ANALISA KERENTANAN WEBSITE FMIPA UNSRAT BERDASARKAN OPEN WEB APPLICATION SECURITY PROJECT TOP 10 FRAMEWORK

Christian Alderi Jeffta Soewoeh[1*], Edwin Tenda[2], Eliasta Ketaren[3], Wisard Widsli Kalengkongan[4], Mahardika Inra Takaendengan[5]

[1,2,3,4,5] *Program Studi* Sistem *Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sam Ratulangi*
JL. Kampus Unsrat Bahu, Kleak, Malalayang, Kota Manado, Sulawesi Utara 95115
**Email: christian.suwuh@unsrat.ac.id*

Abstract

One of the preventive steps to minimize the adverse effects of cyberattacks is to carry out a vulnerability assessment whose results can be analyzed according to the OWASP Top 10 framework. According to the 2021 BSSN cybersecurity monitoring results, cyberattacks in the higher education sector are increasing. Therefore, it is important for higher education institutions such as FMIPA UNSRAT to improve their cyber security and strengthen the protection of their vital information infrastructure. By following the recommendations given in this study, it is hoped that it can help FMIPA UNSRAT improve website security protection and prevent cyber attacks that can harm their important information.
Keyword: *Vulnerability, OWASP, Cybersecurity Attack*

Abstrak

Salah satu langkah preventif untuk meminimalisir dampak buruk serangan siber adalah dengan melakukan penilaian kerentanan yang hasilnya dapat dianalisa sesuai framework OWASP Top 10. Menurut hasil monitoring keamanan siber BSSN tahun 2021 menunjukkan bahwa serangan siber pada sektor pendidikan tinggi semakin meningkat. Oleh karena itu, penting bagi institusi pendidikan tinggi seperti FMIPA UNSRAT untuk meningkatkan keamanan siber mereka dan memperkuat perlindungan infrastruktur informasi vital mereka. Dengan mengikuti rekomendasi yang diberikan dalam penelitian ini, diharapkan dapat membantu FMIPA UNSRAT dalam meningkatkan perlindungan keamanan website dan mencegah serangan siber yang dapat membahayakan informasi penting mereka.
Kata Kunci: Vulnerability, OWASP, Serangan Keamanan Siber

1. Pendahuluan

Di era digital yang ditambah dengan situasi pandemi, kecakapan dalam pemanfaatan teknologi informasi pada segala bidang khususnya layanan pendidikan tinggi di Indonesia menjadi suatu keniscayaan. Oleh sebab itu pemerintah menggalakkan program Gerakan Nasional Literasi Digital yang bertujuan meningkatkan kemampuan publik dalam menguasai dan menggunakan teknologi digital. Adapun 4 Pilar dari Literasi Digital yaitu *Digital Culture*, *Digital Skills*, *Digital Ethics*, dan *Digital Safety*. Penyelenggara layanan pendidikan tinggi di Indonesia perlu memahami betapa pentingnya literasi digital khususnya digital safety karena sektor pendidikan menjadi sasaran empuk bagi serangan siber. Berdasarkan target serangan, Sektor akademik menempati urutan teratas dengan menyumbang 34% dari total 9749 sebaran kasus serangan siber jenis *web defacement* di Indonesia pada tahun 2020[1]. Posisi ini terus berlanjut dengan menyumbang 37% dari total 5940 serangan *web defacement* pada laporan di tahun 2021, walaupun secara jumlah kasus terjadi penurunan[2].

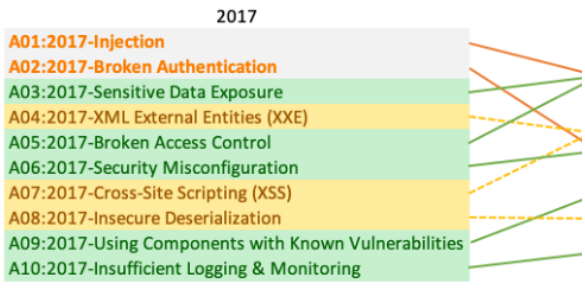
Laporan monitoring serangan Siber ini dapat kita hubungkan dengan pengukuran Indeks Literasi Digital di Indonesia pada tahun 2021 yang berada pada posisi sedang dengan skor indeks 3,49 (skala 1-5). Skor Pilar *Digital Skill* adalah *3,44*, Pilar *Digital Ethics 3,53*, Pilar *Digital Safety* 3,10, dan Pilar *Digital Culture* 3,90. Pilar *Digital Culture* merupakan pilar dengan skor tertinggi, sedangkan pilar Digital Safety adalah pilar paling rendah[3]. Lewat studi ini dapat kita lihat dan sadari bahwa masyarakat umum telah dapat beradaptasi dengan budaya digital namun jika membandingkan dengan tren serangan siber, maka literasi keamanan digital harus ditingkatkan.

Berdasarkan hasil monitoring dan studi literasi digital dari pemerintah ini, hal yang perlu diperhatikan oleh penyelenggara layanan pendidikan tinggi dalam hal keamanan digital adalah bagaimana menjaga infrastruktur informasi vital terhadap serangan siber seperti *web defacement* seperti amanat Perpres Nomor 82 Tahun 2022 tentang perlindungan Infrastruktur Informasi Vital (IIV). Perpres ini bertujuan untuk mengatur dan memperkuat kerangka hukum perlindungan IIV, termasuk peningkatan kesadaran dan kesiapan dalam menghadapi serangan siber. Melalui Perpres Nomor 82 Tahun 2022, diharapkan akan tercipta sistem perlindungan yang kuat dan efektif untuk melindungi infrastruktur informasi vital dari serangan

keamanan siber di Indonesia.

Berdasarkan tren serangan siber jenis *web defacement* terhadap sektor akademik atau perguruan tinggi, maka keamanan situs web perguruan tinggi sangat penting untuk dijaga karena serangan *web defacement* dapat mengubah tampilan situs web dan menunjukkan pesan yang tidak pantas atau merusak reputasi institusi pendidikan. Pentingnya keamanan situs web perguruan tinggi dapat diwujudkan dengan memperkuat sistem keamanan teknologi informasi, meningkatkan kesadaran dan pengetahuan tentang keamanan siber di kalangan staf institusi pendidikan, serta melakukan pembaruan dan pemantauan secara berkala terhadap sistem keamanan yang sudah ada. Ketidakmampuan institusi pendidikan untuk melindungi situs web mereka dari serangan peretasan dapat berdampak negatif pada reputasi institusi dan citra perguruan tinggi tersebut.

Salah satu kerangka kerja yang dapat diimplementasikan untuk mengukur keamanan situs web adalah *Open Web Application Security Project TOP 10.* OWASP Top 10 adalah dokumen standar dalam menganalisa keamanan aplikasi berbasis Web[4]. OWASP menyediakan seperangkat tools *open-source* seperti *owasp zap* yang dapat digunakan dalam membantu menilai adanya celah pada situs web. *Vulnerability Assessment* adalah proses mendefinisikan, mengidentifikasi, mengklasifikasikan, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan dan memberikan organisasi melakukan penilaian dengan pengetahuan, kesadaran, dan latar belakang risiko yang diperlukan untuk memahami ancaman terhadap lingkungannya dan bereaksi dengan tepat[5]. Hasil dari penilaian kerentanan ini dapat kita kaji lebih dalam berdasarkan dokumen OWASP Top 10 seperti yang pernah dilakukan pada penelitian sebelumnya[6] [7]seperti terdapat pada Gambar 1

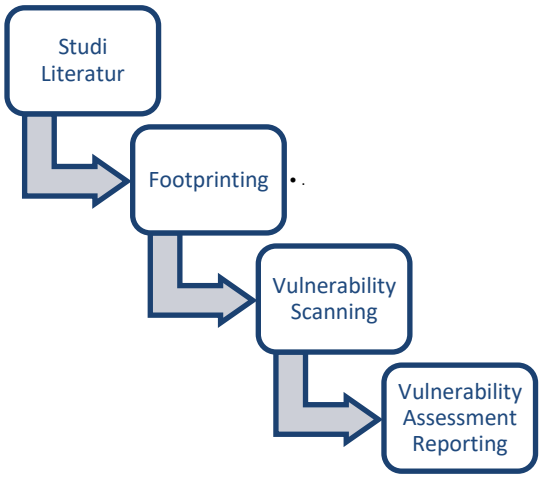


.

Gambar 1. *OWASP TOP 10 2021*

2. Metode Penelitian

Metode yang digunakan pada penelitian ini adalah *Vulnerability Assessment* untuk memindai celah keamanan dari situs web FMIPA Unsrat dengan menggunakan *tools vulnerability scanning owasp zap*. Tahapan penelitian seperti digambarkan pada Gambar 1.



Gambar 2. Tahapan Penelitian

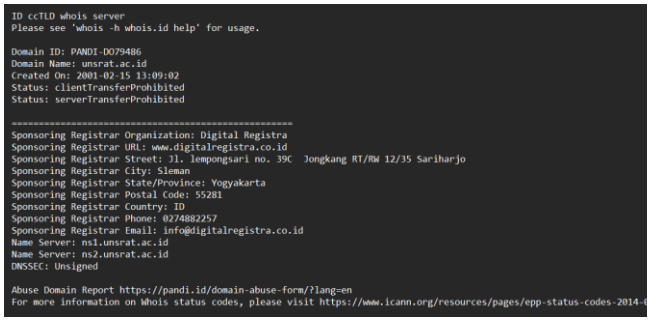
1. Studi Literatur dilakukan dengan melakukan penelusuran pada jurnal-jurnal ilmiah nasional dan referensi mengenai peraturan pemerintah dan kebijakan mengenai infrastuktur informasi vital.
2. *Footprinting* adalah Teknik pengumpulan informasi tentang target atau sasaran yang akan diserang. Cara ini dilakukan pada tahap awal dalam serangan siber, sebelum melakukan langkah-langkah selanjutnya seperti *scanning*. Tujuan dari pengumpulan informasi adalah untuk memperoleh informasi yang cukup tentang target, sehingga serangan siber dapat dilakukan dengan lebih efektif dan efisien. Beberapa cara yang dapat dilakukan seperti melakukan pencarian di mesin pencari, memperoleh informasi dari situs web publik, menggunakan alat pencari informasi seperti WHOIS , DNS lookup, Nmap. Hal ini juga ditemui pada penelitian yang lain[8]
3. *Vulnerability Scanning* adalah tahapan dilakukannya pemindaian kerentanan dengan mengggunakan *tools vulnerability scanning* seperti OWASP ZAP seperti pada penelitian terdahulu[9] [10] [11]. tujuan yang ingin dicapai yaitu mencari celah keamanan yang terdapat pada target mencakup beberapa seperti *SQL Injection, Cross Site Scripting* (XSS), *Personally Identifiable Informatin Disclosure, Path Transversal, Private IP Disclosure* pada suatu sistem operasi atau aplikasi.
4. *Vulnerability Assessment Reporting,* Pada tahap ini kita memberikan Analisa terkait hasil pemindaian kerentanan keamanan situs web dan memberikan rekomendasi perbaikan berdasarkan OWASP TOP 10, seperti yang pernah dilakukan peneliti sebelumnya[12].

Tabel 1. Tools pada Analisis Kerentanan

Tahapan	**Tools**
Footprinting	WhoIS, Zenmap
Vulnerability Scanning	OWASP ZAP
Vulnerability Assessment Reporting	OWASP TOP 10

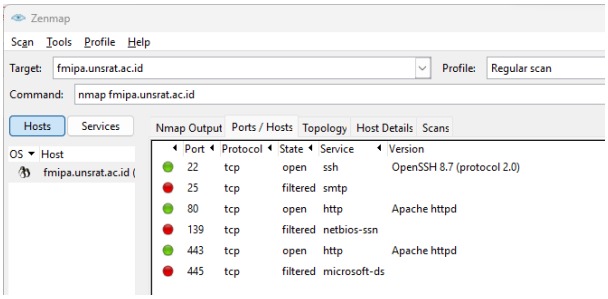
3. Hasil dan Pembahasan

3.1 Footprinting



Gambar 3. Hasil Footprinting dengan WhoIS

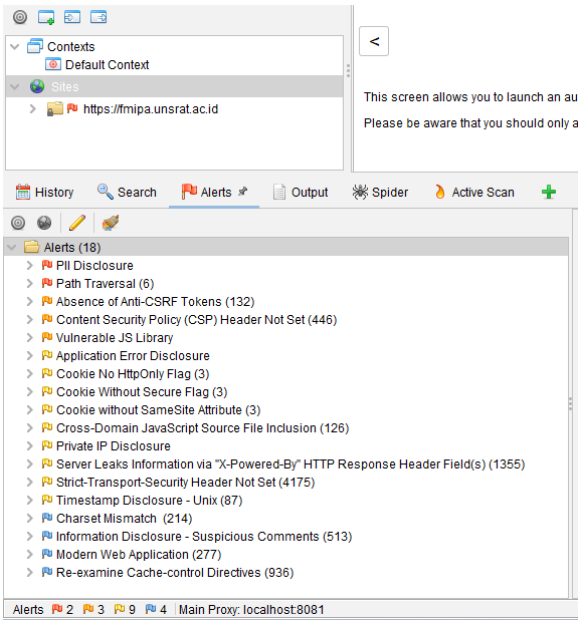
Pada Tahap *Footprinting* kita dapat mendapatkan informasi *mengenai Domain ID, Domain Name, Sponsoring Registrar Organization, Server Name* lewat tools *WhoIS* seperti Pada Gambar 2. Lewat tools *Zenmap* kita juga memperoleh informasi Port pada server beserta statusnya seperti pada Gambar 3



Gambar 4. Hasil *Footprinting* dengan *Zenmap*

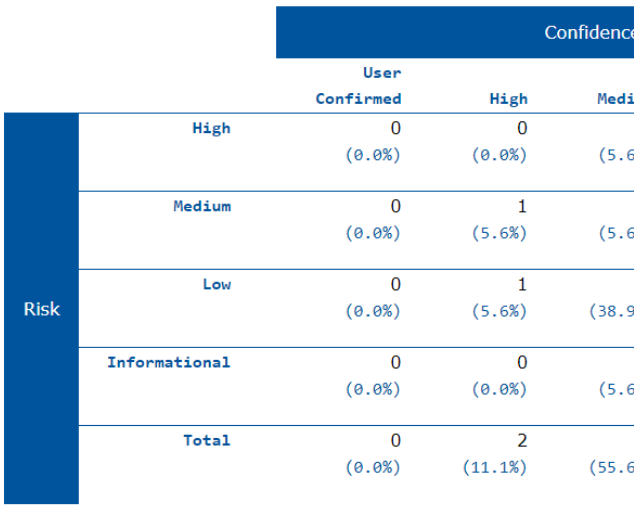
3.2 Vulnerability Scanning

Pada Tahap ini , kita melakukan pemindaian terhadap target website lewat tools OWASP ZAP untuk memperoleh informasi celah keamanan seperti pada Gambar 4.



Gambar 5. Hasil Vulnerability Scanning dengan OWASP ZAP

Dalam pemindaian ini terdapat 18 kerentanan dengan level *high* sampai *informational* sehingga *website* tergolong cukup berisiko. Pada keretanan dengan risk level *high* diperoleh nilai 11.1% yaitu *PII Disclosure* dan *Path Traversal*. Pada kerentanan dengan risk level *medium* diperoleh nilai 16,7% , yaitu *Absence of Anti-CSRF Tokens*,*Content Security Policy (CSP) Header Not Set , Vulnerable JS Library.* Pada kerentanan dengan risk level *low* diperoleh nilai 50%, yaitu *Application Error Disclosure, Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cookie without SameSite Attribute, Cross-Domain JavaScript Source File Inclusion, Private IP Disclosure, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s), Strict-Transport-Security Header Not Set, Timestamp Disclosure - Unix* . Sedangkan kerentanan dengan risk level *Informatonal* diperoleh nilai 22.2%, yaitu *Charset Mismatch, Information Disclosure - Suspicious Comments, Modern Web Application, Re-examine Cache-control Directives.* Hasil ringkasan dari pencarian celah keamanan dapat dilihat pada Gambar 6.



		Confidence		
		User Confirmed	High	Medi
Risk	High	0 (0.0%)	0 (0.0%)	(5.6
	Medium	0 (0.0%)	1 (5.6%)	(5.6
	Low	0 (0.0%)	1 (5.6%)	(38.9
	Informational	0 (0.0%)	0 (0.0%)	(5.6
	Total	0 (0.0%)	2 (11.1%)	(55.6

Gambar 6. Ringkasan Hasil Vulnerability Scanning

3.3 Vulnerability Assessment Reporting

Berdasarkan hasil pemindaian celah keamanan, maka selanjutnya kita lakukan analisa terhadap kerentanan keamanan website berdasarkan panduan OWASP TOP 10, khususnya pda risk level *high* dan *low*.

Tabel 1. Vulnerability Assessment dengan OWASP TOP 10

Risk Level	Alert	Alert Tags	Solution
High	PII Disclosure	**OWASP_2021_A04**	Check the response for the potential presence of "personally identifiable information" (PII), ensure nothing sensitive is leaked by the application.
High	Path Traversal	**OWASP_2021_A01**	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.
Medium	Absence of Anti-CSRF	**OWASP_2021_A01**	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the

			OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.
Medium	Content Security Policy (CSP) Header Not Set	**OWASP_2021_A05**	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Medium	Vulnerable JS Library	**OWASP_2021_A06**	Upgrade to the latest version of bootstrap
Low	Application Error Disclosure	**OWASP_2021_A05**	
Low	Cookie No HttpOnly Flag	**OWASP_2021_A05**	
Low	Cookie Without Secure Flag	**OWASP_2021_A05**	
Low	Cookie without SameSite Attribute	**OWASP_2021_A01**	
Low	Cross-Domain JavaScript Source File Inclusion	**OWASP_2021_A08**	
Low	Private IP Disclosure	**OWASP_2021_A01**	
Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	**OWASP_2021_A01**	
Low	Strict-Transport-Security Header Not Set	**OWASP_2021_A05**	
Low	Timestamp Disclosure - Unix	**OWASP_2021_A01**	
Informational	Charset Mismatch		
Informational	Information Disclosure - Suspicious Comments		
Informational	Modern Web Application		
Informational	Re-examine Cache-control Directives		

4. Kesimpulan dan Saran

Berdasarkan panduan OWASP TOP 10 terhadap hasil pemindaian kerentanan pada situs web FMIPA Unsrat, maka situs web yang diuji memiliki beberapa kerentanan keamanan yang perlu segera ditangani. OWASP TOP 10 adalah daftar 10 kerentanan keamanan web yang paling umum terjadi, oleh karena itu, menemukan kerentanan yang terdaftar di dalamnya menunjukkan bahwa sistem atau aplikasi yang diuji tidak sepenuhnya aman dan memerlukan tindakan untuk mengurangi risiko. Dalam hal ini, dua kerentanan dengan risk level yang tinggi harus ditangani secepat mungkin, diikuti dengan tiga kerentanan dengan risk level sedang. Diharapkan pada penelitian berikutnya aspek keamanan web mendapat perhatian yang cukup sejak pada tahap pengembangan sesuai pedoman OWASP Web Security Testing Framework.

Daftar Pustaka

[1] Badan Siber dan Sandi Negara, "Laporan Tahunan Monitoring Keamanan Siber 2020." Accessed: Jul. 31, 2022. [Online]. Available: https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW/download/LAPORAN%20HASIL%20MONITORING%20KEAMANAN%20SIBER%20TAHUN%202020.pdf

[2] Badan Siber dan Sandi Negara, "Laporan Tahunan Monitoring Keamanan Siber 2021." Accessed: Jul. 31, 2022. [Online]. Available: https://cloud.bssn.go.id/s/ZSdfebRTKW7p8nW/download/LAPORAN%20HASIL%20MONITORING%20KEAMANAN%20SIBER%20TAHUN%202020.pdf

[3] Kementerian Komunikasi dan Informatika RI, "Status Literasi Digital di Indonesia 2021." Accessed: Aug. 01, 2023. [Online]. Available: https://cdn1.katadata.co.id/media/microsites/litdik/Status_Literasi_Digital_diIndonesia%20_2021_190122.pdf

[4] OWASP Foundation, "OWASP TOP 10." https://owasp.org/www-project-top-ten/ (accessed Aug. 03, 2023).

[5] E. I. Alwi and L. B. Ilmawan, "Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment," *INFORMAL: Informatics Journal*, vol. 6, no. 3, pp. 131–135, 2021.

[6] A. Dharmawan, "PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 PADA DOMAIN XYZ. AC. ID," *Electro Luceat*, vol. 8, no. 1, pp. 100–108, 2022.

[7] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *Jurnal Algoritma*, vol. 18, no. 1, pp. 77–86, 2021.

[8] H. Herdianti and F. Umar, "Analisis keamanan website menggunakan teknik footprinting dan vulnerability scanning," *INFORMAL: Informatics Journal*, vol. 5, no. 2, pp. 43–48, 2020.

[9] G. Kusuma, "IMPLEMENTASI OWASP ZAP UNTUK PENGUJIAN KEAMANAN SISTEM INFORMASI AKADEMIK," *Jurnal Teknologi Informasi: Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika*, vol. 16, no. 2, pp. 178–186, 2022.

[10] K. Nisa, M. A. Putra, R. A. Siregar, and M. D. Irawan, "Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)," *Bulletin of Information Technology (BIT)*, vol. 3, no. 4, pp. 216–308, 2022.

[11] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *Jurnal Komtika (Komputasi dan Informatika)*, vol. 5, no. 1, pp. 35–42, 2021.

[12] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal of Computer Engineering, System and Science)*, vol. 6, no. 2, pp. 185–191, 2021.