Jurnal Teknik Informatika dan Teknologi Informasi (JUTITI)
Vol. 3 No. 2 Agustus 2023
E-ISSN: 2827-9387, P- ISSN: 2827-9379, Hal 26-32
DOI: https://doi.org/10.55606/jutiti.v3i2.2853

Perbandingan *Vulnerability Assesment* Menggunakan *Owasp Zap* dan *Acunetix* Pada Sistem Informasi Repositori Politeknik Negeri Indramayu

Riyan Farismana[a,]*, Dian Pramadhana[b]

[ab] Politeknik Negeri Indramayu

Abstract. *The security of web-based systems is an important thing that an organization needs to pay attention to, considering that currently all organizational business processes rely on the web to store and process their data. POLINDRA is also not left behind, which uses web technology to store and process a list of student work repositories into a web-based information system. This requires simultaneous testing and risk assessment to determine the level of existing risks and vulnerabilities. The results of the vulnerability assessment to determine security gaps carried out in the scientific work repository information system on the sista.polindra.ac.id page using two different tools, namely Owasp Zap and Acunetix, have several different results. On Owasp Zap, there were 22 warnings, while Acunetix found 499 warnings. Even though the number of alerts using Acunetix is greater, the alert type results are not as complete as Owasp Zap, which produces 22 alerts, while Acunetix only produces 10 alerts.*

Keywords: *Acunetix, Owasp ZAP, POLINDRA, Repository Information system, vulnerability assessment*

Abstrak. Keamanan sistem berbasis web menjadi satu hal penting yang perlu diperhatikan oleh sebuah organisasi, mengingat saat ini seluruh proses bisnis organisasi mengandalkan web untuk menyimpan dan mengolah data mereka. Tidak ketinggalan juga POLINDRA yang menggunakan teknologi web untuk menyimpan dan mengolah daftar repositori karya mahasiswa kedalam sebuah sistem informasi berbasis web. Untuk itu diperlukan pengujian dan penilaian risiko secara simultan untuk mengetahui tingkat risiko dan kerentanan yang ada. Hasil vulnerability assessment untuk mengetahui celah keamanan yang dilakukan pada sistem informasi repositori karya ilmiah pada halaman sista.polindra.ac.id menggunakan dua tools yang berbeda yaitu Owasp Zap dan Acunetix memiliki beberapa perbedaan hasil yang dimiliki. Pada Owasp Zap terdapat 22 peringatan, sedangkan Acunetix menemukan 499 peringatan. Walaupun jumlah peringatan menggunakan Acunetix lebih banyak, akan tetapi dari hasil alert type tidak selengkap Owasp Zap yang menghasilkan 22 peringatan, sedangkan Acunetix hanya 10 peringatan.

Kata kunci: *Acunetix, Owasp Zap,* POLINDRA, sistem informasi repositori, *vulnerability assessment*

LATAR BELAKANG

Isu keamanan *web*, menjadi salah isu terpenting pada saat ini dimana hampir seluruh data dan informasi berjalan melalui internet. Berdasarkan lanskap keamanan siber Indonesia yang dikeluarkan oleh BSSN tahun 2022, terdapat 2.348 kasus web *defacement* atau serangan yang memanfaatkan kerentanan dari sistem yang terjadi di situs-situs Indonesia (BSSN, 2022).

Keamanan sistem berbasis *web* merupakan satu hal penting diperhatikan dalam pengembangan sebuah *website* (Mayasari, 2020). Bahkan sudah dipersiapkan dari awal pengembangan, sehingga dapat mengurangi kemungkinan serangan yang diakibatkan banyaknya celah dan kerentanan yang tidak diperhitungkan sebelumnya pada saat proses pengembangan, dan menjadikan web yang dibangun menjadi sasaran eksploitasi orang-orang yang tidak bertanggung jawab.

Salah satu yang dapat dilakukan dalam pengamanan *website* adalah melakukan pemindaian terhadap celah keamanan suatu *website* untuk mengetahui celah yang ada (Ziwan A, 2022). Selain itu melakukan deteksi terhadap tingkat kerentanan pada sebuah sistem berbasis *website* merupakan hal yang penting untuk mengetahui sejauh mana risiko pada sistem tersebut (Aryanti & Utamajaya, 2021). Oleh karena itu bagi organisasi khususnya diwajibkan untuk selalu melakukan pemindaian celah keamanan sistem berbasis *website* yang dimilikinya secara konsisten dan simultan, mengingat setiap saat sistem yang dimiliki dapat di serang dengan berbagai alasan.

Received Juny 23, 2023; Revised July 13, 2023; Accepted August 30, 2023
*Corresponding author, riyanfarismana@polindra.ac.id

Politeknik Negeri Indramayu merupakan institusi yang memiliki komitmen untuk menjaga keamanan data pada sistem maupun *website* yang dimiliki. Salah satu upaya yang dilakukan adalah selalu melakukan evaluasi terhadap celah keamanan pada setiap sistem *website* yang terdaftar pada domain polindra. Sistem informasi repositori POLINDRA, merupakan satu dari beberapa sistem yang talah dilakukan pengujian keamanan di dalamnya. Berdasarkan pengujian yang dilakukan sebelumnya terdapat beberapa celah yang ditemukan. Pada pengujian tersebut pemindaian celah menggunakan *tools Owasp Zap* dan terdapat 22 peringatan dengan berbagai tingkat risiko (Farismana, & Pramadhana, 2023).

Sesuai dengan komitmen keamanan data yang dimiliki POLINDRA, maka sistem yang sebelumnya sudah di pindai menggunakan *tools* OWASP ZAP, akan Kembali dilakukan penilaian kerentanan menggunakan tools Acunetix yang diharapkan dapat lebih menggali celah-celah kerentanan yang terdapat di dalam sistem informasi repositori, selain itu penelitian ini juga dimaksudkan untuk melihat perbandingan hasil *vulnerability assessment* terhadap sistem informasi repositori POLINDRA menggunakan *tools Owasp Zap* dan *Acunetix*, sehingga *developer* dapat memperbaiki celah tersebut dan membuat sistem informasi repositori yang menyimpan data akademik civitas POLINDRA menjadi lebih aman dari ancaman serangan sistem.

KAJIAN TEORITIS

Vulnerability Assessment

Vulnerability assessment atau penilaian kerentanan adalah audit berkala penilaian risiko dan kerentanan yang dialukan organisasi dengan standarisasi dan penerapanan sistem keamanan untuk mendorong optimalisasi proses kemanan pada organisasi (Upadhyay & Sampalli, 2020). *Vulnerability assessment* sendiri memiliki fokus untuk mengidentifikasi adanya risiko celah kerentanan dalam pemindaian aplikasi (Setiyani, 2023). Cara kerja *vulnerability assessment* diantaranya

1. Identifikasi asset
   tahap awal adalah mengidentifikasi aset, aset dapat berupa perangkat keras atau perangkat lunak yang terdapat didalam organisasi.
2. *Scanning*
   Tahapan ini yait melakukan *scanning* menggunakan tools untuk mencari kerentanan dan celah kemananan pada sistem yang diidentifikasi. Proses ini bisa dilakukan oleh tim atau pihak luar.
3. Analisis
   Setelah dilakukan *scanning* tim *vulnerability assessment* melakukan analisis terhadap kerentanan yang telah ditemukan, menentukan tingkatan risiko, serta apakah kerentanan yang nyata atu tidak.
4. Evaluasi
   Evaluasi dari hasil analisis untuk melakukan tindakan pencegahan dan pemulihan untuk mengurangi risiko dan dampak dari kerentanan yang ditemukan.
5. Laporan
   Tahap akhir adalah Menyusun laporan dar hasil proses vulnerability assessment yang dilakukan.

Owasp Zap

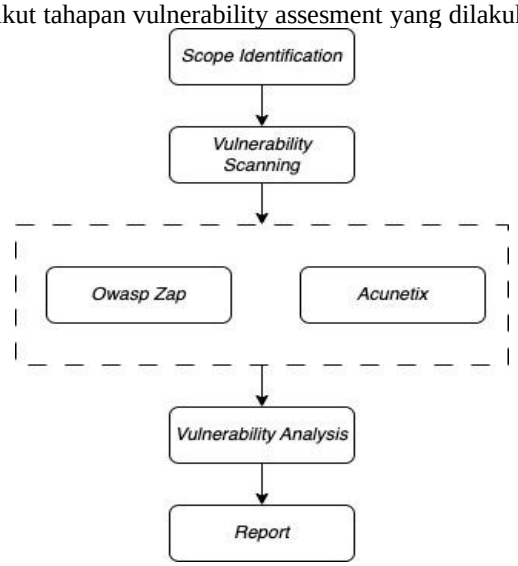
Owasp Zap merupakan *tools* yang cukup popular untuk melihat kerentanan dan keamanan situs, serta dapat membantu memberikan rekomendasi untuk memitigasi kerentanan sebuah situs (Aditama & Negara, 2022). Owasp Zap sendiri merupakan sebuah *tools open source* gratis yang dapat digunakan, dan dirancang khusus untuk pengujian aplikasi berbasis web (Hasibuan & Handoko, 2023). Owas Zap menggunakan pendekatan *Black Box Testing* dimana penguji sangat minim sekali informasi pada sistem yang akan di test.OWASP menggunakan 11 kategori pendekatan pengujian yang melibatkan analisis aktif dari aplikasi untuk setiap kelemahan.

Acunetix

Acunetik merupakan salah satu pelopor teknologi pemindaian kemanan web, memberikan solusi pengujian keamanan situs maupun aplikasi web, dan juga API. Kelebihan Acunetix adalah menghilangkan waktu peryiapan yang lama, penggunaan yang cukup mudah, memberikan keleluasaan bagi tim alam mencari kesalahan, memberikan waktu yang singkat dalam proses *scanning*, serta tidak membebani jaringan ataupun *server.* Acunetix Vulnerability Scanner merupakan sebuah *tools* layanan aplikasi web untuk pengujian keamanan secara otomatis yang mengaudit aplikasi web dengan memeriksa kerentanan seperti *SQL Injection, Cross site scripting*, dan kerentanan web yang dieksploitasi lainnya.

METODE PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode *vulnerability assessment*, dimana berfokus pada tahapan *vulnerability scanning* untuk melakukan pengujian kerentanan menggunakan tools *vulnerability scanner* yang sudah dilakukan menggunakan *Owasp Zap* serta akan di komparasi dengan *tools Acunetix*, kemudian melakukan analisis terhadap hasil pengujian terhadap sistem informasi repositori yang karya ilmiah yang diuji. Berikut tahapan vulnerability assesment yang dilakukan dalam penelitian ini.



Gambar 1. Tahapan Penelitian

1. Tahap pertama penulis melakukan identifikasi ruang lingkup penelitian yaitu dengan memilih sistem informasi repositori karya POLINDRA sebagai target dilakukannya vulnerability assessment, kemudian menentukan batasan-batasan terhadap sistem yang akan diuji yaitu hanya melakukan vulnerability scanning (kerentanan) secara passive attack tanpa melakukan eksploitasi terhadap sistem.
2. Tahap kedua merupakan tahapan digunakan untuk mencari kerentanan pada sistem informasi repositori karya ilmiah menggunakan Owasp ZAP dan Acunetix untuk mencari celah keamanan pada aplikasi web yang di uji.
3. Tahap ketiga dimana hasil dari pemindaian yang dilakukan akan mendapatkan daftar kerentanan dari sistem informasi repositori karya ilmiah kemudian peneliti akan menganalisis informasi-informasi vulnerability yang ditemukan.
4. Tahap kelima yaitu melakukan dokumentasi terkait kerentanan dan hasil analisa kerentanan yang dilakukan, dan memberikan rekomendasi untuk memperbaiki kerentanan pada sistem informasi repositori karya ilmiah.

HASIL DAN PEMBAHASAN

Hasil dan pembahasan vulnerability assessment ini mencakup scope identification, vulnerability scanning menggunakan *Owasp Zap* dan *Acunetix*, *vulnerability analysis*, dan *report menemukan celah di dalam sista.polindra.ac.id,* sehingga *vulnerability assessment* dilakukan dengan berdasarkan kerentanan yang terdapat pada tahap *vulnerability scanning.*

1. Vulnerability Scanning

Vulnerability scanning dilakukan untuk memindai kerentanan yang terdapat didalam sistem informasi repositori karya ilmiah POLINDRA. Tools yang digunakan untuk tahapan ini menggunakan *Owasp Zap* dan *Acunetix.*

a. Owasp Zap

Proses *scanning* menggunakan Owasp Zap telah dilakukan pada penelitian sebelumnya dan memperoleh hasil 22 peringatan dimana terdapat 1 risiko dengan *level high,* 7 risiko *medium,* 9 risiko *low,* dan 5 tingkatan *informational.* Sedangkan dari sisi *confidence* terdapat 3 *level high*, 14 level

medium, dan 5 *level low*. hasil *scanning* yang dilakukan menggunakan Owasp Zap dapat dilihat pada gambar berikut.

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (4.5%)	0 (0.0%)	1 (4.5%)
	Medium	0 (0.0%)	1 (4.5%)	4 (18.2%)	2 (9.1%)	7 (31.8%)
	Low	0 (0.0%)	2 (9.1%)	6 (27.3%)	1 (4.5%)	9 (40.9%)
	Informational	0 (0.0%)	0 (0.0%)	3 (13.6%)	2 (9.1%)	5 (22.7%)
	Total	0 (0.0%)	3 (13.6%)	14 (63.6%)	5 (22.7%)	22 (100%)

Sumber: Farismana, & Pramadhana (2023)
Gambar 2. Hasil *Scanning Owasp Zap*

b. Acunetix

Setelah mengetahui celah kerentanan melalui *vulnerability scanner* menggunakan *Owasp Zap*, selanjutnya peneliti melakukan *scanning* Kembali menggunakan tools yang berbeda yaitu *Acunetix.*

Tabel 1. *Scan Information*

Scan information	
Start url	https://sista.polindra.ac.id
Host	https://sista.polindra.ac.id

Pada tabel 1 diatas menunjukan url sista.polindra.ac.id sebagai domain utama dalam melakukan *vulnerability scanning* menggunakan *Acunetix.*

Tabel 2. Hasil scanning *Acunetix*

Total alert found	**499**
High	*1*
Medium	*4*
Low	*1*
Informational	*493*

Dari total peringatan yang ditemukan menggunakan *Acunetix* terdapat 1 kategori *high*, 4 *medium*, 1 low, dan 493 *informational*, setelah dilakukan pencarian lebih lanjut terdpat keterangan keimpulan peringatan yaitu.

Tabel 3. *Alert Sumary* pada *Acunetix*

Level	**Summary**
High	*Possible database backup*
Medium	*HTML form without CSRF protection*
Low	*Clickjacking : X-frame-option header missing*
Informational	*Broken links*

Berdasarkan hasil *scanning*, *threat level* pada sistem informasi repositori POLINDRA terdapat pada level 3, dimana dijelaskan satu atau lebih kerentanan jenis tingkat tinggi telah ditemukan oleh pemindai. Pengguna jahat dapat mengeksploitasi kerentanan ini dan menyusupi database backend dan/atau merusak situs web sistem informasi repositori.

2. Vulnerability Analysis

Setelah proses *scanning* menggunakan *Owasp Zap* dan *Acunetix*, tahapan selanjutnya adalah melakukan analisis untuk mencari jumlah peringatan dari setiap jenis peringatan, beserta tingkat risiko jenis peringatan tersebut. Tabel 2 merupakan perhitungan peringatan menurut jenisnya.

Tabel 4. *Alert Sumary* pada *Acunetix*

No	*Alert Type*	
	Owasp Zap	*Acunetix*
1	*Hash Disclosure - Mac OSX salted SHA-1*	*Injection(A1)*
2	*Absence of Anti-CSRF Tokens*	*Broken Authentication and Session Management(A2)*
3	*Application Error Disclosure*	*Cross Site Scripting (XSS)(A3)*
4	*Content Security Policy (CSP) Header Not Set*	*Insecure Direct Object Reference(A4)*
5	*Cross-Domain Misconfiguration*	*Security Misconfiguration(A5)*
6	*Hidden File Found*	*Sensitive Data Exposure(A6)*
7	*Missing Anti-clickjacking Header*	*Missing Function Level Access Control(A7)*
8	*Vulnerable JS Library*	*Cross Site Request Forgery (CSRF)(A8)*
9	*Big Redirect Detected (Potential Sensitive Information Leak)*	*Using Components with Known Vulnerabilities(A9)*
10	*Cookie Without Secure Flag*	*UnvalidatedRedirects and Forwards(A10)*
11	*Cookie without SameSite Attribute*	
12	*Cross-Domain JavaScript Source File Inclusion*	
13	*Information Disclosure - Debug Error Messages*	
14	*Server Leaks Version Information via "Server" HTTP Response Header Field*	
15	*Strict-Transport-Security Header Not Set*	
16	*Timestamp Disclosure - Unix*	
17	*X-Content-Type-Options Header Missing*	
18	*Information Disclosure - Suspicious Comments*	
19	*Modern Web Application*	
20	*Re-examine Cache-control Directives*	
21	*Retrieved from Cache*	
22	*User Agent Fuzzer*	
Total	***22***	***10***

Setelah dilakukan analisis terhadap jenis peringatan yang ditampilkan masing-masing *tools* yaitu *Owasp Zap* dan *Acunetix*, terdapat perbedaan jumlah peringatan yang ada dimana *Owasp Zap* menghasilkan 22 peringatan dan *Acunetix* menghasilkan 10 jenis peringatan. Dimana untuk detil jumlah kategori perigatan pada tools Acunetix terdapat pada tabel berikut.

Tabel 5. Jumlah peringatan yang ditemukan

Alert	**Jumlah**
Injection	*No alerts in this category*
Broken Authentication and Session	*No alerts in this category*
ManagementCross Site Scripting (XSS)	*No alerts in this category*
Insecure Direct Object Reference	*No alerts in this category*
Security Misconfiguration	*13*
Sensitive Data Exposure	*495*
Missing Function Level Access Control	*1*
Cross Site Request Forgery	*4*

Using Components with Known Vulnerabilities	*13*
UnvalidatedRedirects and Forwards	*No alerts in this category*

3. Report

Tahapan *report* adalah tim melakukan pembuatan dokumentasi terkait deskripsi kerentanan, *impact*, dan juga rekomendasi perbaikan yang harus dilakukan oleh organisasi. *Report* yang dibuat pada tahapan ini berasal dari *tools Acunetix* yang akan menjadi tambahan informasi dari hasil report menggunakan Owasp Zap pada *vulnerability assesment* sebelumnya dimana terdapat 12 *alert type* dengan deskripsi dan rekomendasi (Farismana & Pramadhana, 20223)

Tabel 6. Hasil *report* kerentanan dan rekomendasi

Kerentanan	**Deskripsi**	**Im*pact***	**Rekomendasi**
Possible database backup	File ini berisi cadangan/dump database. *Acunetix* menyimpulkan nama file ini dari nama domain. Cadangan basis data berisi catatan struktur tabel dan/atau data dari basis data dan biasanya dalam bentuk daftar pernyataan SQL. Cadangan basis data paling sering digunakan untuk membuat cadangan basis data sehingga isinya dapat dipulihkan jika terjadi kehilangan data. Informasi ini sangat sensitif dan tidak boleh ditemukan pada sistem produksi.	File ini mungkin mengungkapkan informasi sensitif. Informasi ini dapat digunakan untuk melancarkan serangan lebih lanjut.	File sensitif seperti cadangan basis data tidak boleh disimpan dalam direktori yang dapat diakses oleh server web. Sebagai solusinya, Anda dapat membatasi akses ke file ini.
HTML form without CSRF protection	CSRF atau XSRF adalah kerentanan di mana penyerang mengelabui korban agar membuat permintaan yang tidak ingin dibuat oleh korban. Oleh karena itu, dengan CSRF, penyerang menyalahgunakan kepercayaan yang dimiliki aplikasi web dengan browser korban. *Acunetix* menemukan formulir HTML yang tidak menerapkan perlindungan anti-CSRF. Lihat bagian 'Rincian serangan' untuk informasi lebih lanjut tentang formulir HTML yang terpengaruh.	Penyerang dapat menggunakan CSRF untuk mengelabui korban agar mengakses situs web yang dihosting oleh penyerang, atau mengeklik URL yang berisi permintaan berbahaya atau tidak sah. CSRF adalah jenis serangan yang memanfaatkan otentikasi dan otorisasi korban ketika permintaan palsu dikirim ke *server web*. Oleh karena itu, jika kerentanan CSRF dapat mempengaruhi pengguna yang memiliki hak istimewa seperti administrator.	Teknik yang direkomendasikan dan paling banyak digunakan untuk mencegah serangan CSRF dikenal sebagai token anti-CSRF, terkadang juga disebut sebagai token sinkronisasi.
Clickjacking : X-frame-option header missing	*Clickjacking* adalah teknik jahat yang menipu pengguna *web* agar mengeklik sesuatu yang	Dampaknya bergantung pada aplikasi web yang terpengaruh.	Konfigurasikan *server web* untuk menyertakan header X-Frame-Options. Konsultasikan referensi

	berbeda dari apa yang pengguna anggap sedang mereka klik, sehingga berpotensi mengungkapkan informasi rahasia atau mengambil kendali komputer mereka saat mengklik halaman web yang tampaknya tidak berbahaya. Server tidak mengembalikan header X-Frame-Options yang berarti situs web ini berisiko terkena serangan clickjacking. Header respons HTTP X-Frame-Options dapat digunakan untuk menunjukkan apakah browser diperbolehkan merender halaman di dalam bingkai atau iframe atau tidak. Situs dapat menggunakan ini untuk menghindari serangan clickjacking, dengan memastikan bahwa kontennya tidak disematkan ke situs lain.		*web* untuk informasi lebih lanjut tentang kemungkinan nilai untuk *header*.
Broken links	Tautan rusak mengacu pada tautan apa pun yang seharusnya membawa pengguna ke dokumen, gambar, atau halaman web, yang sebenarnya menghasilkan kesalahan. Halaman ini ditautkan dari situs web tetapi tidak dapat diakses.	Masalah saat menavigasi situs.	Hapus tautan ke file, atau buat agar dapat diakses.

KESIMPULAN DAN SARAN

Hasil vulnerability assessment untuk mengetahui celah keamanan yang dilakukan pada sistem informasi repositori karya ilmiah pada halaman sista.polindra.ac.id menggunakan dua *tools* yang berbeda yaitu *Owasp Zap* dan *Acunetix* memiliki beberapa perbedaan hasil yang dimiliki. Pada Owasp Zap terdapat 22 peringatan dimana terdapat 1 risiko dengan *level high*, 7 risiko *medium*, 9 risiko *low*, dan 5 tingkatan *informational*. Sedangkan dari sisi *confidence* terdapat 3 *level high*, 14 level *medium*, dan 5 *level low*. Sedangkan *Acunetix* menemukan 499 peringatan dimana terdapat 1 kategori *high*, 4 *medium*, 1 low, dan 493 *informational*. Walaupun jumlah peringatan menggunakan *Acunetix* lebih banyak, akan tetapi dari hasil *alert type* tidak selengkap *Owasp Zap* yang menghasilkan 22 *alert*, sedangkan *Acunetix* hanya 10 *alert.* Meskipun hasil yang didapatkan berbeda, akan tetapi *vulnerability assessment* ini ditujukan untuk menambah pengetahuan terkait tingkat kerentanan yang terdapat dalam sistem informasi repositori POLINDRA sehingga bisa menjadi bahan acuan untuk perbaikan.

DAFTAR REFERENSI

Mayasari, R., Ridha, A. A., Juardi, D., & Baihaqi, K. A. (2020). Analisis Vulnerability pada Website Universitas Singaperbangsa Karawang menggunakan Acunetix Vulnerability. SYSTEMATICS, 2(1), 33-38.

BSSN. (2022). Lanskap Keamaman Siber Indonesia 2022. Badan Siber dan Sandi negara, 25. Jakarta. Diakses dari https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs

Zirwan, A. (2022). Pengujian dan Analisis Keamanan Website Menggunakan Acunetix Vulnerability Scanner. Jurnal Informasi dan Teknologi, 70-75.

Aryanti, D., & Utamajaya, J. N. (2021). Analisis Kerentanan Keamanan Website Menggunakan Metode OWASP (Open Web Application Security Proj

Farismana, R., & Pramadhana, D. (2023). VULNERABILITY ASSESSMENT UNTUK ANALISIS TINGKAT KEAMANAN PADA SISTEM INFORMASI REPOSITORI KARYA ILMIAH POLITEKNIK NEGERI INDRAMAYU. Jurnal Teknik Informatika dan Teknologi Informasi, 3(1), 26-33.

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

Setiyani, L., Syarifudin, N. A., & Rohim, A. (2023). Analisis Celah Keamanan E-Learning Perguruan Tinggi Menggunakan Vulnerability Assessment. Jurnal Inovasi Pengembangan Aplikasi dan Keamanan Informasi Nusantara, 1(1), 1-10.

Aditama, R. V., & Negara, E. S. (2022). Pemindai Kerentanan Terhadap Website Jago Masak Dengan Metode Pengujian Penetrasi OWASP ZAP. Jurnal Mantik, 6(3), 3406-3412.

Hasibuan, A. F., & Handoko, D. (2023). Analisis Keretanan Website Dengan Aplikasi Owasp Zap. Jurnal Ilmu Komputer dan Sistem Informasi, 2(2), 257-270.

Abdillah, M. D., Gunawan, J., Atsil, R. A., & Harahap, A. M. (2023). Analisis Kerentanan Website Mtss Al-Washliyah Bah Gunung Menggunakan Metode Open Web Application Security Project ZAP (OWASP ZAP). Jurnal Sains dan Teknologi (JSIT), 3(1), 61-67.