ANALISIS CELAH KEAMANAN SISTEM INFORMASI RSIA PUTRI SURABAYA MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Tugas Akhir

diajukan untuk memenuhi salah satu syarat

memperoleh gelar sarjana

dari Program Studi Teknologi Informasi

Fakultas Informatika

Universitas Telkom

1202200419

Mahendra Rangga Abimanyu

Program Studi Sarjana Teknologi Informasi

Fakultas Informatika

Universitas Telkom

Surabaya

2024

LEMBAR PENGESAHAN

ANALISIS CELAH KEAMANAN SISTEM INFORMASI RSIA PUTRI SURABAYA MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

(ANALYSIS OF SECURITY GAPS IN RSIA PUTRI SURABAYA INFORMATION SYSTEM USING OPEN WEB APPLICATION SECURITY PROJECT (OWASP))

NIM :1202200419

Mahendra Rangga Abimanyu

Tugas akhir ini telah diterima dan disahkan untuk memenuhi sebagian syarat memperoleh gelar pada Program Studi Sarjana Teknologi Informasi (Kampus Kota Surabaya)
Fakultas Informatika
Universitas Telkom

Surabaya, 15 Agustus 2024
Menyetujui

Pembimbing I,	Pembimbing II,
Kharisma Monika Dian Pertiwi.S.kom.,M.Kom.	Mustafa Kamal.S.Kom.,M.Kom.
NIP: 20950044	NIP: 22820015

Ketua Program Studi
Sarjana Teknologi Informasi,

Bernadus Anggo Seno Aji, S.Kom., M.Kom.
NIP: 23929009

LEMBAR PERNYATAAN

Dengan ini saya, Mahendra Rangga Abimanyu, menyatakan sesungguhnya bahwa Tugas Akhir saya dengan judul Analisis Celah Keamanan Sistem Informasi RSIA Putri Surabaya Menggunakan Metode *Open Web Application Security Project (OWASP)* beserta dengan seluruh isinya adalah merupakan hasil karya sendiri, dan saya tidak melakukan penjiplakan yang tidak sesuai dengan etika keilmuan yang belaku dalam masyarakat keilmuan. Saya siap menanggung resiko/sanksi yang diberikan jika di kemudian hari ditemukan pelanggaran terhadap etika keilmuan dalam buku TA atau jika ada klaim dari pihak lain terhadap keaslian karya,

Surabaya, 15 Agustus 2024
Yang Menyatakan

Mahendra Rangga Abimanyu

ANALISIS CELAH KEAMANAN SISTEM INFORMASI RSIA PUTRI SURABAYA MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Mahendra Rangga Abimanyu[1], Kharisma Monika Dian Pertiwi[2], Mustafa Kamal[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]mahennnn@students.telkomuniversity.ac.id, [2]kharismamonika@telkomuniversity.ac.id,
[3]mustafakamal@telkomuniversity.ac.id

Abstrak

Peningkatan pengguna internet beriringan dengan meningkatnya kejahatan dunia maya, seperti kebocoran informasi, yang menjadi ancaman serius. Keamanan data dan informasi saat ini menjadi prioritas utama untuk menjaga integritas dan kerahasiaan. Rumah Sakit Putri di Surabaya memiliki sistem informasi yang kaya akan informasi pasien, termasuk data rekam medis yang sangat sensitif. Meskipun begitu, RSIA Putri Surabaya tidak pernah melakukan pengujian keamanan sistem informasinya. Oleh karena itu, penelitian ini menggunakan metode OWASP Top 10 2021 dan tools seperti SQLMap, Nmap, ZAP, Burp Suite, Wappalyzer, Wireshark, dan tools yang tersedia di sistem operasi Kali Linux untuk mengidentifikasi celah keamanan. Penelitian ini menemukan tiga kerentanan utama, yaitu A02. *Cryptographic Failures*, A04. *Insecure Design*, dan A06. *Vulnerable and Outdated Components*. Berdasarkan hasil dari temuan ini, peneliti merekomendasikan perbaikan melalui surat validasi hasil penelitian yang disampaikan kepada unit tim IT RSIA Putri Surabaya, yang telah ditandatangani oleh peneliti dan Kepala unit IT RSIA Putri Surabaya.

Kata kunci : Keamanan, OWASP, Rumah Sakit, Sistem Informasi.

Abstract

The increase in internet users goes hand in hand with the increase in cybercrime, such as information leaks, which is a serious threat. Data and information security is currently a top priority to maintain integrity and confidentiality. RSIA Putri Hospital in Surabaya has an information system that is rich in patient information, including very sensitive medical record data. Even so, RSIA Putri Hospital has never tested the security of its information system. Therefore, this research uses the OWASP Top 10 2021 method and tools such as SQLMap, Nmap, ZAP, Burp Suite, Wappalyzer, Wireshark, and tools available on the Kali Linux operating system to identify security gaps. This research found three main vulnerabilities, namely A02. Cryptographic Failures, A04. Insecure Design, and A06. Vulnerable and Outdated Components. Based on the results of these findings, the researcher recommended improvements through a validation letter of research results submitted to the RSIA Putri Hospital IT team unit, which was signed by the researcher and the Head of the Putri Hospital IT unit.

Keywords: Security, OWASP, Hospital, Information System.

1. Pendahuluan

Latar Belakang

Perkembangan teknologi saat ini semakin maju dan modern, hal ini membawa perubahan besar dalam kehidupan manusia. Semakin berkembangnya teknologi informasi membuat maraknya kejahatan-kejahatan di internet yang manusia bisa semakin mudah melakukan tindakan kriminal seperti kejahatan siber[1]. Semakin maraknya pengguna internet di kalangan masyarakat luas, semakin tinggi juga peluang kejahatan siber. Peristiwa estonia pada tahun 2007 dan Georgia pada tahun 2008 merupakan contoh serangan siber dengan pemanfaatan *Distributed Denial of Service* (Ddos)[2]. Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah suatu struktur yang terkait dengan proses pengumpulan, pengolahan, penyajian, analisis, dan penyimpulan informasi, serta penyampaian data yang diperlukan dalam operasional rumah sakit[3]. Hal ini sangat penting untuk dijaga data-data pada sistem informasi rumah sakit, karena data tersebut rentan terhadap kejahatan siber yang dilakukan oleh oknum yang tidak bertanggung jawab. Perlu dilakukannya analisis celah keamanan sistem informasi untuk mengetahui apakah pada sistem informasi pada rumah sakit tersebut rentan terhadap serangan siber. OWASP adalah komunitas profesional keamanan yang mengidentifikasi risiko keamanan aplikasi web paling kritis dalam domain teknologi informasi[4]. Menggunakan metode OWASP bisa mencakup berbagai jenis kerentanan yang dapat mengancam keamanan aplikasi web dan menyediakan langkah-langkah mitigasi yang efektif [5]. Peneliti memilih OWASP karena fokusnya yang spesifik pada sistem informasi, standarnya yang dikenal luas, panduan dan *tools* yang terperinci, pembaruan secara berkala, serta ketersediaan *open source* dan kemudahan implementasi.

Metode ini lebih sesuai dibandingkan dengan ISSAF dan HOTFIT ketika tujuan utama adalah analisis keamanan sistem informasi. *Penetration testing* diperlukan untuk memastikan keamanan sistem informasi dan melindungi data sensitif dari serangan siber, hal ini membuat peneliti menjadi yakin untuk melakukan analisis celah rentan keamanan sistem informasi itu sangat penting untuk dilakukan. Tujuan utama dari OWASP top 10 adalah memberikan pengetahuan kepada IT *Cyber security* dari kesalahan keamanan pada aplikasi web yang memiliki tingkat yang sangat penting[6]. Penelitian ini juga melakukan pembuatan dashboard web yang berisi tentang saat melakukan testing, hasil, rekomendasi perbaikan dan hasil kerentanan yang ditemukan. Studi kasus yang akan menjadi objek penelitian ini adalah website sistem informasi dari RSIA Putri Surabaya. Berdasarkan dari wawancara peneliti, pihak dari Rumah Sakit Putri Surabaya sendiri masih belum pernah melakukan *penetration testing* pada sistem informasi RSIA Putri Surabaya, sedangkan terdapat ribuan data pasien yang harus dijaga privasinya di dalam sistem informasi tersebut. Oleh karena itu, peneliti berniat untuk melakukan analisis celah keamanan sistem informasi RSIA Putri Surabaya ini, guna meminimalisir hal-hal yang tidak diinginkan seperti pencurian data, penyalahgunaan data dan bahkan mengambil ahli sistem oleh pihak penyerang. Untuk itu, dilakukannya *penetration testing* sistem informasi berdasarkan standar keamanan yang ada pada OWASP top 10. Tahapan yang dilakukan peneliti yaitu studi literatur lalu pengumpulan data, melakukan *scanning* sistem informasi pada RSIA Putri Surabaya, *testing*, membuat laporan dan hasil rekomendasi perbaikan berdasarkan standarisasi dari *Common Weakness Enumeration* (CWE). Hasil penelitian ditemukan 3 kerentanan yaitu A02, *Cryptographic Failures*, A04. *Insecure Design* dan A06. *Vulnerable and Outdated Components*.

Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat disimpulkan rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana cara melakukan *penetration testing* sistem informasi RSIA Putri Surabaya menggunakan metode OWASP top 10 2021?
2. Bagaimana hasil dari *penetration testing* sistem informasi RSIA Putri Surabaya dengan metode OWASP top 10 2021?
3. Bagaimana rekomendasi perbaikan terhadap hasil pengujian *penetration testing* sistem informasi RSIA Putri Surabaya?
4. Bagaimana cara memantau *penetration testing* RSIA Putri Surabaya pada dashboard website?

Tujuan

Tujuan dari penelitian ini yaitu untuk menganalisis celah kerentanan sistem informasi RSIA Putri Surabaya, dengan melakukan penetration testing dengan menggunakan metode *OWASP Top 10*.

1. Untuk mengetahui cara *penetration testing* pada sistem informasi RSIA Putri Surabaya menggunakan metode OWASP top 10 2021
2. Untuk mendapatkan hasil dari *penetration testing* sistem informasi RSIA Putri Surabaya menggunakan metode OWASP top 10 2021.
3. Dapat merekomendasikan/perbaikan dari hasil *penetration testing* sistem informasi RSIA Putri Surabaya sesuai standarisasi *Common Weakness Enumeration* (CWE).
4. Dapat melakukan pemantauan SIMRS pada RSIA Putri Surabaya dengan penjelasan setiap celah beserta video dan status celah sudah diselesaikan apa belum.

2. Studi Terkait

2.1 Penelitian Terdahulu

Penelitian terdahulu yang terkait dalam pembahasan analisis celah keamanan pada sistem informasi. Tujuan dari penelitian terdahulu ini untuk dijadikan bahan perbandingan dan kesamaan dari peneliti. Berikut adalah list dari peneliti terdahulu :

A. Penelitian berjudul "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)" yang dilakukan oleh Syarif Hidayatullah dan Desky Saptadiaji menggunakan metode OWASP Top 10 untuk menguji keamanan situs web. Penelitian ini memiliki kesamaan dengan peneliti yang menggunakan metode yang sama, yaitu OWASP Top 10. Namun, perbedaan terletak pada versi OWASP yang digunakan penelitian ini menggunakan OWASP Top 10 tahun 2017, sedangkan peneliti menggunakan versi yang lebih baru, yaitu OWASP Top 10 tahun 2021.

B. Penelitian yang berjudul "Pengujian Keamanan dengan Metode OWASP Top 10 pada Website EformHelpdesk" oleh Rangga Renaldi Yusuf dan Teguh Nurhadi Suharsono menggunakan metode OWASP Top 10 tahun 2021 untuk mengevaluasi keamanan situs web. Penelitian ini memiliki kesamaan dengan peneliti yang juga menggunakan metode OWASP Top 10 2021. Namun, perbedaannya terletak pada objek yang diuji, di mana penelitian ini fokus pada situs web EformHelpdesk, sementara peneliti menggunakan objek SIMRS.

C. Penelitian berjudul "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10" yang dilakukan oleh Yudiana, Anggi Elanda, dan Robby Lintang Buana, menggunakan metode OWASP Top 10 untuk menganalisis keamanan sistem informasi berbasis web. Penelitian ini memiliki kesamaan dengan peneliti yang juga menerapkan metode OWASP Top 10. Namun, perbedaannya terletak pada versi OWASP yang digunakan, di mana penelitian ini menggunakan OWASP Top 10 tahun 2017, sedangkan peneliti menggunakan versi OWASP top 10 2021.

D. Penelitian berjudul "Evaluasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) dengan Metode HOT FIT di RSUD Andi Makkasau Kota Parepare" oleh Andi Dermawan Putra mengevaluasi kualitas SIMRS di rumah sakit tersebut. Penelitian ini memiliki kesamaan dengan peneliti dalam hal objek yang diteliti, yaitu SIMRS, namun perbedaannya terletak pada rumah sakit yang dianalisis serta metode yang digunakan. Sementara peneliti metode OWASP, dan metode HOT FIT untuk evaluasi.

E. Penelitian berjudul "Analisis Keamanan Website dengan Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) di Rumah Sakit XYZ" oleh Agus Rochman, Rizal Rohian Salam, dan Sandi Agus Maulana, berfokus pada analisis kerentanan pada Sistem Informasi Manajemen Rumah Sakit (SIMRS). Penelitian ini memiliki kesamaan dengan peneliti dalam hal analisis kerentanan pada SIMRS, namun berbeda dalam pendekatan yang digunakan. Penelitian ini menggabungkan dua metode, yaitu ISSAF dan OWASP, untuk melakukan evaluasi keamanan, sementara peneliti hanya menggunakan metode OWASP.

2.2 Dasar Teori

2.2.1 OWASP Top 10 2021

Open Web Application Security Project (OWASP) adalah lembaga nirlaba yang memiliki fokus pada peningkatan keamanan perangkat lunak. OWASP adalah kerangka kerja untuk meningkatkan keamanan situs web[2]. Metode yang diambil dari OWASP ini yaitu OWASP top 10 2021 yang digunakan sebagai standar analisis celah kerentanan sistem informasi pada RSIA Putri Surabaya. OWASP Top 10 2021 adalah daftar utama kerentanan keamanan yang dapat mengancam ketahanan suatu situs web. Daftar ini dikeluarkan oleh komunitas OWASP dan terus mengalami evolusi sesuai dengan perkembangan teknologi situs web dan aplikasi web yang terus berlanjut[10]. Diantaranya yaitu:

A01. Broken Access Control

Sebanyak 94% aplikasi yang diuji menunjukkan *broken access control*. Terdapat 34 *Common Weakness Enumeration* (CWE) terkait *Broken Access Control* yang lebih sering muncul dibandingkan kategori keamanan lainnya[14]

A02. Cryptographic Failure

Sebelumnya dikenal sebagai pengungkapan data sensitif, fokus sekarang adalah pada kegagalan kriptografi yang sering mengakibatkan pengungkapan data atau infiltrasi sistem oleh peretas[14].

A03. Injection

Aplikasi telah diuji untuk beberapa jenis injeksi, dan 33 *Common Weakness Enumeration* (CWE) yang terkait dengan kategori ini menduduki peringkat kedua dalam kejadian yang paling banyak terjadi dalam aplikasi. Skrip cross-site sekarang termasuk dalam cakupan kategori ini dalam edisi terbaru.[14].

A04. Insecure Design

Merupakan kategori baru untuk tahun 2021, dengan fokus pada risiko yang terkait dengan *insecure design*. Jika peneliti benar-benar ingin bergeser dalam industri, ini memerlukan lebih banyak penggunaan *threat modeling*, pola dan prinsip desain yang aman, serta arsitektur referensi.[14].

A05. Security Misconfiguration

Aplikasi telah diperiksa untuk berbagai kesalahan konfigurasi. Dengan konfigurasi perangkat lunak yang semakin kompleks, kategori ini meningkat, termasuk XML *External Entities* (XXE)[14].

A06. Vulnerable and Outdated Components

Sebelumnya disebut "*Using Components with Known Vulnerabilities*," kategori ini naik dari peringkat sembilan pada 2017 ke posisi kedua. Ini adalah isu umum yang kini menjadi fokus uji dan penilaian risiko kami[14].

A07. Identification and Authentication Failures

Sebelumnya dikenal sebagai *Broken Authentication*, *Identification and Authentication Failures* kini termasuk dalam CWE yang terkait dengan kegagalan identifikasi. Meskipun masih penting dalam OWASP Top 10, standar kerangka kerja yang meningkat membantu mengatasi masalah ini[14].

A08. Software and Data Integrity Failures

Kategori baru dalam OWASP TOP 10 2021 menekankan risiko dari asumsi terhadap pembaruan perangkat lunak, data krusial, dan pipeline CI/CD tanpa verifikasi integritas, dengan fokus utama pada CWE 18 yang mencakup *Insecure Deserialization*, yang sebelumnya tercantum dalam OWASP TOP 10 2017.

A09. Security Logging and Monitoring Failures

Kategori ini meluas untuk mencakup berbagai jenis kegagalan, menantang untuk diuji, dan kurang terwakili dalam data CVE/CVSS. Namun, kegagalan dalam kategori ini dapat langsung mempengaruhi visibilitas, pemicu peringatan insiden, dan investigasi forensik[10].

A10. Server-Side Request Forgery

Data menunjukkan insiden yang jarang terjadi meskipun tingkat pengujian melebihi rata-rata. Kategori ini mencerminkan situasi di mana para ahli industri menganggap penting, meskipun tidak secara eksplisit terlihat dalam data saat ini[10]

3. Sistem yang Dibangun

3.1 Alat dan Bahan Penelitian

3.1.1 Hardware

Berikut *Hardware* yang digunakan dalam penelitian, yaitu:

Tabel 1. *Hardware*

NO	Nama	Spesifikasi
1.	Model	Windows 10 Pro 64-bit
2.	Processor	Intel core i3-4160 3,60 Ghz
3.	Graphic Card	NVIDIA GeForce GT 1030
4.	RAM	12 Gb

3.1.2 Software

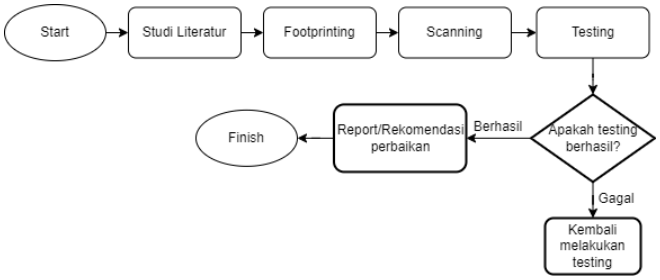
Berikut *software* yang digunakan dalam penelitian, yaitu:

Tabel 2. *Software*

NO	Nama	Spesifikasi	Fungsi
1.	***Virtualbox***	**version 7.0.12.9484**	***Software Virtual Machine***
2.	**Kali Linux**	**kali-linux-2023.3-virtualbox-amd64**	**Sistem Operasi**
3.	**SQL Map**	**version 1.7.11 1030**	***A3. Injection***
4.	**ZAP**	**version 2.14.0**	***Scanning clickjacking, vulnerability***
5.	**burpsuite**	**burpsuite community edition version v2023.9.1**	***A07. Identification and authentication failures, A10. Server Side Request Forgery, A08. Software and Data Integrity Failures***
6.	**Nmap**	**version 7.94**	***Scanning, Identification State, Port, Server.***
7.	**Wappalyzer**	-	***A06. Vulnerable and Outdated Components***
8.	**Wireshark**	**version 4.2.6**	***A02. Cryptographic Failures***

3.2 Prosedur Penelitian

Studi Literatur mengumpulkan data dan informasi terkait penetration testing, OWASP Top 10 2021, dan sistem informasi rumah sakit. *Footprinting* mengumpulkan data seperti IP, server, port, dan sistem operasi, peneliti juga melakukan wawancara dengan unit Tim IT Rumah Sakit. *Scanning* Mengidentifikasi dan memprioritaskan kerentanan dengan tools seperti ZAP. *Testing* melakukan penetration testing sesuai standar OWASP Top 10 2021. *Reporting* membuat laporan hasil *penetration testing*. *Rekomendasi* menyusun panduan untuk memperbaiki sistem informasi rumah sakit.

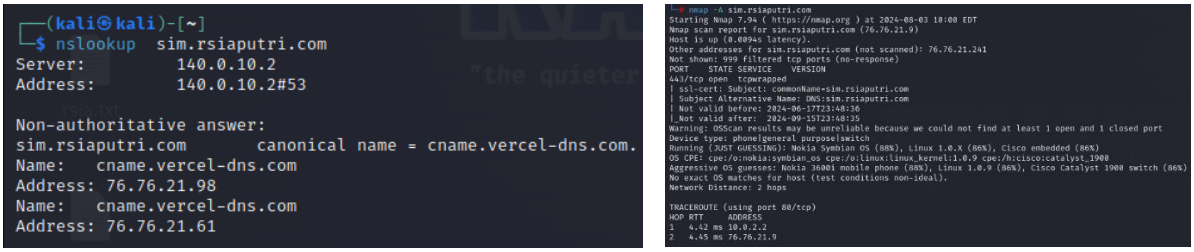


Gambar 1. Flowchart prosedur penelitian

4. Evaluasi

4.1 Hasil *Footprinting*

Dalam tahap *footprinting*, dilakukan analisis menggunakan berbagai tools untuk mengumpulkan informasi tentang domain dan infrastruktur host. Berdasarkan hasil dari Nslookup, domain yang dianalisis adalah RSIA Putri Surabaya, dengan alamat server dan alamat IP yang akan dicantumkan jika ditemukan. Selain itu, hasil pemindaian menggunakan Nmap menunjukkan bahwa port 80/tcp terbuka dan digunakan untuk layanan HTTP dengan penyedia Vercel, sementara port 443/tcp juga terbuka namun dilindungi oleh tcpwrapped. Dari analisis sistem operasi, dapat diperkirakan bahwa host menggunakan *Oracle Virtual Box*, *QEMU*, atau *bay network embedded*. Sertifikat SSL yang digunakan oleh host ini valid dari tanggal 17 Juni 2024 hingga 15 September 2024, dengan nama umum (*Common Name*) RSIA Putri Surabaya. Hasil bisa dilihat pada gambar 3 dan gambar 2.



Gambar 2. Hasil *Scanning* menggunakan nslookup (kanan) dan nmap (kiri)

Tabel 3. Hasil *Footprinting*

No	Tools	Hasil yang ditemukan
1.	Nslookup	Domain, Alamat server, Alamat IP, *Canonical Name.* Bisa dilihat pada gambar 3
2.	Nmap	**Open Port:** **PORT STATE SERVICE VERSION** **port 80/tcp Open HTTP Vercel** **port 443/tcp Open tcpwrapped** **Sistem Operasi:** **(JUST GUESSING) *Oracle Virtual box, QEMU, bay network embedded*.**

4.2 Hasil *Scanning*

Hasil dari *scanning* menggunakan *ZAP* bisa dilihat pada Gambar 4, bahwa dari hasil *scanning* ini terdapat "*missing anti-clickjacking head, CSP Header not set* dan *Cross Domain Misconfiguration"* yang memiliki *medium risk* dengan respon HTTP. Tanpa perlindungan *Anti-Clickjacking*, situs web bisa dimanipulasi oleh penyerang

untuk menipu pengguna agar mengklik sesuatu yang tidak mereka sadari, seperti tombol atau tautan berbahaya. Tidak adanya header *Content Security Policy* (CSP) juga memungkinkan penyerang untuk menyisipkan skrip berbahaya dalam halaman web yang kemudian dieksekusi oleh pengguna. Lalu jika terjadinya *Cross Domain Misconfiguration*, bisa menyebabkan kebocoran informasi penting atau memberikan kesempatan bagi penyerang untuk mengakses data yang tidak seharusnya mereka miliki.

Gambar 4. Hasil *Scanning vulnerability assesment* menggunakan ZAP

4.3 Hasil *Testing*

4.3.1 A01. Broken Access Control

Pada analisis *Broken Access Control* ini dilakukan secara manual dengan login sebagai user dan mengganti URL. Pertama, peneliti login sebagai user, lalu sebagai user, peneliti mengecek apakah menu-menu berjalan normal layaknya user biasa dan apakah semua menu berjalan normal atau ada terjadinya *broken access*. Selanjutnya, peneliti mengganti atau menambahkan URL "/user" menjadi "/admin". Hasil dari testing dengan cara manual ini, menunjukkan bahwa menu berjalan normal dan tidak ditemukan bug atau role menu yang rusak. Untuk hasil testing dengan menambahkan role admin pada URL, seperti yang terlihat pada lampiran 1, akan terjadi 404 not found. Maka, hasil dari keseluruhan testing ini tidak mengindikasikan adanya *Broken Access Control*. Resikojika terjadinya *Broken Access Control* yaitu pengguna memperoleh untuk mengakses data atau fungsi yang seharusnya dibatasi. Ini bisa mengarah pada *unauthorized access to resources* dan *privilege escalation*, resiko iniberdasarkan dari CWE 285: *Improper Authorization.*

4.3.2 AO2. Cryptographic Failures

Pada testing kali ini, dilakukan analisis *cryptographic failures* dengan cara menganalisis sertifikat dan *cipher suite* yang tercapture oleh *tools* Wireshark. Dari hasil analisis ini, ditemukan bahwa beberapa *cipher suite* yang digunakan oleh RSIA Putri Surabaya telah usang atau tidak aman. Hasil analisis sertifikat menunjukkan bahwa semua sertifikat aman dan tervalidasi hingga tahun 2027, serta diterbitkan oleh *Internet Security Research Group* (ISRG). Lampiran 2 menunjukkan *cipher suite* yang digunakan oleh RSIA Putri Surabaya. *Cipher suite* adalah sekumpulan algoritma kriptografi yang digunakan dalam protokol keamanan jaringan seperti TLS (*Transport Layer Security*) dan SSL (*Secure Sockets Layer*). Dalam analisis yang dilakukan, ditemukan bahwa beberapa cipher suite yang digunakan adalah usang dan tidak direkomendasikan lagi seperti TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) yang usang menurut jurnal dari NIST SP 800, karena rentan terhadap serangan *cryptographic* seperti *man-in-the-middle* (MITM) dan serangan *downgrade*. Penggunaan *cipher suite* yang lemah dapat mengakibatkan data sensitif menjadi rentan terhadap dekripsi oleh pihak yang tidak berwenang, mengancam integritas dan kerahasiaan informasi pasien.

4.3.3 A03. Injection

Penetration testing kali ini dilakukan menggunakan tools dan manual dengan cara melakukan “#1*” dan “' OR '1'='1” pada search bar. Lalu di sqlmap dilakukan dengan cara *scanning* 3 parameter yang dimiliki oleh RSIA Putri Surabaya, yaitu /responsivevoice.js?key=lrLmRPNS, /v1/api/authenticate, dan https://sim.rsxyz.com/sign-in. Testing dilakukan dengan membuka SQLMAP di Kali Linux, lalu memulai scan *injection* pada setiap parameter satu per satu. Pada SQLMAP, peneliti memasukkan link RSIA Putri Surabaya seperti contoh "-u rsxyz.com/v1/api/authenticate --dbs". Arti dari "--dbs" ini yaitu menginstruksikan SQLMAP agar menampilkan daftar basis data jika injection ditemukan .Lalu, /responsivevoice.js?key=lrLmRPNS yang tercapture menggunakan Burp Suite pada HTTP History menunjukkan bahwa permintaan ini terkait dengan pembuatan skrip JavaScript dari URL tersebut dengan “**key”** sebagai parameter, dan lrmRPNS sebagai token yang diperlukan oleh skrip untuk berfungsi dengan benar. Setelah itu, peneliti menunggu hasilnya. Hasil dari *testing injection* ini dilakukan dengan scanning 3 parameter, dan hasilnya seperti yang terlihat pada lampiran 3, "*parameter does not seem to be injectable*", yang berarti tools SQLMAP tidak menemukan indikasi bahwa 3 parameter tersebut rentan terhadap serangan SQL injection.

4.3.4 A04. Insecure Design

Dilakukan secara manual, dengan meng-inspect halaman *login* dan mencoba *login*. peneliti menuju ke halaman *login*. Lalu klik kanan pada mouse, peneliti pilih menu "*inspect*". Lalu peneliti cari "*form*" pada hasil *inspect* tersebut untuk melihat apakah ada kecacatan dalam laman login. Setelah itu, peneliti mencoba *login* dengan *username* salah atau *password* yang salah. Hasilnya, ditemukan pop-up pada *login* yang muncul ketika *username*

atau *password* salah. Hal ini mempermudah penyerang untuk mengetahui mana *username/password* yang benar dan salah. Bisa dilihat pada lampiran 4

4.3.5 A05. Security Misconfiguration

Penetration testing *Security Misconfiguration* ini dilakukan dengan cara *directory listing* menggunakan tools dirb. Peneliti menggunakan *wordlist directory listing* agar proses *scanning* bisa lebih maksimal. Salah satu cara untuk mendeteksi *security misconfiguration* adalah dengan mencari direktori atau file yang tidak terlindungi dengan baik di server target. Buka tools dirb di Kali Linux. Lalu peneliti masukkan link RSIA Putri SURABAYA. Contohnya seperti ini "dirb https://rsxyz.com ~/(filename wordlistnya)" bisa dilihat pada lampiran 5. Lalu hasilnya adalah ditemukan 3 link dengan kode status yang berbeda-beda. Link pertama memiliki kode 307, yang artinya server merespons dengan redirect sementara. Link kedua memiliki kode 200, yang berarti sukses dan dapat diakses. Link terakhir memiliki kode 308, yang artinya server merespons dengan redirect permanen. Tidak ada indikasi *directory listing* yang aktif di server yang digunakan oleh RSIA Putri Surabaya. Semua URL yang ditemukan menunjukkan file atau redirect, bukan daftar direktori yang terbuka.

4.3.6 A06. Vulnerability and Outdated Components

Menggunakan tools ekstensi yaitu Wappalyzer untuk mengidentifikasi teknologi yang digunakan RSIA Putri Surabaya dan menganalisis teknologi yang sudah usang atau kadaluarsa. Disini menggunakan tools Wappalyzer, peneliti download Wappalyzer di ekstensi Google. Lalu pergi ke rsxyz.com. Klik ikon ekstensi, lalu pilih Wappalyzer. Contohnya bisa dilihat pada lampiran 6. Hasil dari penetration testing *Vulnerable and Outdated Components* menggunakan ekstensi Wappalyzer memberikan informasi apa saja yang ditemukan. Hasilnya menunjukkan bahwa server yang digunakan yaitu Vercel, terdapat multiple IPs, menggunakan javascript framework berupa react dan emotion yang tidak ada versinya dan Firebase yang digunakan masih menggunakan versi 8.10.1, sedangkan versi terbaru adalah 9.x. Menggunakan versi Firebase yang usang dapat membuka berbagai kerentanan yang serius, seperti bypass otentikasi, serangan XSS, dan bug yang mengganggu fungsionalitas aplikasi. Rekomendasi untuk melakukan scanning source code.

4.3.7 A07. Identification and Authentication Failures

Menggunakan tools Burp Suite, penetration testing ini dilakukan dengan cara *dictionary attack* berdasarkan CWE 521: *Weak Password Requirements* sebanyak 202 kali. Peneliti menggunakan password list global. Daftar dari *password list* ini digunakan dalam serangan *dictionary attack*, di mana seorang penyerang mencoba mencocokkan kata sandi dari daftar tersebut dengan kata sandi yang digunakan. Caranya yaitu, buka Burpsuite, pada tab *Intruder*, di bagian kanan, pilih "clear $" terlebih dahulu, lalu tambahkan "$" pada bagian depan dan belakang *password*, seperti contoh "password:$"123"$". Setelah itu, menuju bagian *Payload*, pilih *Payload* set: 1 dan *Payload type*: *simple list*. Pilih load untuk meng-upload *list password* yang telah di-download oleh peneliti. Lalu pilih *Start Attack* dan tunggu hasilnya. Peneliti melakukan *testing* sebanyak 202 kali, seperti pada lampiran 7, tetapi tidak ditemukan kerentanan. Hal ini ditunjukkan oleh *status code* 400 pada masing-masing *list password*. Status code 400 artinya "*Bad Request*", yang berarti server tidak dapat memproses permintaan yang dikirim oleh peneliti.

4.3.8 A08. Software and Data Integrity Failures

Penelitian ini fokus pada pengujian *endpoint* API /v1/api/rawat-jalan/monitoring untuk menilai potensi kerentanan perangkat lunak dan integritas data. Pengujian melibatkan modifikasi parameter "noRm, namaPasien, dan dokterId" dengan nilai tidak valid, serta uji kerentanan *Cross-Site Scripting* (XSS) dengan menyisipkan kode "<script>alert('XSS')</script>" pada parameter poli. Hasil pengujian menunjukkan bahwa aplikasi merespons dengan *status cod*e 200 OK dan memberikan data kosong saat parameter diubah dengan nilai tidak valid, menandakan aplikasi menjaga integritas data dengan baik. Saat menyisipkan kode berbahaya, aplikasi merespons dengan *status cod*e 400 *Bad Request*, menunjukkan aplikasi aman dari serangan XSS. Pengujian *pagination* dengan mengubah parameter "pageSize" dari 10 menjadi 2 juga menunjukkan bahwa aplikasi berfungsi sesuai dengan parameter yang dikirim. Secara keseluruhan, aplikasi menunjukkan kemampuan yang baik dalam menangani parameter, input berbahaya, dan pagination, serta menjaga keamanan dan integritas data dengan efektif.

4.3.9 A09. Security Loging and Monitoring

Disini peneliti mendapat izin untuk *login* sebagai admin, hal ini dilakukan dengan cara manual melalui *login* menjadi admin, lalu dilakukan pengecekan, apakah sistem melakukan pencatatan dan monitoring. Caranya yaitu, *Login* sebagai admin, lalu melakukan analisa secara manual, apakah ada sistem *monitoring* pada *role* admin, dan pada role *admin*, peneliti menemukan bahwa ada menu *monitoring* yang berfungsi untuk mencatat siapa saja yang *login* atau *logout*, dan bahkan bisa melakukan *logout* paksa pada *user* yang *login*. Hasilnya yaitu, di menu admin RSIA Putri Surabaya, terdapat menu *Monitoring* dan Pengguna, bisa dilihat pada lampiran 9. Seperti pada menu

Monitoring disini admin bisa memonitoring siapa saja yang baru *login* dan *logout* dan juga ada keterangan waktu *login/logout*, IP, *Login ID*, dan *User Level.*

4.3.10 A10. Server-Side Request Forgery

Testing SSRF(*Server-side Request Forgery)* pada sistem informasi RSIA Putri Surabaya, peneliti menguji parameter *ip_address* pada endpoint /v1/api/authenticate untuk mengidentifikasi potensi kerentanan. Peneliti mengirimkan berbagai nilai untuk parameter tersebut, termasuk URL dan IP internal seperti http://169.254.169.254/latest/meta-data/ dan http://127.0.0.1:8080 seperti contoh bisa dilihat pada lampiran 10. Hasil pengujian menunjukkan bahwa server memberikan respon *status code* 200 OK meskipun URL/IP yang digunakan tidak relevan atau panjang input tidak melebihi 25 karakter, serta respon dengan *status code* 400 *Bad Reques*t jika panjang input karakter melebihi dari 25 karakter. Ini mengindikasikan bahwa parameter *ip_address* tidak mengungkapkan data internal atau data yang sensitif, dan validasi panjang input yang diterapkan di bagian *ip_address* mengurangi risiko SSRF. Berdasarkan hasil ini, tidak ada indikasi kerentanan SSRF dari pengujian tersebut.

4.4 Dashboard Website Penelitian

Lampiran 14 menunjukkan tampilan dashboard web yang berisi video demo dan penjelasan saat melakukan *testing*. Pada dashboard website terdapa keterangan *open vulnerabilities* dan *closed vulnerabilities* yang menunjukan status pada testing A01 hingga A10.

4.5 Rekomendasi Perbaikan

Tabel 4. Hasil kerentanan dan rekomendasi

Kerentanan	**Ditemukan**	**Perbaikan**
A02. Cryptographic Failures	Ada penggunaan *cipher suite* yang usang	Gunakan algoritma kriptografi yang direkomendasikan, seperti AES untuk enkripsi dan SHA-256 untuk hashing. Perbaikan ini berdasarkan standarisasi dari CWE 310: *Cryptographic Issues*
A04. Insecure design	Pop up pada halaman login muncul ketika *username* atau *password* salah, ini akan membuat penyerang lebih mudah mengetahui jika salah satu dari *username* atau *password* yang digunakan penyerang itu salah.	Gunakan *error message* yang umum dan tidak memberikan detail spesifik tentang apakah *username* atau *password* yang salah, ini adalah rekomendasi perbaikan berdasarkan CWE 209: *Generation of Error Message Containing Sensitive Information*
A06. Vulnerable and Outdated Components	*Firebase* yang digunakan masih menggunakan versi 8.10.1 sedangkan yang terbaru versi 9.x	Perbaikan berdasarkan standarisasi CWE 1104: *Use of Unmaintained Third-Party Components* yaitu audit secara berkala semua komponen yang digunakan untuk memastikan bahwa mereka tetap *up-to-date* dengan versi terbaru dan bebas dari kerentanan yang diketahui.

5. Kesimpulan

Peneliti mengevaluasi kerentanan SIMRS di RSIA PUTRI SURABAYA menggunakan metode OWASP Top 10 2021 dan menemukan tiga kerentanan utama: *A02. Cryptographic Failures, A04. Insecure Design, dan A06. Vulnerable and Outdated Components*. Kerentanan ini disebabkan oleh penggunaan *cipher suite* yang usang, desain pop-up yang menampilkan *username/password* yang salah, serta komponen perangkat lunak yang ketinggalan zaman. Ini dapat membahayakan keamanan data sensitif pasien. Peneliti merekomendasikan perbaikan berdasarkan pedoman *Common Weakness Enumeration* (CWE). Selain itu, peneliti menyusun surat validasi hasil penelitian dan dashboard web yang mencakup video pengujian serta daftar penjelasan OWASP Top 10. Surat validasi ditandatangani oleh peneliti dan Kepala Unit IT RSIA Putri Surabaya sebagai langkah awal untuk meningkatkan keamanan sistem informasi rumah sakit.

Daftar Pustaka

[1] Marufah, N., Rahmat, H. K., & Widana, I. D. K. K. (2020). Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia. NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7(1), 191-201.

[2] Open Web Application Security Project. (2021). SQL Injection. OWASP. https://owasp.org/www-community/attacks/SQL_injection .

[3] Andi Dermawan Putra, Muhammad Siri Dangnga, & Makhrajani Majid. (2020).”Evaluasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) Dengan Metode HOT FIT di RSUD Andi Makkasau k

[4] Andria. (2020). “Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux”. Generation Journal, 4(2).

[5] Priyawati, D., Rokhmah, S., & Utomo, I. C. (2022). Website Vulnerability Testing and Analysis of Website Application Using OWASP. International Journal of Computer and Information System (IJCIS), 3(3).

[6] Hidayatullah, S., & Sapta Aji, D. (2021). “Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)".Jurnal Algoritma,18(1). https://doi.org/10.33364/algoritma/v.18-1.8

[7] Glemser, T. (2022). OWASP Top 10. Datenschutz Und Datensicherheit - DuD, 46(11).https://doi.org/10.1007/s11623-022-1685-5

[8] Ferrara, P., Mandal, A., Cortesi, A., & Spoto, F. (2019). “Static Analysis for the OWASP IoT Top 10 2018”. Proceedings of SPIoT’19.)

[9] Yudiana, Y., Elanda, A., & Buana, R. L.(2021).“Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10”. CESS (Journal of Computer Engineering,System and Science), 6(2).https://doi.org/10.24114/cess.v6i2.2477729

[10] Yum Thurfah Afifa Rosaliah, Jayanta, B. H. (2021). Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM. Senamika, 2(September).

[11] Putra, A. D., Dangnga, M. S., Program, M. M., Kesehatan, S., Fakultas,M., Kesehatan, I., & Parepare, U. M. (n.d.). Januari 2020 pISSN 2614-5073(Vol. 1, Issue 1). http://jurnal.umpar.ac.id/index.php/makes

[12] Riyandhanu, I. O. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. Jurnal Informasi Dan Teknologi. https://doi.org/10.37034/jidt.v4i3.236

[13] Glemser, T. (2022). OWASP Top 10. DatenschutzUndDatensicherheit-DuD,46(11).https://doi.org/10.1007/s11623-022-1685-5

[14] Open Web Application Security Project. (2021, November 23). OWASP Top 10 - 2021.OWASP . https://owasp.org/www-project-top-ten/

[15] Andria. (2020). “Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux”. Generation Journal, 4(2). https://doi.org/10.29040/ijcis.v3i3.90

[16] Raazi, I. M., Studi, P., & Informasi, T. (2023). Sistem Informasi Manajemen Kepegawaian dengan Metode NIST SP 800-115 pada Universitas Islam Negeri Ar-Raniry. Tugas Akhir. Fakultas Sains dan Teknologi, Universitas Islam Negeri Ar-Raniry.

[17] Dwiyanto, S. (2020). “Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap”. PROSISKO: Jurnal Pengembangan RisetDan Observasi Sistem Komputer, 7(2). https://doi.org/10.30656/prosisko.v7i2.2522

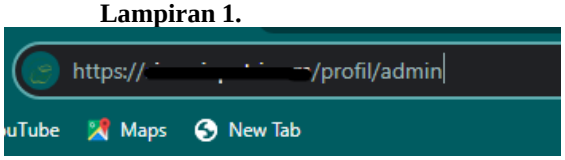
[18] Rochman, A., Rohian Salam, R., Sandi Agus Maulana Sekolah Tinggi Manajemen Ilmu Komputer, dan, & Likmi, S. (2021). “Analisis Keamanan Website dengan Information System Security Assessment Framework(ISSAF) dan Open Web Application Security Project, 2(4).

[19] Yusuf, Rangga Renaldi, and Teguh Nurhadi Suharsono. (2023) "PENGUJIAN KEAMANAN DENGAN METODE OWASP TOP 10 PADA WEBSITE EFORMHELPDESK." *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi dan Teknik*. Vol. 5. 2023.

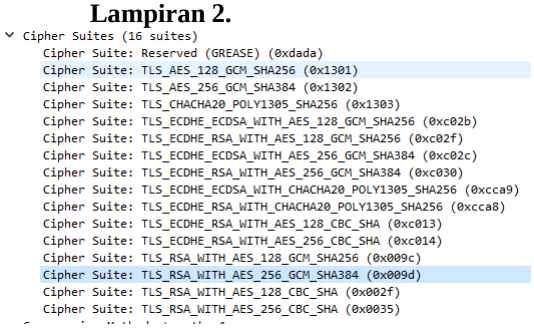
[20] Jurnal H, Putu N, Rainita A, Agung A, Callysta Athalia I, Ananta P, et al. Jurnal Informatika Dan Teknologi Komputer Analisis Perbandingan Vulnerability Scanning Pada Website Dvwa Menggunakan Owasp Nikto Dan Burpsuite. 2023;3(Juli

Lampiran

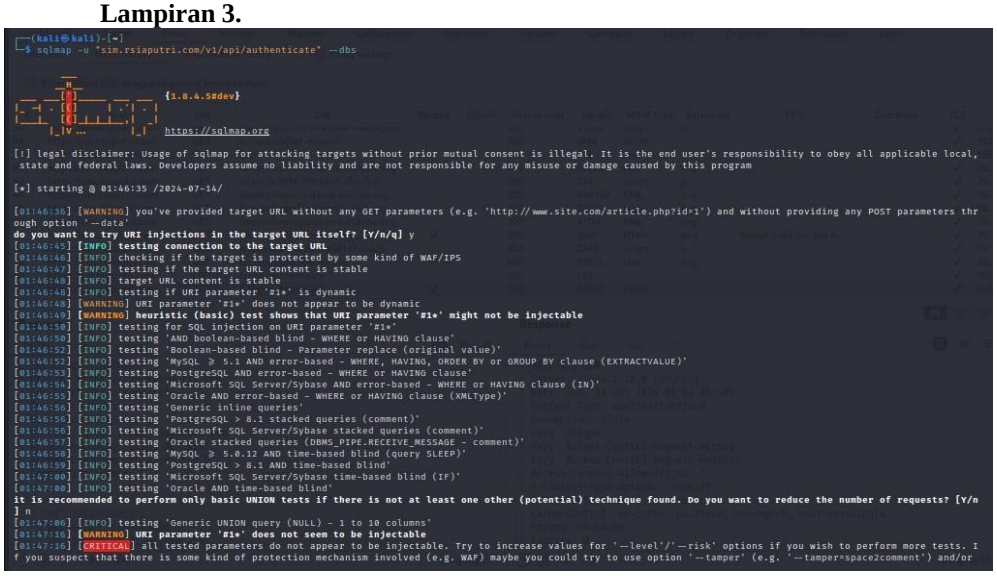
Lampiran 1.



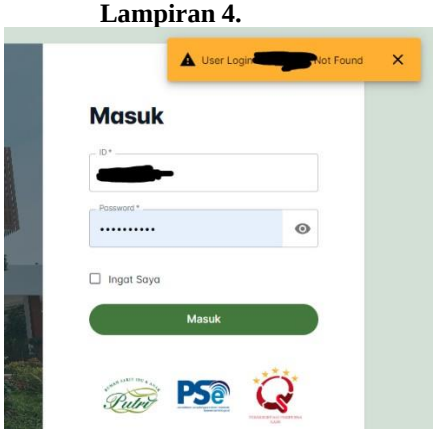
Lampiran 2.



Lampiran 3.



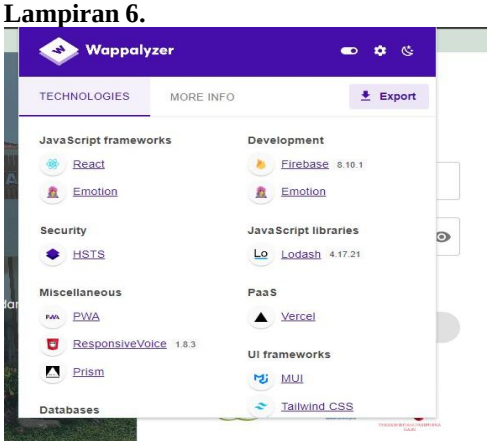
Lampiran 4.



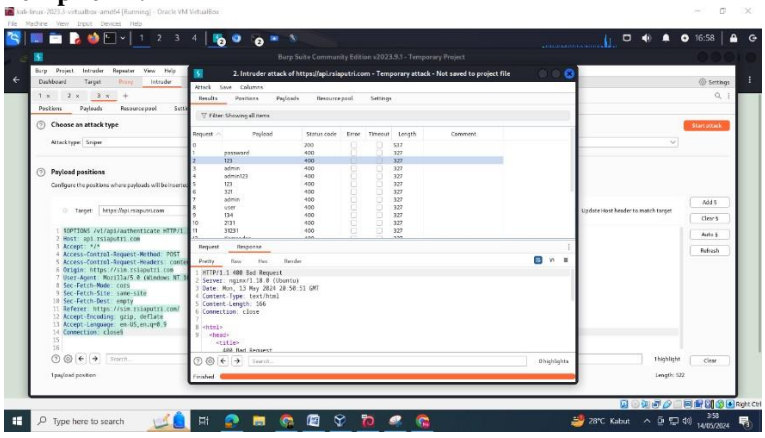
Lampiran 5.

```
┌──(kali㉿kali)-[~]
└─$ dirb https://sim.rsiaputri.com/ ~/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jul 23 02:21:23 2024
URL_BASE: https://sim.rsiaputri.com/
WORDLIST_FILES: /home/kali/common.txt

-----------------

GENERATED WORDS: 4729

---- Scanning URL: https://sim.rsiaputri.com/ ----
+ https://sim.rsiaputri.com/_src (CODE:307|SIZE:15)
+ https://sim.rsiaputri.com/favicon.ico (CODE:200|SIZE:15406)
^[[B^[[B^[[B
+ https://sim.rsiaputri.com/render/https://www.google.com (CODE:308|SIZE:15)

-----------------
END_TIME: Tue Jul 23 02:26:38 2024
DOWNLOADED: 4729 - FOUND: 3
```

Lampiran 6.



Lampiran 7.



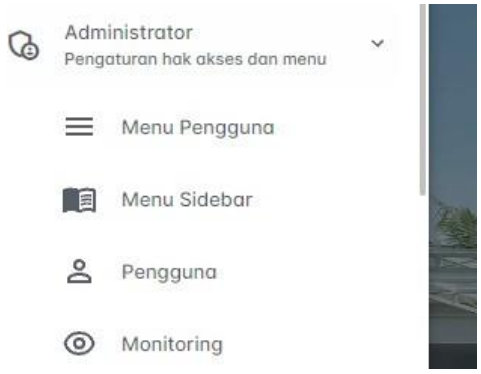
Lampiran 8.

Request

Pretty Raw Hex

```
1 GET /v1/api/rawat-jalan/monitoring?poli=anak&filter=&pageSize=10&pageNo=0&sortBy=id&
  sort=desc&startDate=2024-07-27&endDate=2024-07-27&noRm=12345&namaPasien=&namaDokter=&
  jenisPembiayaan=&dokterId=&jadwalId= HTTP/1.1
2 Host: api.rsiaputri.com
3 Sec-Ch-Ua:
4 Accept: application/json, text/plain, */*
5 Sec-Ch-Ua-Mobile: ?0
6 Authorization: Bearer
  eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIyMDIzMDUwMDkyIiwiZXhwIjoxNzIyMDc5ODAyLCJpYXQiOjE3MjIwN
  jkwMDJ9.T_arPjPxJsUCGsEL16vJK6Q3xOkIHOymEWAzMk1KjNU
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/115.0.5790.171 Safari/537.36
8 Sec-Ch-Ua-Platform: ""
9 Origin: https://sim.rsiaputri.com
10 Sec-Fetch-Site: same-site
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://sim.rsiaputri.com/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
```

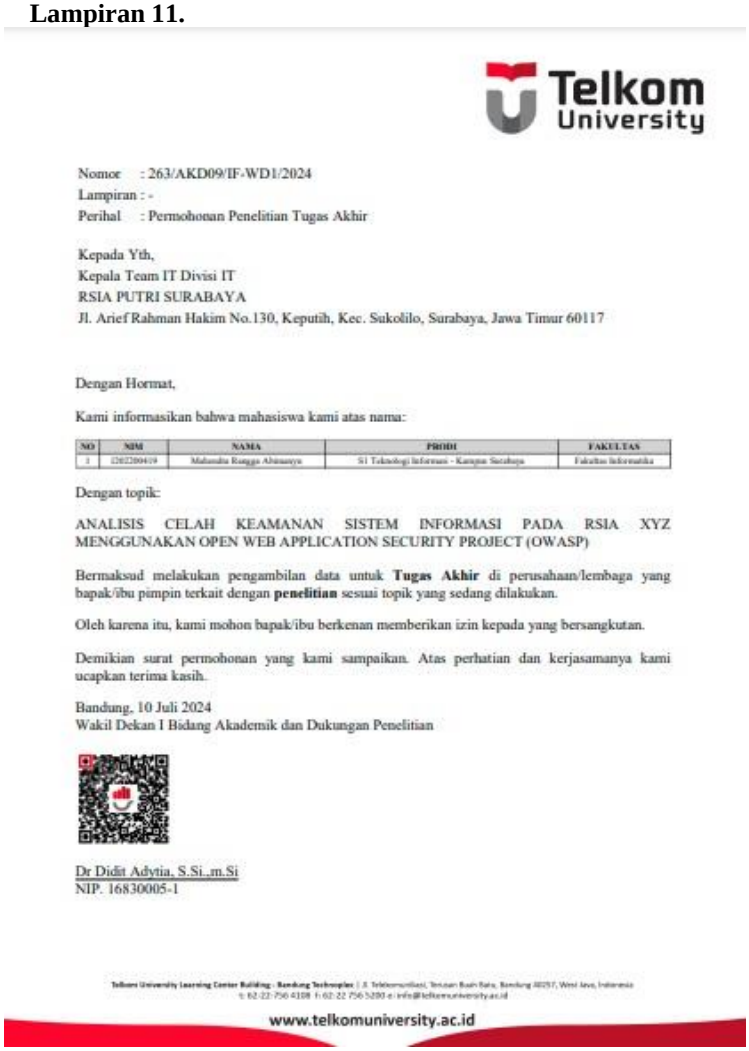
Lampiran 9.



Lampiran 10

```
Referer: https://sim.rsiaputri.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: open

{
  "id":"2023050092",
  "password":"Komandan80",
  "ip_address":"http://127.0.0.1:8080",
  "token":null
}
```

Lampiran 11.



Telkom University

Nomor : 263/AKD09/IF-WD1/2024
Lampiran : -
Perihal : Permohonan Penelitian Tugas Akhir

Kepada Yth,
Kepala Team IT Divisi IT
RSIA PUTRI SURABAYA
Jl. Arief Rahman Hakim No.130, Keputih, Kec. Sukolilo, Surabaya, Jawa Timur 60117

Dengan Hormat,

Kami informasikan bahwa mahasiswa kami atas nama:

NO	NIM	NAMA	PRODI	FAKULTAS
1	[illegible]	[illegible]	[illegible]	[illegible]

Dengan topik:

ANALISIS CELAH KEAMANAN SISTEM INFORMASI PADA RSIA XYZ MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP)

Bermaksud melakukan pengambilan data untuk **Tugas Akhir** di perusahaan/lembaga yang bapak/ibu pimpin terkait dengan **penelitian** sesuai topik yang sedang dilakukan.

Oleh karena itu, kami mohon bapak/ibu berkenan memberikan izin kepada yang bersangkutan.

Demikian surat permohonan yang kami sampaikan. Atas perhatian dan kerjasamanya kami ucapkan terima kasih.

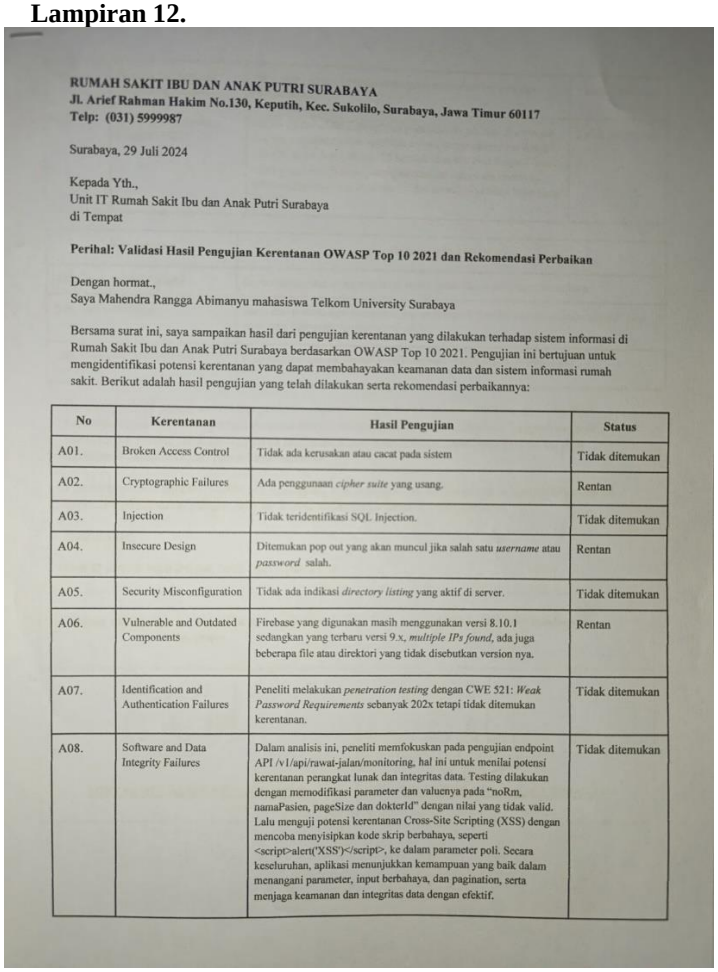
Bandung, 10 Juli 2024
Wakil Dekan I Bidang Akademik dan Dukungan Penelitian

Dr Didit Adytia, S.Si.,m.Si
NIP. 16830005-1

[illegible]

www.telkomuniversity.ac.id

Lampiran 12.



RUMAH SAKIT IBU DAN ANAK PUTRI SURABAYA
Jl. Arief Rahman Hakim No.130, Keputih, Kec. Sukolilo, Surabaya, Jawa Timur 60117
Telp: (031) 5999987

Surabaya, 29 Juli 2024

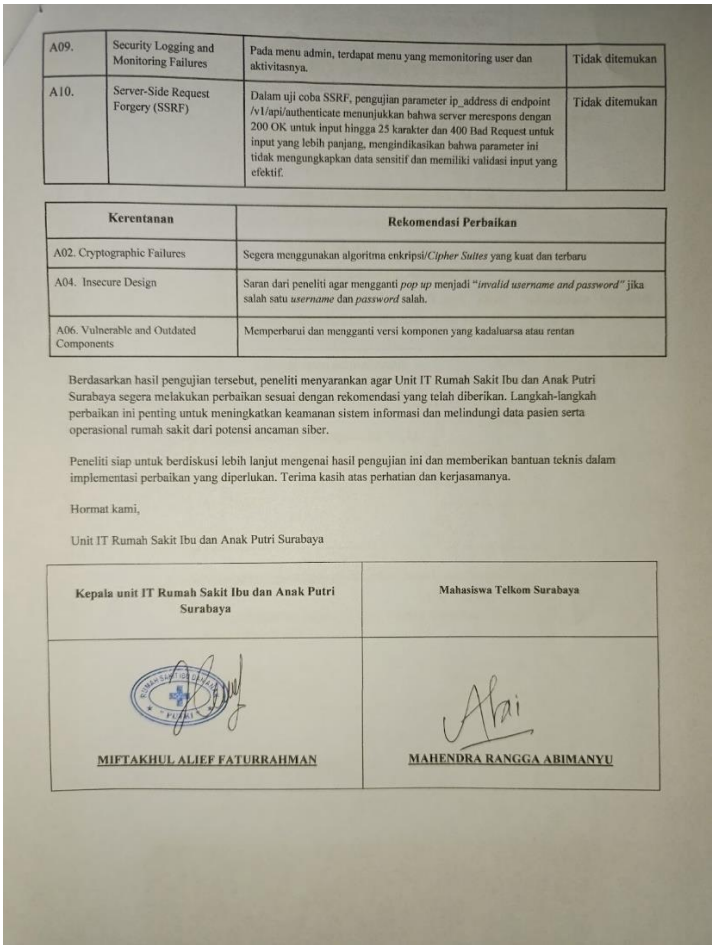
Kepada Yth.,
Unit IT Rumah Sakit Ibu dan Anak Putri Surabaya
di Tempat

Perihal: Validasi Hasil Pengujian Kerentanan OWASP Top 10 2021 dan Rekomendasi Perbaikan

Dengan hormat.,
Saya Mahendra Rangga Abimanyu mahasiswa Telkom University Surabaya

Bersama surat ini, saya sampaikan hasil dari pengujian kerentanan yang dilakukan terhadap sistem informasi di Rumah Sakit Ibu dan Anak Putri Surabaya berdasarkan OWASP Top 10 2021. Pengujian ini bertujuan untuk mengidentifikasi potensi kerentanan yang dapat membahayakan keamanan data dan sistem informasi rumah sakit. Berikut adalah hasil pengujian yang telah dilakukan serta rekomendasi perbaikannya:

No	Kerentanan	Hasil Pengujian	Status
A01.	Broken Access Control	Tidak ada kerusakan atau cacat pada sistem	Tidak ditemukan
A02.	Cryptographic Failures	Ada penggunaan *cipher suite* yang usang.	Rentan
A03.	Injection	Tidak teridentifikasi SQL Injection.	Tidak ditemukan
A04.	Insecure Design	Ditemukan pop out yang akan muncul jika salah satu *username* atau *password* salah.	Rentan
A05.	Security Misconfiguration	Tidak ada indikasi *directory listing* yang aktif di server.	Tidak ditemukan
A06.	Vulnerable and Outdated Components	Firebase yang digunakan masih menggunakan versi 8.10.1 sedangkan yang terbaru versi 9.x, *multiple IPs found*, ada juga beberapa file atau direktori yang tidak disebutkan version nya.	Rentan
A07.	Identification and Authentication Failures	Peneliti melakukan *penetration testing* dengan CWE 521: *Weak Password Requirements* sebanyak 202x tetapi tidak ditemukan kerentanan.	Tidak ditemukan
A08.	Software and Data Integrity Failures	Dalam analisis ini, peneliti memfokuskan pada pengujian endpoint API /v1/api/rawat-jalan/monitoring, hal ini untuk menilai potensi kerentanan perangkat lunak dan integritas data. Testing dilakukan dengan memodifikasi parameter dan valuenya pada "noRm, namaPasien, pageSize dan dokterId" dengan nilai yang tidak valid. Lalu menguji potensi kerentanan Cross-Site Scripting (XSS) dengan mencoba menyisipkan kode skrip berbahaya, seperti <script>alert('XSS')</script>, ke dalam parameter poli. Secara keseluruhan, aplikasi menunjukkan kemampuan yang baik dalam menangani parameter, input berbahaya, dan pagination, serta menjaga keamanan dan integritas data dengan efektif.	Tidak ditemukan



A09.	Security Logging and Monitoring Failures	Pada menu admin, terdapat menu yang memonitoring user dan aktivitasnya.	Tidak ditemukan
A10.	Server-Side Request Forgery (SSRF)	Dalam uji coba SSRF, pengujian parameter ip_address di endpoint /v1/api/authenticate menunjukkan bahwa server merespons dengan 200 OK untuk input hingga 25 karakter dan 400 Bad Request untuk input yang lebih panjang, mengindikasikan bahwa parameter ini tidak mengungkapkan data sensitif dan memiliki validasi input yang efektif.	Tidak ditemukan

Kerentanan	Rekomendasi Perbaikan
A02. Cryptographic Failures	Segera menggunakan algoritma enkripsi/*Cipher Suites* yang kuat dan terbaru
A04. Insecure Design	Saran dari peneliti agar mengganti *pop up* menjadi "*invalid username and password*" jika salah satu *username* dan *password* salah.
A06. Vulnerable and Outdated Components	Memperbarui dan mengganti versi komponen yang kadaluarsa atau rentan

Berdasarkan hasil pengujian tersebut, peneliti menyarankan agar Unit IT Rumah Sakit Ibu dan Anak Putri Surabaya segera melakukan perbaikan sesuai dengan rekomendasi yang telah diberikan. Langkah-langkah perbaikan ini penting untuk meningkatkan keamanan sistem informasi dan melindungi data pasien serta operasional rumah sakit dari potensi ancaman siber.

Peneliti siap untuk berdiskusi lebih lanjut mengenai hasil pengujian ini dan memberikan bantuan teknis dalam implementasi perbaikan yang diperlukan. Terima kasih atas perhatian dan kerjasamanya.

Hormat kami,

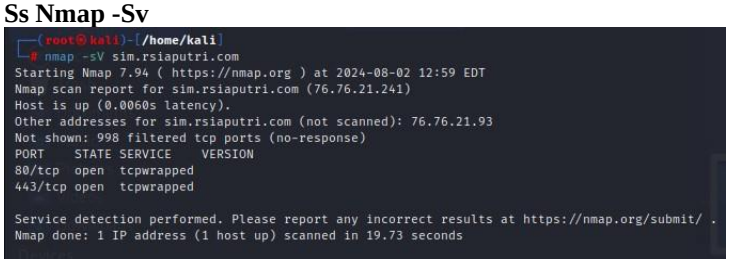
Unit IT Rumah Sakit Ibu dan Anak Putri Surabaya

Kepala unit IT Rumah Sakit Ibu dan Anak Putri Surabaya	Mahasiswa Telkom Surabaya
MIFTAKHUL ALIEF FATURRAHMAN	MAHENDRA RANGGA ABIMANYU

Ss Nmap -A

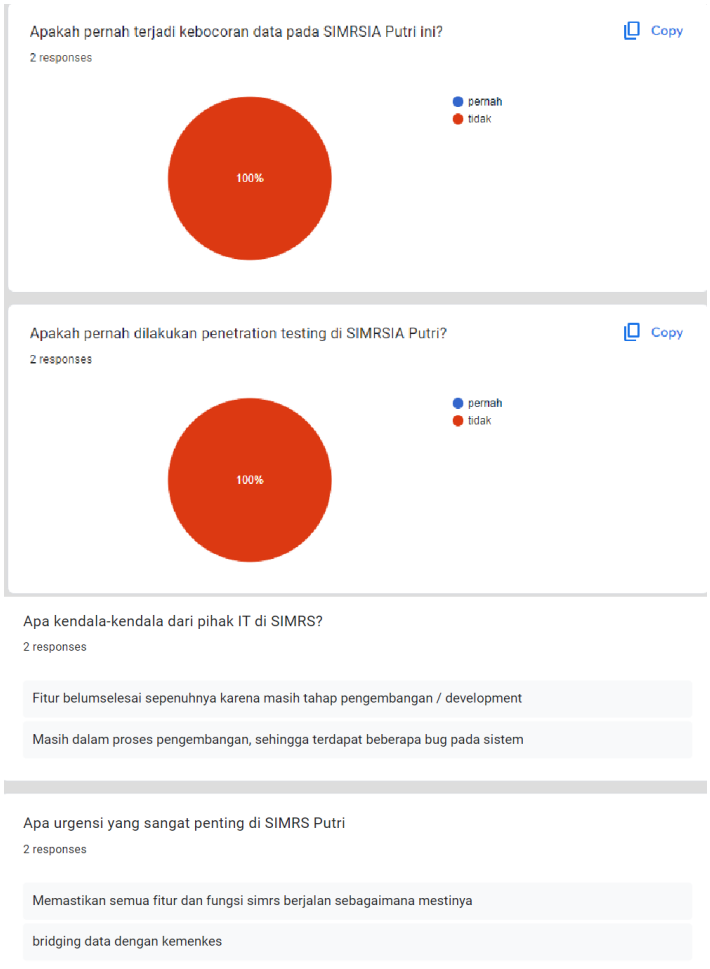
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A sim.rsiaputri.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-02 12:53 EDT
Nmap scan report for sim.rsiaputri.com (76.76.21.61)
Host is up (0.0040s latency).
Other addresses for sim.rsiaputri.com (not scanned): 76.76.21.22
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http       Vercel
|_http-title: Site doesn't have a title (text/plain).
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 308 Permanent Redirect
|     Content-Type: text/plain
|     Location: https:///nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Refresh: 0;url=https:///nice%20ports%2C/Tri%6Eity.txt%2ebak
|     server: Vercel
|     Redirecting...
|   GetRequest, HTTPOptions:
|     HTTP/1.0 308 Permanent Redirect
|     Content-Type: text/plain
|     Location: https:///
|     Refresh: 0;url=https:///
|     server: Vercel
|_    Redirecting...
|_http-server-header: Vercel
443/tcp open  tcpwrapped
| ssl-cert: Subject: commonName=sim.rsiaputri.com
| Subject Alternative Name: DNS:sim.rsiaputri.com
| Not valid before: 2024-06-17T23:48:36
|_Not valid after:  2024-09-15T23:48:35
```

Ss Nmap -Sv

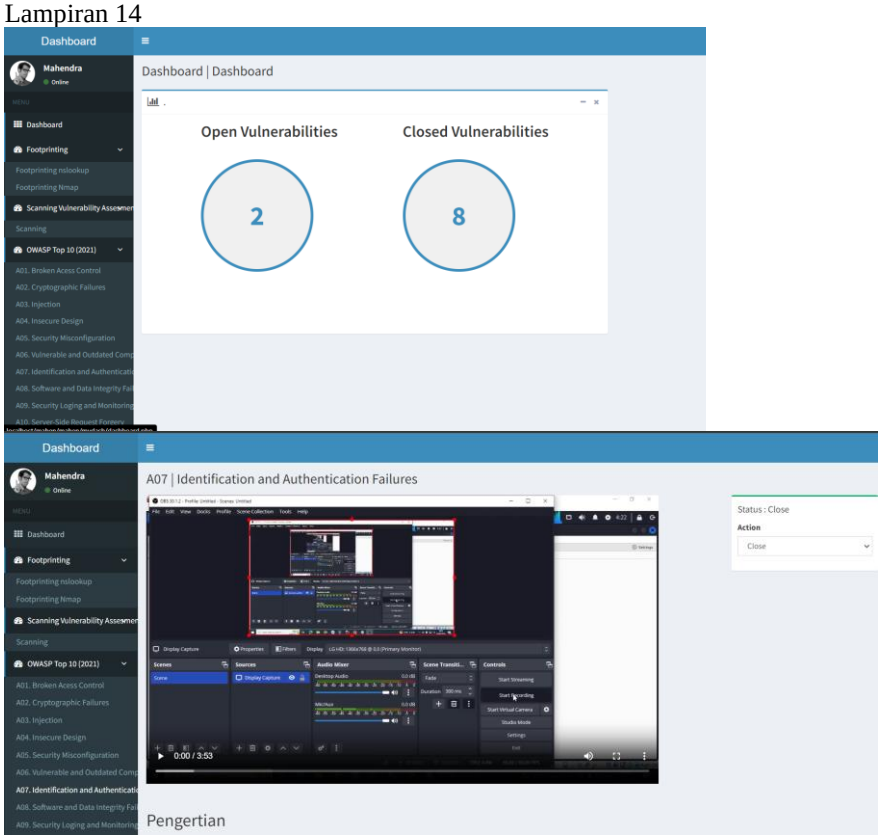


Ss nmap -O

Lampiran 13



Lampiran 14


Dashboard
Mahendra
Online
Dashboard | Dashboard
Open Vulnerabilities
Closed Vulnerabilities
2
8
Dashboard
Mahendra
Online
A07 | Identification and Authentication Failures
Status : Close
Action
Close
0:00 / 3:53
Pengertian