JURNAL TEKNIK INFORMATIKA DAN TEKNOLOGI INFORMASI
Halaman Jurnal: https://ejurnal.politeknikpratama.ac.id/index.php/JUTITI
Halaman UTAMA: https://ejurnal.politeknikpratama.ac.id/index.php

VULNERABILITY ASSESSMENT UNTUK ANALISIS TINGKAT KEAMANAN PADA SISTEM INFORMASI REPOSITORI KARYA ILMIAH POLITEKNIK XYZ

Riyan Farismana [a], Dian Pramadhana[b]
[a] Teknik Informatika, riyanfarismana@polindra.ac.id, Politeknik Negeri Indramayu
[b] Teknik Informatika, dianpramadhana@polindra.ac.id, Politeknik Negeri Indramayu

Abstrak

The large role of information systems in supporting the success of organizational business processes, making security issues an absolute thing to maintain. The world of education also makes information systems a place to store and manage academic data, one of which is scientific work. Polytechnic XYZ has a repository information system for scientific papers and student final assignments managed by librarians to facilitate the archiving of scientific papers by students. Vulnerability assessment is carried out through the stages of information gathering, vulnerability scanning, vulnerability analysis using tools such as robtex.com and Owasp ZAP to find out the security gaps that exist in the repository information system, so that the intellectual property contained therein can be maintained. from the test results found 22 vulnerabilities from high to informational levels, and in the final stage a generating report is carried out which contains a description of the vulnerabilities and solutions to fix dangerous vulnerabilities.
***Keywords**: Owasp ZAP, Repository Information system, vulnerability assessment*

Abstrak

Besarnya peran sistem informasi dalam menunjang keberhasilan proses bisnis organisasi, menjadikan isu keamanan menjadi suatu hal mutlak untuk dijaga. Dunia pendidikan tidak luput pula menjadikan sistem informasi sebagai tempat menyimpan dan mengolah data akademik, salah satunya adalah karya ilmiah. Politeknik XYZ memiliki sistem informasi repositori karya ilmiah dan tugas akhir mahasiswa yang dikelola oleh pustakawan untuk memudahkan pengarsipan karya ilmiah oleh mahasiswa. *Vulnerability assessment* dilakukan melalui tahap *information gathering*, *vulnerability scanning*, *vulnerability analysis* menggunakan *tools* sepeerti robtex.com dan Owasp ZAP untuk mengetahui celah keamanan yang ada didalam sistem informasi repositori tersebut, sehingga kekayaan intelektual yang terkandung didalamnya dapat terjaga. dari hasil pengujian ditemukan 22 kerentanan dari level *high* hingga *informational*, serta di tahap akhir dilakukan *generating report* yang berisi deskripsi kerentanan serta solusi untuk memperbaiki kerentanan yang membahayakan.
Kata kunci: Owasp ZAP, sistem informasi repositori, *vulnerability assessment*

1. PENDAHULUAN

Bocornya data dan informasi serta pencurian kekayaan intelektual merupakan masalah terbesar dalam tindakan *cybercrime* (Riskiyadi & Anggono 2021). Di dalam konteks dunia yang saat ini saling terhubung dan bergantung pada sektor teknologi informasi, keamanan informasi menjadi sangat penting. Apalagi dewasa ini sistem informasi bukan lagi hanya menjadi pendukung bagi sebuah organisasi untuk menunjang proses bisnisnya, akan tetapi menjadi bagian penting dalam menunjang keberhasilan sebuah organisasi hingga menentukan keputusan penting didalamnya. Sehingga keamanan data dan informasi yang terkandung di dalam sistem informasi menjadi suatu hal yang mutlak untuk dijaga (Farismana & Pramadhana, 2022).

Dunia pendidikan khususnya pendidikan tinggi merupakan salah satu yang menjadikan sistem informasi sebagai tempat untuk menyimpan dan mengolah data-data akademik, salah satunya adalah karya ilmiah dan tugas akhir mahasiswa. Politeknik X memiliki Sistem informasi repositori karya ilmiah untuk membantu pustakawan dan jurusan dalam mengelola pengarsipan karya ilmiah yang sebelumnya masih dilakukan secara konvensional menjadi sebuah sistem digital yang baru dan modern.

Sistem informasi repositori merupakan sistem yang diharapkan dapat membantu untuk mengatur pengarsipan data-data tugas akhir yang telah dikerjakan oleh mahasiswa tingkat akhir menjadi lebih rapi,

aman dan mudah untuk dikelola. Seluruh informasi yang berkaitan dengan tugas akhir disimpan dan dikelola di dalam sistem informasi ini dimana *platform* yang digunakan adalah berbasis *website*, tentunya sangat efektif dan memudahkan dalam pengelolaannya karena mahasiswa maupun dosen dapat mendapatkan informasi terkait tugas akhir yang sedang dan sudah dikerjakan. Akan tetapi penggunaan *websit*e sebagai platform sebuah sistem informasi tentunya memiliki banyak risiko, apalagi ditambah sistem yang dibangun tidak memiliki sistem keamanan yang baik yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk memanfaatkan celah keamanan untuk mengambil kekayaan intelektual berupa tugas akhir mahasiswa di Politeknik XYZ.

Salah satu metode untuk mengetahui celah keamanan sebuah sistem adalah *Vulnerability Assessment*. Proses *vulnerability assessment* yang dimaksudkan untuk mendefinisikan ancaman dan risiko yang ditimbulkannya biasanya melibatkan penggunaan alat penguji otomatis, seperti pemindaian keamanan jaringan, yang hasilnya terdaftar dalam laporan *vulnerability assessmen*t (Alwi & Ilmawan, 2021).

Dengan dilakukannya *vulnerability assessment* diharapkan mampu mengetahui celah keamanan yang terdapat didalam sistem informasi repositori karya ilmiah Politeknik XYZ dari berbagai tingkatan kerentanan, sehingga dapat dilakukan perbaikan-perbaikan untuk meningkatkan keamanan sistem informasi itu sendiri.

2. TINJAUAN PUSTAKA

2.1. Penetration testing

Penetration testing (pentest) adalah kegiatan untuk mengevaluasi keamanan dari suatu sistem jaringan komputer. Dari evaluasi tersebut, akan ditemukan kelemahan-kelemahan dalam sistem keamanan suatu jaringan komputer yang bisa dimanfaatkan oleh penyerangnya. Untuk beberapa perusahaan, penetration testing ini merupakan hal yang penting, sebab kegiatan pentest ini bisa meminimalisir terjadinya hal-hal yang tidak diinginkan, salah satunya adalah hacking. Manfaat Penetration testing sebagai berikut:

- Menemukan celah keamanan suatu website
  Manfaat pertama dari penetration testing adalah menemukan celah keamanan suatu website. Seperti yang diketahui, suatu sistem jaringan komputer tidak selalu aman atau terhindar dari kejahatan siber.
- Mampu memperkirakan kerugian bisnis
  Selain untuk bermanfaat untuk sistem keamanan suatu perusahaan, penetration testing juga bermanfaat untuk memperkirakan kerugian bisnis yang akan dialami oleh perusahaan tersebut.

2.2. Vulnerrability assessment

Vulnerability Assessment adalah suatu proses untuk meningkatkan keamanan data penting Anda. Hal ini sangat penting untuk dilakukan demi meningkatkan keamanan data bisnis atau suatu perusahaan. Tujuan dari Vulnerability Assessment adalah untuk melakukan proses identifikasi, evaluasi, dan klasifikasi tingkat kerentanan pada sistem keamanan yang ada pada ekosistem informasi teknologi. Hasil dari identifikasi, evaluasi, dan klasifikasi melalui Vulnerability Assessment akan memberikan pandangan kepada suatu entitas yang mengadakan proses tersebut agar entitas tersebut tahu bahwa ada celah yang bisa disalah gunakan oleh pihak yang tidak bertanggung jawab terkait data penting entitas tersebut.

Vulnerability Assessment akan dilakukan dengan melakukan pemeriksaan secara terperinci dan sistematis pada infrastruktur komputasi suatu bisnis atau perusahaan untuk menentukan kelemahan atau celah yang mungkin bisa ditembus oleh pihak tidak bertanggung jawab dalam desai, implantasi atau prakteknya.

2.3. OWASP

OWASP adalah sebuah organisasi nirlaba yang fokus pada keamanan web app. OWASP banyak menyediakan sumber daya agar Anda bisa mempelajari lebih lanjut tentang keamanan web app. Sebagai salah satu prinsipnya, OWASP memastikan bahwa semua informasi dan materi pembelajarannya bisa diakses dengan mudah dan gratis sehingga semua orang bisa meningkatkan keamanan website mereka. Materi yang mereka sediakan berupa dokumentasi, tools, video, dan forum.

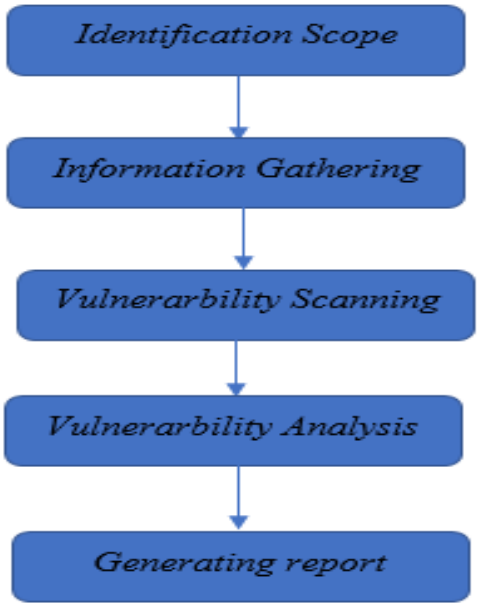
2.4. Owasp ZAP

Zed Attack Proxy (ZAP) adalah aplikasi untuk melakukan pentest untuk menemukan vulnerabilities dalam suatu web applications dengan cara mudah, ZAP menyediakan scanner automatis sebaik bila kita menggunakan tool untuk menemukan vulnerabilities secara manual. Ketika digunakan sebagai server

proxy, ini memungkinkan pengguna untuk memanipulasi semua lalu lintas yang melewatinya, termasuk lalu lintas menggunakan https, itu juga dapat berjalan dalam mode daemon yang kemudian dikontrol melalui REST API. ZAP telah ditambahkan ke dalam Radar Teknologi ThoughtWorks pada 30 Mei 2015 di cincin Percobaan. ZAP awalnya bercabang dari Paros, proxy pentesting lainnya. Simon Bennetts, pemimpin proyek, menyatakan pada tahun 2014 bahwa hanya 20% dari kode sumber ZAP masih dari Paros.

3. METODOLOGI PENELITIAN

Penelitian ini dilakukan dengan menggunakan metode *vulnerability assessment*, dimana penelitian ini berfokus pada tahapan *information gathering* dan *vulnerability scanning* untuk melakukan pengujian kerentanan menggunakan *tools vulnerability scanner*, 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 ilmiah 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 yang penulis gunakan untuk mengumpulkan informasi terkait sistem informasi repositori yang diuji untuk mengumpulkan informasi publik tentang nomor IP, nama domain, *hostname, autonomous system*, dan *route*.
3. Tahap ketiga merupakan tahapan digunakan untuk mencari kerentanan pada sistem informasi repositori karya ilmiah menggunakan Owasp ZAP untuk mencari celah keamanan pada aplikasi web yang di uji.
4. Tahap keempat 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.
5. 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.

4. HASIL DAN PEMBAHASAN

Di dalam pengujian kerentanan proses yang dilakukan untuk menemukan celah keamanan pada sistem informasi repositori karya ilmiah, terdapat beberapa tahapan meliputi *information gathering*, *vulnerability scanning*, *vulnerability analysis*, dan *generating report* menggunakan *tools* Owasp ZAP dalam menemukan celah di dalam sistem informasi, sehingga *vulnerability assessment* dilakukan dengan berdasarkan kerentanan yang terdapat pada tahap *vulnerability scanning*. Laporan kerentanan dari pengujian ini berdasarkan rekomendasi yang dilakukan oleh Owasp ZAP.

1. *Information Gathering*

Tahapan *information gathering* bertujuan untuk mengumpulkan berbagai informasi terkait sistem informasi repositori yang diuji untuk mengumpulkan informasi publik tentang nomor IP, nama domain, *hostname*, *autonomous system*, dan *route*. Didalam proses ini penulis menggunakan *tools* robtex.com. berikut hasil information gathering menggunakan robtex.com dan whois. Dari hasil information gathering terdapat beberapa temuan seperti *FQDN*, *Host Name*, *Domain Name*, *Registry*, *TLD*, *Name Server*, *IP Server*, *IP Number*

Setalah diketahui ip number dari domain sistem yang diuji langkah selanjutnya adalah melakukan *dns lookup* terhadap *ip number* yang telah diketahui. Dari domain yang dilakukan pengujian diketahui terdapat beberapa domain atau *hostname* pada level yang sama dibawah domain induk, domain tersebut adalah sebagai berikut.

2. Vulnerability Scanning

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

		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%)

Gambar 2. Hasil *scanning* OWASP ZAP menunjukan perhitungan peringatan berdasarkan risiko dan *confidence*

Dari gambar 1 diatas dapat dilihat terdapat total sebanyak 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*.

Risk			
High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
1 (1)	4 (5)	3 (8)	3 (11)
0 (0)	2 (2)	2 (4)	1 (5)
0 (0)	0 (0)	3 (3)	1 (4)
0 (0)	0 (0)	1 (1)	0 (1)
0 (0)	1 (1)	0 (1)	0 (1)

Gambar 3. Hasil *scanning* OWASP ZAP menunjukan peringatan berdasarkan situs dan risiko

Selain itu terdapat perhitungan peringatan berdasarkan situs dan risiko. Dimana saat melakukan pengujian penulis menggunakan *firefox headless* sebagai *ajax spider* dalam *vulnerability scanning* menggunakan OWASP ZAP.

3. *Vulnerability Analysis*

Setelah proses *scanning* menggunakan Owasp ZAP, tahapan selanjutnya adalah melakukan analisis untuk mencari jumlah peringatan dari setiap jenis peringatan, beserta tingkat risiko jenis peringatan tersebut. Tabel 3 merupakan perhitungan peringatan menurut jenisnya.

Tabel 3. Perhitungan peringatan berdasarkan jenis peringatan

No	Alert type
1	Hash Disclosure - Mac OSX salted SHA-1
2	Absence of Anti-CSRF Tokens
3	Application Error Disclosure
4	Content Security Policy (CSP) Header Not Set
5	Cross-Domain Misconfiguration
6	Hidden File Found
7	Missing Anti-clickjacking Header
8	Vulnerable JS Library
9	Big Redirect Detected (Potential Sensitive Information Leak)
10	Cookie Without Secure Flag
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

4. Generating Report

Tahap *generating report* yaitu melakukan dokumentasi terkait kerentanan dan hasil analisa kerentanan yang dilakukan, dan memberikan rekomendasi untuk memperbaiki kerentanan pada sistem informasi repositori karya ilmiah.

Alert Type	Deskripsi	Solusi
Hash Disclosure - Mac OSX salted SHA-1	Sebuah hash diungkapkan oleh web server	Pastikan hash yang digunakan untuk melindungi kredensial atau sumber daya lainnya tidak dibocorkan oleh server web atau database.
Content Security Policy (CSP) Header Not Set	Lapisan keamanan tambahan yang membantu mendeteksi dan memitigasi jenis serangan tertentu, termasuk *Cross Site Scripting (XSS)* dan serangan injeksi data. Serangan ini digunakan untuk segala hal mulai dari pencurian data hingga perusakan situs atau penyebaran *malware*.	Pastikan bahwa server web, server aplikasi, *load balancing.* Dikonfigurasi
Application Error Disclosure	Halaman ini berisi pesan kesalahan/peringatan yang mungkin mengungkapkan informasi sensitif seperti lokasi file yang menghasilkan pengecualian yang tidak tertangani. Informasi ini dapat digunakan untuk meluncurkan serangan lebih lanjut terhadap aplikasi web.	Tinjau kode sumber halaman ini. Terapkan halaman kesalahan khusus. Pertimbangkan untuk menerapkan mekanisme untuk memberikan referensi/pengidentifikasi kesalahan unik ke klien (*browser)* serta mencatat detail di sisi server dan tidak memaparkannya kepada pengguna.
Vulnerable JS Library	Jquery library yang teridentifikasi, versi 3.3.1 memiliki kerentanan.	Tingkatkan ke versi terbaru jquery.
Missing Anti-clickjacking Header	Respons tidak menyertakan *Content-Security-Policy* dengan arahan *'frame-ancestors*' atau *X-Frame-Options* untuk melindungi dari serangan '*ClickJacking*'.	Pastikan salah satu dari *HTTP Content-Security-Policy* dan *X-Frame-Options* di konfigurasi di semua halaman web yang dikembalikan oleh situs/aplikasi Anda
Cross-Domain Misconfiguration	Pemuatan data web browser dimungkinkan, karena kesalahan konfigurasi *Cross Origin Resource Sharing (CORS)* di server web	Pastikan bahwa data sensitif tidak tersedia dengan cara yang tidak diautentikasi Konfigurasikan *header HTTP "Access-Control-Allow-Origin"* ke kumpulan domain yang lebih ketat, atau hapus semua *header CORS* seluruhnya, untuk memungkinkan browser menerapkan Kebijakan yang Sama dengan cara yang lebih ketat.
Hidden file found	File sensitif dapat diakses atau tersedia. Hal ini dapat membocorkan informasi administratif, konfigurasi, atau kredensial yang dapat dimanfaatkan oleh individu jahat untuk menyerang sistem lebih lanjut atau melakukan upaya rekayasa sosial.	Pertimbangkan apakah komponen .hg benar-benar diperlukan dalam produksi atau tidak, jika tidak maka nonaktifkan.

Server Leaks Version Information via "Server" HTTP Response Header Field	Server web/aplikasi membocorkan informasi versi melalui *header respons HTTP "Server"*. Akses ke informasi tersebut dapat memfasilitasi penyerang mengidentifikasi kerentanan lain yang menjadi sasaran server web/aplikasi	Pastikan bahwa server web Anda, server aplikasi, dikonfigurasi untuk menyembunyikan informasi "Server" atau memberikan detail umum.
Strict-Transport-Security Header Not Set	Mekanisme kebijakan keamanan web di mana server web menyatakan bahwa agen pengguna yang mematuhi (seperti *web browser*) harus berinteraksi dengannya hanya menggunakan koneksi HTTPS yang aman (yaitu HTTP berlapis di atas TLS/SSL).	Pastikan bahwa server web, server aplikasi, *load balance.* Dikonfigurasi untuk menerapkan *Strict-Transport-Security.*
Cookie Without Secure Flag	*Cookie* telah disetel tanpa *secure flag*, yang berarti *cookie* dapat diakses melalui koneksi yang tidak terenkripsi.	Pastikan *cookie* disetel, dan *cookie* harus selalu diteruskan menggunakan saluran terenkripsi
Cross-Domain JavaScript Source File Inclusion	Laman menyertakan satu atau beberapa file skrip dari domain pihak ketiga.	Pastikan file sumber JavaScript dimuat hanya dari sumber terpercaya, dan sumber tidak dapat dikontrol oleh pengguna akhir aplikasi.
Information Disclosure - Debug Error Messages	Respons berisi pesan kesalahan umum yang dikembalikan oleh platform seperti ASP.NET, dan server Web seperti IIS dan Apache.	Nonaktifkan pesan *debug* sebelum aplikasi di publikasikan.

5. KESIMPULAN DAN SARAN

Hasil *vulnerability assessment* untuk mengetahui celah keamanan yang dilakukan pada sistem informasi repositori karya ilmiah pada tahap *information gathering* menemukan beberapa informasi diantaranya ip addrss, route, bgp, asname, lokasi, serta domain pada level yang sama dengan domain yang diuji. kemudian tahapan *vulnerability scanning* terdapat terdapat total sebanyak 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*. Pada tahap *vulnerability analysis* risiko dengan level high bertambah menjadi 2 dengan presentase 9,1 % dari keseluruhan risiko. Pada tahap akhir tahap pendokumentasian risiko dengan spesifikasi deskripsi kerentanan dan solusi yang dapat diterapkan untuk memperbaiki celah kerentanan pada sistem informasi karya ilmiah politeknik XYZ.

DAFTAR PUSTAKA

Riskiyadi, M., & Anggono, A. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Manajemen dan Organisasi*, *12*(3), 239-251.

Alwi, E. I., & Ilmawan, L. B. (2021). Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *INFORMAL: Informatics Journal*, *6*(3), 131-135.

Budiman, A., Ahdan, S., & Aziz, M. (2021). Analisis Celah Keamanan Aplikasi Web E-Learning Universitas Abc Dengan Vulnerability Assesment. *Jurnal Komputasi*, *9*(2).

Farismana, R., & Pramadhana, D. (2022). *Risk Management in Final Semester Exam Information System Using NIST 800-30 Method (Case Study of SMKN 2 Baleendah)*. *2*, 21–27.

Tania, A. M., Setiyadi, D., & Khasanah, F. N. (2018). Keamanan website menggunakan vulnerability assessment. *INFORMATICS FOR EDUCATORS AND PROFESSIONAL: Journal of Informatics*, *2*(2), 171-180.

Aziz, M. A. (2022). Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas XYZ. *Journal of Engineering, Computer Science and Information Technology (JECSIT)*, *2*(1).

Akmal, A. M., Heryana, N., & Solehudin, A. (2022). Analisis Keamanan Website Universitas Singaperbangsa Karawang Menggunakan Metode Vulnerability Assessment. *Jurnal Pendidikan dan Konseling (JPDK)*, *4*(4), 6298-6308.

Septiawan, G. A., Irawan, K. W. S., Mayasari, I., & Listartha, I. M. E. (2022). Analisis Kerentanan XSS dan Rate Limiting Pada Website SMAN 8 Denpasar Menggunakan Framework OWASP ZAP. *Jurnal Informatika Upgris*, *8*(1).

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno. Com*, *22*(2), 418-429.