EVALUASI KEAMANAN SISTEM INFORMASI WEBSITE LEMBAGA XYZ MENGGUNAKAN METODE *PENETRATION TESTING*

SECURITY EVALUATION OF INFORMATION SYSTEMS ON THE XYZ INSTITUTION'S WEBSITE USING PENETRATION TESTING METHOD

Rizky Arya Andita[1], Muhamad Nasrullah[2], Muhammad Ilham Alhari[3]
E-mail: rizkyarya@student.telkomuniversity.ac.id, emnasrul@telkomuniversity.ac.id, ilhamalhari@telkomuniversity.ac.id
[1,2,3] Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University Surabaya

Abstrak

Website lembaga XYZ menyediakan layanan informasi kepada pengguna pengguna. website ini menyimpan data sensitif seperti email, password, nomor telepon, alamat, dan dokumen identitas yang dapat berpotensi menimbulkan risiko jika terjadi kebocoran. Untuk mencegah dari serangan siber yang dapat merusak reputasi lembaga, maka diperlukan pendekatan sistematis untuk menjaga keamanan sistem informasi agar tetap andal dalam menghadapi ancaman keamanan siber. Salah satu metode yang digunakan untuk mengidentifikasi kerentanan pada sistem website adalah pengujian penetrasi. Penelitian ini menggunakan metode analisis keamanan berdasarkan OWASP Top 10 2021. Tujuan penelitian adalah mengevaluasi kemungkinan kerentanan keamanan dalam sistem informasi website lembaga publik tersebut. Proses penelitian melibatkan beberapa tahapan, seperti studi literatur, *planning*, *information gathering*, *vulnerability scanning*, *attacking*, dan *report*. Hasil penelitian ini berupa rekomendasi perbaikan yang diharapkan dapat diimplementasikan untuk mengurangi potensi risiko serangan siber serta menjaga kepercayaan dan reputasi institusi sebagai penyedia layanan informasi yang aman.

Kata kunci: *Keamanan Website, Evaluasi Kerentanan, Uji Penetrasi, OWASP Top 10.*

Abstract

The website of XYZ Institution provides information services to its users. This webbbite stores sensitive data such as email, passwords, phone numbers, addresses, and identity documents, which could pose risks if leaked. To prevent data manipulation and exploitation from cyberattacks that could harm the institution's reputation, a systematic approach is required to safeguard the information system's security and reliability against cybersecurity threats. One method used to identify vulnerabilities in the website system is penetration testing. This study employs a security analysis method based on the OWASP Top 10 2021. The objective of the research is to evaluate potential security vulnerabilities within the public institution's website information system. The research process involves several stages, such as literature review, planning, information gathering, vulnerability scanning, attacking, and reporting. The results of the study include improvement suggestions that are intended to be put into action to minimize the likelihood of cyberattacks and preserve the institution's trust and reputation as a provider of secure services.

Keywords: *Website Security, Vulnerability Assessment, Penetration Testing, OWASP Top 10.*

1. PENDAHULUAN

Di era berkembangnya teknologi saat ini, manusia tidak terlepas dari penggunaan internet. Internet telah merubah berbagai aktivitas manusia menuju gaya hidup digital, memungkinkan pertukaran informasi secara instan[1]. Fenomena ini tidak hanya menciptakan revolusi dalam cara manusia berkomunikasi, tetapi juga memberikan manfaat yang meliputi dunia bisnis, industri, pendidikan, hingga komunikasi [2]. Perkembangan teknologi informasi yang kian

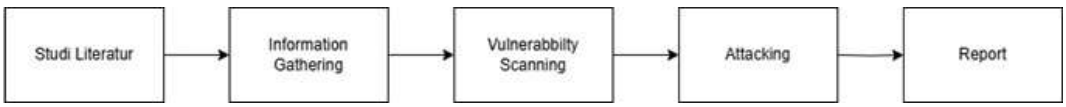
pesat telah membawa banyak manfaat bagi peradaban manusia. Namun, di sisi lain, menimbulkan masalah baru, salah satunya adalah keamanan siber [3]. Kejahatan siber menjadi sebuah masalah serius yang dapat mengancam di bidang ekonomi, politik, hingga pertahanan negara [4]. Di tahun 2022, kerugian global akibat kejahatan siber mencapai angka sekitar US$ 8,44 triliun atau setara dengan Rp 130 triliun. Angka ini mengalami peningkatan signifikan sebesar 40,9 persen dibandingkan tahun sebelumnya, di mana kerugian yang tercatat adalah sekitar US$ 6 triliun[5].

Menurut Badan Siber dan Sandi Negara (BSSN), jumlah anomali lalu lintas internet di Indonesia sangat tinggi, dengan 1,6 miliar anomali pada 2021 dan menurun menjadi 976,4 juta pada 2022 [6]. Di semester 1 tahun 2023, terjadi empat kebocoran data besar: BPJS Ketenagakerjaan (19,5 juta data, Maret 2023), Bank Syariah Indonesia (1,5 TB data oleh ransomware Lockbit), My IndiHome (35 juta data oleh Bjorka, Juni 2023), dan data paspor WNI (34,9 juta data oleh Bjorka, Juli 2023) [7]. Faktor utama meliputi rendahnya kesadaran keamanan siber, kebijakan yang belum memadai, keterbatasan kemampuan teknis, dan kurangnya sinergi sektor publik dan swasta [3].

Penelitian ini berfokus pada pengujian keamanan terhadap website lembaga yang bertujuan untuk mencegah serangan siber yang dapat mengancam kredibilitas dan reputasi lembaga [8]. Selain itu, terdapat data-data pribadi pengguna yang diunggah di website, seperti email, nomor telepon, alamat, Kartu Tanda Penduduk (KTP). Data tersebut sangat sensitif yang apabila lembaga XYZ tidak menguji celah keamanannya menggunakan metode pengujian penetrasi, maka peretas dapat mencuri data penting yang ada dan dapat menimulkan kerugian [9]. Uji penetrasi dilakukan dengan menguji keamanan sistem dengan mensimulasikan sebagai seorang penyerang yang mengeksploitasi kerentanan website [10]. Pendekatan yang dipakai di penelitian ini adalah panduan OWASP Top 10 2021. Panduan ini dipilih karena memberikan wawasan mendalam mengenai kerentanan keamanan yang paling umum ditemui pada website [11]. Hasil dari penemuan kerentanan dapat memberikan panduan bagi pengembang dalam mencegah serta mengatasi risiko yang telah ditemukan [12].

2. METODOLOGI

Metodologi penelitian yang digunakan merupakan kerangka kerja yang terdiri dari serangkaian tahapan mendalam tentang keamanan sistem informasi seperti pada pada Gambar 1.



Gambar 1. Tahapan Penelitian

2.1 Studi Literatur

Studi literatur dilakukan untuk mengidentifikasi dan memahami pengetahuan yang telah dikembangkan dalam bidang keamanan sistem informasi. Melalui tinjauan literatur, jurnal ilmiah, dan sumber lainnya, penelitian ini membangun landasan teoritis terkait konsep keamanan informasi dan metode uji penetrasi.

2.2 *Information Gathering*

Information gathering dilakukan untuk mengumpulkan data yang mendukung pemahaman terhadap struktur dan potensi kelemahan sistem. Tahap ini mencakup pengumpulan data arsitektur jaringan dan informasi terkait pengelolaan sistem.

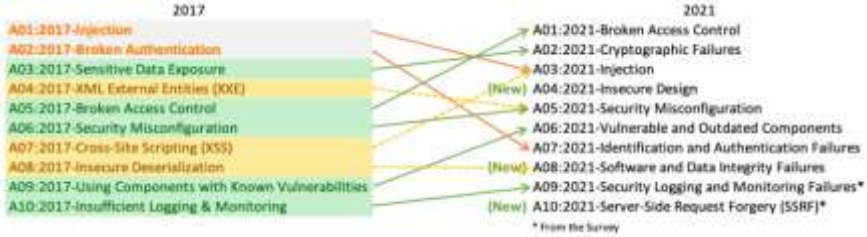
2.3 *Vulnerability Scanning*

Vulnerability scanning adalah proses untuk mengidentifikasi potensi kerentanan dalam suatu sistem. Pemindaian ini menganalisis infrastruktur dan mengidentifikasi titik yang dapat dieksploitasi oleh penyerang.

2.4 *Attacking*

Tahap attacking adalah fase simulasi serangan untuk menguji ketahanan sistem terhadap ancaman. Pada tahap ini dilakukan uji penyerangan dengan teknik serangan *black box*, yaitu jenis penyerangan dengan cara mengevaluasi hasil eksekusi, tanpa memperhatikan detail proses internal atau kode program [13]. Berbagai jenis serangan disimulasikan dengan mengacu pada panduan OWASP Top 10 2021.

OWASP Top 10 adalah dokumen bagi pengembang web untuk keamanan web yang didasarkan pada kesepakatan umum komunitas mengenai ancaman kerentanan yang paling serius pada website [14].



Gambar 2. Pembaruan OWASP 2021

2.5 *Reporting*

Proses terakhir dalam penelitian ini adalah *reporting*, yaitu pembuatan laporan mencakup deskripsi kerentanan, tingkat risiko, serta rekomendasi perbaikan yang disampaikan kepada pihak lembaga XYZ [15].

3. HASIL DAN PEMBAHASAN

3.1 *Information Gathering*

Untuk mendapatkan gambaran menyeluruh mengenai struktur jaringan website, digunakan *tool* Nmap yang berfungsi untuk mengidentifikasi host aktif dalam jaringan, serta layanan yang berjalan pada masing-masing port dengan menggunakan perintah ‘nmap -sS -sV [nama website]’.

Tabel 2. Hasil Network Mapping Website XYZ

Port	Status	Layanan	Versi
80	Open	http	Apache httpd 2.4.29
443	Open	ssl/http	Apache httpd 2.4.29
8008	Open	http	-
8010	Open	sslx/mpp?	-

Website B memiliki 4 port terbuka: Port 80 dan 443 menjalankan layanan HTTP dan HTTPS dengan Apache 2.4.29 di Ubuntu, *port* 8008 sebagai alternatif port 80, dan *port* 8010 untuk Web Application Firewall (WAF) FortiGate.

3.2 *Vulrnerabbilty Scanning*

Proses *vulnerability scanning* dilakukan menggunakan *tool* OWASP ZAP yang membantu untuk proses mengidentifikasi kemungkinan yang kemungkinan dapat dieksplotasi pada website berdasarkan OWASP Top 10 2021.

Tabel 4. Hasil Pemindaian OWASP ZAP Website XYZ

ID	Jenis Kerentanan	Status
A06:2021	Script Served From Malicious Domain (polyfill)	High
A05:2021	Content Security Policy (CSP) Header Not Set	Medium

ID	Jenis Kerentanan	Status
A05:2021	Missing Anti-clickjacking Header	
A06:2021	Vulnerable JS Library	
A05:2021	Application Error Disclosure	Low
A04:2021	Big Redirect Detected (Potential Sensitive Information Leak)	
A05:2021	Cookie No HttpOnly Flag	
A05:2021	Cookie Without Secure Flag	
A01:2021	Cookie without SameSite Attribute	
A08:2021	Cross-Domain JavaScript Source File Inclusion	
A05:2021	Server Leaks Version Information via "Server" HTTP Response Header Field	
A05:2021	Strict-Transport-Security Header Not Set	
A05:2021	X-Content-Type-Options Header Missing	
A01:2021	Information Disclosure - Sensitive Information in URL	
A01:2021	Information Disclosure - Suspicious Comments	
A03:2021	User Controllable HTML Element Attribute (Potential XSS)	

Beberapa temuan meliputi skrip dari domain berbahaya polyfill, tidak adanya *header* CSP, *Anti-clickjacking*, *Strict-Transport-Security*, dan *X-Content-Type-Options*. Selain itu, ditemukan pustaka JavaScript yang rentan, *Application Error Disclosure*, dan *Big Redirect* yang berpotensi mengungkapkan informasi sensitif. Masalah pada konfigurasi cookie, seperti tidak ada atribut HttpOnly, *Secure*, dan *SameSite*, serta *Cross-Domain JavaScript Source File Inclusion* juga ditemukan. Selain itu, bocornya informasi server melalui *header* "Server", serta *Information Disclosure* melalui URL dan komentar mencurigakan, juga terdeteksi. Terakhir, ditemukan kerentanannya pada atribut elemen HTML yang dapat dimanfaatkan untuk XSS.

3.3 *Attacking*

Uji serangan dilakukan dengan menggunakan beragam *tool* yang berbeda sesuai dengan jenis kerentanan.

1. A01 - *Broken Access Control*

Dalam pengujian ini digunakan *tool* dirsearch yang dapat membantu untuk melakukan pemindaian terhadap berbagai direktori dan file sensitif yang terekspos.

Gambar 3. Hasil Serangan *Broken Access Controll*

Penggunaan *tool* dirsearch menunjukkan hanya berhasil melakukan sebagian kecil pemindaian awal, namun selanjutnya muncul *output error* yang mengakibatkan pemindaian tidak dapat dilanjutkan. Akibat dari *error* ini, pemindaian dinyatakan tidak berhasil dalam mengidentifikasi direktori atau file yang ada di website Lembaga XYZ.

2. A02 - *Cryptographic Failure*

Karena pada serangan *Broken Access Control* pemindaian digagalkan oleh *firewall* dan tidak ditemukan file yang terenkripsi, sehingga pengujian *Cryptographic Failures* tidak dapat dilakukan

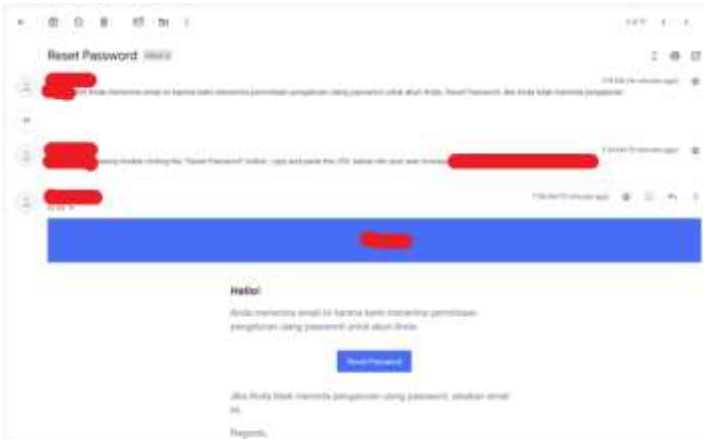
3. A03 – *Injection*

Terdapapat kolom input jenis form yang dapat disisipkan skrip XSS. Setelah input tersebut disimpan, hasilnya muncul *pop-up* yang menunjukkan bahwa serangan XSS berhasil dieksekusi.

Gambar 3. Hasil Serangan *Injection*

4. A04 - *Insecure Design*

Website lembbaga XYZ terdapat fitur *reset password* akun yang dapat dimanfaatkan untuk mengirim *spam* email. Serangan ini dilakukan dengan bantuan Burp Suite, di mana sebanyak 100 permintaan reset password dikirimkan melalui *tool* tersebut.



Gambar 4. Hasil Serangan *Insecure Design*

Hasil dari serangan ini menunjukkan bahwa semua 100 permintaan berhasil diproses oleh sistem, dan sebanyak 100 email permintaan *reset password* masuk ke alamat email yang ditargetkan. Temuan ini mengindikasikan bahwa sistem tidak memiliki mekanisme pembatasan atau deteksi terhadap permintaan *reset password* yang berulang dalam jumlah besar.

5. A05 - *Security Misconfiguration*

Digunakan tool Burp Suite dengan fitur Burp *Clickbandit* yang dirancang untuk mendeteksi kerentanan *clickjacking.*

Gambar 4. Hasil Serangan *Security Misconfiguration*

Hasilnya menunjukkan bahwa website terdapat tulisan "*You've been clickjacked*" yang menandakan bahwa konten dari webbsite tersebut dapat disusupi dan ditampilkan di dalam halaman wensite lain.

6. A06 - *Vulnerable and Outdated Components*

Berdasarkan hasil pemindaian dari OWASP ZAP, ditemukan bahwa website memiliki kerentanan "Vulnerable and Outdated Components". Menggunakan *library* versi lama yang telah diketahui memiliki kelemahan keamanan. Library yang dipakai yaitu jQuery Validation 1.14.0, moment.js 2.21.0, moment.js 2.29.1, jQuery 3.3.1, jQuery 3.4.1, Bootstrap 4.0.0, dan jQuery 2.1.4.

7. A07 - *Identification and Authentication Failures*

Dilakukan proses brute force untuk mencoba menebak *username* dan *password* admin. Halaman login terdapat 3 inputan, yaitu *email*, *password* dan *capthca*. Adanya *capthca* memungkinkan serangan *brute force* tidak bisa dilakukan karena memerlukan verifikasi input manual. Uji serangan awal dilakukan dengan menggunakan alat Burp Suite, di mana parameter captcha dihapus.

Gambar 5. Hasil Serangan *Identification and Authentication Failures*

Hasil pengujian menunjukkan bahwa implementasi captcha pada website yang diuji cukup efektif dalam mencegah serangan brute force. Meskipun parameter captcha dihapus dari permintaan HTTP, website tetap memaksa pengguna untuk menyelesaikan tantangan captcha sebelum melanjutkan proses login.

8. A08 - *Software and Data Integrity Failures*

Pemindaian menggunakan OWASP ZAP menemukan kerentanan *Cross-Domain JavaScript Source File Inclusion* pada website. Mencantumkan skrip dari domain yang tidak terpercaya dapat membahayakan keamanan website sehingga dapat dieksploitasi oleh pengguna yang tidak bertanggung jawab. Namun hasil pemindaian ZAP ini tidak valid karena semua domain yang dicurigai memang kredibel dan punya nama, yakni *cloudflare, jsdelivr,d dan video.js*.

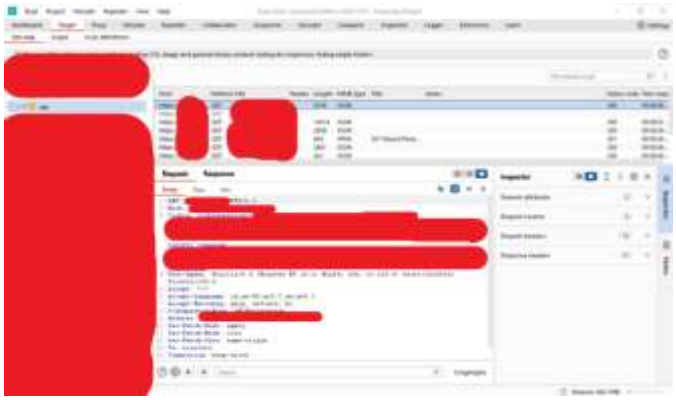
9. A09 - *Security Logging and Monitoring Failures*

Website lembaga XYZ telah mengimplementasikan WAF yang dapat mencegah serangan berbagai serangan. WAF yang dipakai diketahui menggunakan FortiWeb. Sehingga dapat

disimpulkan bahwa website tidak memiliki kerentanan *Security Logging and Monitoring Failures.*

10. A10 - *Server-Side Request Forgery*

Sebagai langkah awal pengujian, dilakukan pencarian parameter API sebagai pintu masuk serangan SSRF.



Gambar 5. Hasil Serangan *Server-Side Request Forgery*

Dengan menggunakan *tool* Burp Suite melalui fitur *sitemap* website lembaga XYZ. Hasilnya, tidak ditemukan parameter StockApi yang merupakan pintu masuk untuk melakukan eksploitasi, melainkan hanya ditemukan directory "api" merupakan API yang dapat digunakan untuk serangan SSRF. Dengan demikian, tidak ada celah SSRF yang teridentifikasi pada website.

3.4 *Reporting*

Terdapat hasil *reporting* yang merupakan tabbel yang berisi rangkuman attacking yang akan diberikan kepada pihak Lembaga XYZ.

Tabel 4. Hasil Pemindaian OWASP ZAP Website XYZ

ID	Kategori	Tool	Temuan	Rekomendasi Perbaikan
A01:2021	*Broken Access Control*	dirsearch	Tidak ditemukan	-
A02:2021	*Cryptographic Failures*	Manual	Tidak ditemukan	-
A03:2021	*Injection*	Manual	Serangan XSS pada input form	Menerapkan filter dari data input yang ketat
A04:2021	*Insecure Design*	Burpsuite	Melakukan *reset password* tanpa batas	Membatasi permintaan untuk *reset password*
A05:2021	*Security Misconfiguration*	Burpsuite	Serangan *clickjacking*	Mengatur header HTTP X-Frame-Options dengan atribut ‘SAMEORIGIN’ atau ‘DENY’
A06:2021	*Vulnerable and Outdated Components*	ZAP	Mengguankan library versi lama yang telah diketahui kerentanannya	Memperbarui library jQuery Validation, moment.js, dan Bootstrap
A07:2021	*Identification and Authentication Failures*	Burpsuite	Tidak ditemukan	-
A08:2021	*Software and Data Integrity Failures*	ZAP	Tidak ditemukan	-
A09:2021	*Security Logging and monitoring*	Manual	Tidak ditemukan	-

ID	Kategori	Tool	Temuan	Rekomendasi Perbaikan
A10:2021	*Server-Side Request Forgery*	Manual	Tidak ditemukan	-

4. KESIMPULAN

Dalam pengujian yang dilakukan menggunakan berbagai *tool* pada website lembaga XYZ. Kerentanan yang ditemukan meliputi *Injection*, di mana serangan XSS dapat tereksekusi pada input form, mitigasinya adalah dengan menerapkan filter ketat pada data input. Selanjutnya, *Insecure Design* dengan memanfaatkan fitur *reset password* secara tanpa batas, yang dapat dicegah dengan membatasi jumlah permintaan *reset password*. Kerentanan *Security Misconfiguration* dilakukan dengan serangan clickjacking menggunakan tool Burp Suite, untuk mengatasi kerentanan ini yaitu dengan mengatur header HTTP X-Frame-Options dengan atribut 'SAMEORIGIN' atau 'DENY. Terakhir, kerentanan *Vulnerable and Outdated Components*, penggunaan library versi lama seperti jQuery Validation, moment.js, dan Bootstrap yang rentan dapat ditangani dengan memperbarui komponen tersebut ke versi terbaru. Hasil dari proses attacking dirangkum pada tahap reporting yang menjabarkan kategori kerentanan OWASP Top 10 201, *tool* yang dipakai, temuan, dan rekomendasi perbaikan yang dapat membantu pengembang website dalam mengetahui dan mengatasi masalah keamanan yang ada di website lembaga XYZ.

5. DAFTAR RUJUKAN

[1] S. Rohaya, “INTERNET: Pengertian, Sejarah, Fasilitas, dan Koneksi” 2008. [Online]. Available: http://dhani.shingcat.com,

[2] R. Mochamad, “Literasi Internet Sehat Terhadap Siswa Sekolah Dasar Di Desa Tanjakan Banten”, Community Engagement and Emergence Journal (CEEJ), vol. 2, no. 1, pp. 116–119, Sep. 2020.

[3] A. . Muftiadi, T. P. M. . Agustina, and M. . Evi, “Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman Phishing terhadap Layanan Online Banking”, Jurnal Ilmiah Teknik, vol. 1, no. 2, pp. 60–65, Aug. 2022.

[4] M. DI Kejahatan Siber Indonesia, M. Rizki Hapizon, and K. Rizki, “Analisis Kerjasama Cybersecurity Indonesia-Australia dalam.” [Online]. Available: https://media.neliti.com/

[5] Bisnis Tekno, “Kerugian Akibat Kejahatan Siber di Dunia Tembus Rp129.643 Triliun Artikel ini telah tayang di Bisnis.com dengan judul "Kerugian Akibat Kejahatan Siber di Dunia Tembus Rp129.643 Triliun.” [Online]. Available:https://teknologi.bisnis.com/read/20221212/84/1607768/kerugian-akibat-kejahatan-siber-di-dunia-tembus-rp129643-triliun

[6] Antara News, “BSSN harapkan perbankan respon cepat pemberitahuan anomali internet.” Nov. 13, 2023. [Online]. Available: https://www.antaranews.com/berita/3823224/bssn-harapkan-perbankan-respon-cepat-pemberitahuan-anomali-internet

[7] dataindonesia.id, “Deret Kasus Kebocoran Data RI pada 2023, dari BSI hingga Paspor.” [Online]. Available: https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor.

[8] Putri, D. E. (2023). Vulnerability assessment pada website portal manajemen informatika Politeknik Lp3i. *Bulletin of Network Engineer and Informatics, 1*(2), 42–50.

[9] Nurelia, F., Putri, S., Utomo, Y. B., & Kurniasari, I. (2024). Pengaruh Penetration Testing Dalam Menguji Celah Keamanan Pada Website (Studi Kasus: Dinas Kependudukan dan Pencatatan Sipil Kota Kediri). *Jurnal Multinetics*, *2*, 121–128.

[10] Sunaringtyas, S., & Prayoga, D. (2021). Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada Layanan Single Sign-On. *Edu Komputika Journal*, *8*(1), 48-56.

[11] Ramadhan, M. F. A., & Ilmananda, A. S. (2024). Analisis Ancaman Keamanan Pada Sistem Informasi Akademik Kampus Menggunakan Metode OWASP ZAP. *Jurnal Mahasiswa Teknik Informatika*, *8*(1), 7985–7991.
[12] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi kerentanan keamanan aplikasi website menggunakan metode OWASP (Open Web Application Security Project) untuk penilaian risk rating. *Creat. Inf. Technol. Journal*, *4*(4), 264-270.
[13] Arfani, A. R. Y. ., Kasih, P. ., & Pamungkas, D. P. . (2022). Pengujian Aplikasi Presensi dengan Black box Testing dengan Metode Equivalence Partitioning dan Boundary Value Analysis. *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, *6*(1), 338–343.
[14] Listartha, I. M. E., Premana Mitha, I. M. A., Arta, M. W. A., & Arimika, I. K. M. W. Y. (2022). Analisis kerentanan website SMA Negeri 2 Amlapura menggunakan metode OWASP (Open Web Application Security Project). *SIMKOM*, 7(1), 23-27.
[15] Pujiarto, B., Utami, E., & Sudarmawan, S. (2013). Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing (Kasus: Universitas Muhammadiyah Magelang). *Data Manajemen Dan Teknologi Informasi (DASI)*, *14*(2), 16.