Vulnerability Assessment pada Website Rekruitasi Asisten (IRIS) Fakultas Rekayasa Industri menggunakan Nikto dan Nessus

1st Muliya Dewi
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
muliyadewi@student.telkomuniversity.ac.id

2nd Avon Budiono
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
avonbudi@telkomuniversity.ac.id

3rd Umar Yunan Kurnia Septo Hediyanto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

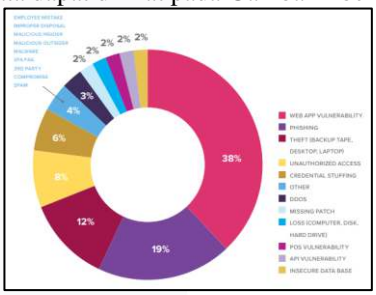
Abstrak—Perkembangan teknologi dan IT saat ini sudah sangat pesat, salah satunya adalah dengan adanya penggunaan website sebagai penunjang berbagai aktivitas manusia. Berdasarkan kemudahan tersebut hampir seluruh perusahaan, industri, hingga institusi pendidikan memiliki website untuk menunjang proses bisnis beserta aktivitas yang ada didalamnya. Fakultas Rekayasa Industri (FRI) sebagai fakultas yang mengedepankan teknologi juga memanfaatkan teknologi website untuk menunjang proses administratif. Salah satu kegiatan administratif di Fakultas Rekayasa Industri (FRI) yang memanfaatkan teknologi website adalah proses rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri (FRI). Namun dari semua kemudahan dan dampak positif dari website, terdapat juga ancaman terhadap keamanan website itu sendiri. Oleh karena itu, untuk mengamankan website diperlukan metode vulnerability assessment untuk mengetahui celah kerentanan yang ada agar dapat diperbaiki sebelum terjadi penyerangan atau eksploitasi oleh pihak yang tidak bertanggung jawab. Dalam penelitian ini akan dilakukan vulnerability assessment menggunakan dua tools utama yaitu Nikto dan Nessus. Hasil yang didapat setelah proses vulnerability scan dan vulnerability assessment menujukkan jenis kerentanan dan tingkat risiko yang berbeda. Hasil tool Nikto menunjukkan 13 celah kerentanan pada sistem. Tool Nessus menunjukkan 136 celah kerentanan yang terdiri dari 6 level critical, 3 level high, 12 level medium, 8 level low, dan 107 level informational.

***Kata kunci— vulnerability assessment, vulnerability scan, vulnerability analysis, nikto, nessus*.**

I. PENDAHULUAN

Perkembangan teknologi dan IT saat ini sudah sangat pesat, salah satunya adalah dengan adanya penggunaan *website*. Dengan adanya penggunaan *website* ini dapat memberikan dampak positif, khususnya untuk membantu kegiatan dan pekerjaan manusia yang awalnya masih bersifat manual menjadi teroromatisasi dengan sistem, selain itu dengan penggunaan *website* memungkinkan informasi dapat diakses dimana saja dan kapan saja tanpa adanya batasan tempat dan waktu. Berdasarkan kemudahan tersebut hampir seluruh perusahaan, industri, pemerintahan, hingga institusi pendidikan memiliki *website* untuk menunjang proses bisnis beserta aktivitas yang ada didalamnya.

Namun dari berbagai kemudahan dan dampak positif dari pemanfaatan teknologi *website*, terdapat ancaman terhadap keamanan dari *website* itu sendiri. *Website* sebagai penyedia informasi tentunya menyimpan banyak data-data sensitif baik data pengguna maupun data yang ada dalam *website*. Berdasarkan data dari F5 Labs dalam artikel "*Lesson Learned from A Decade Data Breach*" penyebab utama adanya insiden kebocoran data adalah *web application vulnerability* (Boddy & Pompon, 2017). Grafik mengenai penyebab kebocoran data dapat dilihat pada Gambar 1 berikut.



GAMBAR 1
PENYEBAB INSIDEN KEBOCORAN DATA MENURUT F5 LABS

Dari gambar diatas, *web application vulnerability* mencapai angka 38% dari seluruh penyebab kebocoran data. Menurut Badan Siber dan Sandi Negara (BSSN) beberapa kerentanan yang banyak ditemui pada *website* diantaranya adalah *cross-site scripting* (XSS), *clickjacking*, *posible burteforce*, *insecure direct object reference*, SQL *injection*, *uncrypted communication*, *cleartext submission password*, *week password*, *sensitive data exposure*, dan *directory listing* (Badan Siber dan Sandi Negara, 2022).

Dari data diatas maka diperlukan pengamanan terhadap aplikasi *website* menggunakan metode *vulnerability assessment* untuk melihat celah kerentanan pada sebuah aplikasi web untuk meminimalisir bahkan menghindari adanya kebocoran data. Target pada penelitian ini adalah salah satu *website* milik Fakultas Rekayasa Industri Universitas Telkom. *Website* tersebut adalah website yang digunakan untuk proses administratif rekruitasi asisten praktikum dan laboratorium. Dalam melakukan *vulnerability assessment* pada *website* IRIS, menggunakan dua *tools* yaitu Nikto dan Nessus.

Tujuan dari penelitian ini adalah menerapkan metode *vulnerability assessment* yang terdiri dari tahap *vulnerability*

scan dan *vulnerability analysis* untuk memenemukan celah kerentanan terhadap web target. Selain itu dalam penelitian ini juga bertujuan merekomendasikan solusi perbaikan berdasarkan celah kerentanan yang ditemukan pada tahap *vulnerability scan* menggunakan Nikto dan Nessus.

II. KAJIAN TEORI

A. *Website*

Website merupakan sekumpulan halaman yang berisi data dan informasi yang disediakan melalui internet yang dapat diakses tanpa adanya batasan waktu dan tempat serta dipublikasikan baik oleh perorangan maupun organisasi. *Website* dapat menyediakan banyak informasi seperti berita, politik, hukum, budaya, hiburan, ekonomi, dan masih banyak informasi lainnya yang dapat disediakan, *website* menampilkan informasi dalam tulisan text, gambar, audio, bahkan video (Primastomo et al., 2015).

B. *Vunerability Assessment*

Vulnerability assessment merupakan proses penting untuk menyelidiki kerentanan, kelemhan, serta kekurangan dalam sebuah sistem. Dengan melakukan *vulnerability assessment* dapat membantu lembaga, organisasi, maupun perorangan dalam menghilangkan masalah keamanan sebelum ditemukan lebih dulu oleh *hacker* dan terjadinya eksploitasi untuk keuntungan moneter dan tujuan jahat lainnya. Dengan adanya kemajuan signifikan dalam teknologi komputasi berbasis desktop, *website*, dan *mobile* maka akan semakin luas jangkauan komplikasi terkait keamanan sebuah sistem (Navamani et al., 2018).

C. *Threat*

Threat atau ancaman merupakan konsekuensi dari adanya kerentanan dan celah keamanan pada sistem. Setiap keadaan atau peristiwa yang dapat menimbulkan dampak buruk pada operasi, aset, individu, organisasi, atau negara melalui sistem informasi yang berasal dari akses yang tidak sah, penghancuran (*destruction),* pengungkapan (*disclosure)*, proses modifikasi informasi, dan atau penolakan terhadap layanan (*denial of service*) dapat dikatakan sebagai threat atau ancaman yang dapat membahayakan sistem, serta merugikan berbagai pihak baik dari segi pengguna maupun pemilik website (NIST Cybersecurity Framework Team, 2018).

D. Nikto

Nikto adalah pemindai server web *open source* (GPL) yang melakukan pengujian komprehensif terhadap server web untuk beberapa item, termasuk lebih dari 6700 file/program yang berpotensi berbahaya, memeriksa versi usang lebih dari 1250 server, dan masalah khusus versi di lebih dari 270 server. Nikto2 juga dapat melakukan pemeriksaan terhadap file *indeks* pada *web server* serta mencari beberapa opsi pada HTTP, Nikto2 juga memiliki kemampuan untuk mengetahui tentang server web dan apa saja *software* yang di pasang. Nikto2 memiliki fitur-fitur diantaranya yaitu, mendukung SSL, proksi HTTP, pemeriksaan server yang kadaluarsa, *multiple server* dan *port scanning*, *host authentication*, dapat melakukan hasil *report* dalam *plain text*, XML, HTL, dan NBE/CSV format (Karangle et al., 2019).

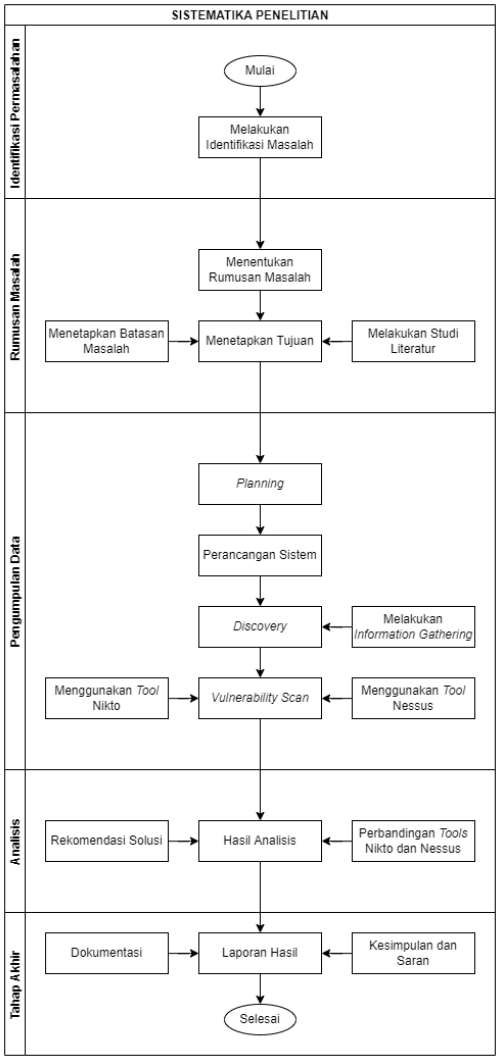
E. Nessus

Nessus merupakan salah satu alat untuk melakukan *vulnerability scanner* yang populer didunia. Dengan Nessus memungkinkan untuk melakukan pemindaian terhadap *misconfiguration* terhadap *software* yang terpasang pada sistem. Didalamnya juga termasuk melakukan pemindaian terhadap *port* dan versi *software* yang terpasang pada sistem, selain itu Nessus juga dapat melakukan pemindaian kerentanan untuk mendeteksi kegiatan *remote hacker* dalam mengontrol dan mengakses data sensitif pada suatu sistem, melakukan penolakan terhadap tumpukan TCP/IP, dan audit PCI DSS. Dalam proses *vulnerability scan* Nessus dapat melakukan pemindaian terhadap aplikasi *website*, misalnya mendeteksi *SQL Injection* dan *Cross Site Scripting* (Daud et al., 2014).

III. METODE

A. Skema Pemecahan Masalah

Skema pemecahan masalah dalam penelitian ini berbentuk bagan yang berisi tahapan yang dilakukan, yang dijabarkan secara sistematis, terstruktur, serta deskriptif. Pada skema ini terbagi atas beberapa tahapan yaitu tahap awal, tahap pengujian, tahap analisis, dan tahap akhir. Ilustrasi terkait sistematika penelitian ini digambarkan dalam seperti pada Gambar 2 berikut.



GAMBAR 2
SKEMA PEMECAHAN MASALAH

1. Identifikasi Permasalahan
   Tahap awal dalam penelitian ini merupakan identifikasi permasalahan. Dalam tahap ini meliputi kegiatan observasi terhadap objek penelitian serta fokus permasalahan apa yang akan diselesaikan menggunakan metode yang dipilih pada bagian kerangka berfikir sebelumnya.
2. Rumusan Masalah
   Tahap rumusan masalah merupakan tahapan lanjutan dari proses identifikasi masalah, setelah adanya rumusan permasalahan maka dilanjutkan dengan penetapan tujuan penelitian. Untuk mencapai tujuan tersebut dilakukan penentuan batasan masalah agar penelitian tidak meluas dan terfokus pada tujuan, selain ini dalam penelitian ini juga dilakukan studi literatur sebagai bahan acuan yang bersumber dari buku, jurnal, dan tutorial yang didapatkan dari sumber yang terpercaya.
3. Pengumpulan Data
   Tahap pengujian merupakan tahapan dimana peneliti melakukan proses identifikasi data-data apa saja yang diperlukan untuk menunjang penelitian dan sesuai dengan permasalahan yang dihadapi. Dalam proses pengumpulan data peneliti menggunakan data primer, dengan cara mengumpulkan data langsung dari alamat *website* IRIS. Dalam proses pengumpulan data menggunakan metode *information gathering* dengan memanfaatkan *command* yang disediakan dalam sistem operasi Kali Linux yaitu *ping* dan *whois*. Setelah mendapatkan cukup informasi dari *website* target tahap selanjutnya adalah melakukan *vulnerability scan* menggunakan *tools* Nikto dan Nessus.
4. Analisis
   Tahap analisis merupakan tahapan untuk melakukan analisa terhadap hasil *vulnerability scan* yang sudah didapatkan pada tahapan sebelumnya yaitu tahap pengumpulan data. Dalam penelitian ini dilakukan proses analisis terhadap hasil *vulnerability scan* yang telah dilakukan menggunakan *software* Nikto dan Nessus. Dalam tahap analisis ini dilakukan klasifikasi kerentanan berdasarkan level estimasi risiko, merekomendasikan solusi, serta membandingkan hasil yang didapatkan dari hasil *vulnerability scan* menggunakan Nikto dan Nessus.
5. Tahap Akhir
   Tahap Akhir merupakan tahap yang dilakukan menilai keterkaitan dari tahap pengujian dan tahap analisis. Dalam penelitian ini mengulas hasil yang sudah didapatkan menggunakan *tools* Nikto dan Nessus.

IV. HASIL DAN PEMBAHASAN

A. Tahap *Planning*

Tahap *planning* merupakan tahap melakukan perencanaan untuk menentukan website target yang akan diuji. Rincian mengenai website target dapat dilihat pada Tabel 1 berikut.

TABEL 1
WEBSITE TARGET DALAM PENELITIAN

No	Nama Domain	Sub Domain
1.	virtualfri.id	iris.virtualfri.id

Selain penentuan target yang telah disebutkan diatas pada tahap *planning* juga ditentukan mengenai spesifikasi rancangan sistem yang digunakan dalam penelitian terhadap website IRIS Fakultas Rekayasa Industri. Terdapat dua tipe instrumen perangkat dalam perancangan sistem yang digunakan, yaitu instrumen *hardware* dan instrumen *software*.

1. Instrumen *Hardware*
   Instrumen *hardware* merupakan komponen perangkat keras yang digunakan untuk pengujian *vulnerability assessment* dalam penelitian ini. Rincian mengenai instrumen *hardware* yang digunakan pada penelitian ini dijelaskan pada Tabel 2 berikut.

TABEL 2
INSTRUMEN *HARDWARE*

Komponen *Hardware*	Informasi	
Acer Aspire 5 (*Main OS*)	*Processor*	Intel(R) Core (TM) i3-8130U CPU @ 2.20GHz 2.21 GHz
	Memory	8,00 GB RAM
	Hardisk	1 TB
	Operating System	Windows 11 64-bit (212H, 22000.739)

2. Instrumen *Software*
   Instrumen *software* merupakan komponen perangkat lunak yang digunakan untuk pengujian *vulnerability assessment* dalam penelitian ini. Rincian mengenai instrumen *software* yang digunakan pada penelitian ini dijelaskan pada Tabel 3 berikut.

TABEL 3
INSTRUMEN *SOFTWARE*

Tipe	Komponen *Software*	Informasi
Operating System	Windows 11	64-bit (212H, 22000.739)
	Kali Linux	2022.2
Tools	Nikto	2.1.6
	Nessus	10.2.0
	Vmware Workstation	16.1.2

B. *Information Gathering*

Dari skenario *information gathering* yang telah dilakukan menggunakan *command ping* dan *whois* menggunakan sistem operasi Kali Linux, didapatkan beberapa informasi mengenai *website* target yaitu *website* rekruitasi asisten praktikum dan laboratorium Fakultas Rekayasa Industri. Hasil dari proses *information gathering* menggunakan *command ping* dan *whois* dijabarkan pad Tabel 4 berikut.

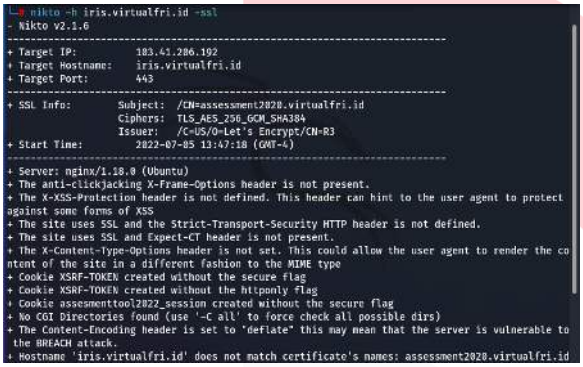
TABEL 4
HASIL *INFORMATION GATHERING*

No	*Command*	Hasil
1	*Ping*	IP: 103.41.206.192
2	*Whois*	*Domain* ID: PANDI-DO3307516 Tanggal Daftar: 22-09-2020 Tanggal Pembaruan: 22-09-2021 Tanggal Kadaluarsa: 22-09-2022

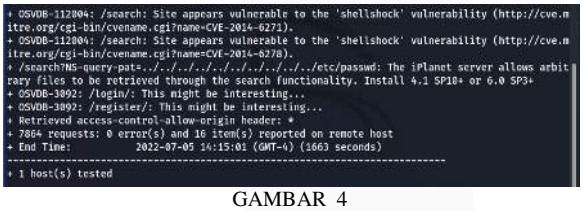
C. *Vulnerability Scan*

1. *Vulnerability Scan* menggunakan Nikto

Pemindaian menggunakan Nikto dijalankan pada sistem operasi Kali Linux dengan *command* eksekusi yaitu menggunakan *command* "Nikto -h". Hasil pemindaian dapat dilihat pada Gambar 3 dan 4 berikut.



GAMBAR 3
HASIL PEMINDAIAN MENGGUNAKAN NIKTO (1)



GAMBAR 4
HASIL PEMINDAIAN MENGGUNAKAN NIKTO (2)

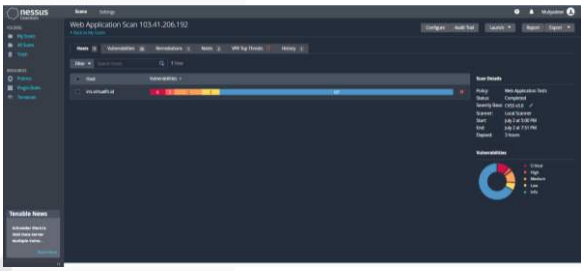
Penjelasan lebih rinci mengenai hasil celah kerentanan menggunakan *tool* Nikto yang ditemukan pada *website* IRIS Fakultas Rekayasa Industri dapat dilihat pada Tabel 5 berikut.

TABEL 5
PENJELASAN HASIL PEMINDAIAN *TOOL* NIKTO

Celah Kerentanan	Keterangan
The anti-clickjacking X-Frame Option header is not present.	Belum dilakukan proses penyuntingan pada *X-Frame-Option header*.
The X-XSS-Protection header is not defined	Pada bagian *X-XSS-Protection header* belum ditentukan.
The site uses SSL *and the Strict-Transport-Security header is not defined.*	Pada bagian HTTP *Strict-Transport-Security* belum didefinisikan. Hal ini bertujuan untuk meningkatkan keamanan *opt-in* untuk mengirim komunikasi melalui HTTPS.
The site uses SSL *and Expect-CT header is not present.*	pada bagian *Expect-CT* belum dilakukan penyuntingan.
The X-Content-Type-Option header is not set.	*Cookie* XSRF-TOKEN yang dibuat tidak menggunakan *secure flag*
Cookie XSRF-TOKEN *is created without the httponly flag.*	*Cookie* XSRF-TOKEN yang dibuat tidak menggunakan *httponly flag*
No CGI *Directories found.*	Tidak ditemukan direktori CGI.
The Content-Encoding header is not set to "deflate".	*Content-encoding* tidak diatur menjadi *deflate.*
Hostname 'iris.vitualfri.id' *does not match certificate's name* 'assessment2020. virtualfri.id'	Ketidaksesuaian antara informasi yang ada pada *hostname* dan sertifikat.
OSVDB-112004: /search: *Site appears with vulnerable to 'shellshock' vulnerable* – CVE-2014-6271	*Website* IRIS memiliki kerentanan terhadap CVE-2014-6271
OSVDB-112004: /search: *Site appears with vulnerable to 'shellshock' vulnerable* – CVE-2014-6278	*Website* IRIS memiliki kerentanan terhadap CVE-2014-6278
OSVDB-3092: */login/* dan OSVDB-3092: */register/*	Kerentanan pengungkapan informasi dimana memungkinkan *hacker* menulis pada *file system.*

2. *Vulnerability Scan* menggunakan Nessus

Pemindaian menggunakan *tool* Nessus dijalankan pada sistem operasi Windows dan menggunakan *browser* Google Chrome. Pemindaian ini dilakukan menggunakan fitur pada Nessus yaitu "*Web Application Tests*". Hasil pemindaian dapat dilihat pada Gambar 5 berikut.



GAMBAR 5
HASIL PEMINDAIAN MENGGUNAKAN NESSUS

Penjelasan lebih rinci mengenai hasil celah kerentanan menggunakan *tool* Nessus yang ditemukan pada *website* IRIS Fakultas Rekayasa Industri dapat dilihat pada Tabel 6 berikut.

TABEL 6
PENJELASAN HASIL PEMINDAIAN *TOOL* NESSUS

Risk Level	*Score*	*Vulnerability*
Critical	10.0	PHP *Unsupported Version Detection*.
Critical	9.8	*Apache Httpd (Multiple Issues).*
High	7.5	CGI *Generic* SQL *Injection*
High	7.5	PHP < *7.3.24 Multiple Vulnerabilities.*
Medium	6.1	*JQuery 1.2 < 3.5.0 Multiple XSS.*
Medium	5.3	PHP < *7.3.28 Email Injection.*
Medium	5.0	*Web Application Information Disclosure.*
Medium	5.0	*Git Repository Served by Web Server.*
Medium	4.3	*Web Application Potentially Vulnerable to Clickjacking.*

Low	2.6	*Web Server Transmits Cleartext Credentials.*
Low	2.6	*Web Server Uses Basic Authentication Without* HTTPS.
Low	-	*Web Servers Allow Password Auto Completions.*

D. *Vulnerability Analysis*

Tahap *vulnerability analysis*, analisis ini mengacu pada hasil yang didapatkan pada tahap *vulnerability scan* yang dilakukan sebelumnya. Dari proses analisis ini dikemukakan mengenai rekomendasi solusi dan perbaikan dari hasil celah keamanan yang telah didapatkan pada tahap *vulnerability scan* menggunakan tools Nikto dan Nessus. Uraian detail mengenai rekomendasi solusi dan perbaikan terhadap celah kerentanan yang didapatkan dapat dilihat pada Tabel 7 berikut.

TABEL 7
REKOMENDASI SOLUSI DAN PERBAIKAN

No	Celah Kerentanan	Rekomendasi Solusi dan Perbaikan
1.	*Software Unsupported Version*	Upgrade versi *software* yang terpasang pada web server, dalam penelitian ini adalah melakukan *upgrade* pada beberapa *software* berikut: - PHP dari versi 5.5.38 menjadi versi 7.3.x / 7.4.x / 8.0.x - *JQuery* dari versi 3.2.1 menjadi versi 3.5.0 - *Apache* dari versi 2.4.51 menjadi 2.4.54
2.	*Clickjacking*	Melakukan pengaturan pada *HTTP X-Frame-Options* atau *Content-Security Policy* menjadi *DENY* untuk memblokir penggunaan *tag iframe*, sedangkan untuk mengizinkan penggunaan *tag iframe* pada alamat yang sama dapat dirubah menjadi *SAMEORIGIN*. Dengan menerapkan pengaturan seperti diatas dapat mencegah konten pada halaman *website* untuk direnderoleh situs lain saat menggunakan *tag iframe*.
3.	*Cross-Site Scripting (XSS)*	Melakukan penentuan *header* pada pada bagian *X-XSS-Protection header*, melakukan *encoding* menggunakan *htmlspecialchars()*, serta memastikan bahwa halaman hanya menjalankan konten secara dinamis serta tidak mendukung *tag* yang tidak diinginkan.
4.	*SQL Injection (Blind)*	Melakukan pengaturan pada *HTTP X-Frame-Options* menjadi *DENY* atau *SAMEORIGIN* dan menggunakan *'frame ancentors'* pada *Content Security Policy* untuk semua respons konten.
5.	*Insecure Communication*	Melakukan konfigurasi pada SSL, menyelaraskan *hostname* dengan nama pada sertifikat agar komunikasi yang ada pada *website* dapat terenkripsi dan lebih aman (HTTPS).
6.	*Delete unused files/software*	Melakukan pengecekan terhadap *files* dan *software* yang terpasang dalam sistem agar tidak menjadi kerentanan yang dimanfaatkan oleh *hacker*.

V. KESIMPULAN

Berdasarkan metode *vulnerability assessment* yang telah dilakukan terhadap *website* IRIS Fakultas Rekayasa Industri (FRI) menggunakan *tools* Nikto dan Nessus berdasarkan *risk level* kerentanan yang ada, disimpulkan bahwa dalam *tool* Nikto ditemukan 14 kerentanan terhadap serangan *clickjacking*, XSS, SSL, *coockie*, dan *database*. Sedangkan pada *tool* Nessus ditemukan kerentanan dengan *risk level critical* berjumlah 6, *high* berjumlah 3, *medium* berjumlah, 12, *low* berjumlah 8, dan *informational* berjumlah 107. Kerentanan tertinggi adalah mengenai *PHP Unsupported Version Detection* dengan score 10.0 yang mana yaitu tidak didukungnya versi yang terpasang saat ini akan menyebabkan *patch* yang ada menjadi tidak aman sehingga dapat dieksploitasi oleh *hacker*. Untuk meminimalisisr adanya kerentanan sistem maka dapat melakukan pengecekan secara berkala terhadap *software* yang digunakan pada *website* untuk meminimalisir adanya *software* usang yang dapat dieksploitasi oleh *hacker*.

REFERENSI

Badan Siber dan Sandi Negara. (2022). *Laporan Tahunan Monitoring Keamanan Siber 2*. 54–55. https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw

Boddy, S., & Pompon, R. (2017). *THREAT INTELLIGENCE REPORT Lessons Learned from a decade of DATA breaches*. *November*.

Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014). A case study on web application vulnerability scanning tools. *Proceedings of 2014 Science and Information Conference, SAI 2014*, 595–600. https://doi.org/10.1109/SAI.2014.6918247

Karangle, N., Mishra, A. K., & Khan, D. A. (2019). Comparison of Nikto and Uniscan for measuring URL vulnerability. *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, 1–6. https://doi.org/10.1109/ICCCNT45670.2019.8944463

Navamani, B. A., Yue, C., & Zhou, X. (2018). Discover and Secure (DaS): An Automated Virtual Machine Security Management Framework. *2018 IEEE 37th International Performance Computing and Communications Conference, IPCCC 2018*, 1–6. https://doi.org/10.1109/PCCC.2018.8711239

NIST Cybersecurity Framework Team. (2018). Framework for improving critical infrastructure cybersecurity.

Proceedings of the Annual ISA Analysis Division Symposium, *535*, 9–25.

Primastomo, A., Cintamurni, E. U., Areanto, F., Hadiwijaya, G., & Noviana, R. (2015). *Analysis of Virtual Worker Website freelancer.com*. 175–180. https://doi.org/10.1109/icts.2015.7379894