CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 7, No. 1, Mei 2024,, hlm. 56-61

Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) Dan Information Systems Security Assessment Framework (ISSAF)

Saerozi Alfan Nugroho[1], Tri Rochmadi[2]

[1,2] Universitas Alma Ata
Email: 203100122@almaata.ac.id, trirochmadi@almaata.ac.id

Abstrak

Satudasawarsa terakhir indonesia telah memiliki pengguna internet sebanyak 174 juta, peningkatan sebesar 17% *internet usage* dalam kurun waktu satu tahun. Peningkatan juga dipengaruhi oleh tumbuhnya 25 juta komunitas *online* selama bulan januari 2020. Lonjakan pengguna internet ini menunjukkan kesiapan indonesia dalam mengadopsi praktik *E-government*. Diskominfo magelang yang merupakan sebuah layanan pemerintahan daerah telah membuat kemajuan dalam memanfaatkan teknologi informasi dan komunikasi. Teknologi yang dihasilkan adalah sebuah *web* sistem informasi bernama "Pusaka Magelang". Dalam memperkuat keamanan situs *web* pusaka magelang, maka diperlukan proses *security assesment*. Proses ini memerlukan sebuah *framework* OWASP dan ISSAF. Dengan menggunakan metode eksperimen, hasil pengujian menggunakan OWASP berhasil mengidentifikasi sebanyak 27 kerentanan dengan rincian 5 *severity high*, 5 *severity medium* 11 *severity low* dan 7 *informational*. Dari kerentanan yang ditemukan kemudian ditindak lanjuti dengan menilai tingkat risiko menggunakan OWASP *Risk Rating* diperoleh hasil skor *likelihood* sebesar 5,678 dan *impact* sebesar 5,9. Terakhir proses pengujian menggunakan kerangka ISSAF berhasil menemukan celah *sensitive data exposure* berupa *info.php()* yang bisa diakses secara publik sedangkan pengujian menggunakan teknik *SQL Injection* gagal dilakukan karena tidak berhasil mendapatkan *database* target.

Kata kunci: *Internet Usage, Vulnerability Assessment, E-government, Vulnerability Assesment, OWASP, ISSAF.*

Security Analysis Of Magelang Pusaka Information System Using Open Web Application Security Project (OWASP) And Information Systems Security Assessment Framework (ISSAF)

Abstract

In the last decade Indonesia has had 174 million internet users, a 17% increase in internet usage in one year. The increase was also influenced by the growth of 25 million online communities during January 2020. This surge in internet users shows Indonesia's readiness to adopt E-government practices. Diskominfo Magelang, which is a local government service, has made progress in utilizing information and communication technology. The resulting technology is a web information system called "Pusaka Magelang". In strengthening the security of the Pusaka Magelang website, a security assessment process is required. This process requires an OWASP and ISSAF framework. Using the experimental method, the test results using OWASP successfully identified 27 vulnerabilities with details of 5 high severity, 5 medium severity 11 low severity and 7 informational. From the vulnerabilities found, it was then followed up by assessing the level of risk using the OWASP Risk Rating, resulting in a likelihood score of 5.678 and an impact of 5.9. Finally, the testing process using the ISSAF framework succeeded in finding sensitive data exposure in the form of info.php() which can be accessed publicly while testing using SQL Injection techniques failed because it did not succeed in getting the target database...

***Keywords**: Internet Usage, Vulnerability Assessment, E-government, Vulnerability Assesment, OWASP, ISSAF.*

1. PENDAHULUAN

Indonesia merupakan negara yang tergolong sebagai negara berkembang satu dasawarsa ini telah menunjukkan peningkatan pesat dalam penggunaan internet (Effendy et al., 2020). Berdasarkan laporan digital yang dibuat oleh *We Are Social* (*Hootsuite)*, pengguna internet di indonesia pada awal januari 2020 sudah mencapai angka 174 juta pengguna (Hidayatulloh & Saptadiaji, 2021). Walaupun belum menyamai negara-negara maju hal tersebut telah dapat menggambarkan bahwa indonesia sudah siap untuk beralih menuju pada penerapan *e-government.* Implementasi *e-government* adalah suatu bentuk perubahan baru yang diharapkan dari sebuah negara yang berkembang(Effendy et al., 2020).

Berbicara layanan pemerintahan, Diskominfo Kabupaten Magelang telah mengimplementasikan

kemajuan TIK dengan membuat *website* khusus bernama pusaka magelang yang memiliki tujuan untuk menampilkan sumber informasi publik terhadap jalanya pembangunan wilayah magelang (Mubarokah & Hariyanti, 2023). Layanan pemerintahan daerah seperti *website* pusaka magelang ini harus memiliki standar keamanan sistem yang baik. Ketika ada serangan siber yang menyerang, sistem website tersebut masih bisa dapat diakses. Keamanan sangat penting bagi proses tata kelola teknologi informasi guna mengurangi celah ancaman pada berbagai aset yang sangat penting meliputi kerahasiaan, keutuhan dan ketersedianya (Syahindra et al., 2022).

Tujuan dilakukanya penelitian ini adalah untuk melakukan *assesment* keamanan *website*, mencari apa saja kerentanan yang memiliki potensi merusak sistem yang ada pada *website* tersebut dan menganalisa dampak apa saja yang dapat terjadi jika kerentanan tersebut benar-benar ada pada *website*. Proses penelitian yang dilakukan penulis menggunakan jenis penelitian eksperimental dengan melewati beberapa tahapan yang sudah ditentukan oleh penulis. Hasil analisa tersebut nantinya dapat membantu pengelola dan pengembang sistem untuk mencegah dan mengatasi dampak risiko yang di temukan pada sistem. *Assesment* kerentanan diharapkan berdampak bagi pengguna dengan memberi wawasan kerentanan apa saja yang telah ditemukan (Herman et al., 2023).

2. TINJAUAN PUSTAKA

Mengingat untuk meningkatkan keamanan *website* dari serangan diatas maka perlu diterapkan proses pengujian keamanan *(security assesment) website* pusaka magelang guna mengetahui tingkat kerentanan agar terhindar dari serangan yang tidak bertanggung jawab. Tahapan *Vulnerability Assesement* yang digunakan penulis untuk menganalisa kerentanan *website* pusaka magelang adalah dengan menggunakan 2 *framework* yaitu *framework* OWASP dan *framework* ISSAF.

Keamanan informasi juga suatu hal yang sangat penting bagi setiap individu atau organisasi, terutama dalam era serba digital saat ini dimana informasi sangat mudah untuk dicari maupun disalahgunakan (Elan Maulani et al., 2023). Keamanan informasi mengacu pada proses dan sebuah metode tentang bagaimana dalam melindungi informasi terkait data pribadi yang ada dari segala bentuk kejahatan siber (Rochmadi & Pasa, 2021). Maraknya penggunaan internet dikalangan masyarakat luas juga menjadi salah satu faktor bertambahnya peluang kejahatan siber (Thurfah Afifa Rosaliah & Hananto, 2021). BSSN juga merilis TOP 10 prediksi ancaman siber pada tahun 2023 diantaranya *Ransomware, Data Breach*, Serangan *APT, Phishing, Cryptojacking, DDOS*, Serangan *RDP, Social Engineering, Web Defacement, AI dan IoT Cybercrime* (Siber & Negara, 2023).

3. METODOLOGI PENELITIAN

Penelitian dilakukan dengan objek https://pusaka.magelangkab.go.id sebagai target pengujian. Penelitian menggunakan *Pre-Experiment Design* dengan *One Shot Case Study*, kerangka kerja yang digunakan mengikuti OWASP dan ISSAF kemudian dipadukan dengan beberapa *tools* pilihan yang sudah ditentukan dalam penelitian.

3.1. Analisis Kebutuhan

Untuk menunjang proses pengujian sistem yang dilakukan oleh peneliti, perangkat yang digunakan terdiri dari perangkat lunak (*software)* dan perangkat keras (*hardware*) dengan spesifikasi sebagai berikut :

Tabel 1. Analisis kebutuhan

No	Perangkat	Spesifikasi
1.	Laptop	HP 245 G8 Notebook PC, AMD Ryzen 3250U, RAM 8, SSD 256
2.	*Operating System*	*Windows 11 Home Single Language 64 bit dan Kali Linux*
3.	*Application Software*	*Virtual Box Oracle version 7.0.12*

3.2. Metode OWASP

Tahapan dalam metode OWASP terdiri dari *information gathering, network mapping, exploit* dan *reporting* (Mu'min et al., 2022). *Tools netcraft* digunakan pada tahap *information gathering, network mapping* menggunakan *Nmap*, tahap *exploit* menggunakan OWASP ZAP dan terakhir proses *reporting* menggunakan OWASP TOP 10.

Tabel 2. Tahap OWASP

No	Tahap	*Tools*
1.	*Information gathering*	*Netcraft*
2.	*Network mapping*	*Nmap*
3.	*Exploit*	*OWASP ZAP*
4.	*Reporting*	*OWASP TOP 10*

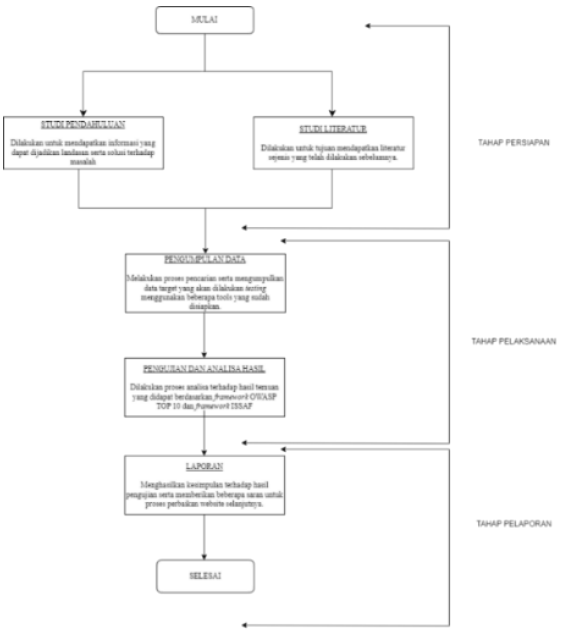
3.3. Metode ISSAF

Fase pendekatan dengan metode ISSAF terdiri dari *planning and preparation*, *Assesment*, dan *Clean Up Destroy and Artifact* (Costaner & Musfawati, 2020). *Planning and preparation* dalam tahap pengujian menggunakan *whois* dan *Nmap*. Selanjutnya pada tahap *Assesment* proses ini terdiri dari *vulnerability identification* dengan *tools nikto*, sedangkan untuk *penetration testing* menggunakan *tools SQLMap* dan *dirsearch*.

Tabel 3. Tahap ISSAF

No	Tahap	*Tools*
1.	*Planning and preparation*	*Whois, Nmap*
2.	*Assesment*	*Nikto, SQLMap, Dirsearch*
3.	*Clean Up and Destroy Artifact*	*Nikto*

2.1 Alur peneltian



Gambar 2. Alur penelitian

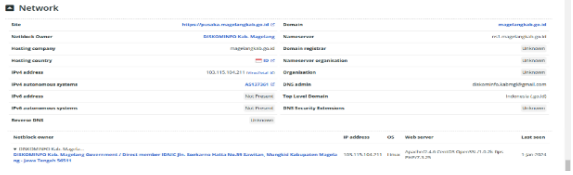
Alur penelitian yang dilakukan penulis dibagi menjadi tiga tahap. Pertama tahap persiapan dengan melakukan studi pendahuluan mencari informasi target di lingkungan Diskominfo Magelang sekaligus untuk melakukan proses perijinan. Kedua tahap pelaksanaan, setelah data di dapatkan dalam hal ini *domain website* target, tahap ini mulai melakukan observasi terhadap *website* yang akan diuji dengan menggunakan *methode* dan *tools* yang telah disiapkan. Tahap pelaporan, laporan kemudian dianalisa secara komprehensif dan sistematis menggunakan metode OWASP dan ISSAF untuk dilaporkan hasil temuanya kepada pihak Diskominfo agar dilakukan upaya perbaikan sistem.

4. HASIL DAN PEMBAHASAN

4.1. Pencarian Celah Keamanan dengan OWASP

4.1.1. Information gathering

Pada tahap *information gathering* dilakukan pencarian informasi terkait *website* yang diteliti, berikut adalah hasil pencarian menggunakan *Netcraft* terlihat pada Gambar 2.



Gambar 1. Hasil *Netcraft*

Hasil *Netcraft website* Pusaka Magelang disajikan pada Tabel 4.

Tabel 4. Temuan *information gathering*

No	Jenis Temuan	Deskripsi
1.	*Domain*	Magelangkab.go.id
2.	*Name server*	Ns1.magelangkab.go.id
3.	*Domain register*	*Unknown*
4.	*Alamat IP*	103.115.104.211
5.	*Sistem Operasi*	*Linux CentOS*
6.	*Web Server*	*Apache version 2.4.6*
7.	*PHP*	*PHP version 7.3.25*

4.1.2. Network mapping

14. Tahap ini dilakukan *port scanning* untuk mengetahui detail *port* apa saja yang terbuka. Berikut hasil *scanning port* terhadap *website* Pusaka Magelang disajikan dalam Tabel 5.

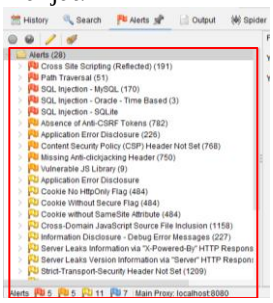
Tabel 5. Informasi detail *Port* dan *Service* yang terbuka

Port	*State*	*Service*	*Version*
21/tcp	*open*	*ftp*	*ProFTPD or KnFTPD*
22/tcp	*open*	*ssh*	*OpenSSH 7.4 (protocol 2.0)*
80/tcp	*open*	*http*	*Apache httpd 2.4.6*
443/tcp	*open*	*ssl/http*	*Apache httpd 2.4.6 (CentOS), OpenSSL 1.0.2k-fps, PHP/7.3.25*
1723/tcp	*open*	*pptp*	*Mikrotik (Firmware:1)*
2000/tcp	*open*	*Bandwith-test*	*Mikrotik bandwith-test server*

Berdasarkan Tabel 5, dapat dilihat hasil pemindaian menggunakan *nmap* didapatkan hasil mengenai *port-port* yang terbuka, yaitu *port* 21, 22, 80, 443, 1723 dan 2000.

4.1.3. Exploit

OWASP ZAP digunakan dalam tahap ini untuk menemukan kerentanan pada sistem. Hasil *scanning* yang berhasil teridentifikasi kemudian di kategorikan sesuai OWASP TOP 10. Dari daftar kerentanan tersebut selanjutnya dilakukan penilaian risiko menggunakan OWASP *Risk Rating* untuk mengukur seberapa besar dampak terhadap *website* jika terkena serangan lebih lanjut.



Gambar 3. Hasil scanning *website*

Gambar 3. merupakan hasil dari proses pemindaian terhadap *website* pusaka.magelangkab.go.id. pemindaian tersebut menghasilkan kerentanan sebanyak 27 yang berhasil teridentifikasi. Dengan rincian 5 *severity high*, 5 *medium*, 11 *low* dan 7 *informational*. Kategori *severity high* dan *medium*

yang akan dijadikan fokus pengkategorian sekaligus *reporting* menggunakan OWASP TOP 10.

Tabel 6. Pengkategorian kerentanan terhadap OWASP TOP 10

No	*Kerentanan*	Kategori OWASP
1.	*Path Traversal*	OWASP_A01_2021
2.	*Absence of Anti-CSRF Tokens*	
3.	*Cross Site Scripting (Reflected)*	OWASP_A03_2021
4.	*SQL Injection – MySQL*	
5.	*SQL Injection-Oracle-Time Based*	
6.	*SQL Injection-SQLite*	
7.	*Application Error Disclosure*	OWASP_A05_2021
8.	*Missing Anti-clickjacking Header*	
9.	*Content Security Policy (CSP) Header Not Set*	
10.	*Vulnerable JS Library*	OWASP_A06_2021

Tabel 6 berisi daftar kerentanan yang sudah dikategorikan berdasarkan OWASP TOP 10, selanjutnya kerentanan tersebut dinilai menggunakan metode OWASP *Risk Rating*. *OWASP Risk Rating* memiliki 4 tahapan dalam menentukan *likelihood* dan *impact*. Tahapan tersebut yaitu *threat agent factor, vulnerability factors, technical impact dan business impact* (Aryanti et al., 2021).

$$Likelihood = \frac{Threat\ Agent\ Factor + Vulnerability\ Factors}{2}$$

$$Impact = \frac{Technical\ Impact + Business\ Impact}{2} \quad (1)$$

Rumus (1) adalah rumus untuk menghitung skor keseluruhan l*ikelihood* dan *impact*. Hasil skor yang telah diasumsikan berdasarkan dengan ketentuan OWASP *Risk Rating* dihitung untuk menemukan nilai dari *threat agent factor, vulnerability factors, technical impact, dan business impact.* Dari penilaian tersebut didapatkan skor secara keseluruhan *likelihood* dan *impact* yang dihasilkan dari sistem informasi Pusaka Magelang adalah 5,6875 dan 5,9. Skor 5.6875 untuk *likelihood*, skor 5,9 untuk *impact*. Untuk *risk* atau risiko keduanya termasuk *medium* yang artinya dampak yang diberikan oleh *website* tersebut rendah. Skor keseluruhan dapat dilihat pada Tabel 7.

Tabel 7. Skor keseluruhan faktor

	Faktor 1	**Faktor 2**	**Faktor 3**	**Faktor 4**	**Total**	***Risk***
Threat Agent Factors	9	2,9	7	9	27,9	*5,6875*
Vulnerability Factors	9	3	4,6	1	17,6	
Technical Impact	4,6	2	1	9	16,6	5,9
Business Impact	1	1	2	3	7	

4.1.4. Reporting

Tabel 8. *Reporting* dengan OWASP TOP 2021

Risk level	*Alert*	*Alert tags*	*Solution*
High	*Cross Site Scripting*	*OWASP 2021 A03*	*Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid*
High	*Path Traversal*	*OWASP 2021 A01*	*Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications.*
High	*SQLInjection MySQL*	*OWASP 2021 A03*	*Do not trust client side input, even if there is client side validation in place*
High	*SQL Injection Oracle Time Based*	*OWASP 2021 A03*	*Do not trust client side input, even if there is client side validation in place*
High	*SQLInjection SQLLite*	*OWASP 2021 A03*	*Do not trust client side input, even if there is client side validation in place*
Medium	*Absence of Anti CSRF Tokens*	*OWASP 2021 A01*	*Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid*
Medium	*Application Error Disclosure*	*OWASP 2021 A05*	*Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user*
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	*Missing Anti-clickjacking Header*	*OWASP 2021 A05*	*Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web*

Risk level	*Alert*	*Alert tags*	*Solution*
			pages returned by your site/app.
Medium	*Vulnerability JS Library*	*OWASP 2021 A06*	*Please upgrade to the latest version of bootstrap*

4.2. Pengujian Celah Keamanan dengan ISSAF

4.2.1. Planning and preparation

Fase ini merupakan tahap awal untuk mulai mengumpulkan informasi dari target yang akan dilakukan *penetration testing*. Fase ini terdiri dari *information gathering* dan *network mapping*.

1. *Information gathering*

Tabel 9. Hasil *information gathering (whois)*

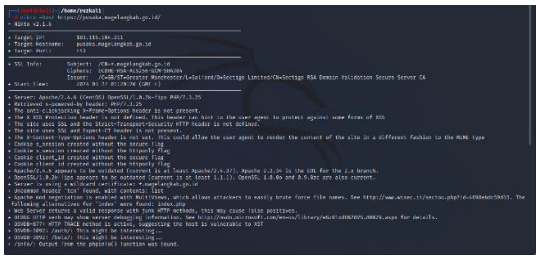
No	Jenis temuan	Deskripsi
1	*Domain ID*	PANDI – D0199241
2	*Domain Name*	magelangkab.go.id
3	*Created On*	2006-01-16 13:35:16
4	*Expiration Date*	2025-02-01 23:59:59
5	*IP Address*	103.115.104.207
6	*IP Location*	Jawa Tengah-Magelang-Diskominfo Kab. Magelang
7	*Name Servers*	NS1.MAGELANGKAB.GO.ID NS2.MAGELANGKAB.GO.ID
8	*Registrar Organization*	Kementerian Komunikasi dan Informatika
9	*Registrar Street*	JL. Medan Merdeka Barat No. 9
10	*Registrar City*	Jakarta Pusat
11	*Registrar State/Province*	Jakarta
12	*Registrar Postal Code*	10110
13	*Registrar Country*	ID
14	*Registrar Phone*	622138433507
15	*Registrar Email*	hostmaster@pandi.id
16	*Admin ID*	-
17	*Admin Name*	-

2. *Network Mapping*

Pemetaan jaringan menggunakan *nmap* mendapatkan *port* TCP yang terbuka sebanyak 6, diantaranya *port* 21, 22, 80, 443, 1723, dan 2000. Sedangkan *port* UDP yang terbuka ditemukan sebanyak 3 diantaranya *por*t 53, 161, dan 1701.

4.2.2. Assesment

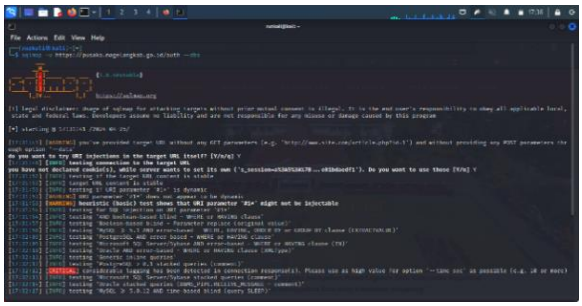
1. Vulnerability identification



Gambar 4. Hasil *vulnerbility identificatio*n menggunakan *nikto*

Berdasarkan Gambar 4, hasil *vulnerability identification* dengan *nikto* diketahui terdapat informasi kerentanan seperti tidak adanya *anti clickjacking* yang terpasang, *XSS Protection header* tidak ada, *Strict Transport Security HTTP Header* yang tidak ditemukan, *Expect CT header* yang tidak ada. Selain itu ditemukan informasi yang lain diantaranya versi *web server Apache* yang telah usang dan *OpenSSL* yang ketinggalan zaman.

2. *Penetration testing*



Gambar 5. Hasil Melakukan Pengujian *SQLMap*

Gambar 5 menunjukkan bahwa hasil pengujian SQLInjection untuk mendapatkan database target dengan tools sqlmap tidak berhasil dilakukan karena semua parameter yang diuji tidak dapat disuntikkan.

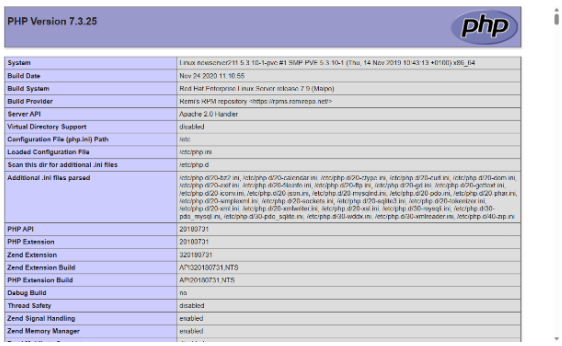
Tabel 10. Hasil *Penetration Testing tools Dirsearch*

3. Status *code*	4. *path*
5. 200	6. */info*
7. 200	8. */info.php*

Setelah dilakukan uji coba pada *status code* 200 yang ditemukan, penguji menemukan file data yang dapat diakses secara *public* tanpa perlu memasuki *website* target. *Path URL* tersebut adalah */info* dan */info.php*, *path* tersebut memberikan informasi sensitif berisi detail konfigurasi *web server* yang digunakan pada *website* pusaka.magelangkab.go.id.

4.2.3. Clean Up and Destroy Artifact

1. *Reporting*



Gambar 6. Tampilan *info.php()*

Reporting kerentanan menghasilkan bahwa pengujian *SQLInjection* tidak berhasil dilakukan. Sedangkan untuk pengujian *sensitive data exposure* berhasil ditemukan *path* dari *info.php()*, *path* tersebut

memuat informasi konfigurasi *web server* yang digunakan oleh *website* Pusaka Magelang. *Reporting* yang dibuat disertakan juga saran perbaikan sebagai petunjuk agar sistem dapat diperbaiki segera.

2. *Clean Up and Destroy Artifact*

Informasi yang didapatkan dari hasil proses pengujian harus dipastikan benar-benar terhapus dalam sistem penguji.

5. KESIMPULAN DAN SARAN

Hasil dari proses penelitian (*security assesment*) menggunakan *framework* OWASP dan ISSAF dapat disimpulkan bahwa dengan metode OWASP diperoleh kerentanan sebanyak 27 *vulnerabilities* dengan rincian 5 *severity high*, 5 *medium*, 11 *low* dan 7 *informational*. Dari kerentaan tersebut kemudian dilakukan analisa menggunakan OWASP *Risk Rating* dan menghasilkan nilai skor *likelihood* 5,6875 lalu untuk skor *impact* mendapatkan nilai 5,9. Pengujian menggunakan kerangka ISSAF dengan teknik *SQLInjection* tidak berhasil dilakukan, sedangkan teknik *sensitive data exposure* diperoleh informasi data sensitif berupa informasi detail mengenai web server target dalam hal ini yaitu *info.php()* yang dapat diakses secara publik. Kedua metode tersebut bekerja dengan sangat baik dan efektif dalam mencari kerentanan suatu *website*.

Berdasarkan kesimpulan ada beberapa saran untuk *website* Pusaka Magelang yang perlu dilakukan perbaikan ataupun diterapkan untuk memperbaiki keamanan agar lebih *secure* terhadap serangan *attacker*. Pertama mulai untuk memperbaharui web server *(Apache 2.4.6)* dan *OpenSSL 1.0.2.2k-fips* ke dalam versi yang terbaru. Selanjutnya perlu adanya tindakan untuk mengkonfigurasi, mengatur *php.info()* agar tidak lagi dapat dilihat secara *public*, informasi tersebut harus tersembunyi dengan benar agar penyerang tidak dapat memiliki celah dalam memperhitungkan serangan.

DAFTAR PUSTAKA

Aryanti, D., Dan, N., & Utamajaya, J. N. (2021). ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA. *Jurnal Nasional Indonesia*, *1*(3), 15–25.

Costaner, L., & Musfawati, D. (2020). ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING). *JIPI (Jurnal Ilmiah Penelitian Dan Pemebelajaran Informatika)*, 45–55.

Effendy, T., Jurusan, W., Informatika, M., Sains, F., Teknologi, D., Sunan, U., & Yogyakarta, K. (2020). *EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA KANTOR WILAYAH KEMENTERIAN HUKUM DAN HAM DIY*. *3*(1), 1–6.

Elan Maulani, I., Herdianto, T., Febri Syawaludin, D., & Oga Laksana, M. (2023). Dwi Febri Syawaludin. *Medika Oga Laksana Jurnal Sosial Dan Teknologi (SOSTECH)*, *3*(2), 99–102.

Herman, Riadi, I., Kurniawan, Y., & Ainur Rafiq, I. (2023). Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (ISSAF). *Analisis Keamanan Website Menggunakan Information System Security Asessment Framework (ISSAF)*, *9*(1), 126–136. https://doi.org/10.37012/jtik.v9i1.1439

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma*, 77–86. http://jurnal.itg.ac.id/

Mubarokah, F., & Hariyanti, P. (2023). *Cyber Pr Pemerintah Kabupaten Magelang Dalam Implementasi Kebijakan Satu Data Indonesia*.

Mu'min, Muh. A., Fadlil, A., & Riadi, I. (2022). Analisis Keamanan Sistem Informasi Akademik Menggunakan Open Web Application Security Project Framework. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *6*(3), 1468. https://doi.org/10.30865/mib.v6i3.4099

Rochmadi, T., & Pasa, I. Y. (2021). Measurement of Risk and Evaluation of Information Security Using The Information Security Index in BKD XYZ Based on ISO 27001/SNI. *CyberSecurity Dan Forensik DIgital*, *4*(1), 38–43. https://doi.org/10.14421/csecurity.2021.4.1.2439

Siber, B., & Negara, D. S. (2023). *ANNUAL REPORT BADAN SIBER DAN SANDI NEGARA*.

Syahindra, I. P. S., Primasari, C. H., & Irianto, A. B. P. (2022). EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011. *EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011*, *16*(2), 165–182.

Thurfah Afifa Rosaliah, Y., & Hananto, B. (2021). Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx. *Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA) Jakarta-Indonesia*.