TEKNOMATIKA
JURNAL INFORMATIKA DAN KOMPUTER

ISSN: 1979-7656 e-ISSN: 3031-0865
DOI: 10.30989/teknomatika.v17i1.1311

Vol. 17, No. 1, Mei 2024, pp. 56-64

Analisis Kerentanan pada Domain Repository Unjaya Menggunakan Kerangka Information System Security Assessment Framework (ISAFF)

Ahmad Nurhidayat[a,1], Nofa Shintia[a,2], Muhammad Fahrur.R[a,3], Alfirna Rizqi Lahitani,[a,4*]
[a]Universitas Jenderal Achmad Yani Yogyakarta, Jl. Siliwangi, Ringroad Barat, Banyuraden, Gamping, Sleman DIY
[1]nur26691@gmail.com, [2]shintiadfhr@gmail.com, [3]muhammadfahrur19@gmail.com, [4]alfirnalahitani@gmail.com
[*]Penulis koresponden

Diterima	Direvisi	Disetujui	Dipublikasikan
4/3/2024	27/5/2024	27/5/2024	28/5/2024

ABSTRACT

Vulnerability analysis on the Unjaya Repository website uses the ISSAF method for identifying and grouping identified vulnerabilities.. The purpose is to provide an in-depth understanding of the vulnerabilities that exist on the Repository site as a basis for the corrective steps needed to reduce security risks. The methods are information gathering, network mapping, vulnerability exposure, vulnerability grouping, IP addresses, active ports. Scanning using Nikto Scanner and Helium Security, 24 vulnerabilities detected in four levels, namely high, medium, low and informational. The results found at a high level of vulnerability in the form of disclosure of PII, at a medium level such as the absence of an Anti-CSRF Token, at a low level such as Application Error Disclosure, and at an information level such as Authentication Request Identified. This proves that there is a significant potential risk to the security of the Unjaya Repository site.

KEYWORDS

Vulnerability Assesment, Website, ISAFF

ABSTRAK

Analisis kerentanan website Repositori Unjaya menggunakan metode Information System Security Assessment Framework (ISSAF) untuk mengidentifikasi dan mengelompokkan kerentanan yang teridentifikasi guna meningkatkan keamanan situs. Tujuan analisis ini adalah memberikan pemahaman yang mendalam tentang kerentanan yang ada pada situs Repository Unjaya serta landasan bagi langkah-langkah perbaikan yang diperlukan untuk mengatasi kerentanan yang terdeteksi guna mengurangi risiko keamanan. Metode yang digunakan meliputi pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, pengelompokan kerentanan dengan pemindaian berupa tampilan konfigurasi perangkat, alamat IP, serta port aktif. Melalui pemindaian menggunakan Nikto Scanner dan Helium Security, 24 kerentanan dapat terdeteksi dalam empat tingkatan, yaitu tinggi, sedang, rendah, dan informasional. Hasil analisis ditemukan pada kerentanan tingkat tinggi berupa pengungkapan informasi PII (Personally Identifiable Information), pada tingkatan menengah seperti ketiadaan Token Anti-CSRF, pada tingkatan rendah seperti Application Error Disclosure, dan pada tingkatan informational seperti Authentication Request Identified. Hal ini membuktikan adanya potensi risiko yang signifikan terhadap keamanan situs Repositori Unjaya.

KATA KUNCI

Vulnerability Assesment, Website, ISAFF

1 PENDAHULUAN

Pertumbuhan teknologi yang semakin pesat memberikan dampak positif pada berbagai bidang, termasuk internet. Website menjadi alternatif bagi korporasi sebagai media promosi maupun media interaksi dengan pelanggan, Website dapat dengan mudah diakses oleh orang banyak dari manapun dan kapanpun. Pada tahun 2015, diperkirakan akan ada lonjakan penggunaan internet sebesar 22 juta pengguna di Indonesia. Tren meningkatnya pengguna internet sudah terlihat sejak tahun 2009 dan diperkirakan akan terus meningkat [1]. Di era digital saat ini, *website* menjadi bagian tak terpisahkan di kehidupan manusia sehari-hari. *Website* digunakan dalam semua aspek kehidupan, termasuk sebagai sumber informasi utama setelah media sosial. *Website* adalah sekumpulan halaman atau homepage yang berisi informasi, saling terhubung antara satu halaman dengan halaman lain [2]. Namun, keamanan informasi adalah aspek kritis yang tidak boleh diabaikan. Untuk menjaga keamanan *website*, penting untuk melakukan uji kerentanan secara berkala guna mengidentifikasi potensi masalah keamanan yang dapat dieksploitasi oleh pihak jahat.

Hasil identifikasi kerentanan ini dapat memberikan saran perbaikan kepada pengelola *website* atas kerentanan yang ditemukan, sehingga tindakan pencegahan dan perbaikan dapat diambil untuk menjaga integritas dan keamanan data yang disimpan dan diproses dalam sistem *website* tersebut. Menurut Butler dan Cantrell " integritas merupakan citra dapat dipercaya, jujur dari seseorang atau kelompok dalam ruang lingkup organisasi." [3]. Keamanan informasi menjadi kunci utama dalam sebuah sistem informasi. Masih banyak pengelola sistem informasi yang kurang memperhatikan aspek keamanan. Tidak bisa dipungkiri ada beberapa sistem yang memiliki celah kerentanan dan berisiko terjadi serangan.

Penelitian sebelumnya oleh Rochman, Salam, dan Maulana dengan judul "Analisis Keamanan Website dengan *Information System Security Assessment Framework* (Issaf) dan *Open Web Application Security Project* (Owasp) di Rumah Sakit Xyz". Membahas tentang analisis keamanan website menggunakan Information System Security Assessment Framework (ISSAF) dan Open Web Application Security Project (OWASP) [4]. Hasil pengujian mengungkapkan masalah keamanan pada webserver Sistem Informasi HRD, termasuk notifikasi kesalahan, halaman HTML publik, dan masalah autentikasi, serta akses database yang tidak sah. Penelitian ini menunjukkan efektivitas ISSAF dan OWASP dalam mengidentifikasi kerentanan keamanan, dan menekankan pentingnya pengujian keamanan serta pemeliharaan rutin pada perangkat keras, perangkat lunak,

jaringan, dan server [4]. Penelitian lain dilakukan oleh I Gede Ary Suta Sanjaya, Gusti Made Arya Sasmita, dan Dewi Made Sri Arsa dari Universitas Udayana pada tahun 2020 berjudul "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF" [---]. Hasil penelitian menunjukkan bahwa website Lembaga X memiliki kerentanan terhadap serangan XSS dan SQL Injection, serta memiliki port TCP yang tidak terlindungi dan bug sistem yang berpotensi menjadi celah keamanan. Untuk mengatasi masalah ini, disarankan untuk melakukan validasi pada tingkat PHP guna mencegah serangan SQL Injection dan XSS, menutup port TCP yang tidak terpakai, dan memperbaiki bug sistem.

Universitas Jenderal Achmad Yani Yogyakarta memiliki situs layanan *repository* yaitu *https://repository.unjaya.ac.id*. Layanan ini merupakan layanan yang disediakann untuk menyimpan, mengelola, dan menyebarkan berbagai informasi dan materi akademik. Ini mencakup dokumen-dokumen seperti tugas akademik, jurnal penelitian, riset mahasiswa, publikasi ilmiah, dan berbagai bentuk data yang relevan dengan lingkungan akademik. Namun sampai saat ini, *website* Repository Unjaya, masih berstatus *"Not Secure"* saat diakses. Keterangan ini muncul tepat diatas kiri homepage *website* berdekatan dengan *domain http://repository.unjaya.ac.id*. Kelemahan ini dapat menyebabkakn terjadinya penyalahgunaan dari data-data penting yang tersimpan di *website* tersebut. Status *"Not Secure"* menunjukkan bahwa koneksi antara pengguna dan *website* tidak terenkripsi, sehingga data yang dikirimkan dan diterima melalui *website*, rentan terhadap potensi peretasan atau penyadapan.

Berbagai macam metode dapat digunakan untuk melakukan kajian kerentanan, beberapa metode yang paling banyak digunakan adalah *Information System Security Framework (ISSAF)*, *OWASP* versi 4, dan *OSSTMM* [3]. Pemilihan metode ISSAF dalam penelitian ini, karena metode ini menawarkan pendekatan yang komprehensif dan terstruktur [5]. Penelitian ini dilakukan untuk *"Analisis Kerentanan Pada Domain Repository Unjaya Menggunakan Information System Security Assessment Framework (ISAFF)"*, dan bertujuan untuk

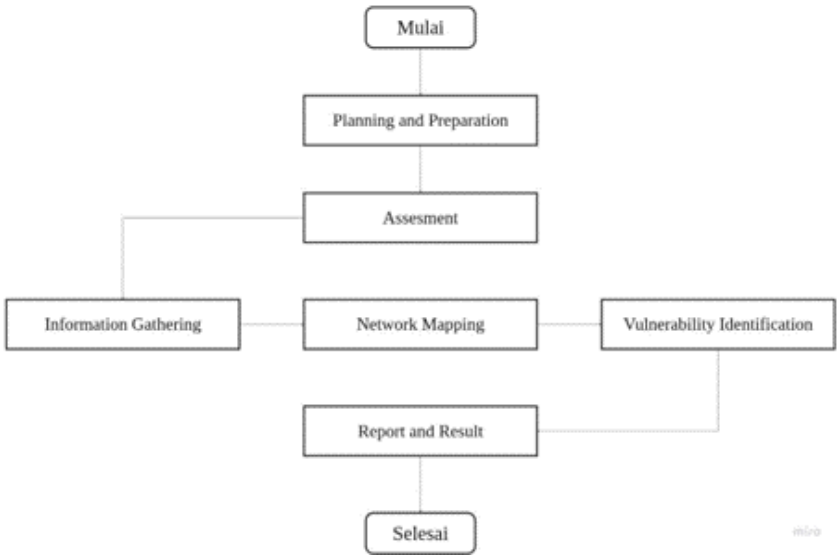
1. Mengidentifikasi potensi masalah keamanan di website Repository Unjaya.
2. Memberikan saran perbaikan berdasarkan temuan kerentanan.
3. Menekankan pentingnya pemeliharaan rutin pada perangkat keras, perangkat lunak dan server.

2 METODE PENELITIAN

Penelitian ini menggunakan metode ISSAF, adapun beberapa tahap diantaranya pengumpulan informasi, perencanaan, dan persiapan adalah tahap awal penelitian. Tahap selanjutnya adalah identifikasi kerentanan pada situs web Repository Unjaya. Ini adalah penilai an kerentanan pada situs web Repository Unjaya yang perlu dilakukan. Tahap selanjutnya adalah menentukan metode yang paling cocok untuk proses penilaian kerentanan, yaitu *information System Security Assessment Framework (*ISSAF). Pada tahap terakhir, setiap kerentanan yang ditemukan dievaluasi secara menyeluruh, dan setiap kerentanan yang ditemukan dievaluasi dengan menggunakan *tools* yang sudah ditentukan [6]. Sebelum memulai penelitian, evaluasi menyeluruh terhadap web dilakukan. Proses ini juga melibatkan penelitian mendalam, yang mencakup tinjauan literatur dan analisis lanskap keamanan data terbaru untuk memastikan bahwa penelitia n yang dilakukan memiliki dasar pengetahuan yang kuat dan terinformasikan. Langkah selanjutnya dalam penilaian kerentanan pada situs web Repository Unjaya adalah mengidentifikasi setiap ke an masalah keamanan yang ada. Ini penting untuk memahami setiap ke an kerentanan yang terjadi pada situs web.

Pada penelitian ini dipilih ISSAF sebagai dasar untuk melakukan evaluasi kerentanan dengan tingkat ketelitian yang optimal [7]. Kerangka kerja ini berfokus pada penemuan kerentanan melalui penggunaan alat pemindaian, khususnya alat *Helium Security*, untuk melakukan evaluasi menyeluruh terhadap situs web Repository Unjaya. Metode ini bertujuan untuk menemukan, menilai, dan mengelompokkan setiap kerentanan yang ditemukan, sehingga memberikan pemahaman yang menyeluruh tentang situasi keamanan situs web yang relevan. Dalam proses pemindaian, alat tersebut mampu mengidentifikasi konfigurasi perangkat, alamat *Internet Protocol*, serta

mengungkap *port-port* yang aktif [8]. Pemindaian ini telah ter-automatisasi dan meliputi pengevaluasian menyeluruh terhadap target, menyelesaikan proses evaluasi hanya dalam waktu singkat [9]. Hasil dari evaluasi kerentanan ditampilkan dalam bentuk diagram persentase yang menggambarkan empat tingkatan kerentanan: tinggi, sedang, rendah, dan informasional. Informasi hasil pemindaian dapat diakses melalui sisi tampilan.



Gambar 1. Alur Penelitian

Gambar 1 menggambarkan serangkaian langkah yang akan dijalani dalam proses penelitian ini. Mulai dari langkah awal *Planning and Preparation* pada tahap ini mempersiapkan alat, bahan dan metode yang akan digunakan dalam penelitian ini. Langkah kedua adalah *Assesment*, tahapan ini akan dibagi menjadi 3 proses yaitu proses *Information gathering* untuk mendapatkan informasi dan struktur dari domain Repository Unjaya. Proses kedua dalam tahap *assesment* adalah *Network Mapping* untuk melakukan pemetaan *port-port* yang berpotensi mengancam keamanan website. Proses ketiga dari tahap *assesment* adalah *vulnerability identification* untuk menemukan celah kerentanan menggunakan *nikto scanner* dan *helium security*. Dan tahap terakhir pada penelitian ini adalah menyusun laporan secara terstruktur dari hasil temuan penelitian ini.

2.1 Alat Penelitian

Untuk menilai kerentanan yang ada pada situs web Repository Unjaya, penelitian ini menggunakan *Information System Security Assessment Framework (ISSAF)*. Penelitian ini berkonsentrasi pada tahap identifikasi kelemahan. Pada tahap assessment, peneliti menemukan celah kerentanan di situs web Repository Unjaya dengan menggunakan alat *scanner Nikto* dan *Helium Security*. Berikut alur pada proses penelitian menggunakan *Information System Security Assessment Framework (ISSAF)*.

Pada tahap mengumpulkan informasi, merencanakan prosedur penilaian kerentanan, dan memberikan izin kepada pengelola untuk melakukan penelitian pada situs web Repository Unjaya untuk memberikan perlindungan hukum kepada peneliti dan pengelola. Selain itu, menyiapkan alat untuk mendukung penelitian. Perangkat yang digunakan untuk melakukan penilaian kerentanan yaitu perangkat komputer atau laptop dengan spesifikasi cukup untuk menjalankan sistem operasi Linux Ubuntu.

1. Sistem Operasi Ubuntu 22.04 Jammy

   Digunakan sebagai sistem operasi untuk menjalankan proses pengujian menggunakan *Information System Security Assessment Framework (ISSAF)*.
2. Software *Google Chrome*
3. Situs Web *sitereport.netcraft.com*
4. Software *Zenmap* 7.80

5. Software *Nikto Scanner 2.1.5*
6. Situs Web *Helium Security*

2.2 Bahan Penelitian

Bahan yang digunakan dalam penelitian ini adalah situs web Repository Unjaya http://repository.unjaya.ac.id sebagai media informasi untuk mahasiswa yang dijadikan sebagai objek penilaian kerentanan.

3 HASIL DAN PEMBAHASAN

3.1 Information Gathering

Tahap awal dalam evaluasi kerentanan situs web adalah *Information Gathering*, di mana peneliti memanfaatkan alat *Netcfraft* melalui situs web *sitereport.netcraft.com* untuk mengumpulkan data yang relevan [12]. Penelitian ini menggunakan hasil pemindaian dengan *Netcraft* yang telah diuraikan dalam gambar dibawah, memberikan gambaran detail mengenai hasil *scanning* yang mencakup informasi yang diperlukan untuk analisis kerentanan pada situs web yang dievaluasi. Hasil pemindaian menggunakan tools *netcraft* diperoleh informasi mengenai *Internet Protocol* dan infromasi umum tentang situs web Repository Unjaya.

Tabel 1. Hasil Pemindaian

No	Informasi	Hasil
1	*Site title*	*Welcome to Repository Unjaya - Repository Unjaya*
2	*Date first seen*	*February 2021*
3	*Site*	*http://repository.unjaya.ac.id*
4	*Netblock Owner*	*PT SELARAS CITRA TERABIT*
5	*Hosting company*	*Terabit Network*
6	*Housting Country*	*ID*
7	*IPv4 address*	*103.247.15.35*
8	*Reverse DNS*	*ip-35-15-247.terabit.net.id*
9	*Main Domain*	*unjaya.ac.id*
10	*Nameserver*	*ns1.fastcloud.id*
11	*OS*	*Linux*
12	*Web Server*	*Apache/2.4.52 Ubuntu*
13	*Last seen*	*18-Nov-2023*
14	*Top Level Domain*	*Indonesia (.ac.id)*
15	*DNS admin*	*teknis@qwords.co.id*

Tabel 1 memuat hasil informasi detail mencakup informasi website yang diperlukan sebagai bagian dari perencanaan dan persiapan untuk analisis kerentanan pada situs web Repository Unjaya.

3.2 Network Mapping

Tahap *network mapping* merupakan proses penting dalam penilaian keamanan situs web, bertujuan untuk memperoleh gambaran konfigurasi jaringan pada target yang dievaluasi. Di tahap ini, peneliti memanfaatkan alat *Zenmap* untuk melakukan pemetaan jaringan [13]. Informasi yang telah terkumpul sebelumnya menjadi landasan untuk mendapatkan topologi jaringan yang terkait dengan situs web Repository Unjaya, termasuk memberikan informasi mengenai perangkat yang terhubung, alamat IP, dan port-port yang terbuka, yang digunakan dalam mengidentifikasi potensi kerentanan keamanan yang ada dalam infrastruktur jaringan tersebut.

Tabel 2. Hasil Menggunakan Zenmap

No	Informasi	Hasil
1	*Open Port*	*80/tcp http Apache httpd 2.4.52 ((Ubuntu))*
2	*Closed Port*	*20/tcp ftp-data*
3	*Closed Port*	*21/tcp ftp*
4	*Closed Port*	*443/tcp https*
5	*Scanned Port*	*1000*
6	*Hosting Country*	*ID*
7	*IPv4 Address*	*103.247.15.35*
8	*Reverse DNS*	*ip-35-15-247.terabit.net.id*

Tabel 2 menunjukan hasil proses *Network Mapping* menunjukkan bahwa satu port yaitu port 80, memiliki status terbuka dengan protokol *TCP (Transmission Control Protocol)*, bersama dengan tiga port lain yaitu port 20, 21 dan 443, menunjukkan status tertutup. Port 80 ini , akan dikonfigurasi untuk layanan web melalui protokol *HTTP*, dan tidak memiliki sertifikat keamanan berupa *SSL(Secure Socket Layer)* yang terpasang sehingga rentan terhadap berbagai jenis serangan keamanan karena dapat dieksploitasi oleh layanan yang berjalan di dalamnya.

3.3 Vulnerability Identification

Proses identifikasi kerentanan adalah tahapan yang terfokus pada proses identifikasi potensi kelemahan pada sistem Repository Unjaya, untuk melakukan analisis yang komprehensif terhadap struktur dan perilaku sistem, mengidentifikasi potensi celah keamanan, serta mengevaluasi risiko yang terkait dengan setiap kelemahan yang terdeteksi. Tahapan *Vulnerability Identification* melalui 2 tahap yaitu :

1) Nikto Scanner

Nikto Scanner adalah sebuah alat pengujian yang telah menguji ribuan program yang termasuk dalam kategori file berbahaya serta ratusan versi aplikasi yang tidak diperbarui, menawarkan kemampuan untuk memeriksa berbagai indeks file melalui server HTTP [10]. Dalam langkah pertama penilaian kerentanan pada Repository Unjaya, proses dimulai dengan penggunaan alat *Nikto* untuk meraih informasi lebih rinci tentang situs web target. *Nikto Scanner* dijalankan pada

lingkungan sistem operasi Linux Ubuntu 22.04 Jammy. Perintah yang dieksekusi untuk memulai pemindaian adalah '*nikto -h http://repository.unjaya.ac.id/ -o result.html*'. Proses pemindaian yang dilakukan oleh *Nikto* berlangsung selama kurang lebih 10 menit. Hasil dari pemindaian menggunakan *Nikto Scanner* ditampilkan dalam Tabel 3.

Tabel 3. Hasil Pemindaian Nikto Scanner

No	Kerentanan
1	*The anti-clickjacking X-Frame-Options header is not present.*
2	*No CGI Directories found (use '-C all' to force check all possible dirs)*
3	*"robots.txt" contains 1 entry which should be manually viewed.*
4	*Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x8be 0x5f8177f6c3415*
5	*DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.*
6	*/cgi/export/repository/RDFXML/cart32.exe: request cart32.exe/cart32clientlist*

Tabel 3. berisi informasi dari hasil pemindaian *Nikto Scanner*. Hasil ini memberikan gambaran awal terkait kelemahan potensial pada web Repository Unjaya yang akan dianalisis lebih lanjut untuk meningkatkan keamanan dan mengurangi risiko kerentanan. Hasil pemindaian dengan menggunakan *Nikto Scanner*, ditemukan juga kerentanan seperti *The anti-clickjacking X-Frame-Options header is not present, No CGI Directories found (use '-C all' to force check all possible dirs), "robots.txt" contains 1 entry which should be manually viewed*, maka situs web Repository Unjaya terindikasi terdapat celah kerentanan *Cross Slide Scripting (XSS)*, yang memungkikan terjadinya serangan pada situs web Repository Unjaya.

2) Helium Security

Helium Security merupakan alat otomatis dalam penilaian kerentanan berbasis cloud yang menyediakan solusi kuat dalam mengidentifikasi dan mengevaluasi kerentanan keamanan. *Platform* ini dirancang untuk mendeteksi serta menganalisis sejumlah besar kerentanan yang berkaitan dengan berbagai aspek keamanan sistem, termasuk tetapi tidak terbatas pada *security headers*, *SSL/TLS Scanner*, dan kerentanan lainnya yang relevan. *Helium Security* menyediakan berbagai perangkat lunak untuk membantu penilaian kerentanan aplikasi, dan menghasilkan hasil rekap yang rapi. Saat ini, *Helium Security* akan menambah fitur baru untuk melakukan Audit Kesesuaian Konfigurasi Keamanan. Fitur ini memungkinkan untuk memeriksa apakah sistem memenuhi standar keamanan teknologi global [11].

Tabel 4. Risk Level Vulnerability

Risk Level	***Number of Alerts***
High	1
Medium	7
Low	8
Informational	8

Tabel 4. berisi hasil yang jelas tentang tingkat risiko yang dihadapi oleh situs web tersebut. Oleh karena itu, langkah-langkah perbaikan dan tindakan korektif perlu segera diambil untuk mengatasi kerentanan-kerentanan yang teridentifikasi dan mengurangi risiko keamanan yang terjadi. Persentase risiko pada tingkat tinggi, dimana nilai kerentanan mencapai 4,2% yaitu PII Disclosure, selanjutnya pada level medium mendapatkan nilai kerentanan 29,2% yaitu *Absence of Anti-CSRF Tokens, Content Security Policy (CSP) Header Not Set, HTTP to HTTPS Insecure Transition in Form Post, Missing Anti-clickjacking Header, Source Code Disclosure - SQL, Sub Resource Integrity Attribute Missing, Weak Authentication Method, selanjutnya pada level low mendapatkan nilai kerentanan 33,3% yaitu Application Error Disclosure, Big Redirect Detected (Potential Sensitive Information Leak), In Page Banner Information Leak, Information Disclosure - Debug Error Messages, Insufficient Site Isolation Against Spectre Vulnerability, Permissions Policy Header Not Set, Server Leaks Version Information via "Server" HTTP Response Header Field, X-Content-Type-Options Header Missing, dan pada level low mendapatkan nilai kerentanan 33,3% yaitu Authentication Request Identified, Charset Mismatch, Information Disclosure - Sensitive Information in URL, Information Disclosure - Suspicious Comments, Modern Web Application, Non-Storable Content, Storable and Cacheable Content, User Controllable HTML Element Attribute (Potential XSS)*. Dari kerentanan yang teridentifikasi pada situs web Repository Unjaya, penting untuk segera mengambil langkah perbaikan guna menangani celah keamanan yang terpapar. Proses perbaikan ini menjadi krusial dalam memitigasi risiko serangan dan pelanggaran keamanan yang dapat merugikan integritas dan keandalan situs web.

4 KESIMPULAN

Dalam analisis kerentanan terhadap situs web Repository Unjaya, berbagai kerentanan keamanan telah teridentifikasi. Dari evaluasi yang dilakukan dengan menggunakan metode *Information System Security Assessment Framework* (ISSAF), serta alat pemindaian seperti *Nikto Scanner* dan *Helium Security*, memiliki 24 kerentanan keamanan dengan level dari *High*, *Medium*, *Low*, dan *Informational*. Terdapat beberapa masalah yang signifikan yang mempengaruhi keamanan situs tersebut. Beberapa kerentanan tingkat tinggi, seperti *PII Disclosure*, dan sejumlah kerentanan tingkat medium seperti *Absence of Anti-CSRF Tokens, HTTP to HTTPS Insecure Transition in Form Post, dan Content Security Policy (CSP) Header Not Set,* menjadi sorotan utama dalam evaluasi. Lebih lanjut, terdapat juga kerentanan tingkat rendah dan informasional yang memberikan gambaran luas tentang kelemahan keamanan situs. Hasil evaluasi menunjukkan bahwa situs web tersebut memiliki kelemahan serius yang mempengaruhi integritas data dan keamanan informasi yang disimpan. Status "Not Secure" pada situs menandakan risiko potensial terkait koneksi yang tidak terenkripsi, meningkatkan potensi untuk peretasan atau penyadapan data.. Upaya peningkatan keamanan situs web melalui penerapan langkah-langkah perlindungan yang sesuai dan perbaikan dalam konfigurasi serta kebijakan keamanan menjadi krusial untuk meminimalkan risiko serangan yang dapat mengancam integritas dan keandalan situs web Repository Unjaya.

5 KONTRIBUSI PENELITIAN

Penelitian ini memberikan kontribusi signifikan dalam memahami dan meningkatkan keamanan informasi pada situs web terutama pada web Repository Unjaya dengan menerapkan *metode Information System Security Assessment Framework* (ISSAF). Pemindaian dilakukan menggunakan *Nikto Scanner* dan *Helium Security*, dan berhasil mengidentifikasi 24 kerentanan keamanan serta membagi 24 kerentanan tersebut kedalam empat tingkatan. Prioritisasi kerentanan, terutama pada tingkat tinggi seperti *PII Disclosure*, memberikan panduan yang jelas bagi pengelola situs untuk menetapkan langkah-langkah perbaikan yang mendesak. Analisis tingkat risiko dengan persentase kerentanan pada masing-masing tingkatan memberikan gambaran menyeluruh tentang sejauh mana situs web terpapar potensi ancaman. Lebih lanjut, penelitian ini menyajikan rekomendasi perbaikan yang dapat membantu pengelola situs merancang strategi keamanan yang lebih terfokus. Status *"Not Secure"* pada situs web menjadi sorotan utama, dan penelitian ini memberikan dasar untuk implementasi langkah-langkah konkret guna meningkatkan enkripsi dan keamanan koneksi pengguna. Dengan demikian, penelitian ini tidak hanya mengidentifikasi

kerentanan, tetapi juga memberikan kontribusi berarti dalam membentuk tindakan perbaikan yang diperlukan untuk melindungi integritas dan keamanan informasi pada situs web Repository Unjaya.

DAFTAR PUSTAKA

[1] Asosias Penyelenggara Jasa Internet Indonesia," apjii.or.id. Available : http://www.apjii.or.id/v2/read/page/halaman-data/9/statistik.html (accessed Feb. 26, 2024).

[2] S. Hidayatulloh And D. Saptadiaji, "Penetration Testing Pada Website Universitas Ars Menggunakan Open Web Application Security Project (Owasp)," *J. Algoritm.*, Vol. 18, No. 1, Pp. 77–86, 2021, Doi: 10.33364/Algoritma/V.18-1.827.

[2] I. G. A. S. Sanjaya, G. M. A. Sasmita, And D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework Issaf," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, Vol. 8, No. 2, P. 113, 2020, Doi: 10.24843/Jim.2020.V08.I02.P05.

[4] A. Rochman, rizal R. Salam, and S. A. Maulana, "Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz," *Jurnal Indonesia Sosial Teknologi*, vol. 2, no. 04, pp. 506–519, Apr. 2021, doi: https://doi.org/10.59141/jist.v2i04.124.

[5] M. A. Nabila, P. E. Mas'udia, And R. Saptono, "Analysis And Implementation Of The Issaf Framework On Osstmm On Website Security Vulnerabilities Testing In Polinema," *Jartel*, Vol. 13, No. 1, 2023, Doi: 10.33795/Jartel.V13i1.511.

[6] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)," JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), vol. 5, no. 1, p. 45, Jun. 2020, doi: https://doi.org/10.29100/jipi.v5i1.1565.

[7] H. Herman, I. Riadi, Y. Kurniawan, And I. A. Rafiq, "Analisis Keamanan Website Menggunakan Information System Security Asessment Framework(Issaf)," *J. Teknol. Inform. Dan Komput.*, Vol. 9, No. 1, Pp. 126–136, 2023, Doi: 10.37012/Jtik.V9i1.1439.

[8] R. Umar, I. Riadi, M. Ihya, And A. Elfatiha, "Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework Issaf," *Jutisi J. Ilm. Tek. Inform. Dan Sist. Inf.*, Vol. 12, No. 1, Pp. 280–292, 2023.

[9] Dan S. A. M. Agus Rochman, Rizal Rohian Salam, "Analisis Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Dan Open Web Application Security Project (Owasp) Di Rumah Sakit Xyz," vol. 2, no. 4, p. 6, 2021.

[10] N. Karangle, A. K. Mishra, and D. A. Khan, "Comparison of Nikto and Uniscan for measuring URL vulnerability," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2019, doi: https://doi.org/10.1109/icccnt45670.2019.8944463.

[11] Erik Andri Budiman and Girindro Pringgo Digdo, "Perancangan Fitur Audit Security Configuration Compliance Pada Aplikasi Helium Security," *Indonesian Journal Computer Science*, vol. 2, no. 2, pp. 67–76, Oct. 2023, doi: https://doi.org/10.31294/ijcs.v2i2.2481.

[12] S. Eko Prasetyo and N. Hassanah, "Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF," *JURNAL ILMIAH INFORMATIKA*, vol. 9, no. 02, pp. 82–86, Sep. 2021, doi: https://doi.org/10.33884/jif.v9i02.3758.

[13] A. Ahmad Aji Guntur Saputra, "Scanning Website menggunakan Zenmap," *Scanning Website menggunakan Zenmap*, Apr. 2020, Accessed: Feb. 26, 2024. [Online]. Available: http://edocs.ilkom.unsri.ac.id/3872/