.2 KB – 125 KB	52.3 KB – 155 KB	0 B	0 B – 4.1 KB

Tabel 5.20 Hasil pengujian pada kondisi docker aktif dengan proses pemindaian secara bersamaan menggunakan Nikto dan Nmap menunjukkan total penggunaan CPU berada pada rentang 6,25% hingga 306,79%, serta total penggunaan memory sebesar 183,53 MB hingga 208,68 MB. Kontainer dengan penggunaan CPU tertinggi adalah nikto_scanner sebesar 139,52%, diikuti oleh vulscanner_web sebesar 93,74% dan nmap_scanner sebesar 68,22%. Kontainer vulscanner_redis mencatat penggunaan CPU paling rendah sebesar 16,5%. Dari sisi memory, vulscanner_web memiliki penggunaan tertinggi hingga 162,5 MB, sementara kontainer lainnya menggunakan memory di bawah 32 MB. Aktivitas network juga cukup tinggi pada pengujian ini. Data sent tertinggi tercatat pada kontainer vulscanner_web sebesar 1,78 MB, disusul oleh nikto_scanner dan nmap_scanner masing-masing sebesar 48,9 KB dan 51,6 KB.

Data received tertinggi juga berasal dari vulscanner_web dengan nilai hingga 1,71 MB, serta vulscanner_redis sebesar 155 KB. Untuk aktivitas disk, vulscanner_web mencatat data read sebesar 5,58 MB dan data write sebesar 28,7 KB. Selain itu, vulscanner_redis menjadi satu-satunya kontainer lain yang mencatat aktivitas write pada disk sebesar 4,1 KB. Kontainer lainnya tidak menunjukkan aktivitas read maupun write pada disk.

5.2.8 Rangkuman Hasil Pengujian

Berdasarkan pengujian yang telah dilakukan yaitu pengujian keamanan menggunakan 2 *tools* dengan masing – masing *tools* memiliki 3 kategori *website* yaitu localhost 1 *device*, localhost dari *device* lain, dan *website* dari internet. Hasil pengujian menunjukkan berbagai jenis kategori kerentanan pada setiap *website*. Hasil pemindaian keamanan menunjukkan hasil *reporting* yang konsisten setelah dilakukan pengujian selama 3 kali. *Platform* ini juga memberikan rekomendasi perbaikan berbasis *generative AI* kepada *user* sesuai dengan hasil *reporting* yang sudah diberikan sebelumnya. Pengujian performa *platform* ini menggunakan ApacheJmeter juga menunjukkan bahwa *platform* ini memiliki tingkat skalabilitas dan reliabilitas yang bagus, terbukti dari *error rate* sebesar 0% dan tidak terjadi *crash* pada seluruh skenario pengujian. *Platform* juga menunjukkan *scalability* yang baik, dengan *throughput* meningkat seiring kenaikan jumlah *request*. Namun, pada skenario beban sangat tinggi, waktu respon mengalami kenaikan signifikan sehingga kinerja menjadi lebih lambat. Secara keseluruhan, *platform* pengujian keamanan server berbasis website ini berhasil melakukan *scanning*, *reporting* dan rekomendasi berbasis AI yang dapat diunduh oleh pengguna dalam format PDF.

Tabel 5. 22 Perbandingan Spesifikasi dan Realisasi

No	Spesifikasi	Realisasi	Tercapai/ Tidak Tercapai
1	Scanning	<i>Platform</i> pengujian keamanan ini dapat melakukan <i>scanning</i> keamanan dengan menggunakan dua <i>tools</i> utama yaitu Nikto dan Nmap yang diintegrasikan dalam sebuah <i>Website</i> dengan fitur <i>scanning</i> diantaranya <i>OS Detection</i> , <i>Port scan</i> , <i>Vulnerability</i> , <i>comprehensive</i> , <i>Basic scan</i> , <i>Full scan</i> , <i>SSL/TSL scan</i> , dan <i>custom scan</i> (menyesuaikan parameter lanjutan).	Tercapai
2	Reporting	<i>Platform</i> ini dapat menyediakan laporan hasil temuan kerentanan pada server berupa ringkasan pemindaian, skor keamanan, <i>chart</i> , analisis keamanan detail dengan kategori tingkat kerentanan <i>Critical</i> , <i>High</i> , <i>Medium</i> , <i>Low</i> , Info. dan menyediakan pelaporan data hasil <i>security scan</i> .	Tercapai
3	Rekomendasi perbaikan	<i>Platform</i> menyediakan rekomendasi perbaikan berbasis <i>generative AI</i> berdasarkan hasil temuan kerentanan dan dapat diunduh oleh <i>user</i> dalam format PDF.	Tercapai

BAB 6

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan pengujian dan analisis yang telah dilakukan, pengembangan *platform* pengujian keamanan server berbasis *website* ini terbukti mampu menjadi solusi yang efektif bagi kompleksitas masalah dalam keamanan server yaitu serangan *cyber* seperti pencurian data, peretasan, serangan kerentanan terhadap *malware* dan berbagai serangan berkelanjutan lainnya. Analisis pengujian menggunakan dua tools utama dengan masing-masing memiliki 3 skenario pengujian membuktikan bahwa *platform* pengujian keamanan server berbasis *website* ini mampu melakukan *scanning* keamanan server dengan berbagai macam metode yang tersedia pada *platform* sesuai kebutuhan pengguna, *platform* ini juga berhasil menyediakan hasil temuan kerentanan secara detail.

Dari hasil rekapitulasi pengujian, *platform* diuji pada berbagai skenario, yaitu pada lingkungan *Localhost* 1 *device*, *Localhost* beda *device*, dan internet. Untuk kategori *Localhost* 1 *device*, durasi rata-rata pemindaian menggunakan nikto berkisar antara 0.99 hingga 1.77 detik, sedangkan nmap menunjukkan durasi rata-rata 174.10 hingga 512.23 detik, dengan hasil konsistensi temuan yang tetap terjaga. Pada kategori *Localhost* beda *device*, durasi rata-rata pemindaian nikto meningkat antara 4.51 hingga 10.12 detik, sementara nmap mencapai 439.81 hingga 989.25 detik dengan hasil yang konsisten. Sementara itu, pengujian terhadap *website* berbasis internet seperti www.pln.co.id, httpbin.org, dan www.komdigi.go.id menunjukkan waktu pemindaian nikto antara 20.18 hingga 82.76 detik, dan durasi nmap antara 358.18 hingga 847.14 detik, yang semuanya tetap menunjukkan konsistensi dalam hasil temuan kerentanan.

Platform ini juga telah diuji *reliability*-nya menggunakan ApacheJMeter yang membuktikan bahwa *platform* “Pengujian Keamanan Server Berbasis *Website*” ini memiliki *reliability* yang baik karena ketika diuji dengan *request* terbanyak sebesar 48.000, *Website* mampu merespons semua permintaan dengan sukses, ditunjukkan oleh tingkat *error* 0% dan tidak adanya *crash*, sehingga *website* berjalan stabil. Meskipun pada skenario beban sangat tinggi, waktu respon mengalami kenaikan signifikan sehingga kinerja *platform* ini menjadi lebih lambat.

Pengujian performa *backend* menunjukkan bahwa penggunaan CPU dan memori meningkat secara bertahap pada saat proses *scanning* berlangsung. Penggunaan CPU rata-rata meningkat dari 7.44% pada kondisi normal menjadi 9.22% saat menggunakan nikto dan 9.84% saat menggunakan nmap. Begitu pula penggunaan memori, yang naik dari 1.50% dalam

kondisi normal menjadi 1.62% saat nikto aktif, dan 1.76% saat nmap berjalan. Hal ini menandakan adanya beban komputasi yang wajar dan proporsional selama proses *scanning* berlangsung.

Sementara itu, hasil pengujian performa *frontend* menunjukkan bahwa sistem masih memberikan respon yang baik hingga 500 pengguna, namun mulai mengalami perlambatan di atas 1000 pengguna, dengan *response time* mencapai 12.644 ms dan *error rate* sebesar 3.51% pada 2000 pengguna. Selain itu, performa tiap *endpoint* menunjukkan beberapa *endpoint* kritikal seperti NMAP, NIKTO, dan DASHBOARD memiliki rata-rata waktu respons di atas 13 detik dengan tingkat *error* di atas 3%, yang menandakan perlunya optimisasi lebih lanjut untuk kestabilan di skenario beban tinggi.

Selain itu, pengujian performa *container* menggunakan Docker Desktop menunjukkan bahwa penggunaan CPU dan memori meningkat sesuai dengan intensitas proses *scanning*. Dari seluruh pengujian, penggunaan CPU total tertinggi tercatat sebesar 306,79% saat dilakukan pemindaian gabungan menggunakan nikto dan nmap, sedangkan penggunaan CPU total terendah terjadi pada kondisi docker aktif tanpa proses pemindaian, yaitu sebesar 19,05%. Untuk penggunaan *memory* total, nilai tertinggi dicapai pada pengujian gabungan tersebut sebesar 208,68 MB, sedangkan nilai terendah tercatat sebesar 155,13 MB pada kondisi tanpa pemindaian. Aktivitas jaringan dan *disk* juga meningkat signifikan terutama saat proses pemindaian dijalankan secara bersamaan dengan *tools* nikto dan nmap, yang menunjukkan bahwa beban sistem terdistribusi sesuai fungsi masing-masing *container*.

Dari hasil pengujian keamanan yang diperoleh, *platform* ini menunjukkan hasil temuan kerentanan yang konsisten pada setiap target yang diuji dan semua data *reporting* kerentanan diperoleh secara *real-time* tidak ada data *dummy* (data tiruan atau data palsu) dengan waktu pengujian yang cukup singkat. *Platform* ini juga memberikan rekomendasi perbaikan berbasis *generative AI* yang relevan dengan hasil temuan kerentanan dan dapat diunduh oleh pengguna dalam format PDF sehingga memberikan gambaran langkah yang harus dilakukan ke depannya oleh pengguna.

Namun, meskipun pengembangan *platform* pengujian keamanan ini efektif untuk menjadi solusi bagi kompleksitas masalah serangan *cyber*, dalam penerapannya masih perlu dilakukan lagi pengembangan secara berkala seperti tambahan integrasi *tools* pengembangan *open source* yang lebih beragam agar dapat mendeteksi keseluruhan OWASP Top 10 daftar risiko keamanan aplikasi web yang paling kritis.

6.2 Saran

Berdasarkan pengujian *platform* “Pengujian Keamanan Server Berbasis *Website*” ini diperlukan beberapa saran untuk pengembangan lebih lanjut. Berikut merupakan saran yang diperlukan untuk pengembangan *platform* “Pengujian Keamanan Server Berbasis *Website*” ini :

1. Tambahkan integrasi *tools* pengujian keamanan yang bersifat *open source* yang lebih beragam agar dapat mendeteksi keseluruhan OWASP Top 10 daftar risiko keamanan aplikasi *web* yang paling kritis.
2. Memperbanyak pengujian keamanan terhadap *website* yang ada di internet. Hal ini dikarenakan setiap *website* memiliki deskripsi kerentanan yang berbeda-beda. *Platform* pengujian keamanan ini memerlukan proses pendefinisian secara spesifik terhadap deskripsi setiap kerentanan tersebut agar hasil pemindaian menjadi lebih akurat dan relevan. Hal ini terjadi karena setiap *website* memiliki karakteristik dan deskripsi kerentanan yang beragam. Oleh karena itu, *platform* pengujian keamanan ini perlu melakukan pendefinisian secara spesifik terhadap tiap kerentanan tersebut, sehingga hasil pemindaian dapat menjadi lebih akurat
3. Mengembangkan fitur admin dan memperkecil kemungkinan adanya bug.

Dari saran-saran penulis di atas, diharapkan Tugas Akhir Capstone Design *platform* “Pengujian Keamanan Server Berbasis *Website*” ini dapat memberikan manfaat yang baik untuk pengembangan selanjutnya.

DAFTAR PUSTAKA

1. Alqausar, D. (2024, Desember 27). *proxsisgroup*. Retrieved from biztech.proxsisgroup.com: <https://infrasec.proxsisgroup.com/membandingkan-metasploit-nessus-dan-acunetix-untuk-kebutuhan-penetration-testing-perusahaan-anda/#%3A~%3Atext%3DNessus-%2CNessus%20adalah%20alat%20pemindaian%20keamanan%20yang%20digunakan%20untuk%20mengidentifikasi%20kere>
2. Ari Marta Tania, Didik Setiyadi, & Fata Nidaul Khasanah. (2018). Keamanan *Website* Menggunakan Vulnerability Assessment. *INFORMATIC FOR EDUCATORS AND PROFESSIONALS*, 171-180.
3. Bai, J. (2021). A Study on Software Vulnerability Prioritization and Management Methods. *Bai, J. (2021). A Study on Software Vulnerability PrioritizInternational Conference on Computer, Information and Telecommunication Systems (CITS)*, 1-5.
4. *Bizplus*. (2025). Retrieved from bizplus.id: <https://bizplus.id/pengertian-dan-metode-security-testi/>.
5. Chongqing kang, Daniel Kirschen, & Timothy C.Green. (2023). The Evolution of Smart Grids. *Proceeding of the IEEE*, 691-693.
6. Cloudeka. (2023). *8 Tahapan Penetration Testing yang Penting dan Akurat*. jakarta: Lintasarta Cloudeka.
7. *CLOUDFLARE*. (2025). Retrieved from cloudflare.com: <https://www.cloudflare.com/learning/security/threats/owasp-top-10/>
8. Dasci, M. (2024). Exploring Nmap Tool: A Comprehensive Analysis. 50.
9. Django. (2025, 6 18). *Django*. Retrieved from docs.djangoproject.com: <https://docs.djangoproject.com/en/5.2/>
10. *Docker*. (2025). Retrieved from docs.docker.com: Diakses pada 7 juli 2025 <https://docs.docker.com>
11. Esra Abdullatif Altulaihan, Abrar Alismail, & Mounir Frikha. (4 march 2023). A Survey on *Web* Application Penetration Testing. *electronics*, 12.
12. F.Fachri. (2023). “OPTIMASI KEAMANAN *WEB* SERVER TERHADAP SERANGAN . 51-58.

13. Foundation, D. S. (2025, Juli 7). *Django*. Retrieved from docs.djangoproject.com: <https://docs.djangoproject.com/en/stable/>
14. Hoky Albani Bardian, & Imam Sutanto. (2025). PENGEMBANGAN APLIKASI VULNERABILITY SCANNER UNTUK MENDETEKSI CELAH KEAMANAN SIBER PADA WEBSITE. *Jurnal Mahasiswa Teknik Informatika*, 4044-4411.
15. Hubli, S. C., & Jaiswal, R. C. (2023). Efficient *Backend* Development with Spring Boot: A Comprehensive Overview. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 11.
16. Kane, S. P., & Matthias, K. (2022). Docker: Up & Running (3rd ed.). *O'Reilly Media*.
17. Lyon, G. (2024). *NMAP.ORG*. Retrieved from nmap.org: nmap.org
18. Ridho, M. R. (2024, march 18). *Telkomuniversity*. Retrieved from Telkomuniversity.ac.id: <https://bee.telkomuniversity.ac.id/panduan-lengkap-macam-macam-jenis-server- serta-fungsinya/>
19. Ruli Dimas Prakoso, & Asmunin. (2018). IMPLEMENTASI DAN PERBANDINGAN PERFORMA PROXMOX DALAM VIRTUALISASI . *JURNAL MANAJEMEN INFORMATIKA*, 79 - 85.
20. Schwartzburg, D. (2023). *FIRST*. Retrieved from first.org: <https://www.first.org/cvss/v4-0/specification-document>
21. Sofyan Mufti Prasetyo, Muhammad Ivan Prayogi Nugroho, Riris Lima Putri, & Opa Fauzi. (2022). Pembahasan Mengenai Front-end *Web Developer* dalam Ruang Lingkup *Web Development*. *Jurnal Multidisiplin Ilmu*, 1015-1020.
22. SULIMAN ALAZMI, & DANIEL CONTE DE LEON. (2022). A Systematic Literature Review on the Caharacteristics and Effectiveness of *Web Application Vulnerability Scanners*. *Digital Object Identifier*, 33200-33219.
23. Sullo, C. (2024). *CIRT.net*. Retrieved from cirt.net: <https://www.cirt.net/sullo>
24. VIncent, W. (2022). Django for Professionals: Production *Websites* with Python & Django. *Django Riffs*.
25. Yusuf Muhyidin, M.Hafid Totohendarto, Erina Undayamayanti, & Salsabilla C. N. (2021). Perbandingan Tingkat Keamanan *Website* Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking. *Jurnal Teknologika*, 1-10.

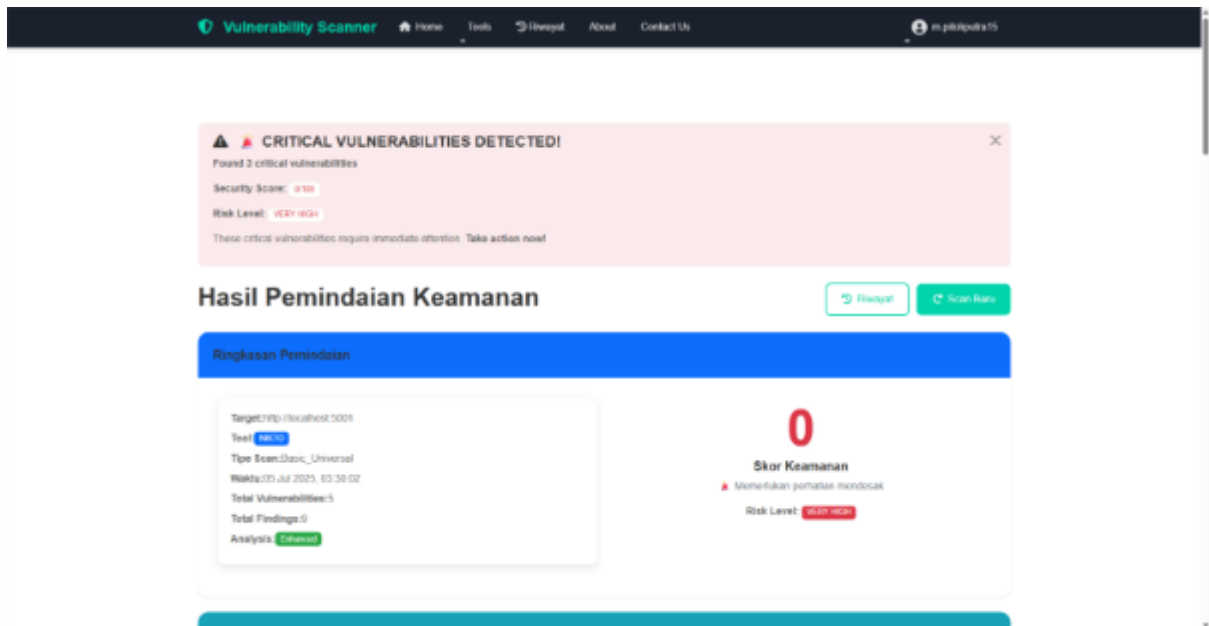
LAMPIRAN

- Link repository Github :

https://github.com/ronald212121/django_final.git

a. Pengujian (*tools nikto*) *Website* localhost 1 *device*

- *Website* 1 (localhost:5001)



Vulnerability Scanner
Home
Tools
Help
About
Contact Us
m.pikiputra15

Analysis Keamanon Detail

5 vulnerabilities
4 info findings

3 CRITICAL

1 HIGH

1 MEDIUM

0 LOW

4 INFO

8 security vulnerabilities, 4 informational findings detected
Tool: NIKTO

Security Vulnerabilities Detected (NIKTO)

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected at login form at login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
SEVERE	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Informational Findings (4)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/3.1.1.3
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Vulnerability Scanner
Home
Tools
Help
About
Contact Us
m.pikiputra15

AI Security Analysis

Enhanced Analysis
Export PDF

Security Analysis with Proper Feature Detection

Enhanced positive security feature recognition

The results of the basic scan reveal a very high risk level and 5 total vulnerabilities. Here's a breakdown of the vulnerabilities and some recommendations to address them:

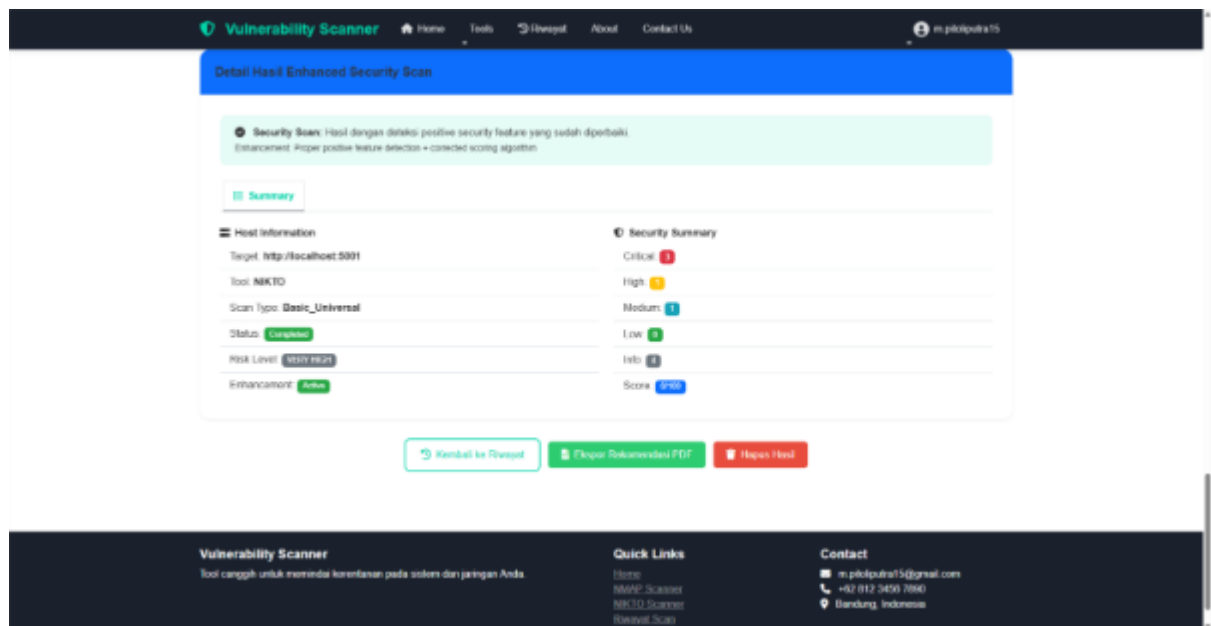
All Recommendations:

1. "Critical vulnerabilities"

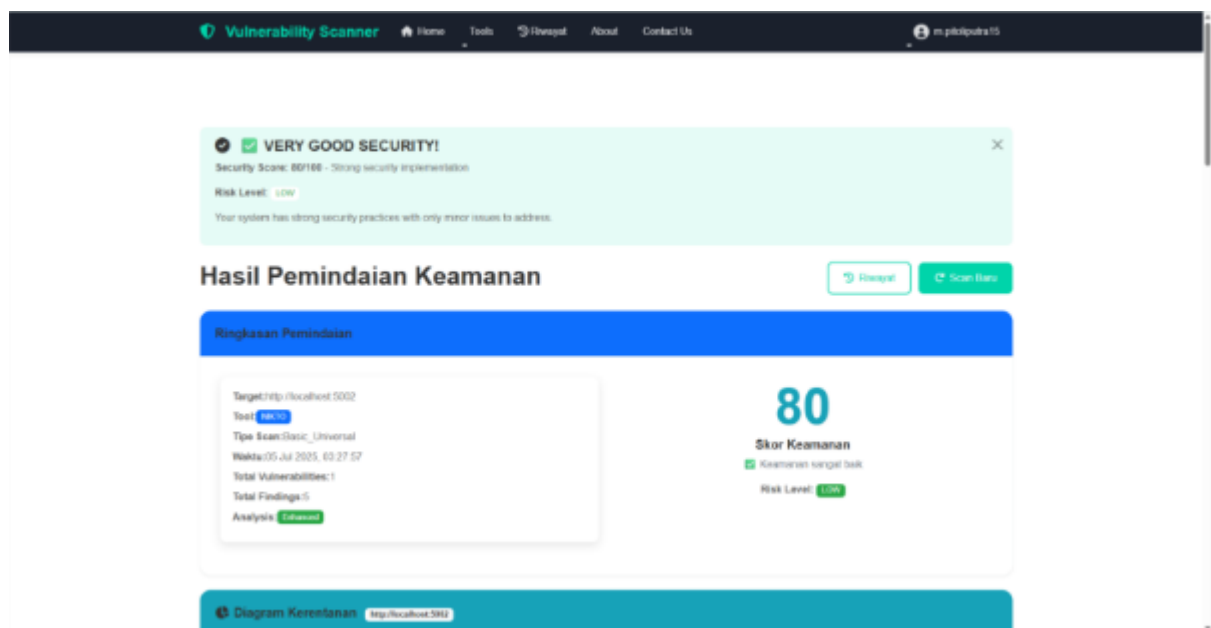
Critical vulnerabilities pose the most significant immediate risk to the system and should be addressed as soon as possible. In this case, there are three critical vulnerabilities:

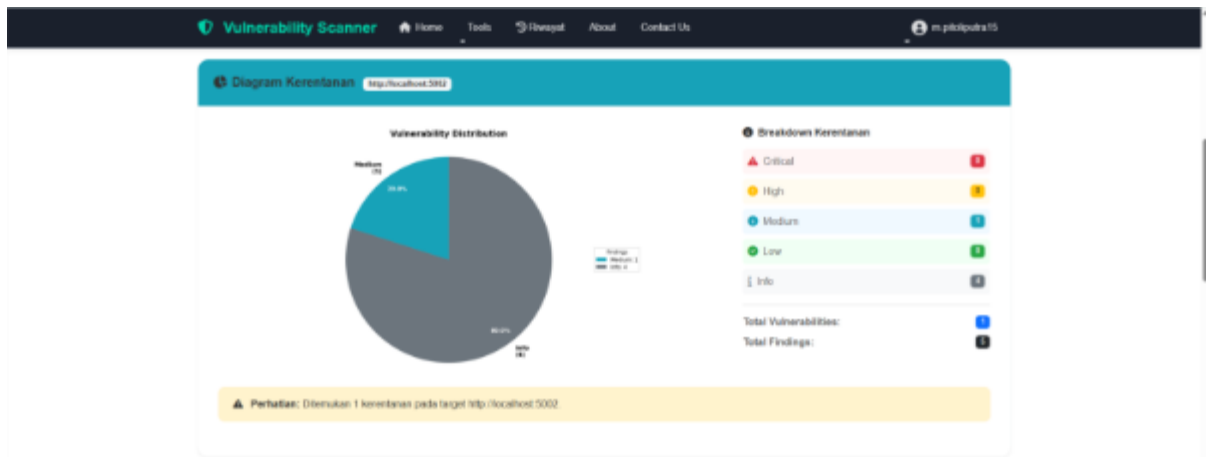
- "Unencrypted Transmission" - Recommendations: Implement SSL/TLS encryption for all communications to ensure data transmitted between the client and the server is encrypted and cannot be intercepted by malicious parties. Configure the server to use SSL/TLS certificates and enforce their use for all connections.
- "Brute Force Protection" - Implement measures to protect against brute force attacks. This can include limiting the number of login attempts within a specific time frame, implementing account lockouts, or using captchas to thwart automated attacks. Consider employing a web application firewall (WAF) that provides built-in brute force protection.

Tampilkan Selengkapnya



- Website 2 (localhost:5002)





Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra13

Analisis Kerentanan Detail

1 vulnerability 4 info findings

0 Critical 1 High 1 Medium 1 Low 4 Info

1 security vulnerabilities, 4 informational findings detected
Test: NIKTO

Security Vulnerabilities Detected (NKT0)

Severity	Type	Description	Location	Status
High	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Unfixed

Informational Findings (4)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Server: Werkzeug/2.3.7 Python/3.11.13	2024-1-9
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: OPTIONS, HEAD, GET	/
INFO	Server version disclosed in headers	/

Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra13

AI Security Analysis

Enhanced Analysis Export PDF

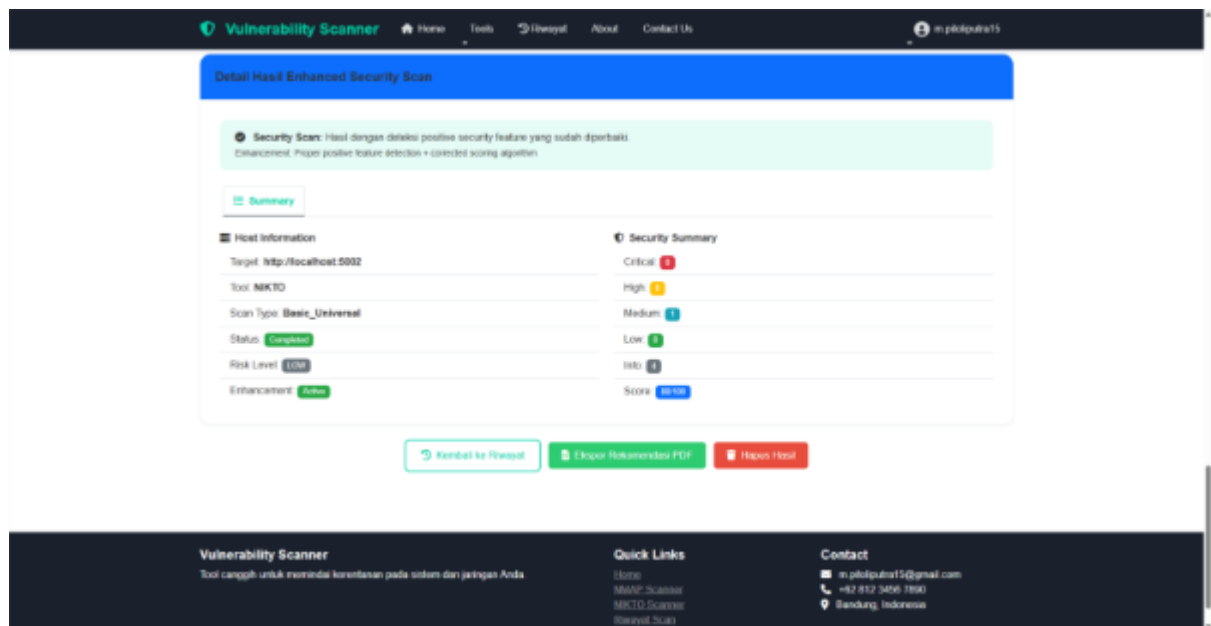
Security Analysis with Proper Feature Detection

Enhanced positive security feature recognition

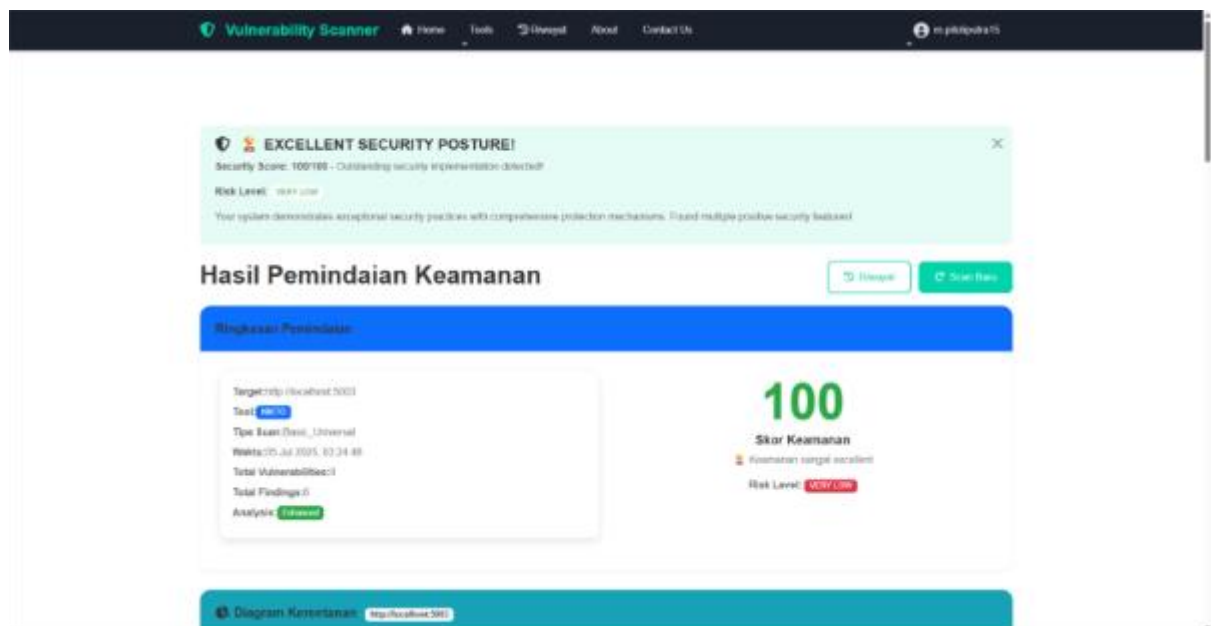
The results of the scan reveal a potential vulnerability: Local file inclusion (LFI). LFI vulnerability often leads to unauthorized access, data breaches, and even remote code execution if not properly addressed, especially if the server is exposed to the internet. Here's how you address this issue:

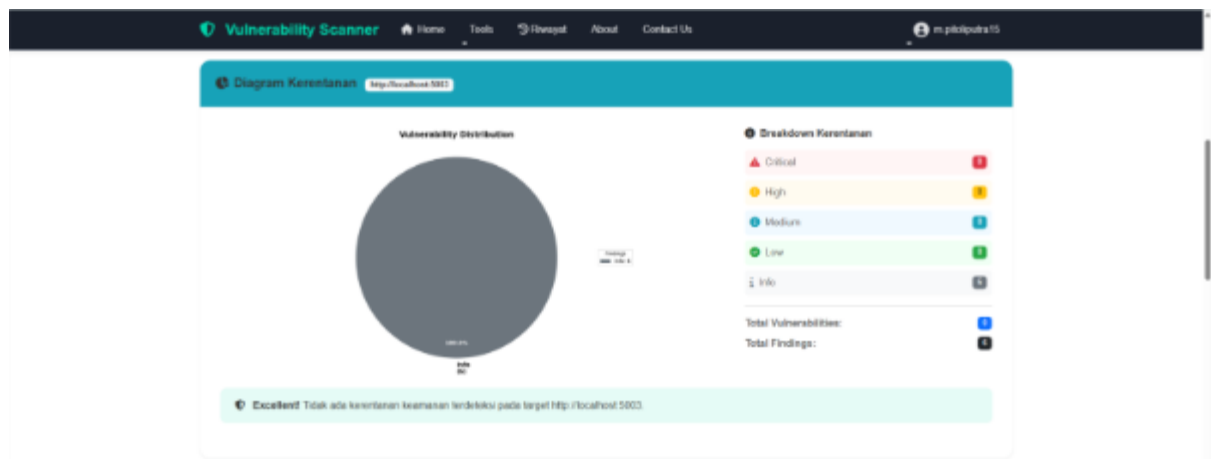
- "Understanding the Vulnerability"**: An LFI vulnerability occurs when a script interprets or executes a file on the server that should not be directly accessible from the web server. This usually happens when untrusted data is not properly validated before processing.
- "Prevention"**:
 - Ensure proper file permissions on the server. Non-public data should have strict permissions to limit any potential impact from a breach.
 - If your application requires loading of configuration files or other scripts, ensure that you validate the file path thoroughly. Avoid the use of arbitrary file paths based on user input where possible.
 - Use secure coding practices and up-to-date language frameworks to ensure known LFI vulnerabilities are minimized.
- "Detection"**:
 - Regularly audit your server logs to identify any suspicious activity. Look for requests to unusual file paths or patterns that might indicate an LFI attempt.
 - Use automated security scanning tools to regularly probe your server for known vulnerabilities.
- "Mitigation"**:
 - If an LFI vulnerability is detected, immediately take the affected server or application offline to prevent further access.
 - Review your application's code for any potential paths where an LFI might occur and apply patches or updates as recommended by the framework or language you use.
 - If you're using a Content Delivery Network (CDN), ensure you keep it updated and apply any security fixes promptly.

Terjemahan Berbahasa Indonesia



- Website 3 (localhost:5003)





Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra10

Analisis Kerentanan Detail

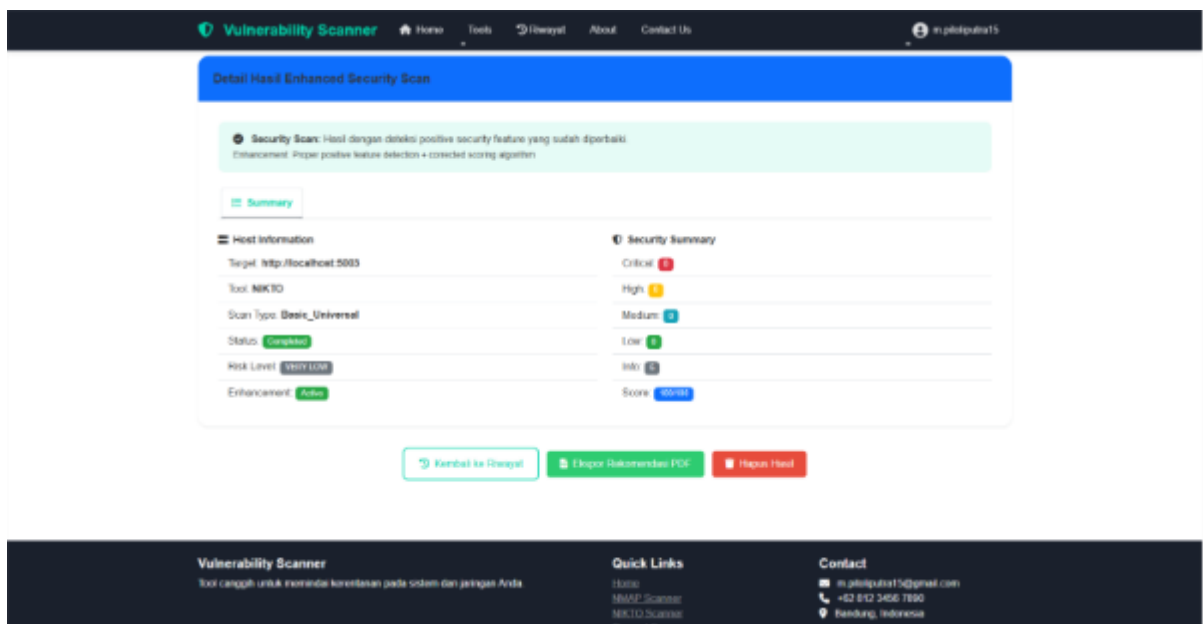
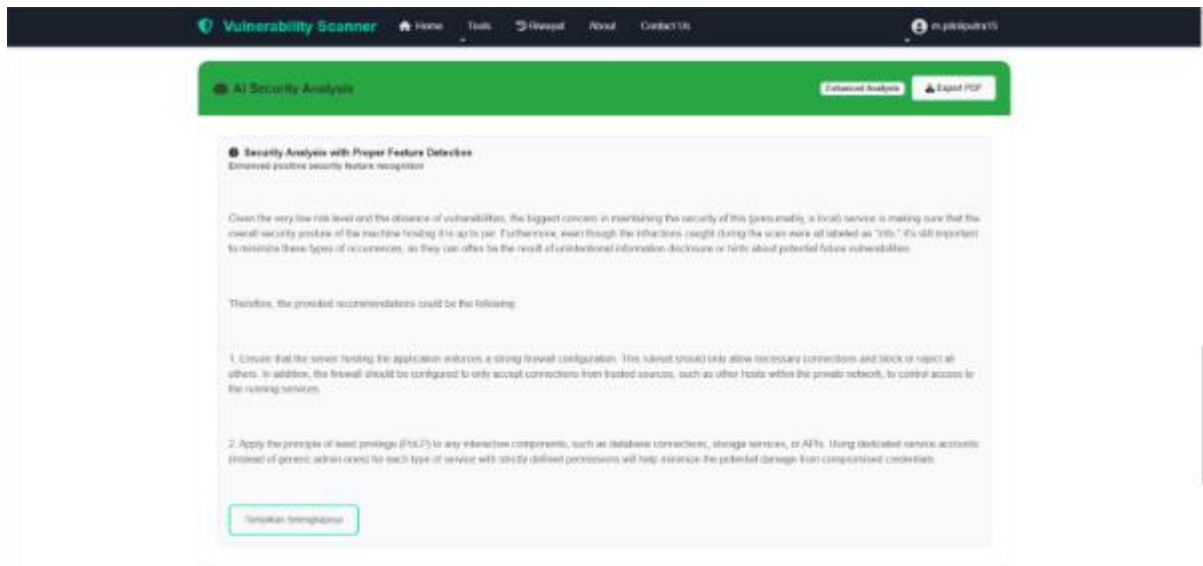
0 Critical 0 High 0 Medium 1 Low 11 Info

0 security vulnerabilities, 11 informational findings selected (total: 11/11)

Informational Findings (11)

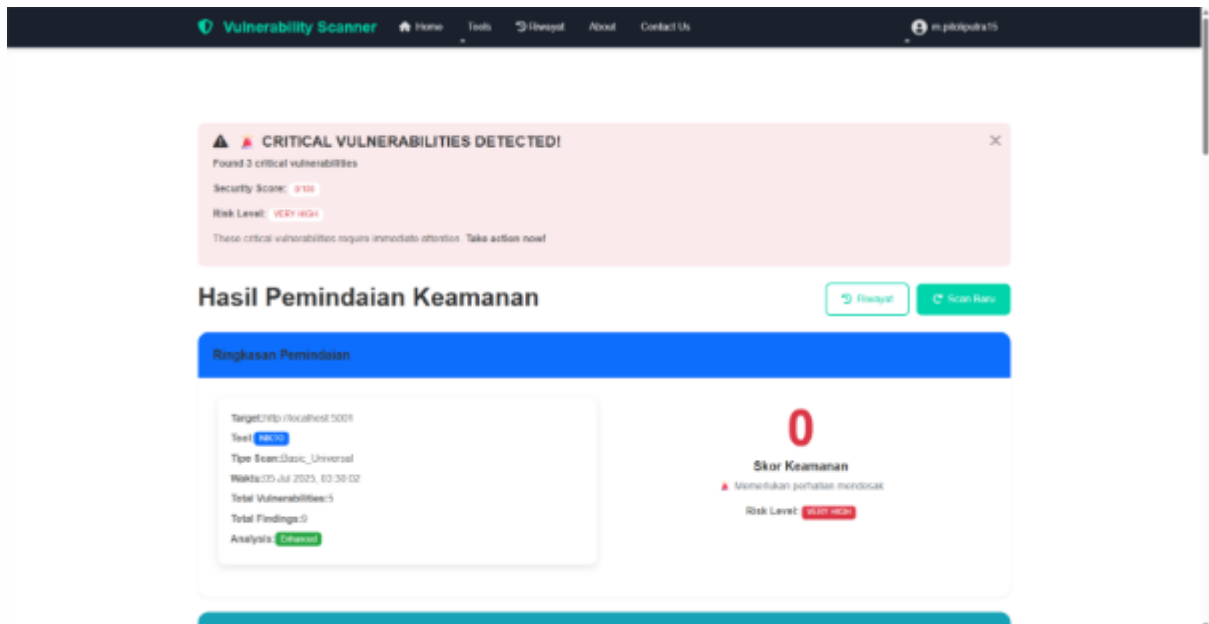
These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Server: Werkzeug/2.3.7 Python/3.11.13	/0.0.0.0
INFO	Uncommon header 'x-geo-protection' found, with contents: 1, mode=block	/
INFO	Uncommon header 'x-frame-options' found, with contents: DENY	/
INFO	Uncommon header 'x-content-type-options' found, with contents: nosniff	/
INFO	Uncommon header 'content-security-policy' found, with contents: default-src 'self', script-src 'self', style-src 'self' unsafe-inline, img-src 'self' data:, connect-src 'self', font-src 'self', object-src 'none', media-src 'self', frame-ancestors 'none'	/
INFO	Uncommon header 'permissions-policy' found, with contents: geolocation(), microphone(), camera()	/
INFO	Uncommon header 'strict-transport-security' found, with contents: max-age=31536000, includeSubDomains	/
INFO	Uncommon header 'referrer-policy' found, with contents: strict-origin when cross origin	/
INFO	Uncommon header 'x-security-level' found, with contents: Maximum	/
INFO	Server version disclosed in headers	/
INFO	Excellent security headers: X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, X-XSS-Protection	/



b. Pengujian *Website (tools nikto)* localhost beda *device*

- *Website 1* (localhost:5001) :



Vulnerability Scanner
Home
Tools
Help
About
Contact Us
m.pikiputra15

Analysis Keamanon Detail

5 vulnerabilities
4 Info Findings

3 CRITICAL

1 High

1 Medium

0 Low

4 Info

8 security vulnerabilities, 4 informational findings detected
Tool: NIKTO

Security Vulnerabilities Detected (NIKTO)

Severity	Type	Description	Location	Status
CRITICAL	SQL Injection	SQL injection vulnerability detected in login form at login	/login	Detected
CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	Detected
CRITICAL	Unrestricted File Upload	Unrestricted file upload vulnerability at /upload	/upload	Detected
SEVERE	Cross-Site Scripting (XSS)	Reflected XSS vulnerability detected at /search	/search	Detected
MEDIUM	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected

Informational Findings (4)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Server: Werkzeug/3.1.3 Python/3.11.13	/3.1.1.3
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: HEAD, GET, OPTIONS	/
INFO	Server version disclosed in headers	/

Vulnerability Scanner
Home
Tools
Help
About
Contact Us
m.pikiputra15

AI Security Analysis

Enhanced Analysis
Export PDF

Security Analysis with Proper Feature Detection

Enhanced positive security feature recognition

The results of the basic scan reveal a very high risk level and 5 total vulnerabilities. Here's a breakdown of the vulnerabilities and some recommendations to address them:

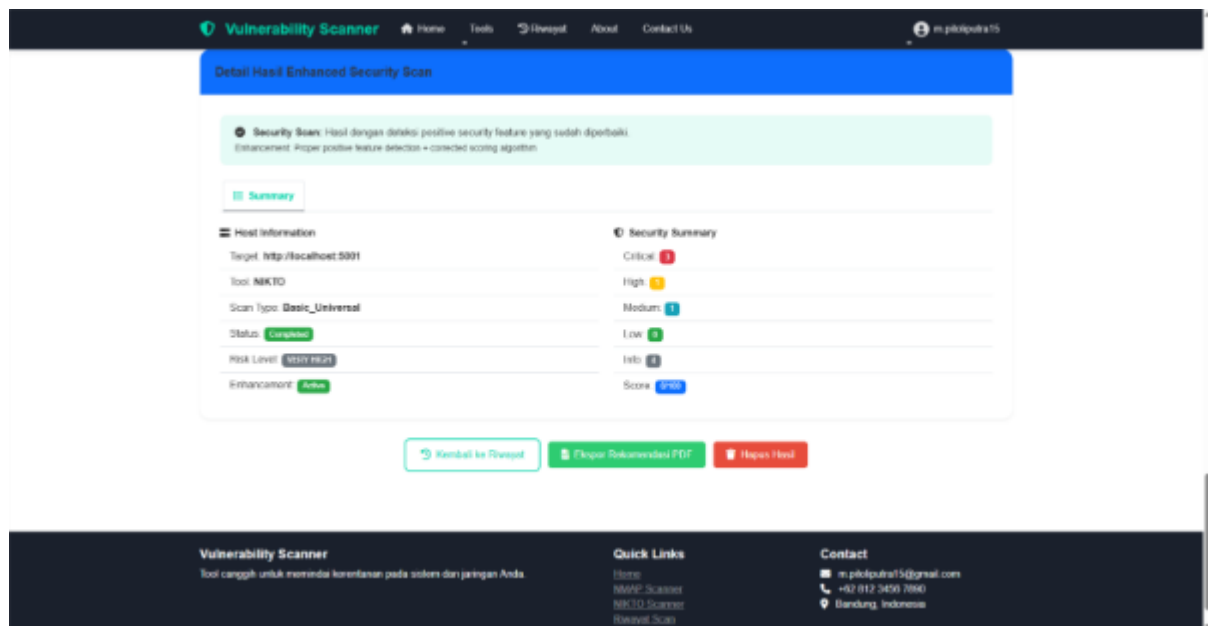
All Recommendations:

1. "Critical vulnerabilities"

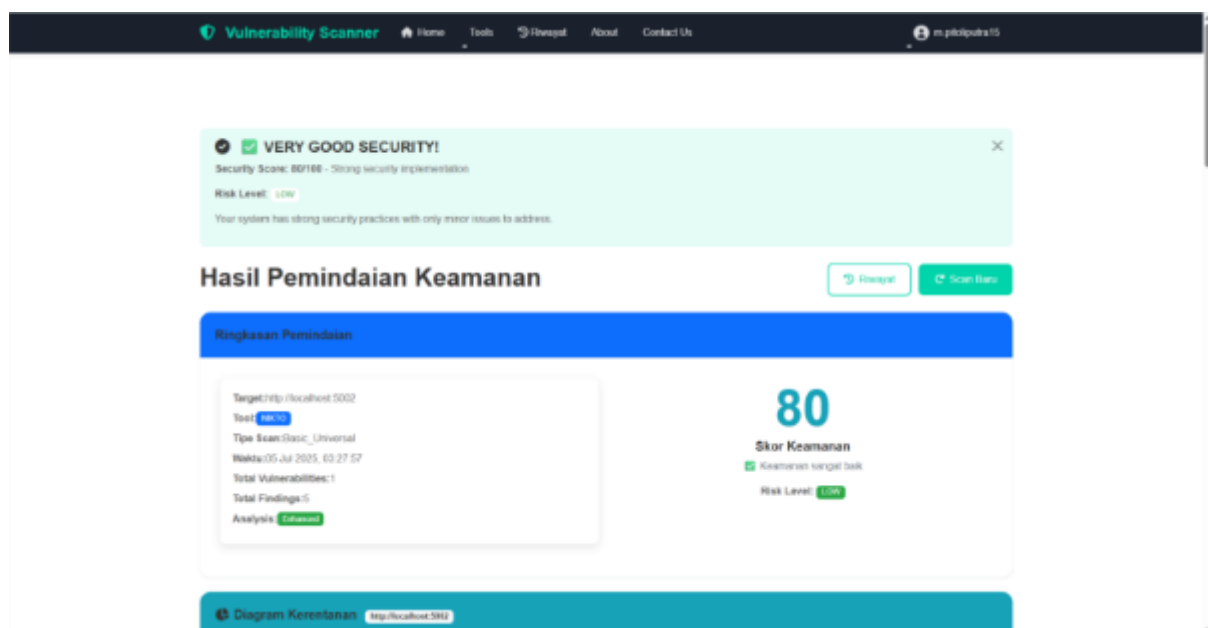
Critical vulnerabilities pose the most significant immediate risk to the system and should be addressed as soon as possible. In this case, there are three critical vulnerabilities:

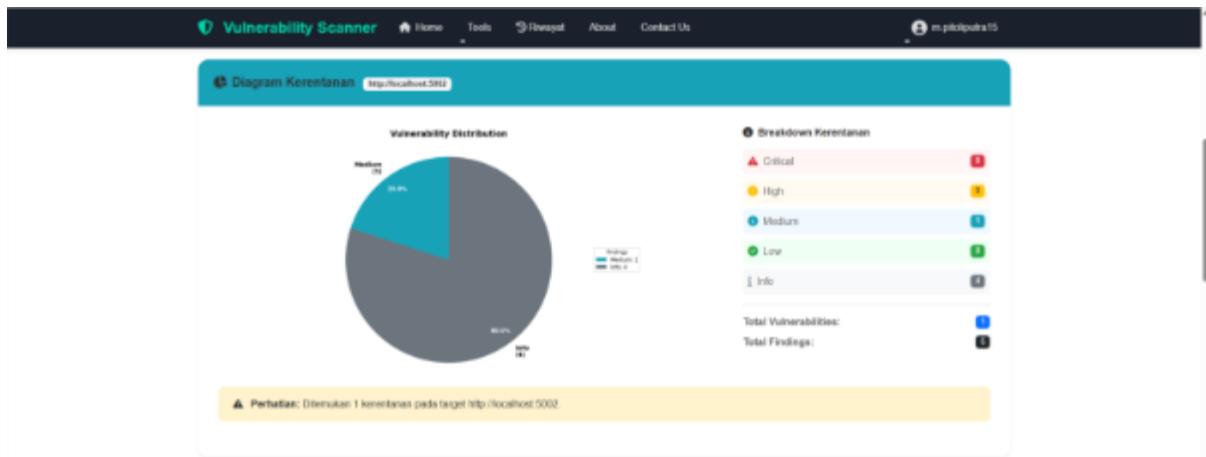
- "Unencrypted Transmission" - Recommendations: Implement SSL/TLS encryption for all communications to ensure data transmitted between the client and the server is encrypted and cannot be intercepted by malicious parties. Configure the server to use SSL/TLS certificates and enforce their use for all connections.
- "Brute Force Protection" - Implement measures to protect against brute force attacks. This can include limiting the number of login attempts within a specific time frame, implementing account lockouts, or using captchas to thwart automated attacks. Consider employing a web application firewall (WAF) that provides built-in brute force protection.

Tampilkan Selengkapnya



- Website 2 (localhost:5002)





Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra13

Analisis Kerentanan Detail

1 vulnerability 4 info findings

0 Critical 1 High 1 Medium 1 Low 4 Info

1 security vulnerabilities, 4 informational findings detected (Test: NIKTO)

Security Vulnerabilities Detected (Nikto)

Severity	Type	Description	Location	Status
High	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Unfixed

Informational Findings (4)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Server: Werkzeug/2.3.7 Python/3.11.13	/, /, /, /
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Allowed HTTP Methods: OPTIONS, HEAD, GET	/
INFO	Server version disclosed in headers	/

Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra13

AI Security Analysis

Enhanced Analysis Export PDF

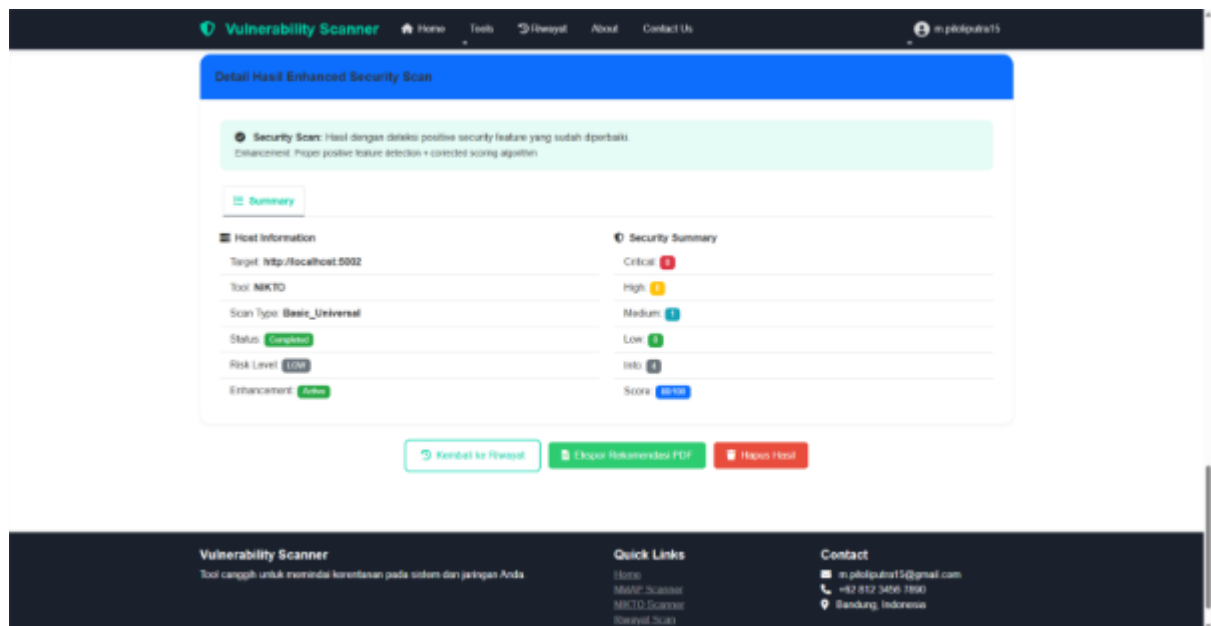
Security Analysis with Proper Feature Detection

Enhanced positive security feature recognition

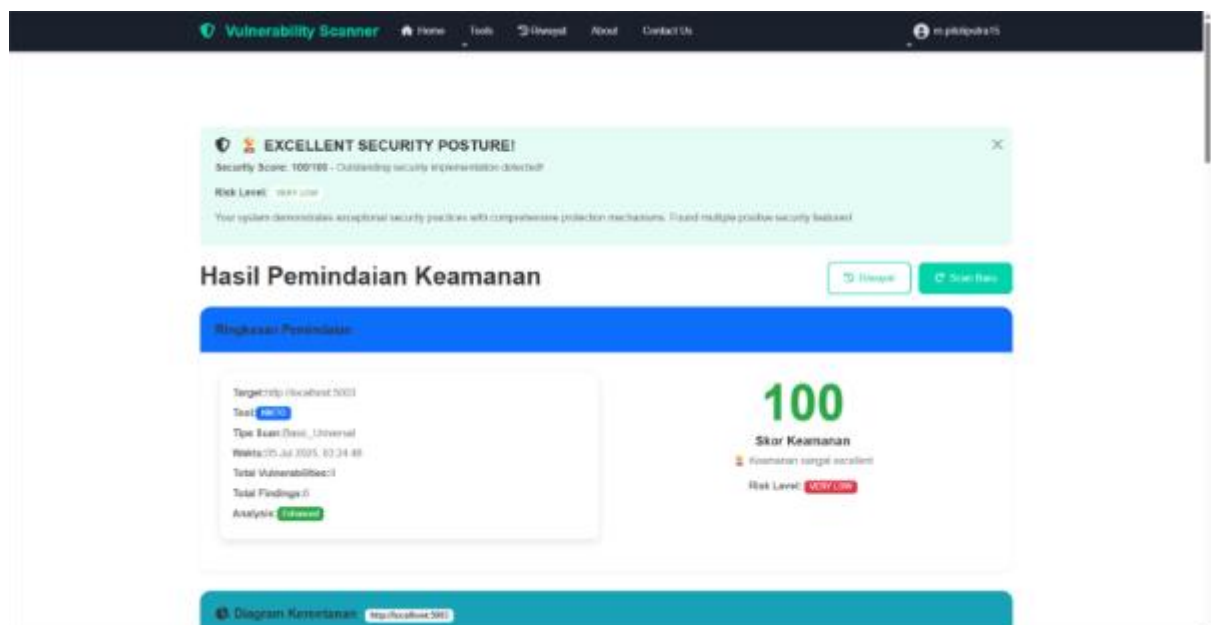
The results of the scan reveal a potentially concerning vulnerability: Local file inclusion (LFI). Vulnerability often leads to unauthorized access, data breaches, and even remote code execution if not properly addressed, especially if the server is exposed to the internet. Here's how you address this issue:

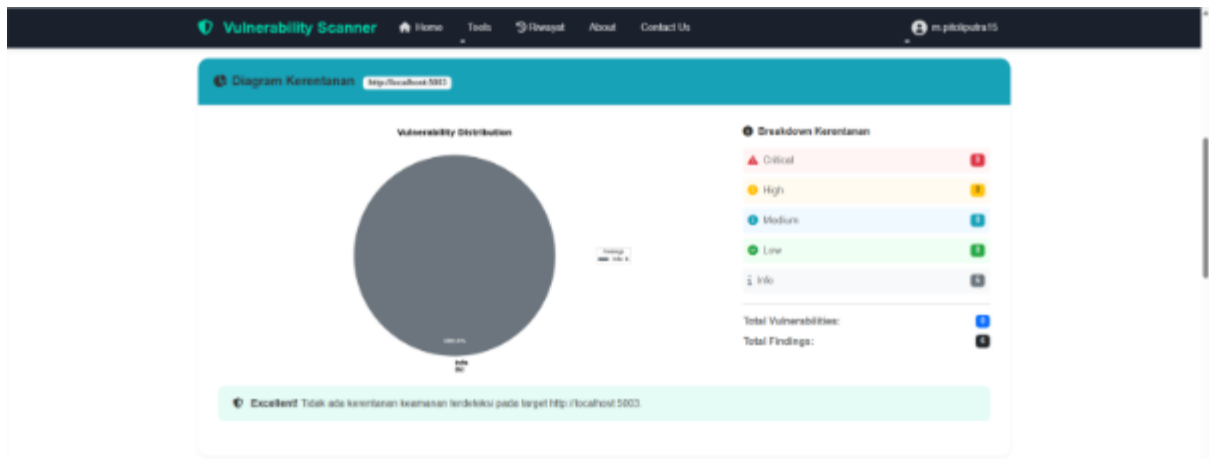
- "Understanding the Vulnerability"**: An LFI vulnerability occurs when a script interprets or executes a file on the server that should not be directly accessible from the web server. This usually happens when untrusted data is not properly validated before processing.
- "Prevention"**:
 - Ensure proper file permissions on the server. Non-public data should have strict permissions to limit any potential impact from a breach.
 - If your application requires loading of configuration files or other scripts, ensure that you validate the file path thoroughly. Avoid the use of arbitrary file paths based on user input where possible.
 - Use secure coding practices and up-to-date language frameworks to ensure known LFI vulnerabilities are minimized.
- "Detection"**:
 - Regularly audit your server logs to identify any suspicious activity. Look for requests to unusual file paths or patterns that might indicate an LFI attempt.
 - Use automated security scanning tools to regularly probe your server for known vulnerabilities.
- "Mitigation"**:
 - If an LFI vulnerability is detected, immediately take the affected server or application offline to prevent further access.
 - Review your application's code for any potential paths where an LFI might occur and apply patches or updates as recommended by the framework or language you use.
 - If you're using a Content Delivery Network (CDN), ensure you keep it updated and apply any security fixes promptly.

Terjemahan Berbahasa Indonesia



- Website 3 (localhost:5003)





Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra10

Analisis Kerentanan Detail

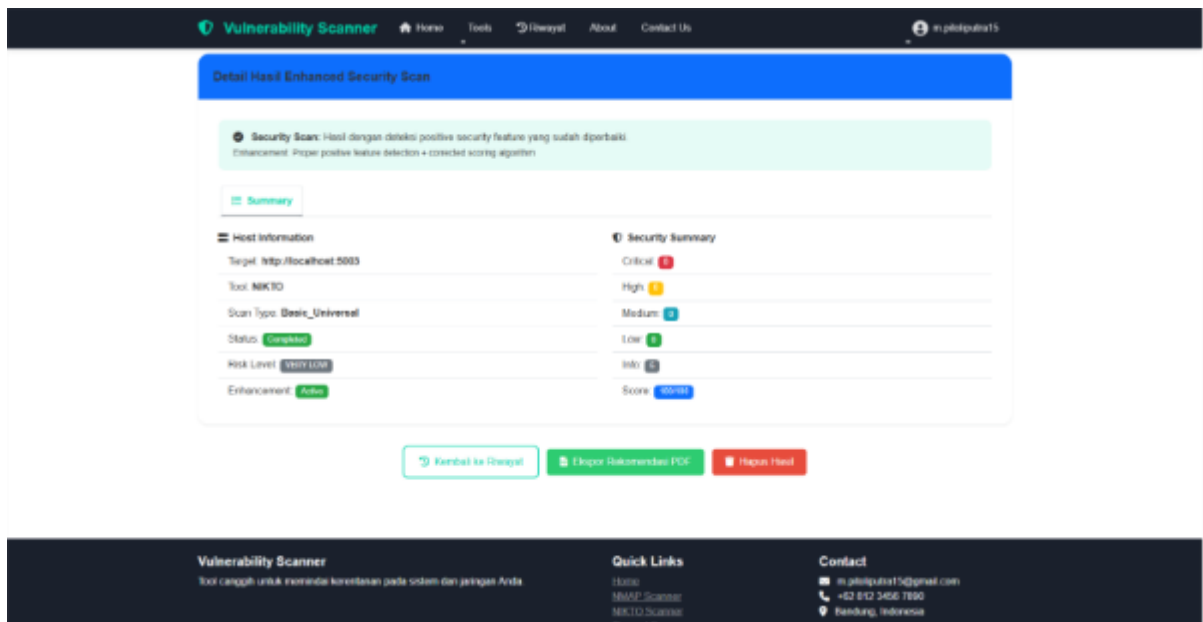
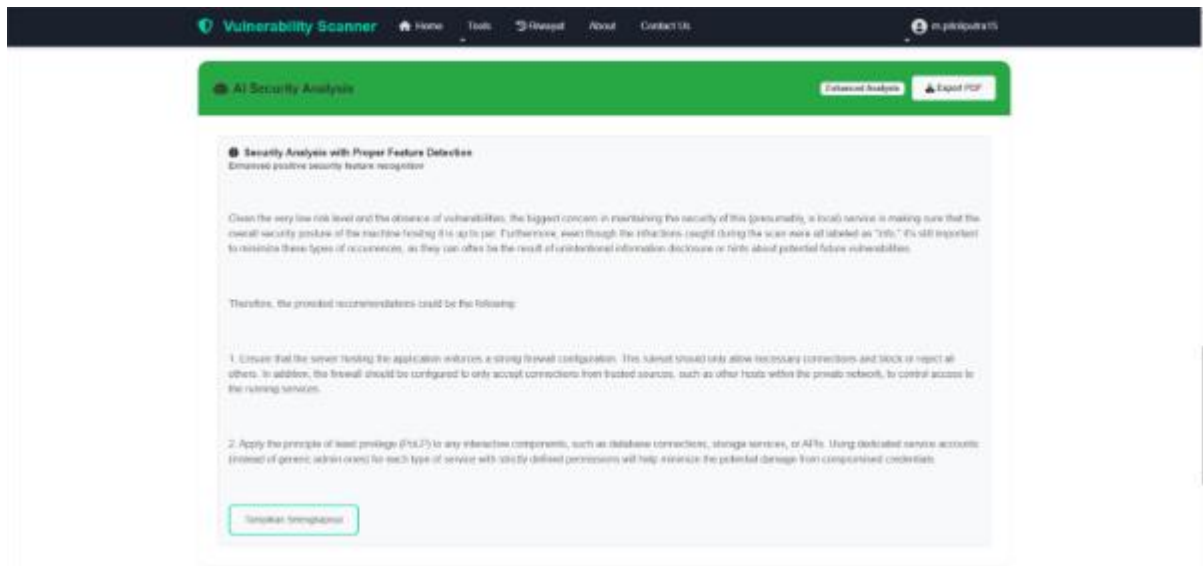
0 Critical 3 High 1 Medium 2 Low 11 Info

0 security vulnerabilities, 11 informational findings selected (total: 11/12)

Informational Findings (11)

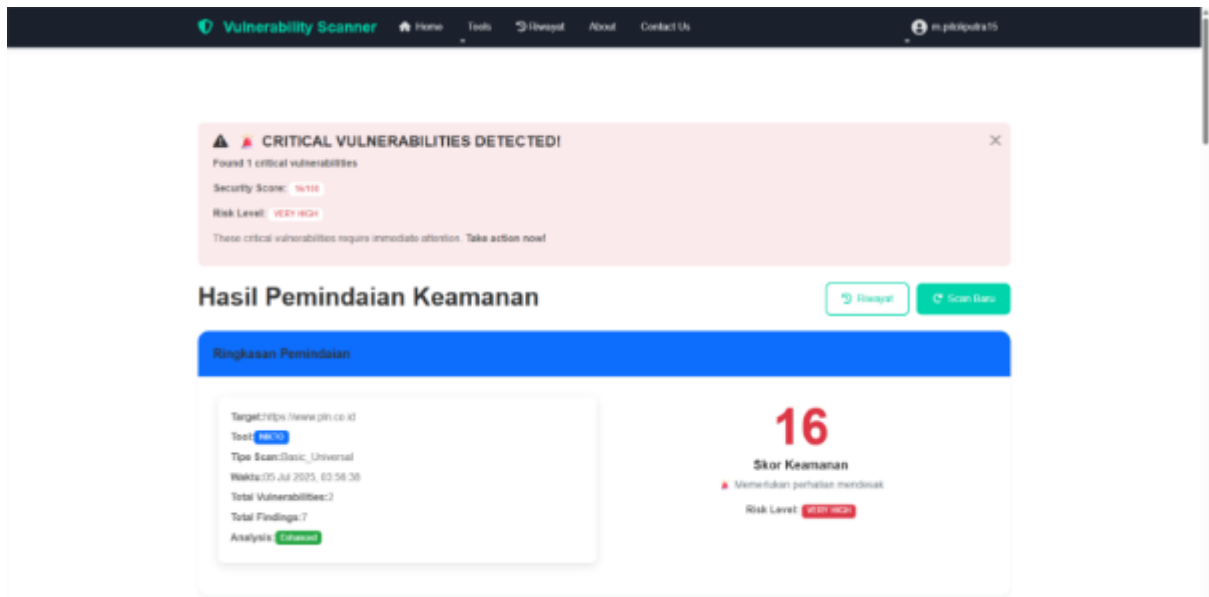
These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Server: Werkzeug/2.3.7 Python/3.11.13	/0:1:1
INFOSEC	Uncommon header 'x-geo-protection' found, with contents: 1, mode=block	/
INFOSEC	Uncommon header 'x-frame-options' found, with contents: DENY	/
INFOSEC	Uncommon header 'x-content-type-options' found, with contents: nosniff	/
INFOSEC	Uncommon header 'content-security-policy' found, with contents: default-src 'self', script-src 'self', style-src 'self' unsafe-inline, img-src 'self' data:, connect-src 'self', font-src 'self', object-src 'none', media-src 'self', frame-ancestors 'none'	/
INFO	Uncommon header 'permissions-policy' found, with contents: geolocation(), microphone(), camera()	/
INFO	Uncommon header 'strict-transport-security' found, with contents: max-age=31536000, includeSubDomains	/
INFO	Uncommon header 'referrer-policy' found, with contents: strict-origin when cross origin	/
INFO	Uncommon header 'x-security-level' found, with contents: Maximum	/
INFO	Server version disclosed in headers	/
INFOSEC	Excellent security headers: X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, X-XSS-Protection	/



c. Pengujian (*tools nikto*) *Website* internet :

- Website 1 (<https://www.pln.co.id>)

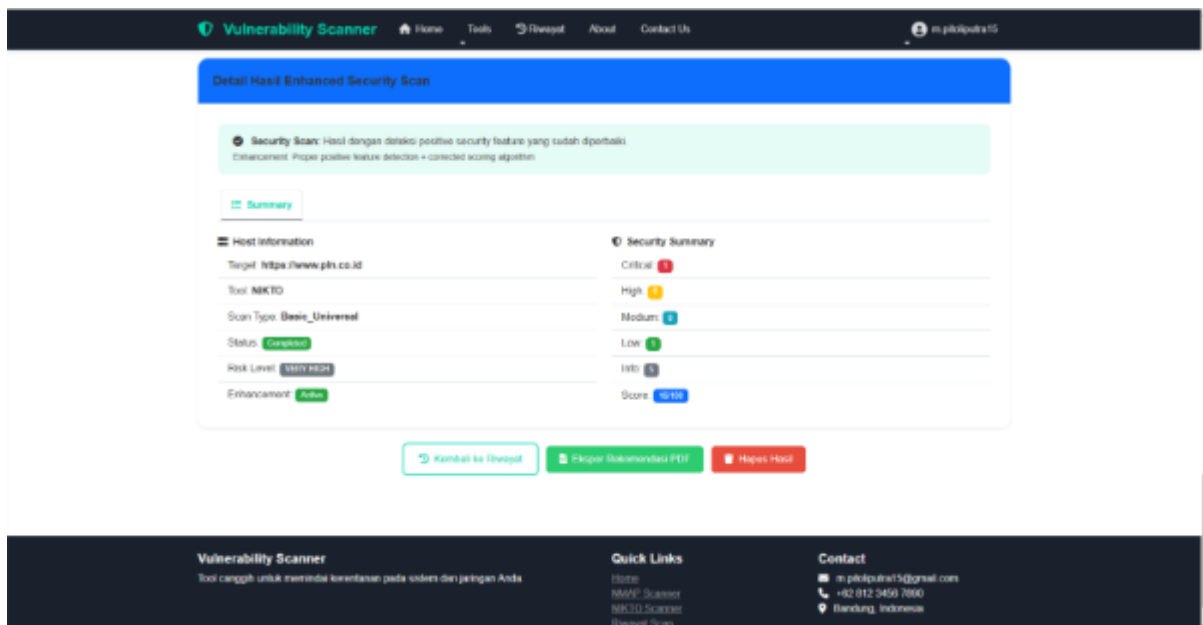
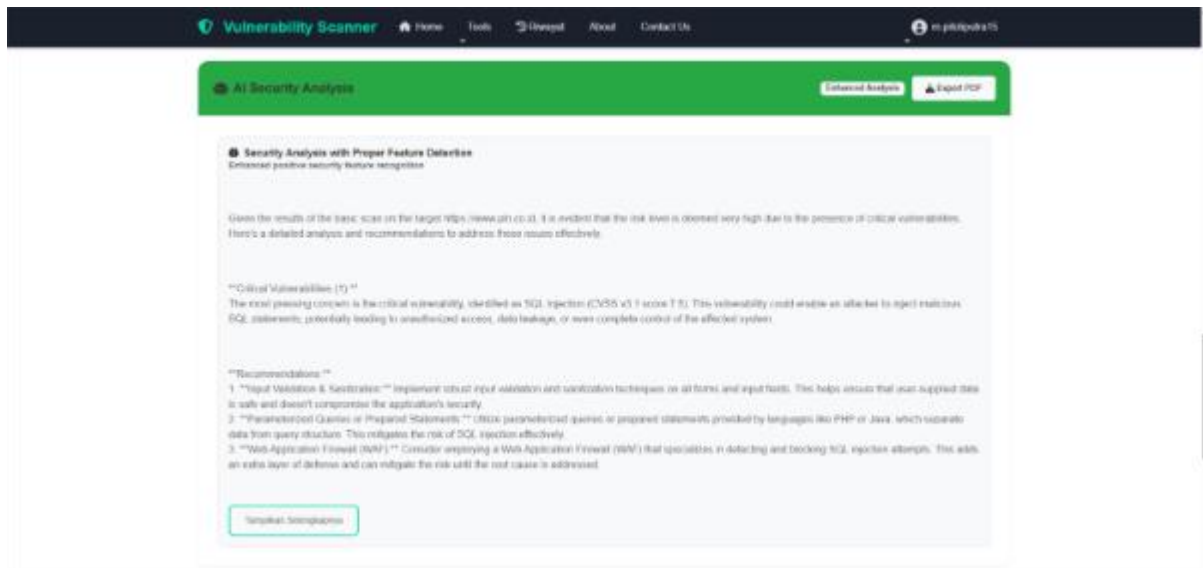


The screenshot displays the 'Analysis Keamanan Detail' window in Burp Suite. It shows a summary of findings: 1 Critical, 0 High, 0 Medium, 1 Low, and 8 Info. Below this, the 'Security Vulnerabilities Detected (NKT0)' section lists two items:

Severity	Type	Description	Location	Status
▲ CRITICAL	Command Injection	Command injection vulnerability detected at /ping	/ping	▲ Exploited
● LOW	Infrastructure Finding	DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/ee659576.aspx for details.	/webui.xicoresoft.com/en-us/library/ee659576.aspx	▲ Exploited

The 'Informational Findings (8)' section notes that these findings provide context but do not represent security vulnerabilities. Below this is a table of findings:

Type	Description	Location
INFO	SSL Info: Subject: CN=*.ipn.co.id	/CN=*.ipn.co.id
INFO	Server: No banner retrieved	/
INFO	Cookie: %5avaaaaaaaaaaaaaaaa_session, created without the httponly flag	/
POSITIVE	Uncommon header 'x-ua-protection' found, with contents: 1, mode=block	/
POSITIVE	Uncommon header 'x-content-type-options' found, with contents: nosniff	/
POSITIVE	Uncommon header 'x-frame-options' found, with contents: SAME-ORIGIN	/
INFO	'robots.txt' retrieved but it does not contain any 'Disallow' entries (which is odd)	/
INFO	Server is using a wildcard certificate: *.ipn.co.id	/



- Website 2 (<http://httpbin.org>)

Vulnerability Scanner

[Home](#)[Tools](#)[Howto](#)[About](#)[Contact Us](#)

m.pitloputra15

Hasil Pemindaian Keamanan

[Howto](#)[Scan Baru](#)

Ringkasan Pemindaan

Target:<http://fdipon.org>

Tool: **Nessus**

Tipe Scan: Basic_Universal

Waktu: 05 Jul 2025, 03:38:08

Total Vulnerabilities: 2

Total Findings: 12

Analysis: **Succeeded**

60

\$kor Keamanan

⚠ Perlu beberapa perbaikan

Risk Level: **MEDIUM**

Vulnerability Scanner Home Tools Reports About Contact Us en.pikiputra15

Diagram Kerentanan

<http://httpbin.org>

Vulnerability Distribution

Severity	Count	Percentage
High	1	14.29%
Medium	2	28.57%
Low	4	57.14%

Breakdown Kerentanan

- ▲ Critical: 0
- High: 1
- Medium: 2
- Low: 4
- i Info: 0

Total Vulnerabilities: 7
Total Findings: 10

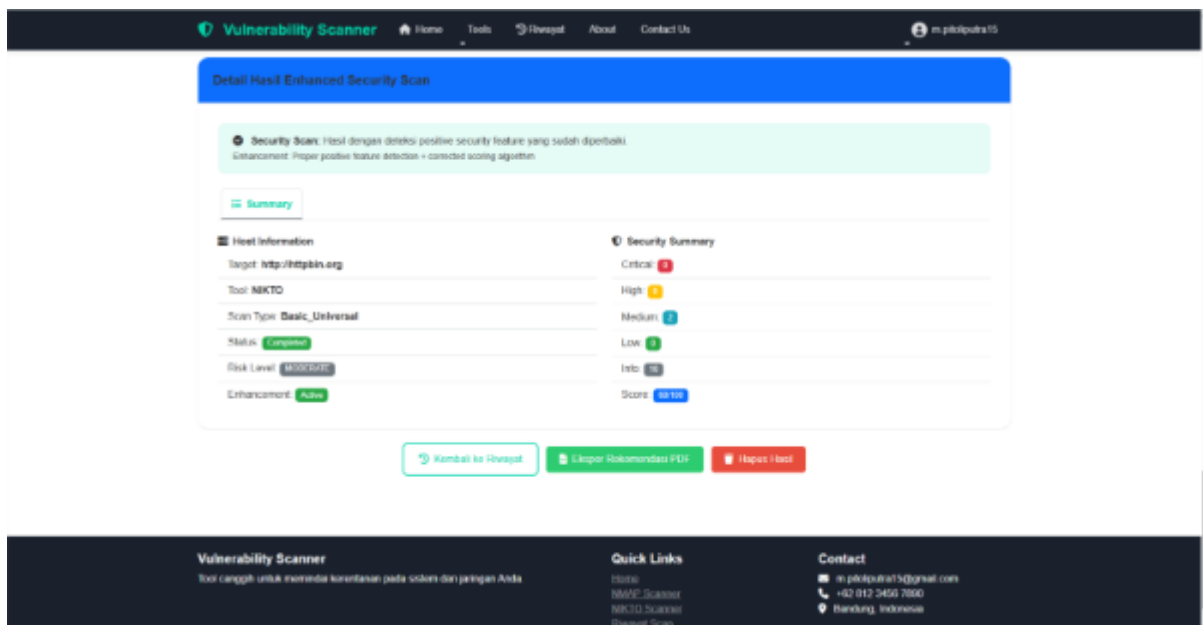
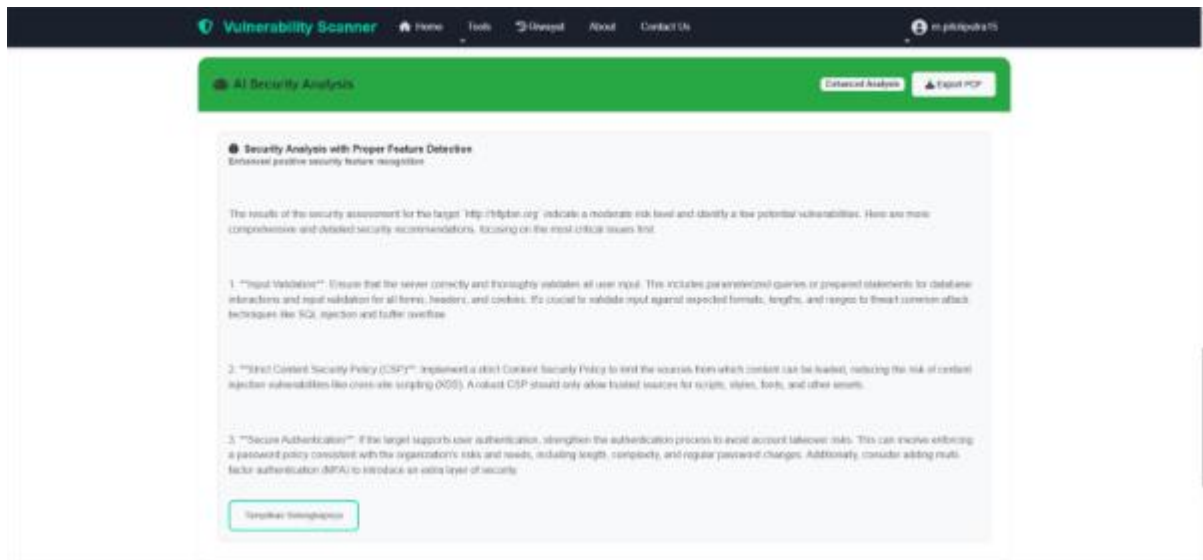
Perhatian: Ditemukan 2 kerentanan pada target <http://httpbin.org>

The screenshot displays the 'Analysis Kasmanan Details' page of the Vulnertool Vulnerability Scanner. The interface is divided into several sections:

- Summary Section:** Shows a total of 10 findings, categorized into 2 security vulnerabilities, 10 informational findings, and 0 high, medium, or low severity items. A note indicates 'Total NIKTO'.
- Security Vulnerabilities Detected (Nikto):** A table listing two detected vulnerabilities:

Severity	Type	Description	Location	Status
High	Infrastructure Finding	Server banner has changed from 'gunicorn/19.9.0' to 'awscli/2.0' which may suggest a WAF, load balancer or proxy is in place	/10.0.0.1	Detected
High	Missing Security Headers	Missing security headers: X-Frame-Options, X-Content-Type-Options, X-XSS-Protection	/	Detected
- Informational Findings (16):** A section indicating that these findings provide context but do not represent security vulnerabilities. Below this is a table of findings:

Type	Description	Location
INFO	Server: gunicorn/19.9.0	/10.0.0.1
INFO	The anti-clickjacking X-Frame-Options header is not present.	/
INFO	Uncommon header 'access-control-allow-origin' found, with contents: *	/
INFO	Uncommon header 'access-control-allow-credentials' found, with contents: true	/
INFO	'robots.txt' contains 1 entry which should be manually viewed.	/
INFO	Server leaks modes via ETags, header found with file: /static/favicon.ico, inode: 32217561900, size: 140182, mtime: 0x4005f10018	/static/favicon.ico
INFO	Uncommon header 'access-control-allow-methods' found, with contents: GET, POST, PUT, DELETE, PATCH, OPTIONS	/
INFO	Uncommon header 'access-control-expose-headers' found, with contents: X-ND	/



- Website 3 (<https://www.komdigi.go.id/>)

Vulnerability Scanner

[Home](#)
[Tools](#)
[Usage](#)
[About](#)
[Contact Us](#)

m.pikipolra15

EXCELLENT SECURITY POSTURE!
✕

Security Score: 100/100 - Outstanding security implementation detected!

Risk Level: VERY LOW

Your system demonstrates exceptional security practices with comprehensive protection mechanisms. Found multiple positive security features!

Hasil Pemindaian Keamanan

[🔄 Ulangi](#)
[🔄 Scan Baru](#)

Ringkasan Pemindaian

Target: <https://www.kondigi.go.id>
Tool: [Nessus](#)
Tipe Scan: Basic, Universal
Waktu: 05 Jul 2025, 03:47:45
Total Vulnerabilities: 0
Total Findings: 0
Analisis: [Selesai](#)

100

Skor Keamanan

Keamanan sangat excellent

Risk Level: [VERY LOW](#)

Vulnerability Scanner Home Tools **Dashboard** About Contact Us en.pikipedia.id

Diagram Kerentanan <https://www.komdigi.go.id>

Vulnerability Distribution

Severity	Count	Percentage
Info	1	100.0%
Low	0	0.0%
Medium	0	0.0%
High	0	0.0%
Critical	0	0.0%

Breakdown Kerentanan

Severity	Count
Critical	0
High	0
Medium	0
Low	0
Info	1

Total Vulnerabilities: 1
Total Findings: 1

Excellent Tidak ada kerentanan keamanan terdeteksi pada target <https://www.komdigi.go.id>.

Vulnerability Scanner Home Tools Helpdesk About Contact Us

Analysis Result Summary Details 0 vulnerabilities 0 info backup

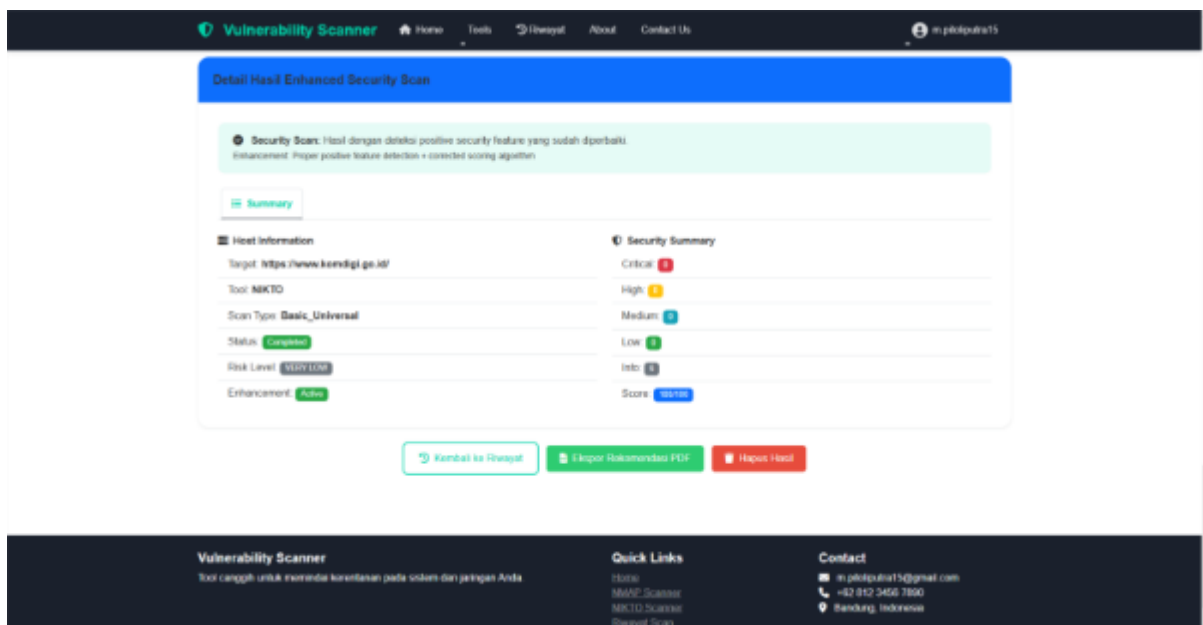
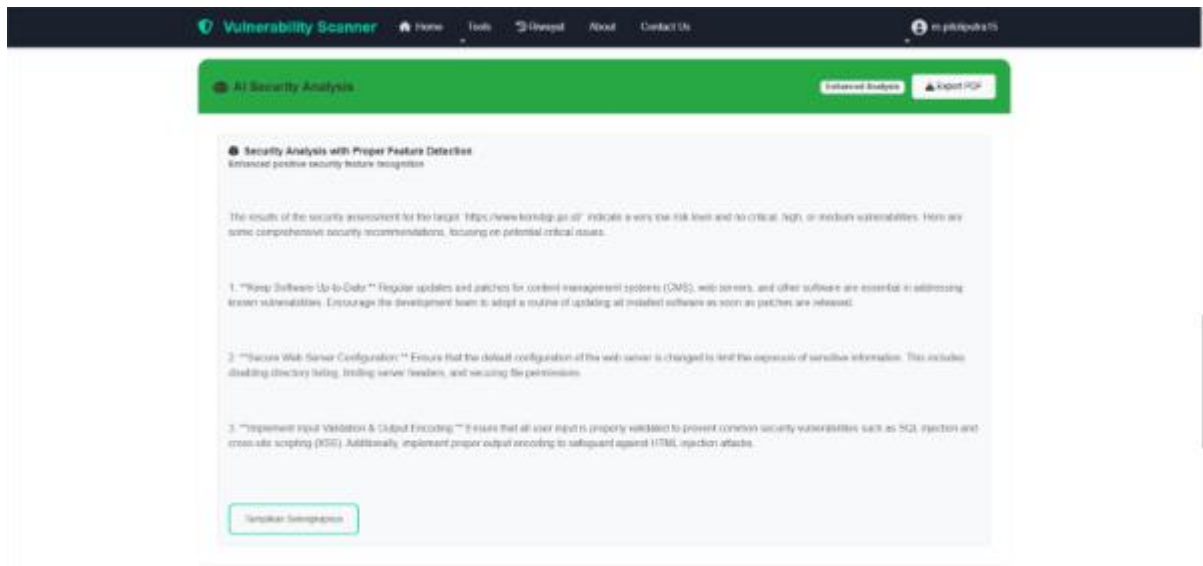
0 Critical 0 High 0 Medium 0 Low 7 Info

0 security vulnerabilities, 7 informational findings detected
Total: 0/0/0

Informational Findings (7)

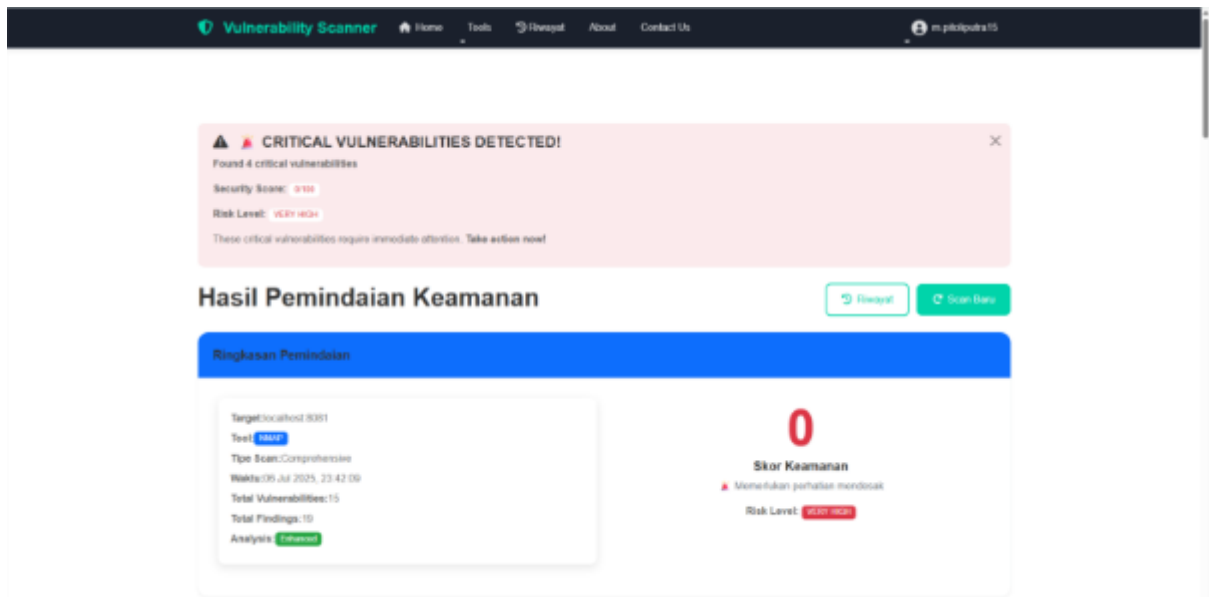
These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	SSL info: Subject: /C=US/ST=Massachusetts/C=Cambridge/A=Acme Technologies, Inc./CN=4240 a domain net	/C=US/ST=Massachusetts/C=Cambridge/A=Acme
INFO	Server: No banner returned	/
INFO	The anti-clickjacking X-Frame-Options header is not present	/
INFO	Uncommon header: x-acme-gmt found, with contents: 0 6798276 1731662040 d048a32	/
INFO	robots.txt returned but it does not contain any 'Disallow' entries (which is odd)	/
INFO	Hostname: www.knowledge.go of does not match certificate's CN '4240 a domain net'	/
PASS	Excellent security headers: X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Content-Security-Policy, Referrer-Policy, X-XSS-Protection	/



d. Pengujian (nmap scanner) *Website* localhost 1 *device*

- *Website* 1 (localhost:8081)



Vulnerability Scanner Home Tools Report About Contact Us m.pikiputra15

Analisis Keamanan Detail 15 vulnerabilities 10 findings

4 Critical 3 High 5 Medium 2 Low 1 Info
10 security vulnerabilities, 4 informational findings detected...
Tool: NMAP

Security Vulnerabilities Detected (NMAP)

Severity	Type	Description	Location	Status
CRITICAL	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
CRITICAL	TELNET Service	Unencrypted telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8012	Port: 8012	Detected
CRITICAL	TCPWRAPPED Service	TCPWRAPPED service detected on port 8013	Port: 8013	Detected
HIGH	Http title Script	Script http title found high severity issue	Port: 8082 HTTP: 12124	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8181	Port: 8181	Detected
HIGH	TCPWRAPPED Service	TCPWRAPPED service detected on port 8188	Port: 8188	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
MEDIUM	POP3 Service	POP3 mail service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
MEDIUM	IMAP Service	IMAP mail service on port 8143 - should use encryption (IMAPS) (MEDIUM)	Port: 8143	Detected

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pitiputra15

46:54:46
SMTP Service
SMTP mail service on port 5825 - ensure proper authentication (MEDIUM)
Port: 5825
Details

46:55:30
HTTP Service
HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)
Port: 8080
Details

47:00:00
http-cookie-flag Script
Script http-cookie-flags found low severity issue
Port: 8080 - http-cookie-flags
Details

47:00:00
http-cookie-flag Script
Script http-cookie-flags found low severity issue
Port: 8080 - http-cookie-flags
Details

Informational Findings (4)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Target host 127.0.0.1 successfully discovered and analyzed	Host Analysis
INFO	14 network services detected and analyzed	Network Services
INFO	Docker analysis: 14 working ports, 9 failed ports detected	Container Environment
INFO	Logic-based scan completed in 14:01 (845.81 seconds)	Performance Analysis

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pitiputra15

AI Security Analysis
Enhanced Analysis
Export PDF

Security Analysis with Proper Feature Detection

Enhanced positive security feature recognition

Critical Vulnerabilities and Immediate Threat Assessment:

- Remote Code Execution (RCE) - CVE-2023-26446:** A remote attacker can exploit improper input validation in the 'url' parameter to execute arbitrary code on the system. This vulnerability poses a severe risk as it allows unauthorized access and potential compromise of the target system.
- SQL Injection - CVE-2023-27049:** A remote attacker can exploit an unprotected SQL query to manipulate the application's database, potentially leading to information disclosure, data tampering, or even full control over the underlying database server.
- Unauthenticated Remote Command Execution - CVE-2023-22912:** The presence of certain files in an accessible directory enables an unauthenticated user to execute arbitrary commands on the server. This could lead to complete system compromise or unauthorized access to sensitive data.
- Information Disclosure - CVE-2023-22913:** Unexpected sensitive information, such as internal files, documentation, and configuration details, is accessible to unauthenticated users. This could expose critical system details and provide an entry point for further attacks.

Scanning Completed

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pitiputra15

Detail Hasil Enhanced Security Scan

Security Scan: Hasil dengan deteksi positive security feature yang sudah diperbaiki.
Enhancement: Proper positive feature detection + corrected scoring algorithm

Summary

Host Information

Target: localhost:8081

Tool: Nmap

Scan Type: Comprehensive

Status: Completed

Risk Level: 1000 (0.00)

Enhancement: Active

Security Summary

Critical: 4

High: 0

Medium: 0

Low: 3

Info: 4

Score: 9/10

Kembali ke Riset

Export Recommended PDF

Hapus Hasil

Vulnerability Scanner
Tool canggih untuk memindai kerentanan pada sistem dan jaringan Anda.

Quick Links
Home
Nmap Scanner
NCCO Scanner
Nmap Scan

Contact
m.pitiputra15@gmail.com
+62 812 3456 7890
Bandung, Indonesia

- Website 2 (localhost:8082)

Vulnerability Scanner

HomeToolsReportsAboutContact Us

m.pikelpuara15

Hasil Pemindaian Keamanan

RecentScan Now

Ringkasan Pemindaian

Target:localhost:8082
Tool:NAAP
Type Scan:Comprehensive
Waktu:07 Jul 2023, 06:49:44
Total Vulnerabilities:5
Total Findings:7
Analysis:Enhanced

54

Skor Keamanan

Perlu beberapa perbaikan

Risk Level:Low

Vulnerability Scanner

HomeToolsReportsAboutContact Us

m.pikelpuara15

Diagram Kerentanan

localhost:8082

Vulnerability Distribution

Medium: 50.0%
Info: 33.3%
High: 16.7%
Low: 0.0%
Info: 0.0%

Breakdown Kerentanan

Critical	0
High	1
Medium	3
Low	2
Info	0

Total Vulnerabilities: 6
Total Findings: 7

Perhatian: Ditemukan 5 kerentanan pada target localhost:8082.

Vulnerability Scanner

HomeToolsReportsAboutContact Us

m.pikelpuara15

Analisis Keamanan Detail

5 vulnerabilities7 info findings

0 Critical0 High3 Medium2 Low2 Info

0 security vulnerabilities, 2 informational findings detected
Tool: NAAP

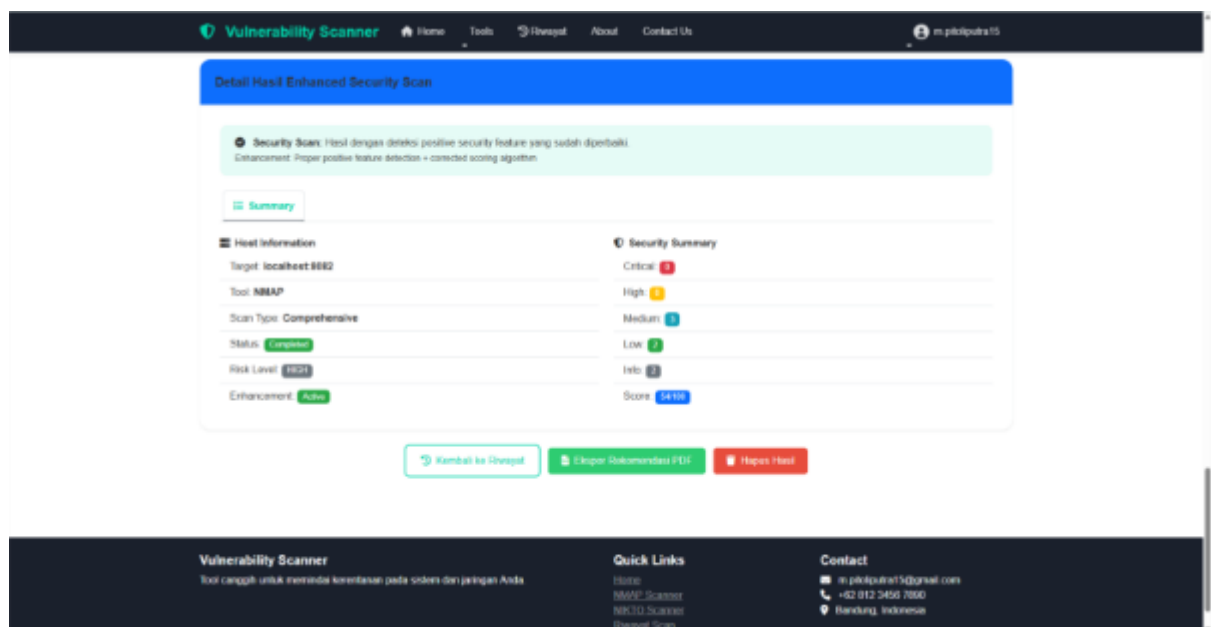
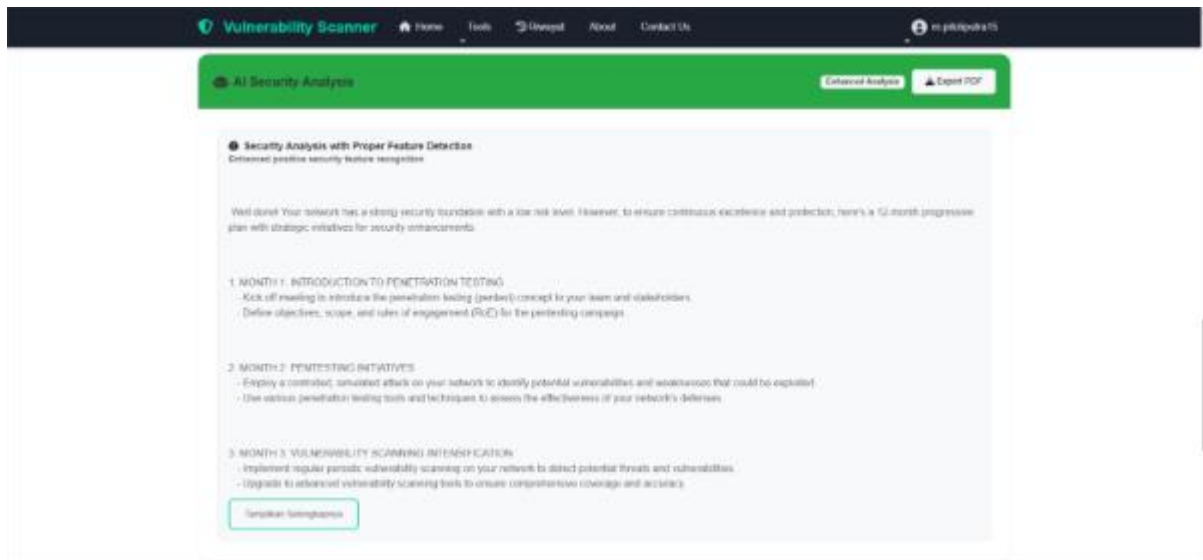
Security Vulnerabilities Detected (NMAP)

Severity	Type	Description	Location	Status
MEDIUM	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8082	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8080	Detected
LOW	http-cookie-flags Script	Script http.cookie-flags found low severity issue	Port: 8082 - http-cookie-flags	Detected
LOW	http-cookie-flags Script	Script http.cookie-flags found low severity issue	Port: 8080 - http-cookie-flags	Detected

Informational Findings (2)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Medium target successfully analyzed with 4 services detected	Medium Environment
INFO	Target specific scan for medium completed in 13.11	Scan Metrics



- Website 3 (localhost:8083)

Vulnerability Scanner

[Home](#)
[Tools](#)
[Usage](#)
[About](#)
[Contact Us](#)

m.pikiputra15

EXCELLENT SECURITY POSTURE!
×

Security Score: 100/100 - Outstanding security implementation detected!

Risk Level: VERY LOW

Your system demonstrates exceptional security practices with comprehensive protection mechanisms. Found multiple positive security features!

Hasil Pemindaian Keamanan

Download
 Scan Now

Ringkasan Pemindaian

Target: localhost:8080
Tool: OWASP
Type: Scan: Comprehensive
Waktu: 07 Jul 2025, 08:58:00
Total Vulnerabilities: 0
Total Findings: 2
Analysis: Completed

100

Skor Keamanan

Keamanan sangat excellent

Risk Level: VERY LOW

Vulnerability Scanner Home Tools Report About Contact Us en.pikipedia.id

1 Diagram Kerentanan localhost:8080

Vulnerability Distribution

Severity	Count	Percentage
Critical	100	100.0%
High	0	0.0%
Medium	0	0.0%
Low	0	0.0%
Info	0	0.0%

Breakdown Kerentanan

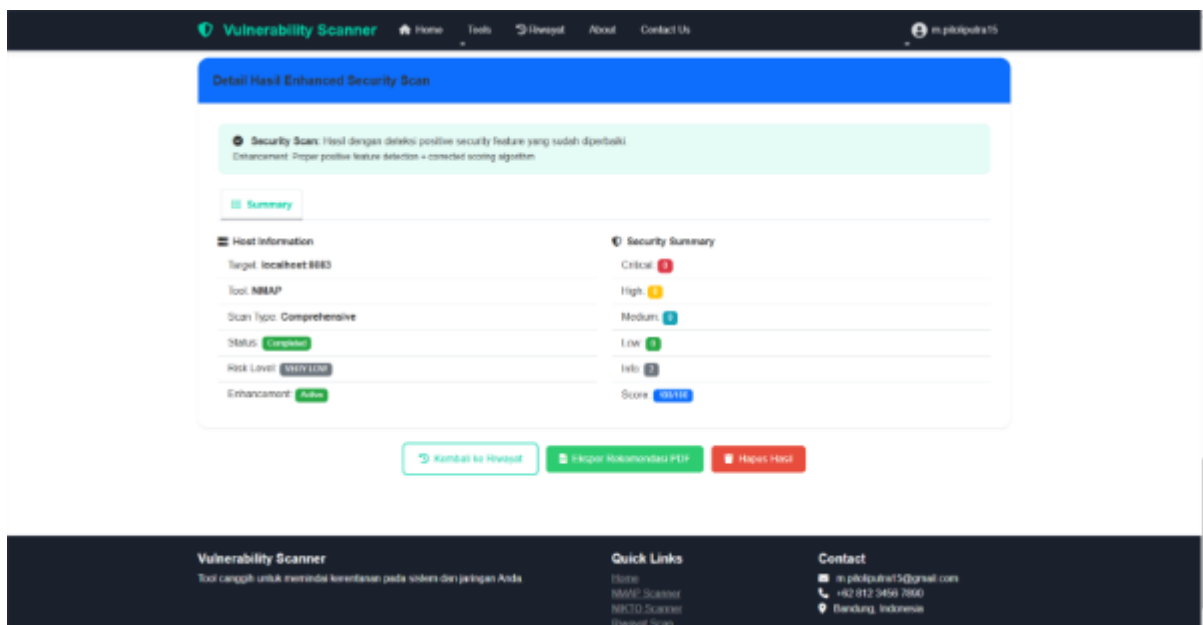
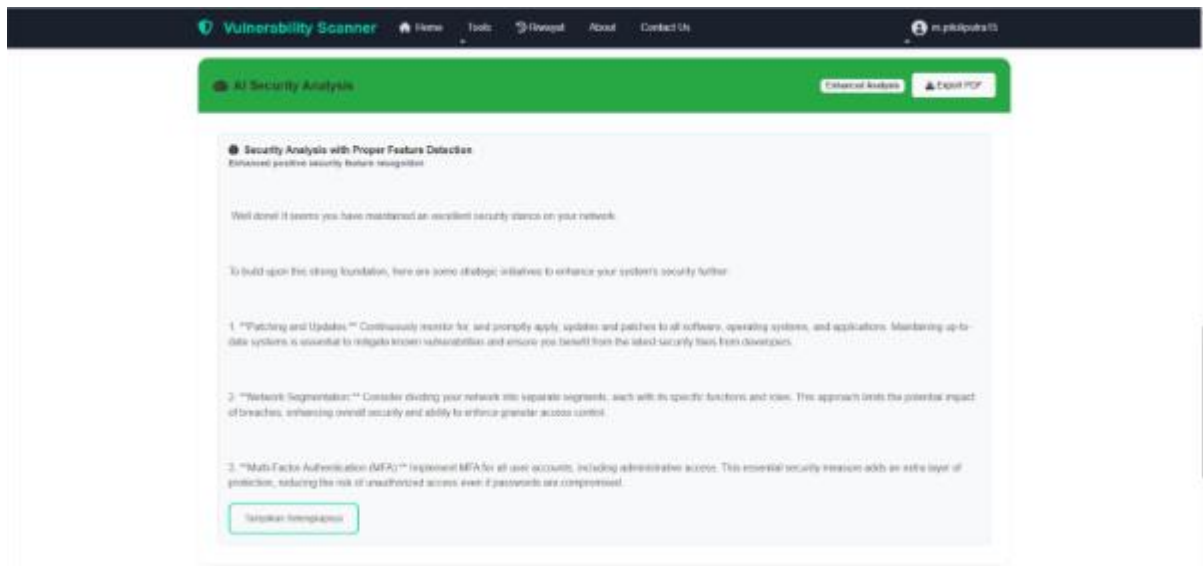
- Critical: 100
- High: 0
- Medium: 0
- Low: 0
- Info: 0

Total Vulnerabilities: 100
Total Findings: 100

Excellent! Tidak ada kerentanan keamanan terdeteksi pada target localhost:8080.

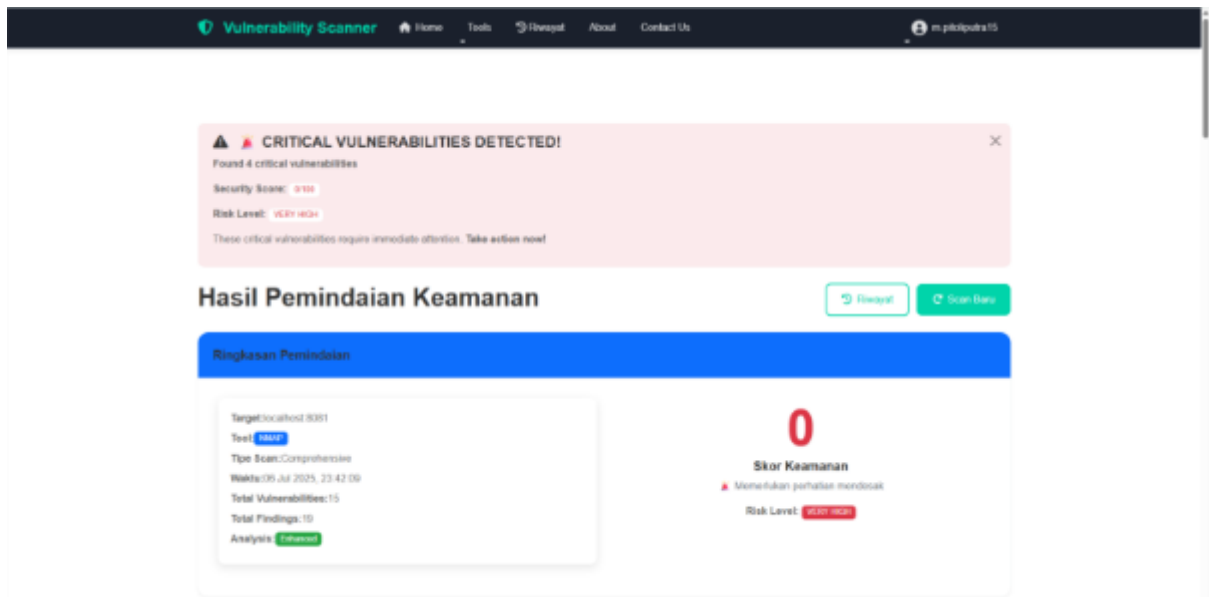
The screenshot displays the 'Vulnerability Scanner' interface. At the top, there's a navigation bar with links: Home, Tools, Report, About, and Contact Us. The main header shows 'Analysis Kasmanan Details' with a sub-header '0 vulnerabilities' and a link to 'Info Findings'. Below this, a summary row shows counts for severity levels: 0 Critical (red triangle), 0 High (red circle), 0 Medium (yellow circle), 0 Low (green circle), and 2 Info (blue square). A note states: '0 security vulnerabilities, 2 informational findings detected Tool: NMAP'. Under the 'Informational Findings (2)' section, a message reads: 'These findings provide context but do not represent security vulnerabilities.' A table follows with two findings:

Type	Description	Location
INFO	Secure target successfully analyzed with 2 services detected	Secure Environment
INFO	Target specific scan for secure completed in 00:01	Scan Metrics



e. Pengujian (*tools* nmap) *Website* localhost beda *device*

- *Website* 1 (localhost:8081)



The screenshot shows the 'Analisis Kerentanan Detail' (Detailed Vulnerability Analysis) for 'localhost:8081'. It displays a table of detected security vulnerabilities, categorized by severity (Critical, High, Medium, Low, Info).

Severity	Type	Description	Location	Status
Critical	FTP Service	Unencrypted FTP service on port 8021 - credentials transmitted in plaintext (CRITICAL)	Port: 8021	Detected
Critical	TELNET Service	Unencrypted telnet service on port 8023 - all data transmitted in plaintext (CRITICAL)	Port: 8023	Detected
Critical	TCPWRAPPED Service	TCPWRAPPED service detected on port 8032	Port: 8032	Detected
Critical	TCPWRAPPED Service	TCPWRAPPED service detected on port 8033	Port: 8033	Detected
High	Http title Script	Script http title found high severity issue	Port: 8082 - HTTP-12024	Detected
High	TCPWRAPPED Service	TCPWRAPPED service detected on port 8181	Port: 8181	Detected
High	TCPWRAPPED Service	TCPWRAPPED service detected on port 8388	Port: 8388	Detected
Medium	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port: 8025	Detected
Medium	HTTP Service	HTTP service on port 8081 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 8081	Detected
Medium	POP3 Service	POP3 mail service on port 8110 - should use encryption (POP3S) (MEDIUM)	Port: 8110	Detected
Medium	IMAP Service	IMAP mail service on port 8142 - should use encryption (IMAPS) (MEDIUM)	Port: 8142	Detected

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pitiputra15

46:54:46
SMTP Service
SMTP mail service on port 5825 - ensure proper authentication (MEDIUM)
Port: 5825
Details

46:55:30
HTTP Service
HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)
Port: 8080
Details

47:00:00
http-cookie-flag Script
Script http-cookie-flags found low severity issue
Port: 8080 - http-cookie-flags
Details

47:00:00
http-cookie-flag Script
Script http-cookie-flags found low severity issue
Port: 8080 - http-cookie-flags
Details

Informational Findings (4)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Target host 127.0.0.1 successfully discovered and analyzed	Host Analysis
INFO	14 network services detected and analyzed	Network Services
INFO	Docker analysis: 14 working ports, 9 failed ports detected	Container Environment
INFO	Logic-based scan completed in 14:01 (841.81 seconds)	Performance Analysis

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pitiputra15

AI Security Analysis
Enhanced Analysis
Export PDF

Security Analysis with Proper Feature Detection
Enhanced positive security feature recognition

Critical Vulnerabilities and Immediate Threat Assessment:

- Remote Code Execution (RCE) - CVE-2023-26446:** A remote attacker can exploit improper input validation in the 'url' parameter to execute arbitrary code on the system. This vulnerability poses a severe risk as it allows unauthorized access and potential compromise of the target system.
- SQL Injection - CVE-2023-27049:** A remote attacker can exploit an unprotected SQL query to manipulate the application's database, potentially leading to information disclosure, data tampering, or even full control over the underlying database server.
- Unauthorized Remote Command Execution - CVE-2023-22912:** The presence of certain files in an accessible directory enables an unauthorized user to execute arbitrary commands on the server. This could lead to complete system compromise or unauthorized access to sensitive data.
- Information Disclosure - CVE-2023-22913:** Unexpected sensitive information, such as internal files, documentation, and configuration details, is accessible to unauthorized users. This could expose critical system details and provide an entry point for further attacks.

Scanning Completed

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pitiputra15

Detail Hasil Enhanced Security Scan

Security Scan: Hasil dengan deteksi positive security feature yang sudah diperbaiki.
Enhancement: Proper positive feature detection + corrected scoring algorithm

Summary

Host Information
Target: localhost:8081
Tool: Nmap
Scan Type: Comprehensive
Status: Completed
Risk Level: 1000 (0.00)
Enhancement: Active

Security Summary
Critical: 4
High: 2
Medium: 0
Low: 3
Info: 4
Score: 9/10

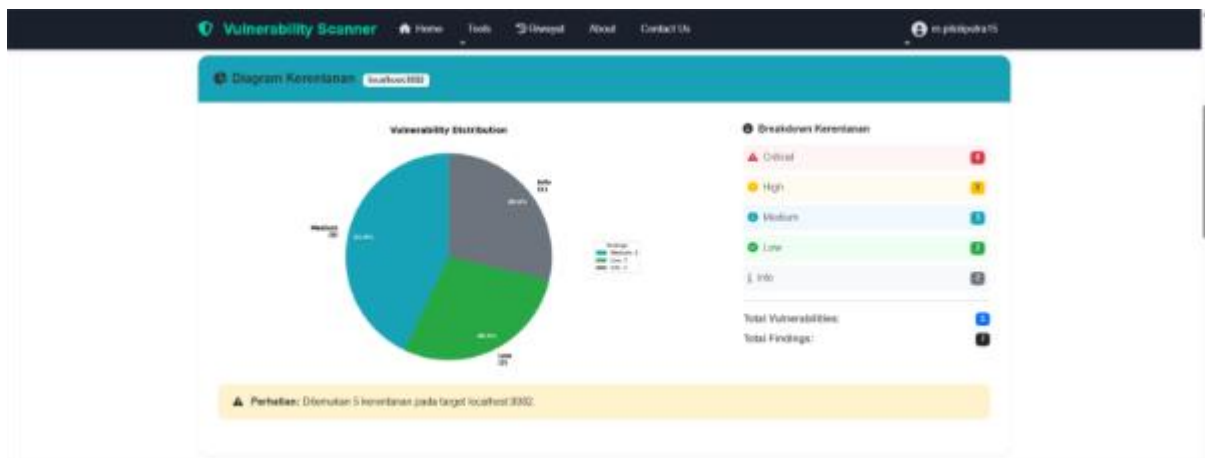
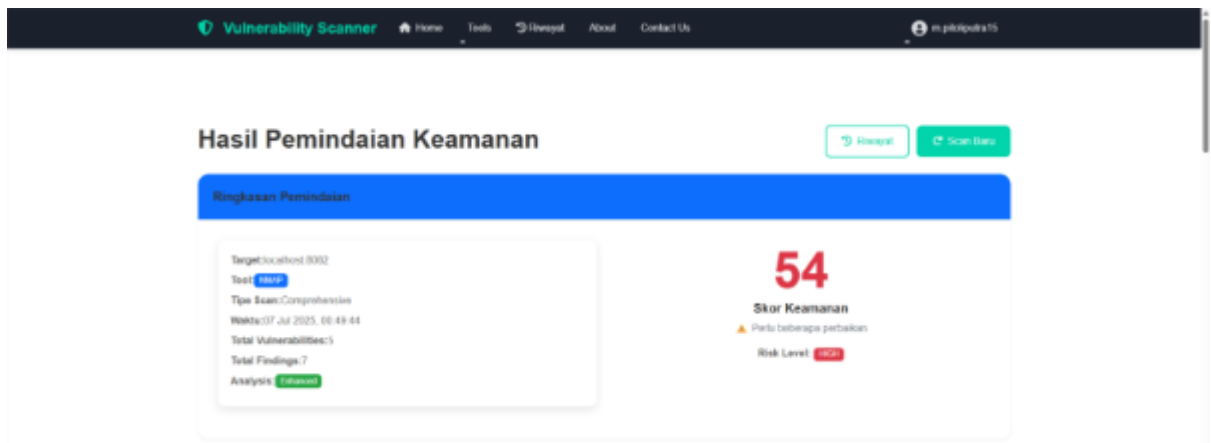
Kembali ke Riset
Export Recommended PDF
Hapus Hasil

Vulnerability Scanner
Tool canggih untuk memindai kerentanan pada sistem dan jaringan Anda.

Quick Links
Home
NMAP Scanner
NCCO Scanner
Nmap Script

Contact
m.pitiputra15@gmail.com
+62 812 3456 7890
Bandung, Indonesia

- *Website 2* (localhost:8082)



Vulnerability Scanner Home Tools / Reveal All About Contact Us im.pildiputra15

Analysis Keenan Detail

3 vulnerabilities 2 Info Settings

0 Critical 0 High 3 Medium 2 Low 2 Info

3 security vulnerabilities, 2 informational findings detected
Tool: NMAP

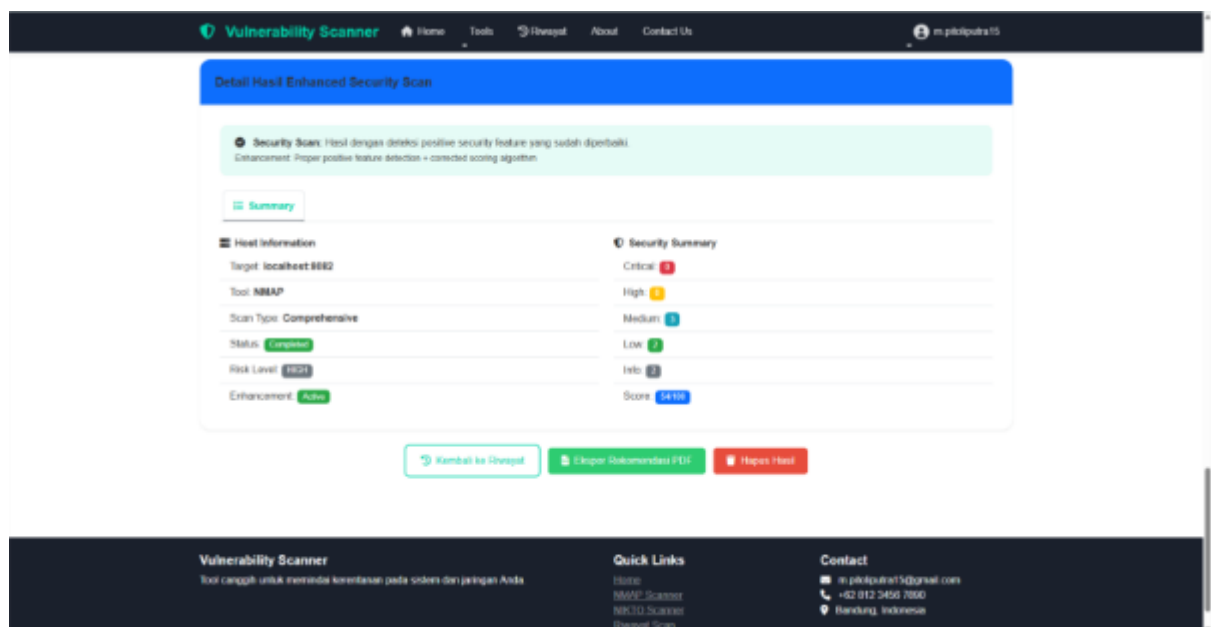
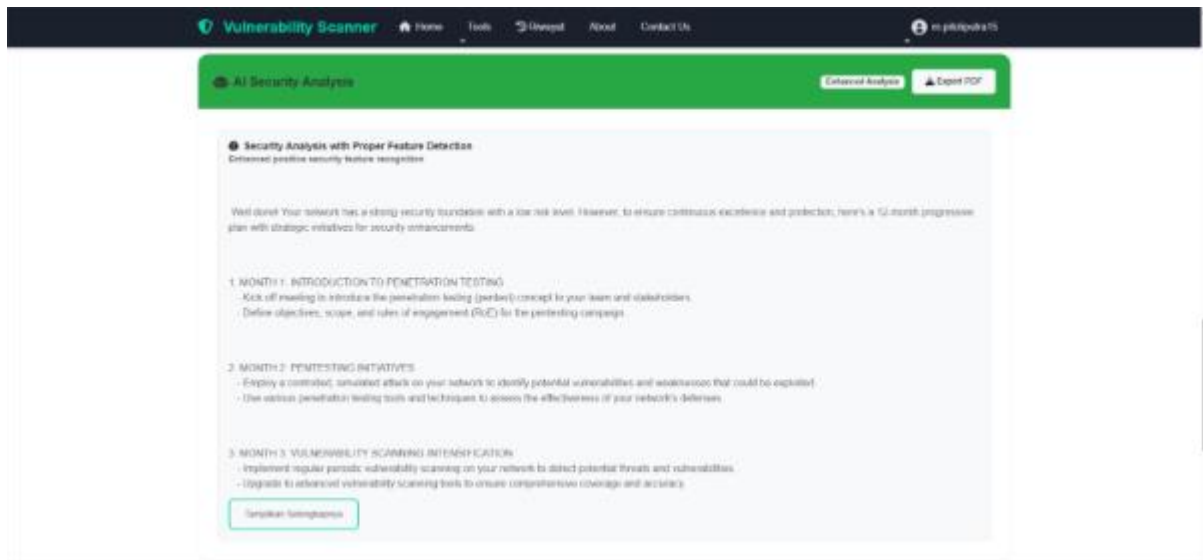
Security Vulnerabilities Detected (NMAP)

Severity	Type	Description	Location	Status
MEDIUM	HTTP Service	HTTP service on port 8082 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 8082	Detected
MEDIUM	SMTP Service	SMTP mail service on port 8025 - ensure proper authentication (MEDIUM)	Port 8025	Detected
MEDIUM	HTTP Service	HTTP service on port 8080 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port 8080	Detected
LOW	Http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port 8082 - http-cookie-flags	Detected
LOW	Http-cookie-flags Script	Script http-cookie-flags found low severity issue	Port 8080 - http-cookie-flags	Detected

Informational Findings (2)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Medium target successfully analyzed with 4 services detected	Medium Environment
INFO	Target specific scan for mediums completed in 13.11	Scan Metrics



- Website 3 (localhost:8083)

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pikiputra15

EXCELLENT SECURITY POSTURE!
Security Score: 100/100 - Outstanding security implementation detected!
Risk Level: VERY LOW
Your system demonstrates exceptional security practices with comprehensive protection mechanisms. Found multiple positive security features!
Reset Scan New

Hasil Pemindaian Keamanan

Ringkasan Pemindaian

Target: localhost:8083
Tool: NMAP
Type Scan: Comprehensive
Waktu: 07 Jul 2025, 00:58:00
Total Vulnerabilities: 0
Total Findings: 2
Analysis: Success

100
Skor Keamanan
Keamanan sangat excellent
Risk Level: VERY LOW

Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pikiputra15

Diagram Kerentanan
localhost:8083

Vulnerability Distribution

Breakdown Kerentanan
Critical 0
High 0
Medium 0
Low 0
Info 2
Total Vulnerabilities: 0
Total Findings: 2

Excellent! Tidak ada kerentanan keamanan terdeteksi pada target localhost:8083.

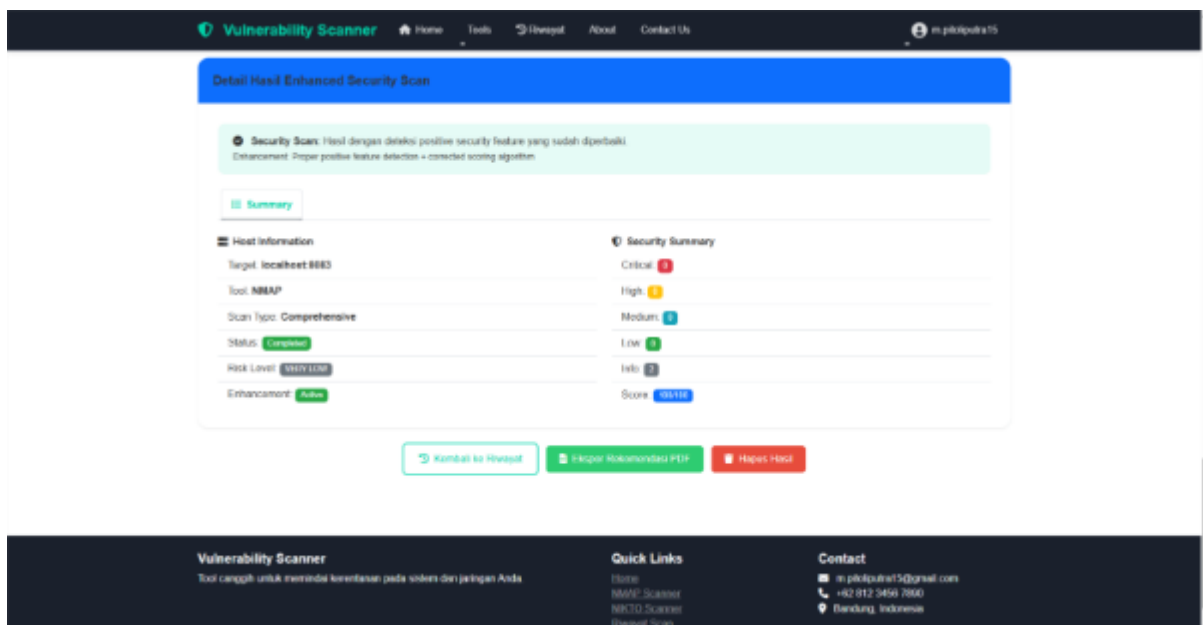
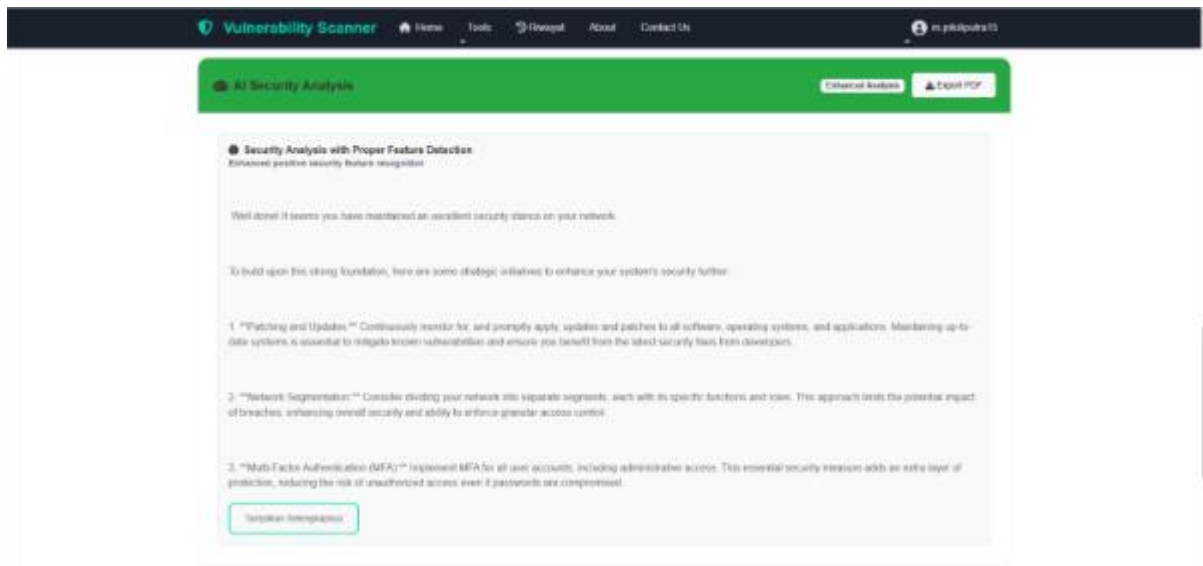
Vulnerability Scanner
Home
Tools
Dashboard
About
Contact Us
m.pikiputra15

Analysis Keamanan Detail
0 vulnerabilities 2 Info Findings

0 Critical 0 High 0 Medium 0 Low 2 Info
0 security vulnerabilities, 2 informational findings detected
Tool: NMAP

Informational Findings (2)
These findings provide context but do not represent security vulnerabilities.

Type Description Location
INFO Secure target successfully analyzed with 2 services detected Secure Environment
INFO Target-specific scan for secure completed in 00:01 Scan Metrics



f. Pengujian (tools Nmap) Website internet

- Website 1 (scanme.nmap.org)

Vulnerability Scanner Home Tools Download About Contact Us m.piliputra15

CRITICAL VULNERABILITIES DETECTED!
Found 2 critical vulnerabilities
Security Score: 0/100
Risk Level: CRITICAL
These critical vulnerabilities require immediate attention. Take action now!

Hasil Pemindaian Keamanan [Download] [Scan Again]

Ringkasan Pemindaian

Target: scanme.nmap.org
Tool: Nmap
Type Scan: Comprehensive
Waktu: 07 Jul 2025, 19:38:34
Total Vulnerabilities: 7
Total Findings: 5
Analysis: [Download]

0
Skor Keamanan
Menandakan performa mendalam
Risk Level: CRITICAL



Vulnerability Scanner Home Tools Download About Contact Us m.piliputra15

Analisis Kerentanan Detail [Vulnerabilities] [Info Findings]

2 Critical 1 High 2 Medium 3 Low 2 Info
7 security vulnerabilities, 5 informational findings detected
Tool: NMAP

Security Vulnerabilities Detected (NMAP)

Severity	Type	Description	Location	Status
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 22 - vulners	Detected
CRITICAL	vulners Script	Script vulners found critical severity issue	Port 80 - vulners	Detected
MEDIUM	http-comments-displayer Script	Script http-comments-displayer found medium severity issue	Port 80 - http-comments-displayer	Detected
MEDIUM	HTTP Service	HTTP service on port 80 - unencrypted web traffic, recommended HTS (SSL/TLS)	Port 80	Detected
LOW	http-sitemap-generator Script	Script http-sitemap-generator found low severity issue	Port 80 - http-sitemap-generator	Detected
LOW	http-security-headers Script	Script http-security-headers found low severity issue	Port 80 - http-security-headers	Detected
LOW	http-headers Script	Script http-headers found low severity issue	Port 80 - http-headers	Detected

Informational Findings (2)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Unknown target successfully assigned with 3 services detected	Unknown Environment
INFO	Target-specific scan for unknowns completed in 02:50	Scan Results

Vulnerability Scanner
Home
Tools
Reports
About
Contact Us
m.pitiputra15

AI Security Analysis
Enhanced Analysis
Export PDF

Security Analysis with Proper Feature Detection

Enhance positive security feature recognition

Critical Vulnerabilities:

1. **"SSH brute force"** (CVSS 4.3 7.3) - The remote system allows for SSH password based authentication, which enables attackers to attempt authentication with commonly used passwords and potentially gain remote code execution without authentication. This issue can be resolved by disabling plain SSH password authentication and allowing only key based authentication.
2. **"HTTP Header Injection"** (CVSS 4.3 7.3) - The remote web server responds to HTTP requests with a "Content Length" header that potentially allows an attacker to craft malicious requests and cause the application to consume excessive resources, potentially leading to remote code execution. This issue can be resolved by ensuring that the application properly validates, sanitizes, or removes the input headers to prevent header injection.

"IMMEDIATE THREAT MITIGATION"

Kembalikan Ke Ringkasan

Vulnerability Scanner
Home
Tools
Reports
About
Contact Us
m.pitiputra15

Detail Hasil Enhanced Security Scan

Security Scan: Hasil dengan deteksi positive security feature yang sudah diperbaiki.

Enhancement: Proper positive feature detection + corrected scoring algorithm

Summary

Host Information

Target: scanme.nmap.org
Tool: NMAP
Scan Type: Comprehensive
Status: Completed
Risk Level: VERY HIGH
Enhancement: Active

Security Summary

Critical: 2
High: 1
Medium: 3
Low: 1
Info: 2
Score: 995

Kembali ke Report
Export Rekomendasi PDF
Hapus Hasil

Vulnerability Scanner
Tool canggih untuk memindai kerentanan pada sistem dan jaringan Anda.

Quick Links
Home
NMAP Scanner
NFOD Scanner
Report Scan

Contact
m.pitiputra15@gmail.com
+62 812 3456 7890
Bandung, Indonesia

151

- Website 2 (neverssl.com)

Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra15

VERY GOOD SECURITY!

Security Score: 80/100 - Strong security implementation

Risk Level: **LOW**

Your system has strong security practices with only minor issues to address.

Hasil Pemindaian Keamanan [Report](#) [Scan Baru](#)

Ringkasan Pemindaian

Target: neverssl.com

Tool: **NMAP**

Type Scan: Comprehensive

Waktu: 09 Jul 2025, 06:10:51

Total Vulnerabilities: 1

Total Findings: 3

Analysis: **Success**

80

Skor Keamanan

Keamanan sangat baik

Risk Level: **LOW**

Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra15

Diagram Kerentanan [neverssl.com](#)

Vulnerability Distribution

Breakdown Kerentanan

- Critical** 0
- High** 1
- Medium** 1
- Low** 1
- Info** 2

Total Vulnerabilities: 3

Total Findings: 3

Perhatian: Ditemukan 1 kerentanan pada target neverssl.com

Vulnerability Scanner Home Tools **Report** About Contact Us m.pikiputra15

Analisis Keamanan Detail [1 vulnerability](#) [3 info findings](#)

0 Critical

0 High

1 Medium

0 Low

2 Info

1 security vulnerabilities, 2 informational findings detected

Tool: NMAP

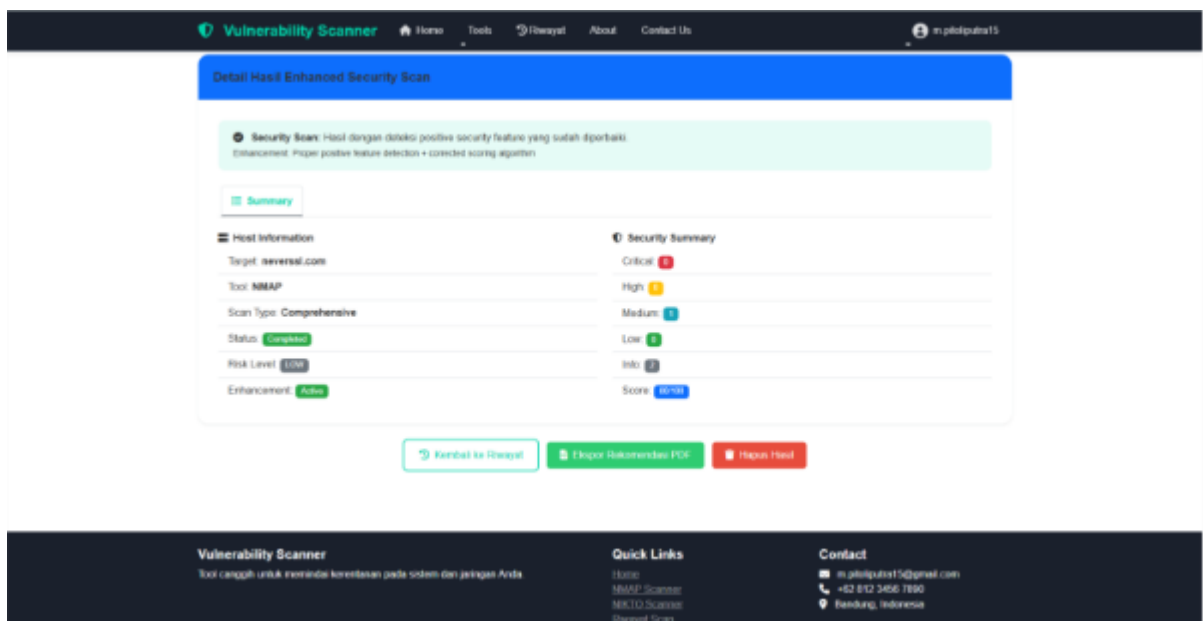
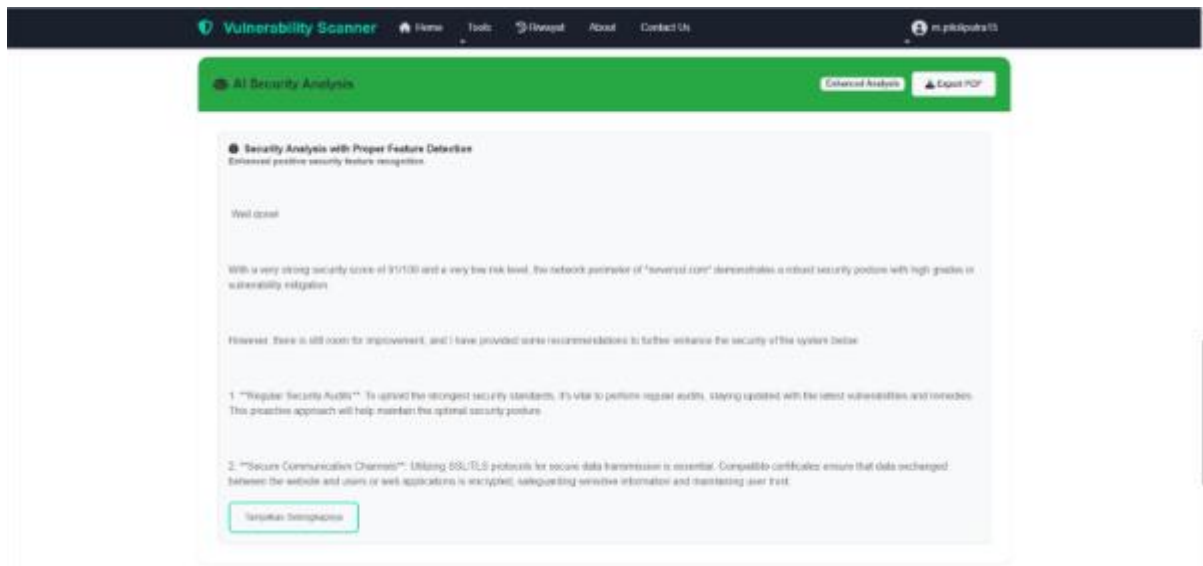
Security Vulnerabilities Detected (NMAP)

Severity	Type	Description	Location	Status
High	HTTP Service	HTTP service on port 443 - unencrypted web traffic, recommend HTTPS (MEDIUM)	Port: 443	Detected

Informational Findings (2)

These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	Unknown target successfully analyzed with 2 services detected	Unknown Environment
INFO	Target-specific scan for unknown completed in 00:05	Scan Metrics



- Website 3 (www.detik.com)

Vulnerability Scanner Home Tools **Overview** About Contact Us m.pikiputra15

EXCELLENT SECURITY POSTURE!

Security Score: 100/100 - Outstanding security implementation detected!

Risk Level: **VERY LOW**

Your system demonstrates exceptional security practices with comprehensive protection mechanisms. Found multiple positive security features!

Hasil Pemindaian Keamanan

Ringkasan Pemindaian

Target: www.detik.com

Tool: **Nmap**

Type Scan: Comprehensive

Waktu: 05 Jul 2025, 16:12:23

Total Vulnerabilities: 0

Total Findings: 4

Analysis: **Excellent**

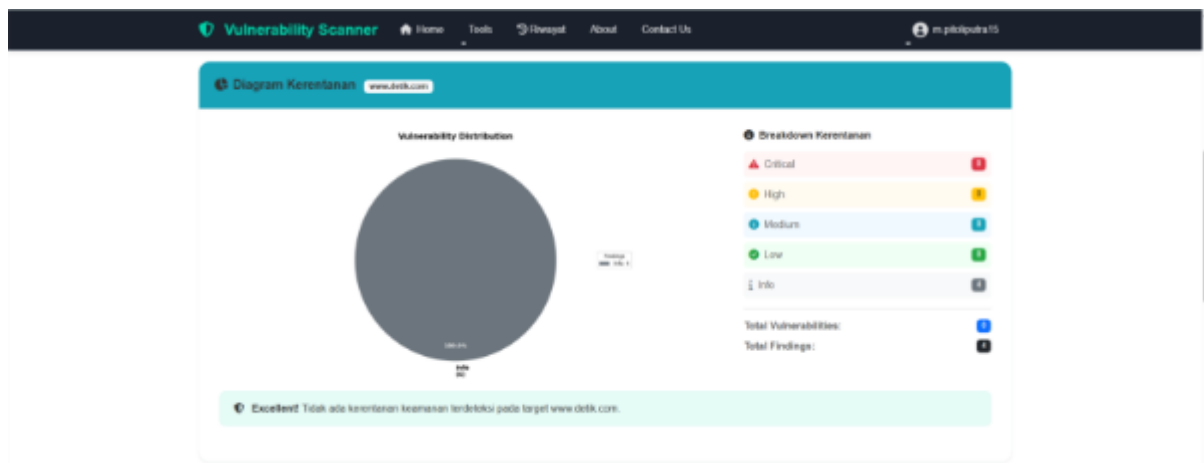
100

Skor Keamanan

Keamanan target excellent

Risk Level: **VERY LOW**

[Refresh](#) [Scan Baru](#)



Vulnerability Scanner Home Tools **Overview** About Contact Us m.pikiputra15

Analisa Keamanan Detail

0 vulnerabilities 4 info findings

0 Critical 0 High 0 Medium 0 Low 2 Info

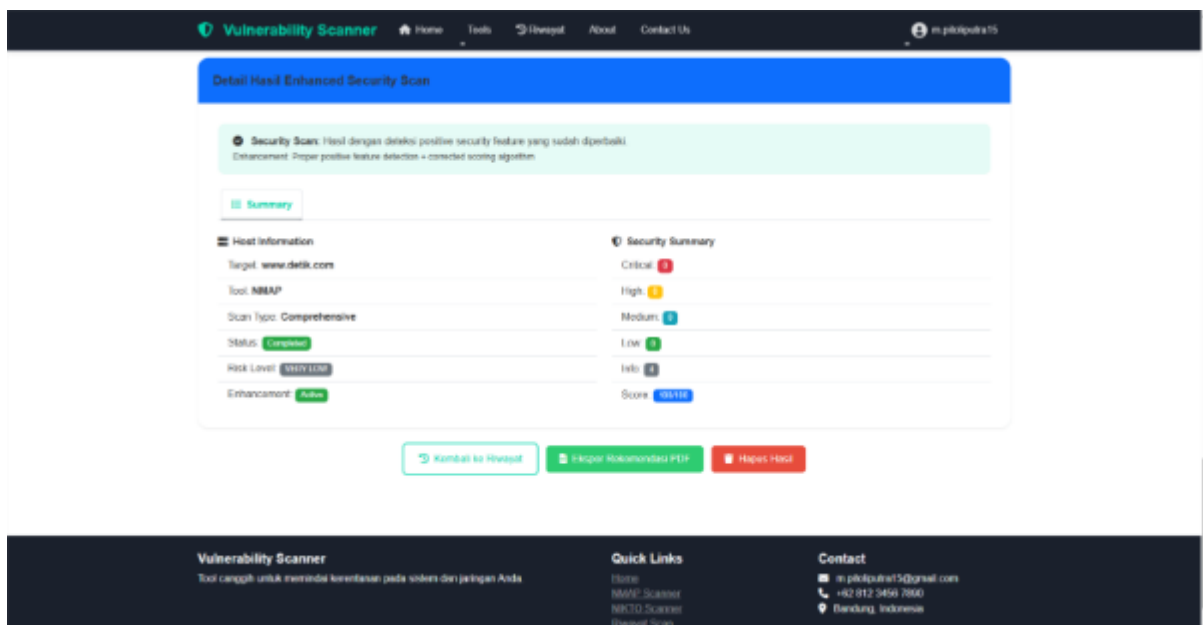
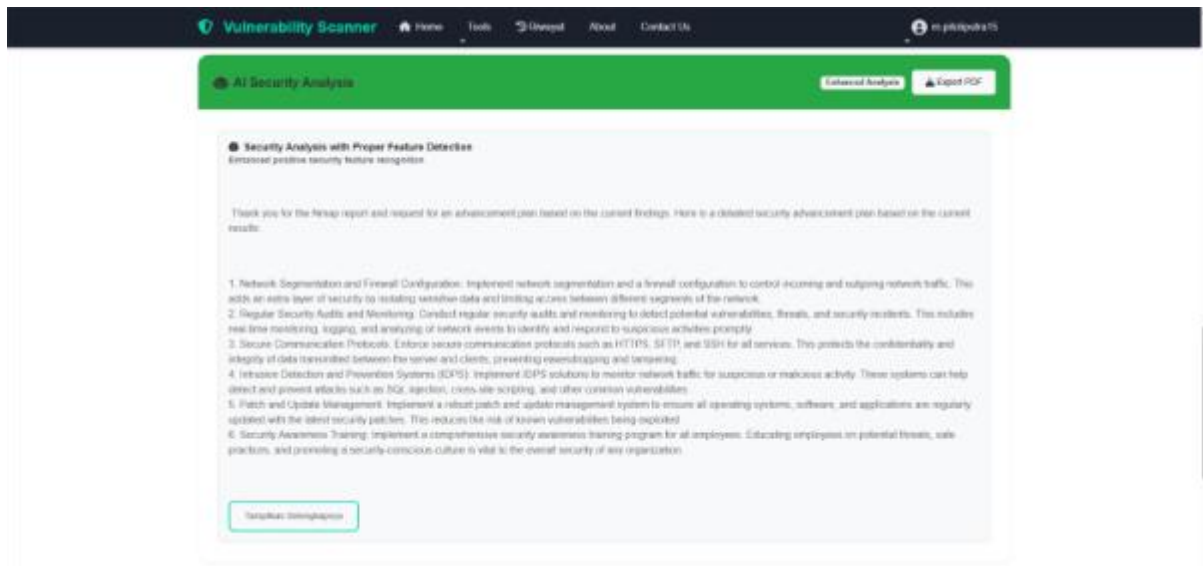
0 security vulnerabilities, 2 informational findings detected

Tool: Nmap

Informational Findings (2)

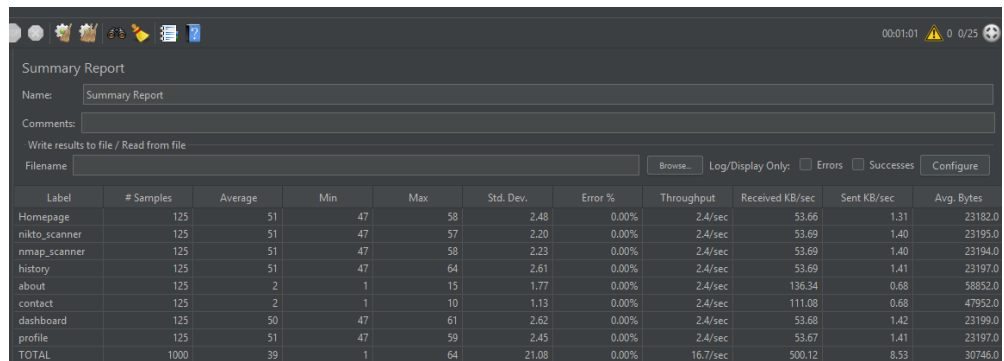
These findings provide context but do not represent security vulnerabilities.

Type	Description	Location
INFO	No open ports detected - target may be behind firewall or using anti-scan protection	Port Scanning
INFO	Target host 203.190.242.211 successfully discovered and analyzed	Host Analysis



g. Pengujian menggunakan apache JMeter

- Pengujian 1



Summary Report

Name: Summary Report

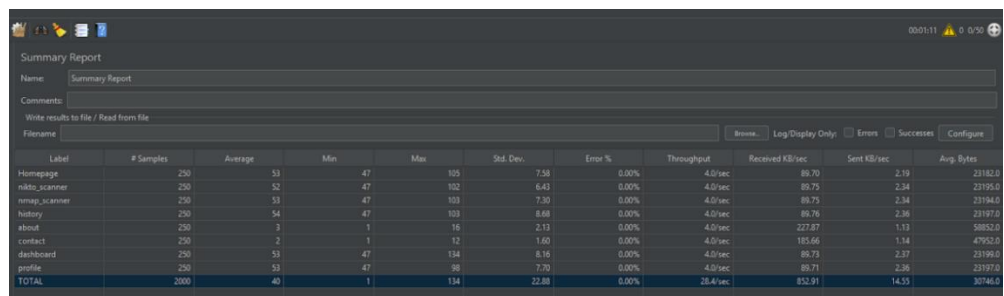
Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: ☐ Errors ☐ Successes

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Homepage	125	51	47	58	2.48	0.00%	2.4/sec	53.66	1.31	23182.0
nikto_scanner	125	51	47	57	2.20	0.00%	2.4/sec	53.69	1.40	23195.0
nmap_scanner	125	51	47	58	2.23	0.00%	2.4/sec	53.69	1.40	23194.0
history	125	51	47	64	2.61	0.00%	2.4/sec	53.69	1.41	23197.0
about	125	2	1	15	1.77	0.00%	2.4/sec	136.34	0.68	58852.0
contact	125	2	1	10	1.13	0.00%	2.4/sec	111.08	0.68	47952.0
dashboard	125	50	47	61	2.62	0.00%	2.4/sec	53.68	1.42	23199.0
profile	125	51	47	59	2.45	0.00%	2.4/sec	53.67	1.41	23197.0
TOTAL	1000	39	1	64	21.08	0.00%	16.7/sec	500.12	8.53	30746.0

- Pengujian 2



Summary Report

Name: Summary Report

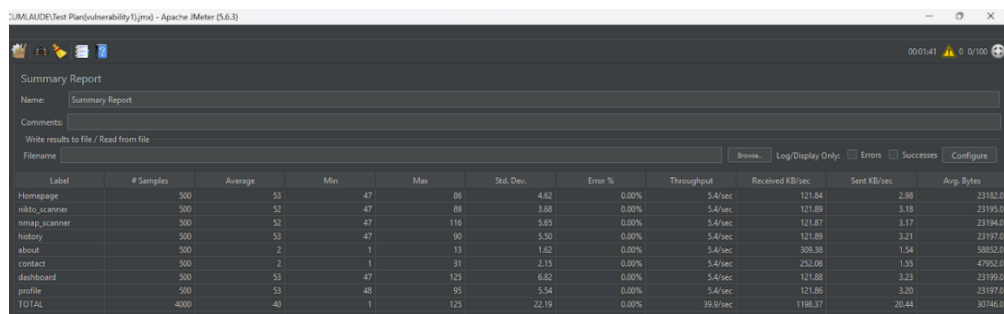
Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: ☐ Errors ☐ Successes

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Homepage	250	53	47	103	7.58	0.00%	4.0/sec	89.70	2.19	23182.0
nikto_scanner	250	52	47	102	6.43	0.00%	4.0/sec	89.75	2.34	23195.0
nmap_scanner	250	53	47	103	7.30	0.00%	4.0/sec	89.75	2.34	23194.0
history	250	54	47	103	8.68	0.00%	4.0/sec	89.76	2.36	23197.0
about	250	3	1	16	2.13	0.00%	4.0/sec	227.87	1.13	58852.0
contact	250	2	1	12	1.60	0.00%	4.0/sec	185.66	1.14	47952.0
dashboard	250	53	47	134	8.16	0.00%	4.0/sec	89.73	2.37	23199.0
profile	250	53	47	86	7.70	0.00%	4.0/sec	89.71	2.36	23197.0
TOTAL	2000	40	1	134	22.88	0.00%	28.4/sec	852.91	14.53	30746.0

- Pengujian 3



Summary Report

Name: Summary Report

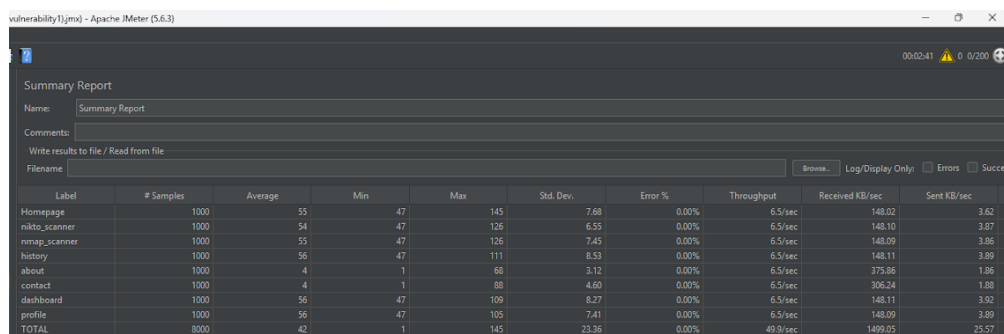
Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: ☐ Errors ☐ Successes

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Homepage	500	53	47	86	4.62	0.00%	5.4/sec	121.84	2.88	23182.0
nikto_scanner	500	52	47	89	3.68	0.00%	5.4/sec	121.89	3.18	23195.0
nmap_scanner	500	52	47	116	5.65	0.00%	5.4/sec	121.87	3.17	23194.0
history	500	53	47	90	5.50	0.00%	5.4/sec	121.89	3.21	23197.0
about	500	2	1	13	1.62	0.00%	5.4/sec	309.38	1.54	58852.0
contact	500	2	1	31	2.15	0.00%	5.4/sec	252.08	1.55	47952.0
dashboard	500	53	47	125	6.82	0.00%	5.4/sec	121.88	3.23	23199.0
profile	500	53	48	95	5.54	0.00%	5.4/sec	121.86	3.20	23197.0
TOTAL	4000	40	1	125	22.19	0.00%	39.8/sec	1186.37	20.44	30746.0

- Pengujian 4



Summary Report

Name: Summary Report

Comments:

Write results to file / Read from file

Filename: Browse... Log/Display Only: ☐ Errors ☐ Successes

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Homepage	1000	55	47	145	7.68	0.00%	6.5/sec	148.02	3.62	23182.0
nikto_scanner	1000	54	47	126	6.55	0.00%	6.5/sec	148.10	3.87	23195.0
nmap_scanner	1000	55	47	126	7.43	0.00%	6.5/sec	148.09	3.86	23194.0
history	1000	56	47	111	8.53	0.00%	6.5/sec	148.11	3.89	23197.0
about	1000	4	1	68	3.12	0.00%	6.5/sec	375.86	1.86	58852.0
contact	1000	4	1	88	4.60	0.00%	6.5/sec	306.24	1.88	47952.0
dashboard	1000	56	47	109	8.27	0.00%	6.5/sec	148.11	3.92	23199.0
profile	1000	56	47	105	7.41	0.00%	6.5/sec	148.09	3.89	23197.0
TOTAL	8000	42	1	145	23.36	0.00%	49.9/sec	1499.05	25.57	30746.0

- Pengujian 5

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec
Homepage	4000	4719	50	19902	2424.48	0.00%	13.0/sec	345.18	
nlbs_scanner	4000	5181	49	20395	2553.07	0.00%	14.0/sec	338.09	
rmmap_scanner	4000	5173	50	19175	2462.96	0.00%	14.0/sec	335.74	
history	4000	5148	50	20112	2372.35	0.00%	14.0/sec	334.22	
about	4000	3354	2	16444	1743.84	0.00%	17.7/sec	845.61	
contact	4000	2713	1	13033	1406.76	0.00%	14.7/sec	627.50	
dashboard	4000	5049	47	20962	2368.98	0.00%	14.7/sec	332.04	
profile	4000	5051	50	19913	2395.85	0.00%	14.7/sec	331.99	
TOTAL	32000	4348	2	20395	2422.48	0.00%	114.2/sec	3428.68	

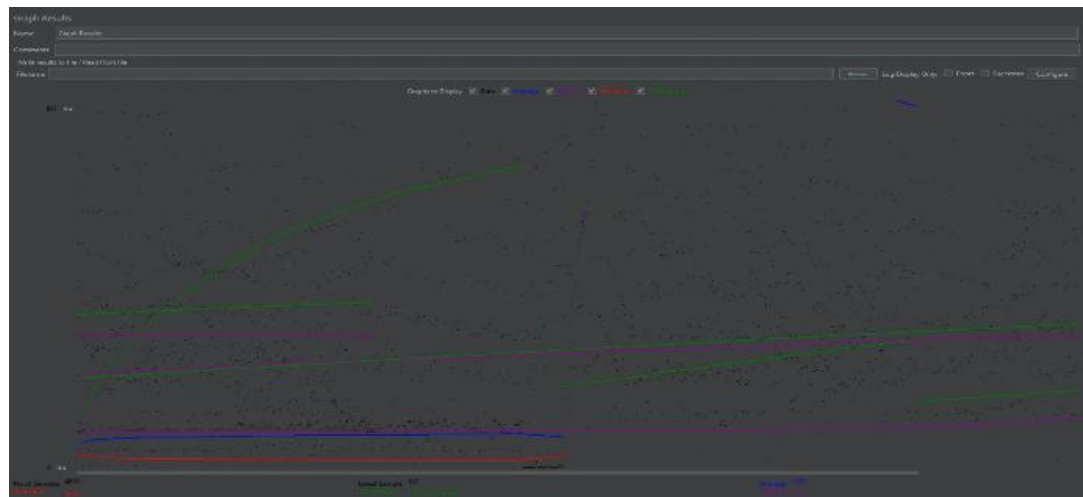
- Pengujian 6

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec
Homepage	6000	6200	51	15237	3108.59	0.00%	14.0/sec	336.10	
nlbs_scanner	6000	6215	49	16081	3122.49	0.00%	14.0/sec	331.14	
rmmap_scanner	6000	6283	49	15915	2960.49	0.00%	14.4/sec	326.87	
history	6000	6213	49	15487	2850.53	0.00%	14.3/sec	323.17	
about	6000	6280	2	11444	2060.78	0.00%	14.2/sec	817.67	
contact	6000	5089	2	9788	1678.69	0.00%	14.2/sec	663.93	
dashboard	6000	6155	49	15415	2854.26	0.00%	14.1/sec	320.56	
profile	6000	6085	50	17514	3108.05	0.00%	14.2/sec	320.56	
TOTAL	48000	6219	2	17514	3108.05	0.00%	111.3/sec	3341.23	

h. Pengujian Backend

- Pengujian 1

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
login	500	394	5	20025	3720.64	0.00%	6.7/sec	149.45	1.12	23796.6
login Subnet	500	3264	27	20301	5223.48	0.00%	6.6/sec	153.03	2.86	23789.6
game Score API	500	387	97	20871	3778.38	0.00%	6.6/sec	153.69	3.40	24019.6
API Game Score	500	383	97	20907	3880.38	0.00%	6.6/sec	153.63	3.46	24019.6
rmmap Score	500	396	97	20891	2981.85	0.00%	6.6/sec	149.40	3.86	23794.6
nlbs Score	500	374	97	20524	3132.37	0.00%	6.6/sec	149.40	3.86	23795.6
Feed Score History	500	1182	97	21736	4872.86	0.00%	6.6/sec	149.42	2.41	23767.6
user Profile	500	1726	97	20983	4883.48	0.00%	6.6/sec	149.43	2.41	23767.6
Log post	500	1882	97	20880	6716.74	0.00%	6.6/sec	153.16	4.86	24009.6
TOTAL	4500	1153	5	20395	4341.68	0.00%	98.6/sec	3346.84	23.86	23774.6



- Pengujian 2

Summary Report

Name:Summary Report

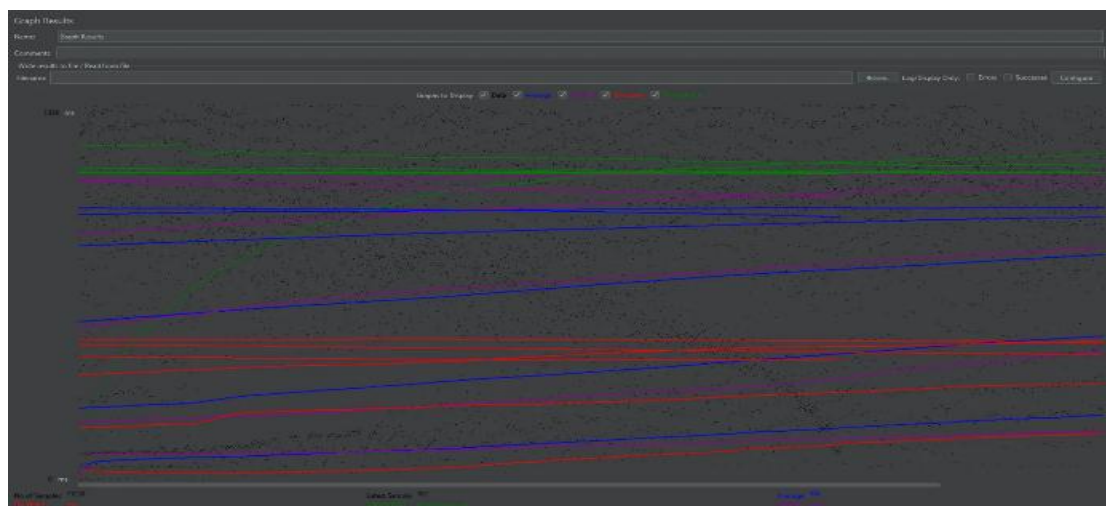
Comments:

Write results to file / Read from file

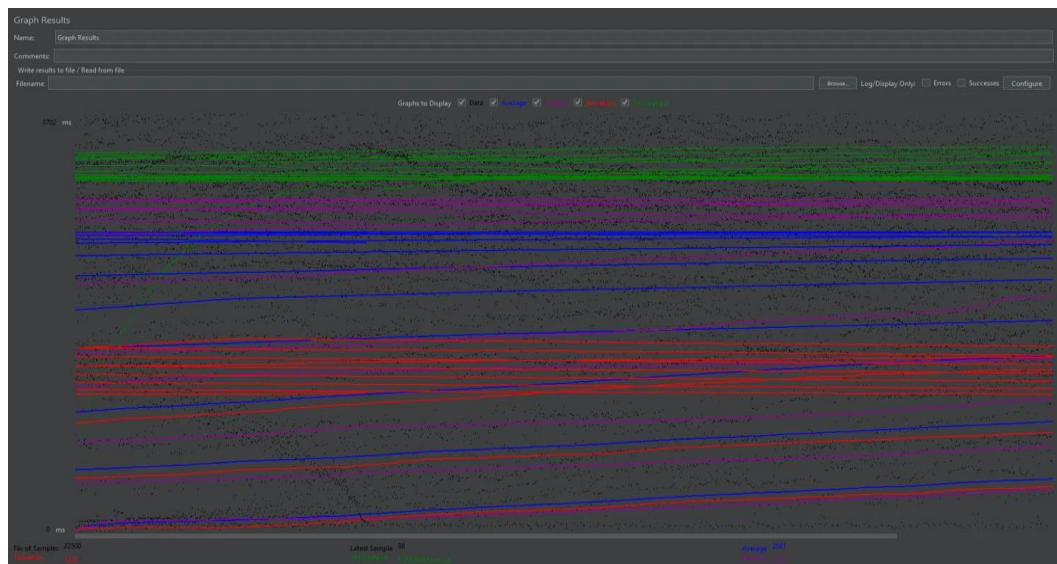
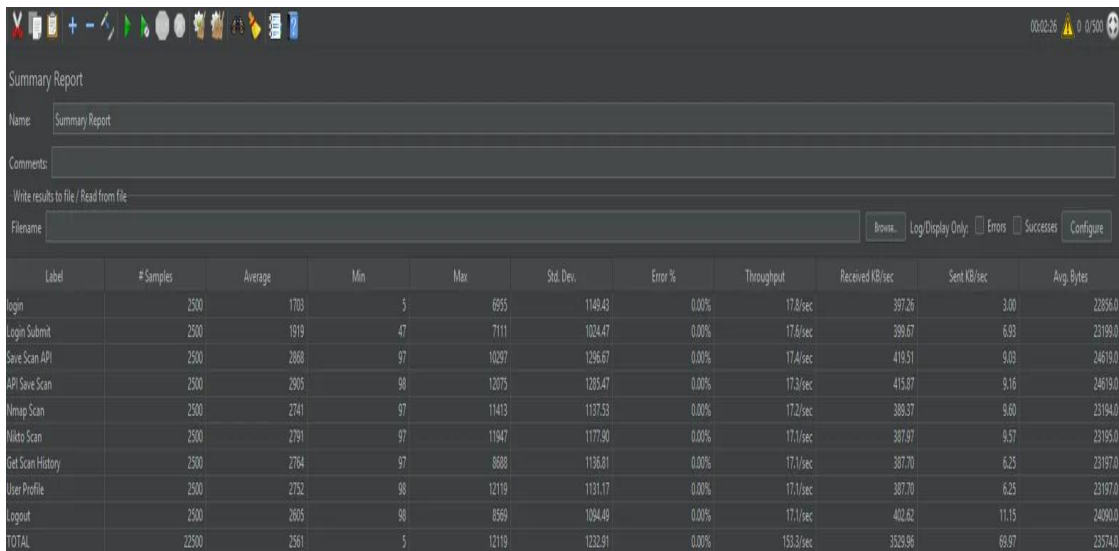
Buttons

HomeLog Display OnlyErrorSuccessCompare

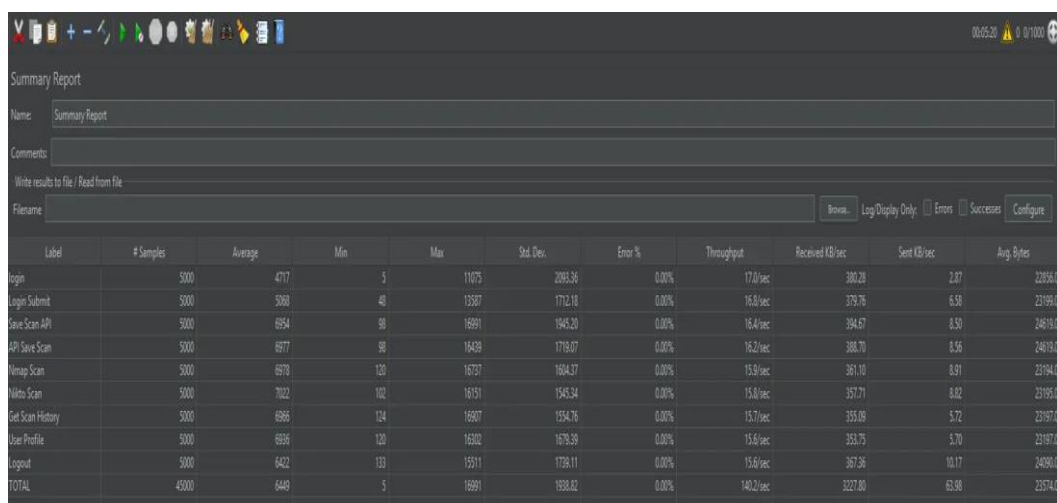
	Total	# Samples	Average	Min	Max	Std. Dev.	Unit %	Throughput	Received (B/sec)	Send (B/sec)	Avg. Delay
logp	1210	719	5	115	111.37	0.00%	17.71sec	395.57	2.89	1205.0	
log n latency	1210	710	47	114	367.38	0.00%	17.59sec	398.38	6.43	1199.0	
Send Size 4K	1210	940	97	101	401.57	0.00%	17.59sec	401.15	9.27	1189.0	
4K latency	1210	107	97	107	411.30	0.00%	17.59sec	410.18	9.21	1189.0	
8K Size	1210	99	97	101	411.30	0.00%	17.59sec	391.41	9.70	1194.0	
8K latency	1210	102	97	101	417.32	0.00%	17.59sec	392.31	9.61	1185.0	
latency history	1210	102	97	107	401.27	0.00%	17.59sec	391.31	9.21	1187.0	
latency profile	1210	97	97	791	401.32	0.00%	17.59sec	391.45	9.11	1187.0	
loglat	1210	61	97	101	401.31	0.00%	17.59sec	400.58	11.21	1189.0	
TOTAL	1210	124	5	101	411.46	0.00%	17.59sec	1247.01	70.11	1207.0	

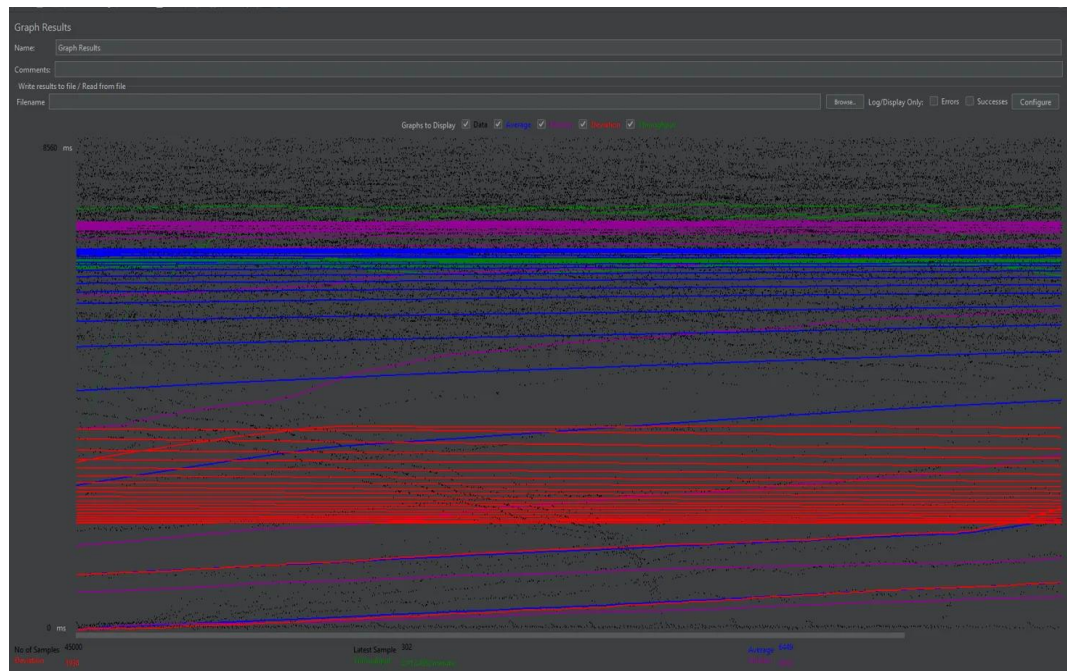


- Pengujian 3



- Pengujian 4





- Pengujian 5

Summary Report

Name: Summary Report

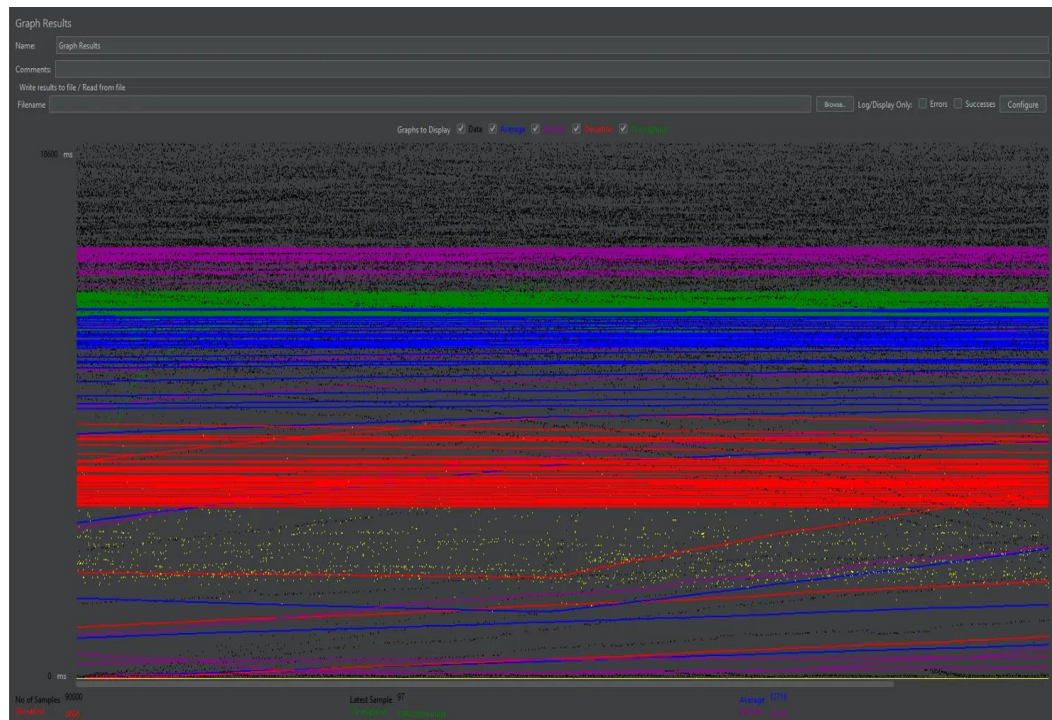
Comments:

Write results to file / Read from file

Filename:

Buttons: [Browse...](#) [Log/Display Only](#) ☐ Errors ☐ Successes [Configure](#)

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
login	10000	9184	1	23537	5635.75	8.88%	18.01/sec	370.48	2.78	21861.5
Login Submit	10000	10418	1	40689	5351.32	11.69%	17.71/sec	359.50	6.14	20794.8
Save Scan API	10000	14756	1	40907	6230.92	14.63%	17.21/sec	362.38	7.97	21452.9
API Save Scan	10000	14398	1	40437	5582.55	12.81%	16.91/sec	361.48	8.08	21346.4
Nmap Scan	10000	14592	1	37339	5818.79	10.62%	16.71/sec	341.43	8.57	20886.5
Nikto Scan	10000	13815	1	33964	6280.17	19.27%	16.51/sec	308.71	7.65	19364.2
Get Scan History	10000	13239	0	38818	5998.86	15.53%	16.41/sec	320.60	5.08	20004.0
User Profile	10000	13046	1	27742	5996.63	15.08%	16.41/sec	322.44	5.11	20100.3
Logout	10000	12373	1	23637	5565.24	11.95%	16.41/sec	345.05	9.45	21532.1
TOTAL	90000	12716	0	40607	6008.66	13.42%	147.41/sec	2991.08	58.14	20782.5

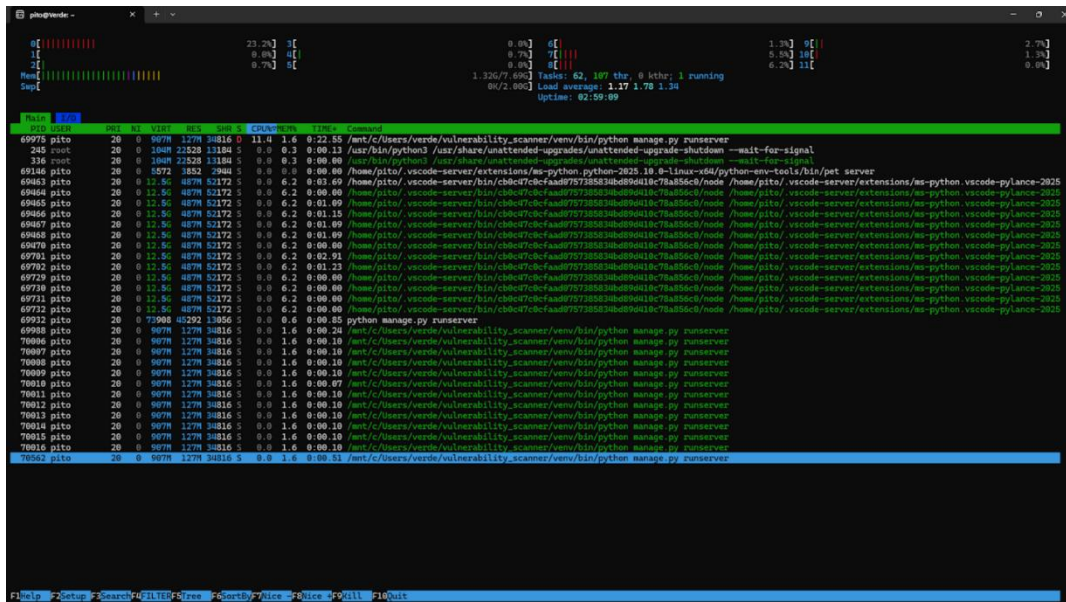


- Pengujian HTOP normal

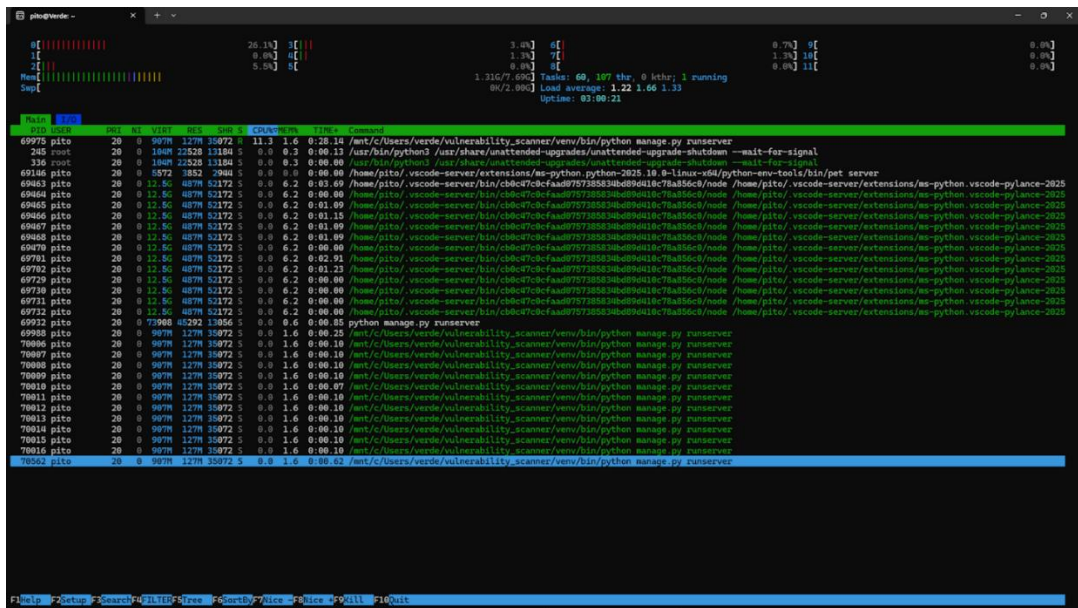
[illegible]

[illegible]

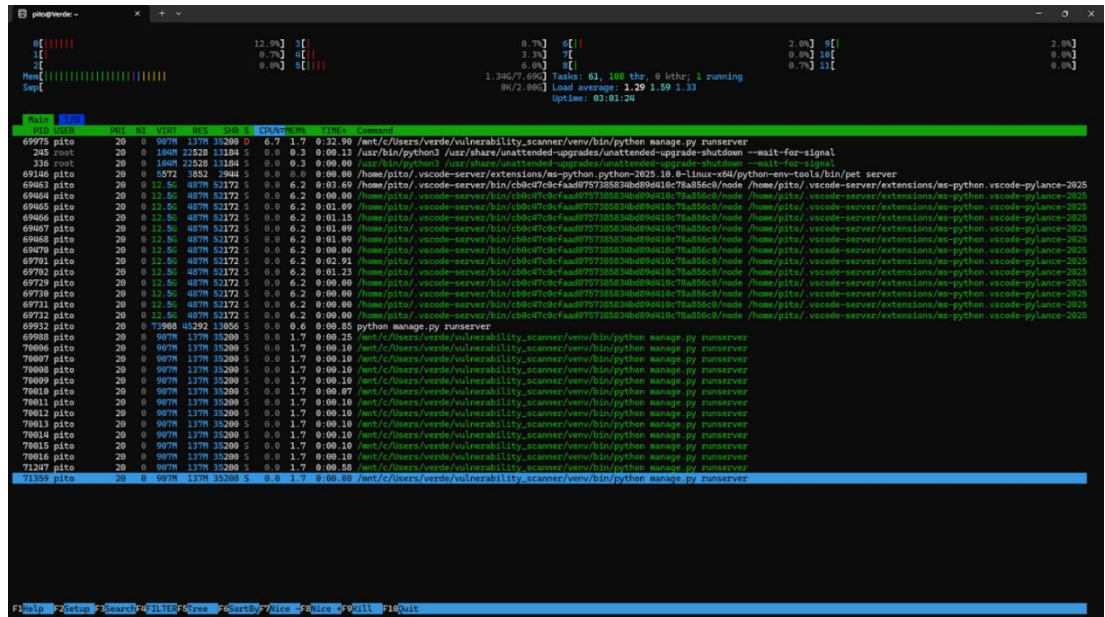
- 163



[illegible][illegible]



- Pengujian Htop Nmap




```

0[|||||] 21.0k 3[ 0.0k] 6[| 1.2k] 9[| 0.7k]
1[| 0.0k] 4[| 0.0k] 7[| 0.2k]
2[| 0.7k] 5[| 0.0k] 8[| 1.3k] 10[| 2.0k]
Mem| 1.33G/7.69G Tasks: 60, 180 thr, 0 kthr, 1 running
Swap| 0k/2.00k Load average: 0.97 1.31 1.25
Uptime: 03:04:08

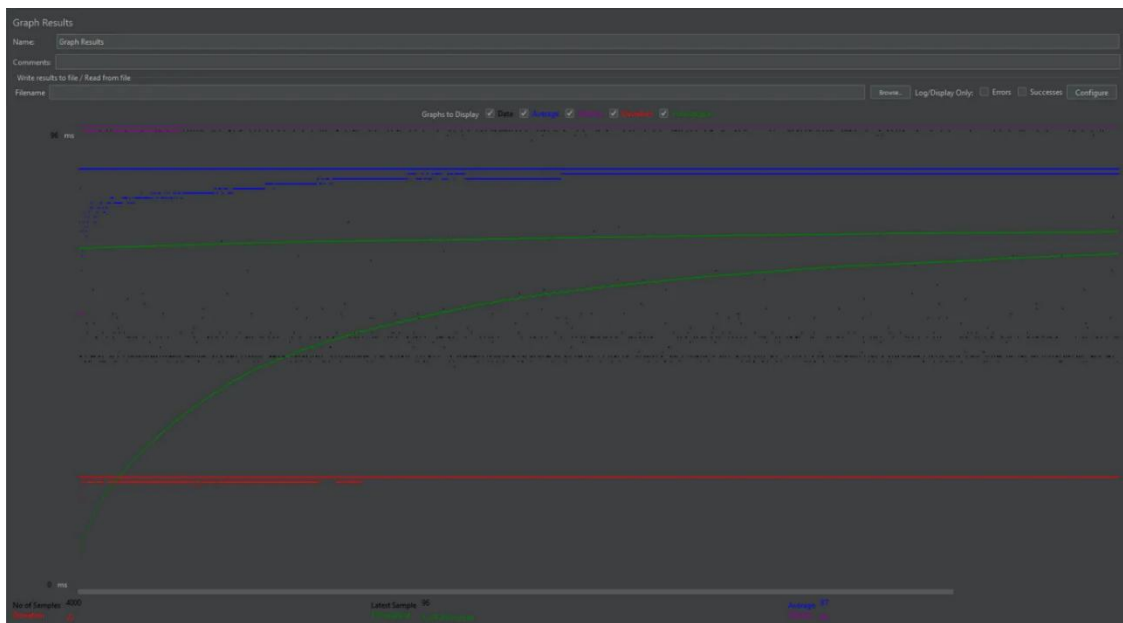
#PID USER PRU NI VIRT RES SHR S CPU% MEM% TIME+ Command
60978 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.27 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
69008 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70006 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70007 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70008 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70009 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70010 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.07 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70011 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70012 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70013 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70014 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70015 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
70016 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.19 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
71307 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.63 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
71359 pito 20 0 990M 130M 35200 S 0.0 1.8 0:00.80 /mnt/c/Users/veede/vulnerability_scanner/venu/bin/python manage.py runserver
69912 pito 20 0 7790k 45292 13056 S 0.0 0.6 0:00.85 python manage.py runserver

```

i. Pengujian Frontend

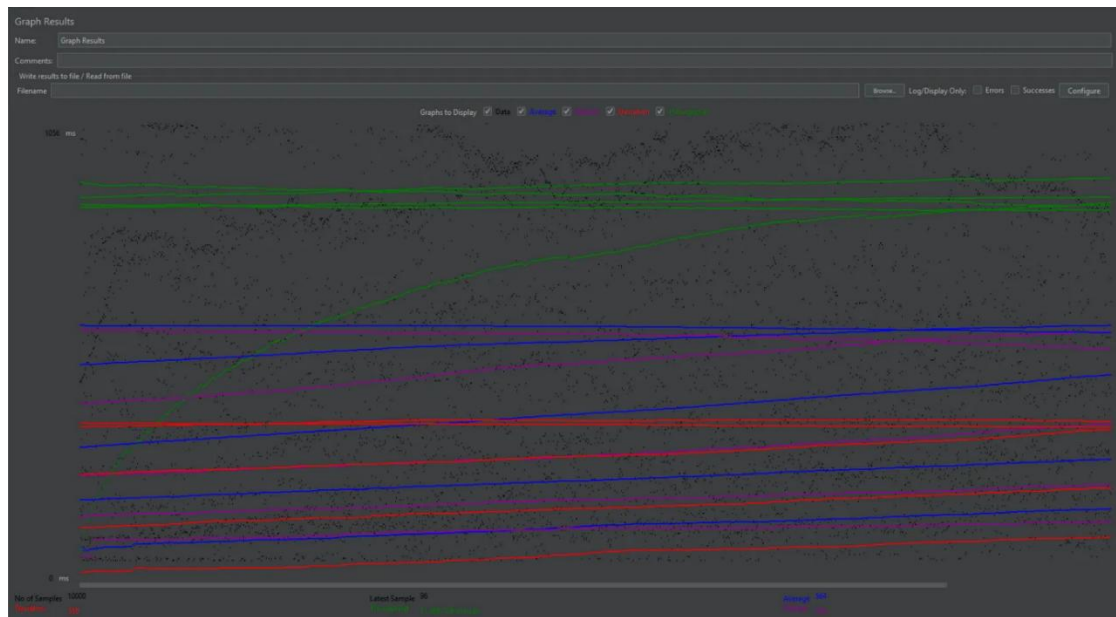
- Pengujian 1

Summary Report											
Name: Summary Report											
Comments:											
Write results to file / Read from file											
Filename: Browse Log/Display Only Errors Successes Configure											
Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec		Avg. Bytes
Tampilan NMAP	300	92	51	126	17.55	0.00%	15.3/sec	347.58	5.86		23194.0
Tampilan NIKTO	300	101	94	131	9.96	0.00%	15.3/sec	347.08	6.59		23193.0
Tampilan HISTORY	300	103	95	127	9.96	0.00%	15.3/sec	347.11	6.25		23193.0
Tampilan ABOUT	300	49	47	57	2.21	0.00%	15.3/sec	881.94	2.94		50852.0
Tampilan CONTACT US	300	49	11	57	3.04	0.00%	15.3/sec	718.60	2.87		47952.0
Tampilan DASHBOARD	300	101	95	127	9.96	0.00%	15.3/sec	347.14	6.51		23193.0
Tampilan PROFILE	300	101	84	127	9.96	0.00%	15.3/sec	347.11	6.25		23193.0
Tampilan HOME	300	101	95	128	9.94	0.00%	15.3/sec	346.99	5.91		23182.0
TOTAL	4000	87	11	131	23.48	0.00%	120.6/sec	3621.01	41.89		30746.0



- Pengujian 2

Summary Report											
Name: Summary Report											
Comments:											
Write results to file / Read from file											
Filename: Browse Log/Display Only Errors Successes Configure											
Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec		Avg. Bytes
Tampilan NMAP	1250	619	52	1614	316.91	0.00%	23.7/sec	537.88	9.07		23194.0
Tampilan NIKTO	1250	630	95	2055	362.47	0.00%	23.7/sec	537.41	6.59		23193.0
Tampilan HISTORY	1250	643	95	2387	368.81	0.00%	23.7/sec	537.28	6.88		23193.0
Tampilan ABOUT	1250	380	47	1650	179.45	0.00%	23.7/sec	1964.34	4.54		50852.0
Tampilan CONTACT US	1250	326	47	1331	222.75	0.00%	23.7/sec	1111.65	4.59		47952.0
Tampilan DASHBOARD	1250	636	96	1815	362.85	0.00%	23.7/sec	537.28	9.77		23190.0
Tampilan PROFILE	1250	645	95	2308	363.60	0.00%	23.7/sec	537.20	6.88		23193.0
Tampilan HOME	1250	616	96	1834	332.73	0.00%	23.7/sec	536.80	6.15		23182.0
TOTAL	10000	564	47	2387	256.15	0.00%	187.8/sec	5635.15	65.38		30746.0



- Pengujian 3

Summary Report

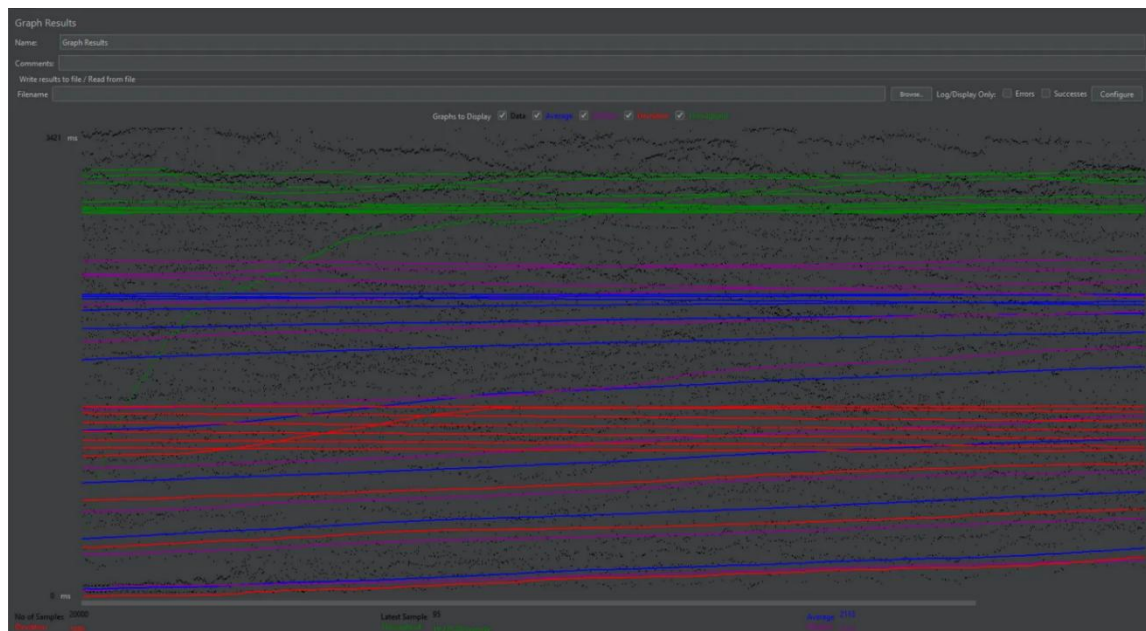
Name: Summary Report

Comments:

Write results to file / Read from file

Filename: Browse Log/Display Only: ☐ Errors: ☐ Successes: ☐ Configure

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Aug. Bytes
Template NMAP	2500	2210	52	8051	1174.99	0.00%	22.1/sec	500.09	8.43	23194.0
Template NIKTO	2500	2379	95	10267	1138.88	0.00%	21.8/sec	495.32	8.84	23195.0
Template NIST	2500	2401	85	10744	1127.28	0.00%	21.7/sec	497.79	8.86	23197.0
Template ABOUT	2500	1569	47	6403	763.45	0.00%	21.6/sec	1243.52	4.14	38952.0
Template CONTACT US	2500	1327	47	6114	659.42	0.00%	21.6/sec	1010.80	4.17	47952.0
Template DASHBOARD	2500	2404	96	8124	1086.50	0.00%	21.5/sec	487.41	8.87	23199.0
Template PROFILE	2500	2388	96	7335	1038.38	0.00%	21.5/sec	487.22	8.78	23197.0
Template HOME	2500	2127	95	8090	964.63	0.00%	21.5/sec	486.80	8.30	23182.0
TOTAL	20000	2113	47	12764	1086.65	0.00%	171.3/sec	5142.64	39.63	30746.0



- Pengujian 4

Summary Report

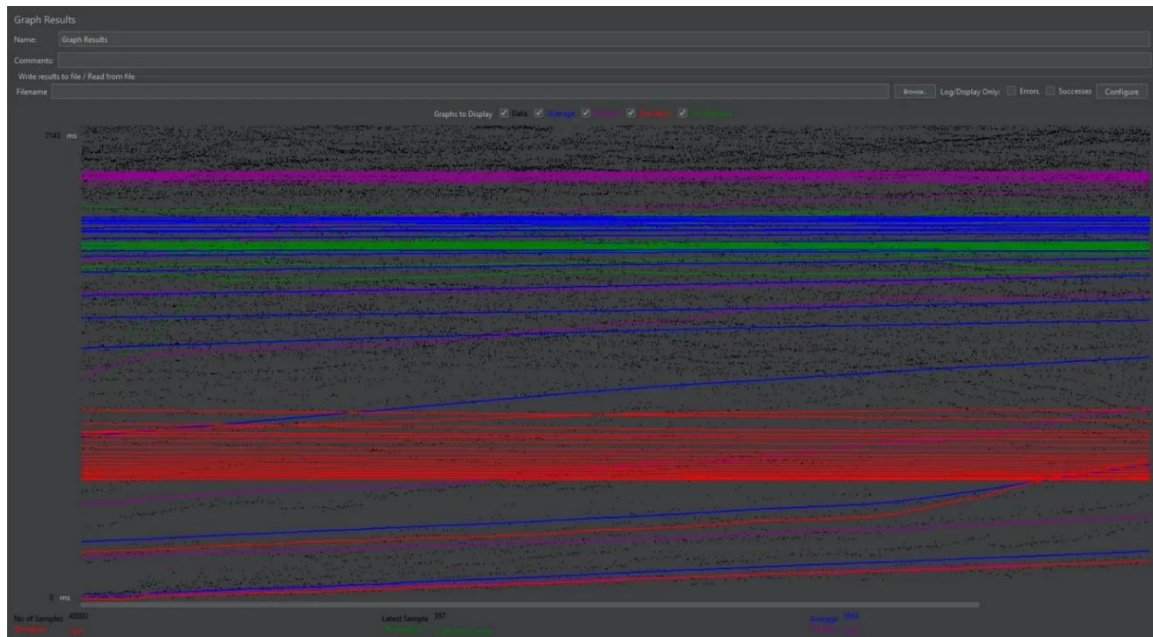
Name: Summary Report

Comments:

Write results to file / Read from file

Filename:

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Templan NMAP	5000	6042	54	12453	2107.24	0.00%	21.0/sec	476.12	8.03	23194.4
Templan NIKTO	5000	6227	95	11623	1824.43	0.00%	20.7/sec	487.60	8.25	23195.6
Templan HISTORY	5000	6243	95	14027	1672.44	0.00%	20.3/sec	493.38	8.28	23197.8
Templan ABOUT	5000	4338	48	8293	1225.44	0.00%	20.1/sec	1153.90	3.84	58852.8
Templan CONTACT US	5000	3999	48	6403	984.21	0.00%	19.8/sec	953.14	3.85	47952.8
Templan DASHBOARD	5000	6238	109	14187	1598.83	0.00%	19.7/sec	486.65	8.12	23199.6
Templan PROFILE	5000	6187	118	11828	1571.74	0.00%	19.6/sec	484.63	8.00	23197.6
Templan HOME	5000	5781	126	13218	1623.26	0.00%	19.6/sec	441.52	7.56	23182.8
TOTAL	40000	5584	48	14027	1871.68	0.00%	196.3/sec	4694.38	54.44	30746.8



- Pengujian 5

Summary Report

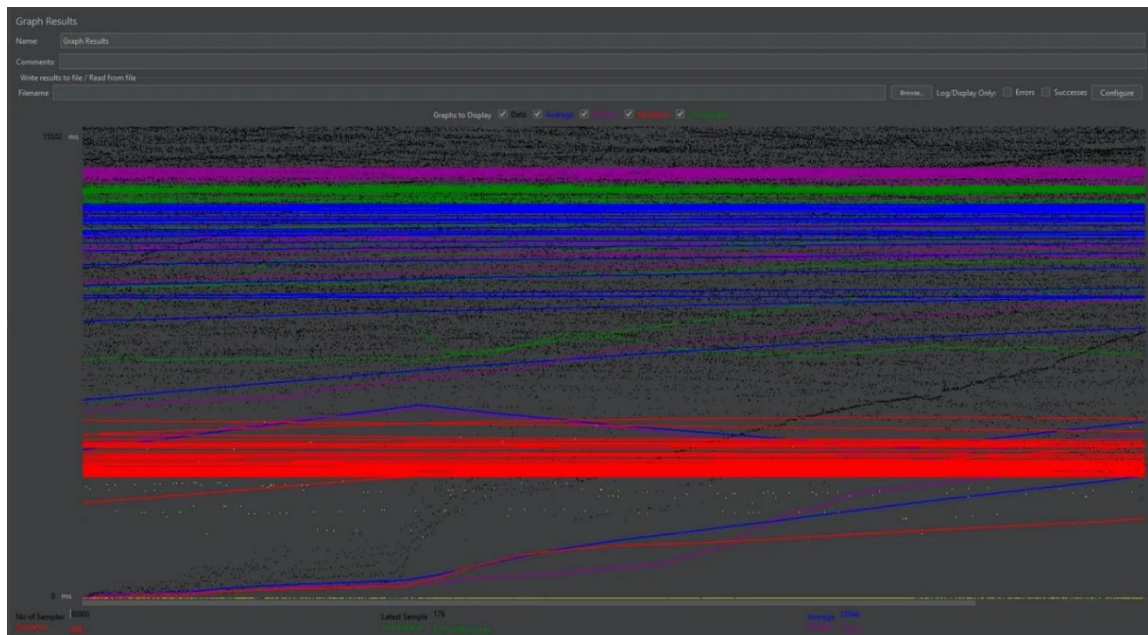
Name: Summary Report

Comments:

Write results to file / Read from file

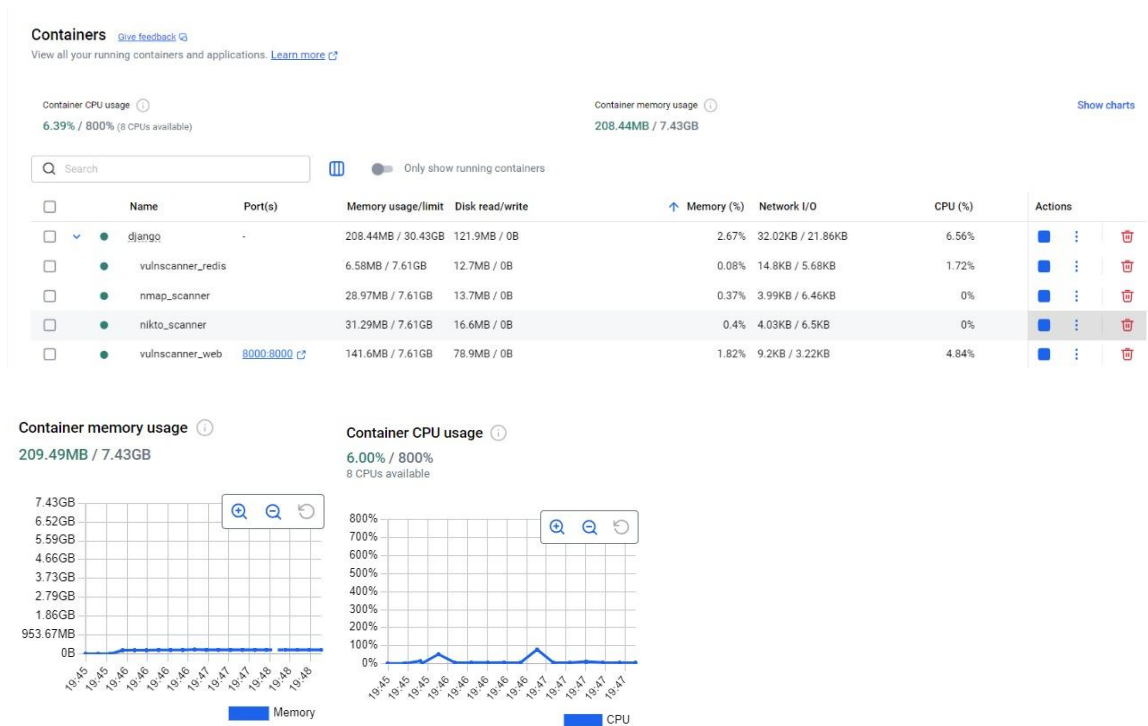
Filename:

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/sec	Sent KB/sec	Avg. Bytes
Templan NMAP	10000	14182	1	24240	4192.12	3.06%	19.8/sec	436.13	7.88	22567.2
Templan NIKTO	10000	14079	1	23611	3775.11	2.85%	19.5/sec	428.75	7.59	22446.6
Templan HISTORY	10000	13914	1	22946	3267.49	3.36%	19.3/sec	418.30	7.53	22508.8
Templan ABOUT	10000	9901	1	17625	2205.84	2.31%	18.6/sec	1054.94	3.51	57553.3
Templan CONTACT US	10000	9414	1	14771	1836.72	1.83%	18.6/sec	856.61	3.53	47122.8
Templan DASHBOARD	10000	14045	1	23454	3646.27	4.25%	18.6/sec	401.51	7.28	22328.8
Templan PROFILE	10000	13818	1	22140	4076.84	3.16%	18.6/sec	397.20	7.13	22140.8
Templan HOME	10000	12818	1	22044	4145.09	4.44%	18.4/sec	390.64	6.76	22271.2
TOTAL	80000	12644	1	24240	4081.53	3.51%	148.6/sec	4276.58	48.21	28687.3



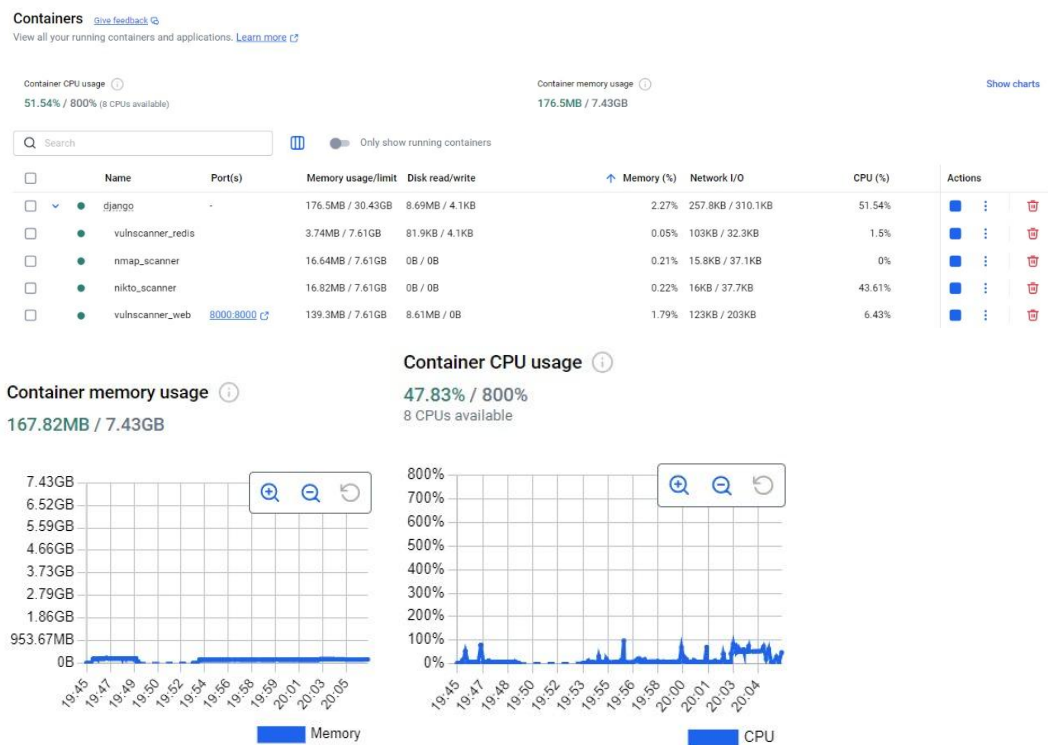
j. Pengujian Docker

1. Docker Aktif tanpa Pemindaian

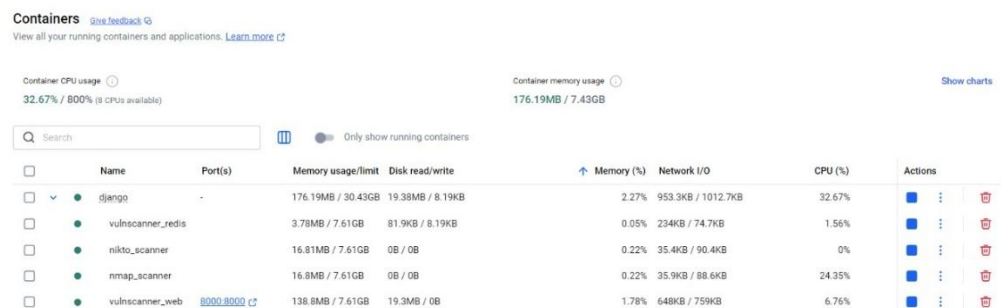


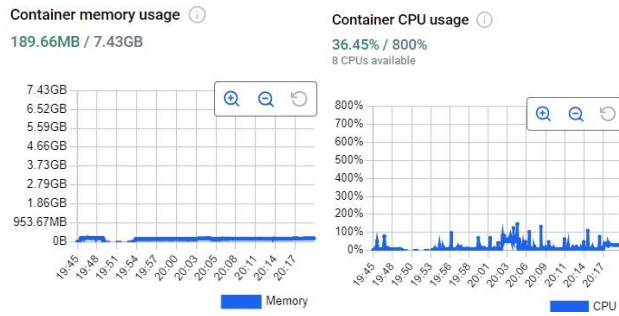
2. Docker Aktif dengan Pemindaian

- Nikto



- Nmap





- Nikto Nmap Bersamaan

Containers [Give feedback](#)

View all your running containers and applications. [Learn more](#)

Container CPU usage ⓘ

155.10% / 800% (8 CPUs available)

Container memory usage ⓘ

183.23MB / 7.43GB

Show charts

☰

Only show running containers

☐	Name	Port(s)	Memory usage/limit	Disk read/write	Memory (%)	Network I/O	CPU (%)	Actions
☐	django	-	183.48MB / 30.43GB	5.58MB / 28.7KB	2.36%	1.22MB / 1.47MB	161.15%	⌵ ⌵ ⌵
☐	vulnscanner_redis	-	3.53MB / 7.61GB	0B / 0B	0.05%	74.5KB / 93.7KB	1.96%	⌵ ⌵ ⌵
☐	nmap_scanner	-	17.04MB / 7.61GB	0B / 0B	0.22%	6.91KB / 16.7KB	33.46%	⌵ ⌵ ⌵
☐	nikto_scanner	-	16.81MB / 7.61GB	0B / 0B	0.22%	7.03KB / 17.1KB	53.79%	⌵ ⌵ ⌵
☐	vulnscanner_web	8000-8000	146.1MB / 7.61GB	5.58MB / 28.7KB	1.87%	1.13MB / 1.35MB	71.94%	⌵ ⌵ ⌵

