Analisis Metode *Open Web Application Security Project* (OWASP) pada Pengujian Keamanan Website: *Literature Review*

Aditya Wibisono Kuncoro
Jurusan Informatika
Fakultas Teknologi Industri, Universitas Islam Indonesia
Yogyakarta, Indonesia
18523217@students.uii.ac.id

Fayruz Rahma, S.T, M.ENG.
Jurusan Informatika
Fakultas Teknologi Industri, Universitas Islam Indonesia
Yogyakarta, Indonesia
fayruz.rahma@uii.ac.id

Abstrak—Keamanan sistem komputer semakin diperlukan dengan meningkatnya pengguna koneksi Internet. Dalam hal ini dapat memicu terjadinya tindak kejahatan pada sistem komputer. Diperlukan pengujian keamanan sistem untuk menemukan celah keamanan dalam mengantisipasi terjadinya tindak kejahatan pada sistem komputer. Makalah ini mengkaji literatur terkait dengan pengujian keamanan sistem komputer menggunakan metode *Open Web Application Security Project* (*OWASP*). Metode *Scoping Review* digunakan dalam seleksi literatur dalam makalah ini, kemudian literatur dipetakan dalam beberapa elemen dan didapatkan 6 literatur yang sesuai. Tujuan dari makalah ini adalah menganalisis penggunaan *framework* OWASP dalam pengujian keamanan sistem komputer. Secara keseluruhan dalam implementasi *framework* telah memberikan hasil yang maksimal dalam pengujian keamanan sistem untuk menemukan celah keamanan, namun beberapa faktor perlu dipertimbangkan dalam proses pengujian keamanan sistem agar hasil pengujian lebih maksimal.

Kata Kunci—Keamanan Sistem, Pengujian Keamanan, OWASP, Celah Keamanan.

I. PENDAHULUAN

Open Web Application Security Project (*OWASP*) merupakan organisasi non profit berfokus pada peningkatan keamanan perangkat lunak [1]. OWASP menjadi *framework* yang digunakan oleh pengembang dan ahli teknologi untuk mengamankan website. *OWASP* memberikan platform bagi pengembang untuk meningkatkan keamanan sistem melalui proyek yang *open-source* bersama dengan *tools* dari *OWASP* sebagai pendukung dalam pengujian sistem.

Web Security Testing Guide (*WSTG*) sebagai panduan kerangka kerja yang dirilis oleh *OWASP* berisikan tahapan-tahapan yang perlu dilakukan dalam melakukan analisis keamanan pada sistem berbasis web [2]. *WSTG* digunakan sebagai panduan komprehensif dalam pengujian keamanan aplikasi dan layanan website. *WSTG* memiliki berbagai macam versi yang selalu diperbarui setiap tahunnya, sampai saat ini versi yang terbaru adalah *WSTG* v4.2.

Keamanan pada sistem komputer digunakan untuk memastikan bahwa sistem tidak memiliki celah, kerentanan dan memberikan akses kepada pihak yang tidak berwenang. *Penetration testing* adalah kegiatan menilai keamanan sistem komputer dengan mensimulasikan serangan dari sumber yang tidak diketahui dan berbahaya serta merupakan aktivitas pengujian keamanan. Mensimulasikan serangan yang dibuat seperti *peretasan*, *jailbreaking*, dan lain-lain. Tujuannya adalah mengidentifikasi serta mengetahui jenis-jenis serangan yang dapat terjadi akibat kerentanan dan kelemahan pada sistem [3].

Penelitian terkait penggunaan metode *OWASP* dalam pengujian keamanan sistem telah banyak dilakukan, beberapa pengujian menyebutkan bahwa metode dan alat sangat berpengaruh terhadap langkah dan hasil dari pengujian keamanan sistem. Objek pengujiannya beragam, alat dan metode nya pun beragam. Setiap metode dan alat yang digunakan memiliki perbedaan, mulai dari tahapannya hingga hasil baik analisis maupun rekomendasinya.

Maka dari itu penulis tertarik untuk melakukan analisis dan riset terhadap penggunaan metode *OWASP* dalam pengujian keamanan sistem. Apa saja fokus dari penelitian yang dilakukan terkait dengan keamanan sistem. Dengan adanya penelitian ini, maka dapat memberi gambaran mengenai pengujian keamanan sistem. Literatur ini dapat digunakan sebagai pertimbangan pengujian keamanan sistem khususnya website menggunakan metode *OWASP* seperti yang telah dilakukan penelitian-penelitian sebelumnya. Tujuan dari penelitian ini adalah menjawab pertanyaan yang terkait dengan penelitian untuk membantu dalam memahami metode yang dapat digunakan dalam pengujian keamanan sistem.

II. METODE

Penelitian ini menggunakan pendekatan *Scoping Review* dengan langkah-langkah utamanya, yaitu identifikasi masalah, identifikasi sumber, pemilihan literatur, pemetaan, pengumpulan literatur, kompilasi dan memberikan hasil serta konsultasi kepada pihak kompeten. Dalam langkah memilih literatur, penulis menerapkan pendekatan *PRISMA* (*Preferred Reporting Item for Systematic Review and Meta-Analysis*) dalam melakukan *literature review*.

A. Pertanyaan Penelitian

Pertanyaan yang terkait dengan penelitian sebagai acuan dalam pencarian sumber literatur dan artikel, bentuk pertanyaan dari penelitian adalah seperti berikut:

- RQ1: Jenis penelitian dan metode apa yang digunakan?
- RQ2: Apa fokus penelitian terkait keamanan sistem informasi?

B. Tahapan Analisis

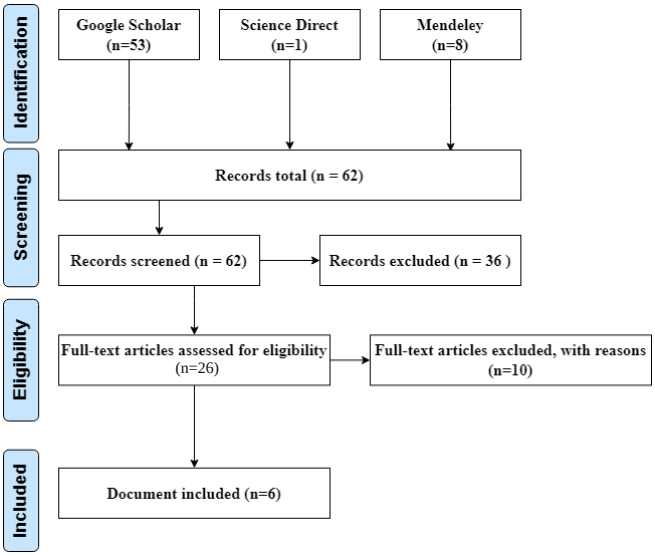
1) Identifikasi Sumber Literatur

Pada tahap ini, peneliti mengidentifikasi sumber-sumber literatur yang relevan dengan menggunakan *database*

penelitian. Penelitian menghasilkan 62 temuan literatur yang relevan dengan topik pengujian keamanan sistem informasi berbasis website.

2) Seleksi Literatur

Pada tahapan ini, dilakukan seleksi terkait literatur dan artikel mengenai keamanan sistem komputer dari *database* penelitian. Pembacaan abstrak dan kesimpulan dari literatur untuk proses seleksi. Kemudian, literatur dianalisis menurut faktor-faktor seperti objek penelitian, metode yang digunakan, dan alat/*tools* yang diimplementasikan dalam penelitian terkait. Dari temuan 62 literatur, 36 diantara nya terdapat perbedaan dalam penggunaan metode sehingga tidak lolos dalam proses *screening*. Kemudian, dari 26 literatur, 10 diantara nya termasuk *full-text articles*. Sehingga terdapat 6 literatur yang memiliki informasi cukup terkait pengujian keamanan sistem informasi berbasis website.



Gambar 1. *Flow Diagram* Pemilihan Artikel Penelitian

3) Pemetaan Literatur yang Digunakan

Pada tahap ini, peneliti menganalisis dan mengumpulkan literatur yang relevan dengan objek penelitian, khususnya masalah keamanan sistem informasi berbasis website. Dari hasil analisis dan pengumpulan literatur, penulis melakukan pengelompokan kemudian disajikan kedalam bentuk tabel matriks.

4) Melaporkan Hasil Analisis Literatur

Pada tahap ini, bentuk tabel matriks pada langkah pemetaan akan dilakukan analisis kembali kemudian merangkum dan menyusun hasil analisis serta membuat laporan hasil analisis berdasarkan literatur terkait, dan kemudian melakukan diskusi dengan pihak yang berkompeten.

5) Konsultasi Dengan Ahli

Konsultasi dengan ahli adalah langkah terakhir dari proses *scoping review*. Tahap ini, konsultasi dengan ahli yang memiliki kompetensi di bidang keamanan sistem yang dilakukan untuk merekomendasikan dan memberi masukkan dari pendekatan *scoping review* berdasarkan hasil analisis yang telah penulis lakukan.

C. Strategi Pemilihan Literatur

Basis data yang digunakan dalam studi literatur adalah *Google Scholar* (*https://scholar.google.com*), *Science Direct (https://www.sciencedirect.com)*, *Mendeley (https://www.mendely.com)*. Kata kunci yang penulis gunakan dalam mencari literatur pada portal *Google Scholar* adalah "Keamanan Sistem Informasi", "OWASP", dan "*Penetration Testing*". Tujuan dari pencarian kata kunci *Penetration Testing* adalah untuk menyaring literatur yang berkaitan dengan pengujian sistem kemudian meninjau literatur yang terkait. Sedangkan, pencarian pada portal *Science Direct* dan *Mendeley*, menggunakan kata kunci "*Penetration Testing Website"*, "*Website-based Information System Security"*, dan *"Web Vulnerability Assesment"*.

TABEL 1. STRATEGI PEMILIHAN LITERATUR

Kata kunci	Kombinasi kata kunci pada portal *Science Direct*	Kombinasi kata kunci pada portal *Mendeley*
Penetration Testing Website	*Penetration Testing Website* AND *OWASP*	*Penetration Testing Website* AND *OWASP*
Website-based Information System Security	*Website-based Information System Security* AND *OWASP*	*Website-based Information System Security* AND *OWASP*
Web Vulnerability Assesment	*Web Vulnerability Assesment* AND *OWASP*	*Web Vulnerability Assesment* AND *OWASP*

Referensi literatur yang terkumpul dari proses pencarian akan mengalami beberapa penyaringan. Penyaringan pertama, dilakukan dengan menilai relevansi literatur berdasarkan judul dan mengliminasi literatur yang tidak bersesuaian. Penyaringan kedua, mengeliminasi literatur yang bukan merupakan jurnal akademik. Selanjutnya, mengeliminasi literatur yang duplikat atau memiliki kesamaan dalam analisis dan pembahasan. Kemudian, memastikan kembali relevansi literatur dengan membaca abstrak dan *skimming* isi literatur.

III. BINGKAI ANALISIS

Berdasarkan 6 literatur yang dianalisis, langkah selanjutnya adalah memetakan literatur yang telah dipilih. Literatur dipetakan sesuai dengan objek pengujian, metode pengujian, serta alat/*tools* yang digunakan.

TABEL 2. KAJIAN PUSTAKA

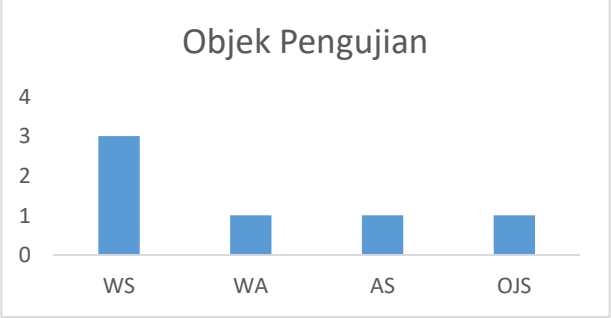
Literatur	Objek	Metode	Alat / *tools*
[4]	WA	OWTT	Acn, BS, ZAP
[5]	WS	OWV4	Bts, WF, WSc, ZAP, WB
[6]	WS	OW, ISF	WIS, Nk, ZAP
[7]	AS	OWTT	ZAP, Arch
[8]	WS	OWTT	Acn, WB
[9]	OJS	OW, ISF	WF, Dr, ZAP, OWCST

WA: Web Application, WS: Web Server, AS: Application System, OWTT: OWASP Top Ten (10), OWV4: OWASP Versi 4, OW: OWASP, ISF: ISSAF, Acn: Acunetix, BS: Burp Suite, ZAP: Zed Attack Proxy, Bts: Brutus, WSc: Web Scarab, WF: WFuzz, WB: Web Browser, WIS: WhoIS, Nk: Nikto, Arch: Arachni, Dr: Dirb, OWCST: OWASP CSRF Tester.

IV. HASIL ANALISIS

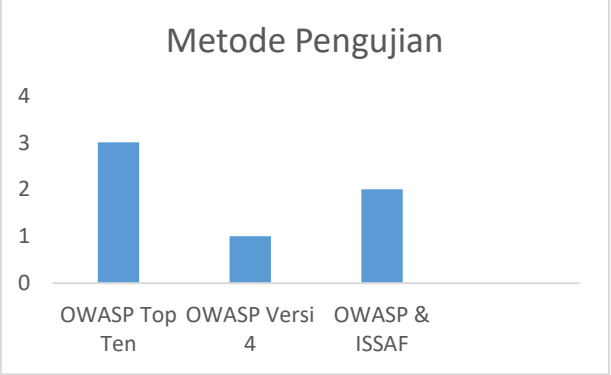
A. *Hasil Analisis*

Analisis yang dilakukan pada literatur yang terkait dengan pengujian keamanan sistem informasi dipertimbangkan berdasarkan sejumlah faktor. Hasil analisis menunjukkan bahwa penelitian terkait pengujian keamanan sistem informasi terutama dilakukan pada aplikasi *web server*.



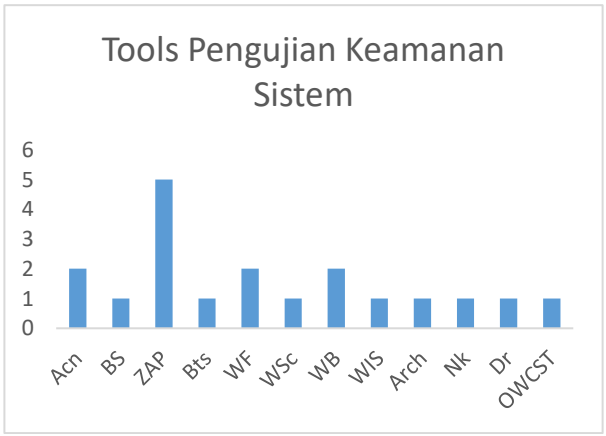
Gambar 2. Diagram Objek Pengujian

Literatur lain mengimplementasikan *framework* OWASP tidak hanya pada *website*, namun juga digunakan pada beberapa sistem yang terhubung kedalam sebuah jaringan. Hali ini dilakukan dalam penelitian untuk efektifitas *framework* untuk bisa dikombinasikan dengan *framework* lainnya dalam menunjang keamanan sistem.



Gambar 3. Diagram Metode Pengujian

Diagram diatas menunjukkan metode yang digunakan dalam penelitian terkait dengan pengujian keamanan sistem informasi khususnya berbasis website. Metode yang digunakan yaitu *OWASP Top Ten*, *OWASP Version 4*, *OWASP & ISSAF*. Metode *OWASP Top Ten* paling sering digunakan dalam penelitian pengujian keamanan sistem. Sedikit perbedaan antara *OWASP Top Ten* dengan *OWASP Version 4*, namun *OWASP Top Ten* jauh lebih populer dan lebih dulu rilis dan digunakan oleh para *developer* dan peneliti untuk mengulas metode *OWASP Top Ten*. Tidak hanya digunakan secara metode tunggal dalam pengujian, *OWASP* dapat dikombinasikan dengan metode lainnya seperti *ISSAF* dalam pengujian keamanan sistem.



Gambar 4. Diagram *Tools* Pengujian Keamanan Sistem

Diagram diatas menunjukkan alat atau *tools* yang digunakan dalam pengujian keamanan sistem informasi khususnya *web based application*, *ZAP* paling dominan dan paling sering digunakan oleh para peneliti. Hal tersebut dikarenakan *ZAP* merupakan *tools* yang dibuat oleh *OWASP* dalam mendukung kinerja pada metode pengujian menggunakan *OWASP*. ZAP bisa digunakan sebagai *web scanning* dan *web pentesting*, dengan fitur dan keunggulan yang dimiliki oleh *ZAP* maka para peniliti dan penguji lebih sering menggunakan *ZAP* sebagai *tools* pengujian. *Tools* yang digunakan dalam pengujian terdapat beberapa topik yaitu *reconnaisance*, *scanning* dan *exploitation*.

B. *Diskusi*

RQ1: Jenis penelitian dan metode apa yang digunakan?

Setelah dilakukan kajian sebanyak 6 literatur, hasil yang didapatkan berdasarkan masing-masing elemen. Pada elemen metode, paling banyak digunakan adalah metode kualitatif. Diketahui dari masing-masing literatur memiliki persamaan dan perbedaan pada setiap komponen dan detail penelitiannya, hal tersebut dapat dipengaruhi oleh tujuan penelitian dan metodologi yang digunakan pada masing-masing penelitian. Selain itu metode pengujian paling banyak digunakan adalah *OWASP Top Ten* sejumlah 3 literatur dengan poin pengujiannya *authenctication*, *authorization* dan *session management*. Pengujian menggunakan *framework OWASP Top Ten* tidak hanya menggunakan metode literatur

kualitatif, namun dapat menggunakan metode kuantitatif [10]. Disamping itu, *OWASP* juga dapat dikolaborasikan dengan metode pengujian lainnya.

RQ2: Apa saja fokus penelitian terkait keamanan sistem informasi?

Pengujian keamanan sistem informasi khususnya pada aplikasi website adalah untuk menemukan celah keamanan atau kesalahan pada sistem yang kemudian diberikan solusi serta langkah yang dapat dilakukan dalam memberikan keamanan serta kenyamanan pengguna sistem. Pengujian keamanan sistem informasi selain memberikan hasil mengenai celah keamanan, namun juga memberikan pemahaman sejauh apa sistem yang telah dibuat. Pengujian dilakukan dengan langkah *penetration testing* berdasarkan kerangka kerja yang telah ditentukan.

Sebanyak 3 literatur [5][6][8], yang dikaji membahas terkait pengujian terhadap *web server* yang dilakukan menggunakan metode OWASP serta dikolaborasikan dengan metode lainnya. Pengujian *web server* dilakukan pada *virtual machine* dengan tujuan tidak mengganggu proses bisnis yang berjalan secara *real-time*. Berdasarkan pengujian yang telah dilakukan, peneliti melakukan analisis dan memberikan rekomendasi terkait implementasi otentifikasi, otorisasi dan manajemen sesi pada sistem informasi [5]. Permintaan pada *web server* disimpan dalam *log file*, celah pada keamanan ini dapat digunakan oleh penyerang dengan masuk sebagai admin dan menghapus *log file* tanpa meninggalkan jejak. Penggunaan mekanisme proxy dalam pengujian penetrasi website lebih baik daripada menghapus *log file* [8]. Pencarian celah keamanan (*vulnerability testing)* dan pengujian celah keamanan (*penetration testing*) dilakukan untuk mengeksploitasi sistem untuk memberikan hasil apakah sistem dapat diakses oleh pihak yang tidak berwenang atau tidak memiliki akses [6].

Sistem informasi berbasis aplikasi website rentan terhadap serangan *session exploitation, cross-site scripting, SQL injection, cross site request forgery, buffer over flow* dan *security misconfiguration*. Dijelaskan pada metode *OWASP* terkait dengan uji penetrasi manual dan uji penetrasi otomatis, yang memiliki perbedaan untuk dapat diimplementasikan pada pengujian keamanan sistem [4]. *Automation testing* atau uji penetrasi otomatis lebih praktis dan memberikan hasil yang cukup baik. Dengan tambahan *manual testing* atau uji penetrasi manual dapat memberikan hasil pengujian yang maksimal, serta rekomendasi keamanan lebih kredibel dan dapat diterapkan oleh pengembang sistem [7]. Ketika sistem dirasa aman dalam pengujian dan penetrasi, namun rekomendasi dalam mengamankan sistem agar tidak mudah disusupi oleh pihak yang tidak memiliki akses juga dapat diberikan. Penerapan keamanan dengan sistem yang terbaru, melakukan *backup* secara berkala, melakukan *update* terhadap sistem yang digunakan dan melakukan pemblokiran kepada pengguna yang tidak memiliki akses masuk yang bertujuan untuk mencegah serangan yang dapat terjadi[9].

V. KESIMPULAN

Penelitian ini memberikan gambaran terkait pengujian keamanan sistem informasi khususnya berbasis aplikasi website. Pengujian keamanan sangat diperlukan dalam memberikan keamanan dan kenyaman kepada pengguna sistem. Dari hasil pencarian celah keamanan dan pengujian celah keamanan dapat ditemukan beberapa kelemahan dan kerentanan pada sistem. Karena kelemahan tersebut dapat diekploitasi oleh pihak yang tidak berwenang dan tidak memiliki akses. Sejak maraknya informasi terkait kebocoran data, penyusupan sistem oleh *hacker* menggambarkan bahwa perlunya dilakukan pengujian keamanan secara berkala dan bertahap untuk memberikan sistem yang baik untuk pengguna. Selanjutnya dari hasil analisis yang telah dilakukan, diketahui bahwa penggunaan metode *OWASP Top Ten* lebih sering digunakan dan alat yang dapat digunakan dalam pencarian dan pengujian keamanan sistem tersedia secara sumber terbuka seperti *ZAP* yang menjadi primadona dalam pengujian keamanan sistem berbasis website. Namun, penelitian dengan fokus pengujian keamanan menggunakan metode *OWASP* versi 4.2 belum banyak ditemukan. Selain itu celah keamanan dan tipe serangan yang semakin beragam, membuat metode yang telah digunakan kurang maksimal.

Rekomendasi untuk penelitian selanjutnya adalah melakukan penelitian lebih lanjut dengan metode selain *OWASP* yang lebih efektif atau dapat dilakukan bersama dengan *OWASP* untuk dilakukan pengujian keamanan sistem informasi berbasis website. Sehingga peneliti dapat melakukan pencarian dan pengujian sistem berdasarkan metode yang efektif dan penggunaan alat yang dapat memberikan rekomendasi terhadap keamanan sistem. Selain itu perlu dilakukan penelitian lanjutan terkait model serangan terbaru yang sulit ditemukan dan diketahui berdasarkan pencarian dan pengujian keamanan sistem guna memberikan hasil pengujian dan rekomendasi kepada administrator serta pengguna dalam mengantisipasi serangan yang dapat terjadi.

DAFTAR PUSTAKA

[1] Owasp, “OWASP Foundation | Open Source Foundation for Application Security.” 2017, [Online]. Available: https://owasp.org/.

[2] V. Drake, “OWASP Web Security Testing Guide v4.2 released.” 2020, [Online]. Available: https://medium.com/@victoriadotdev/owasp-web-security-testing-guide-v4-2-released-7910ea1d7e47.

[3] M. Caselli, F. K. C. I. I. Security, and undefined 2014, “A security assessment methodology for critical infrastructures,” *Springer*, vol. 8985, pp. 332–343, 2016, doi: 10.1007/978-3-319-31664-2_34.

[4] S. Nagpure and S. Kurkure, “Vulnerability Assessment and Penetration Testing of Web Application,” 2018, doi: 10.1109/ICCUBEA.2017.8463920.

[5] R. T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, “Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server,” *Netw. Eng.*

Res. Oper., vol. 1, no. 3, May 2016, doi: 10.21107/NERO.V1I3.29.

[6] A. Rochman, R. Rohian Salam, and S. Agus Maulana, "Analisis Keamanan Website dengan Information System Security Assessment Framework (Issaf) dan Open Web Application Security Project (Owasp) di Rumah Sakit Xyz," *Jurnal Indonesia Sosial Teknologi*, vol. 2, no. 4. pp. 506–519, 2021, doi: 10.36418/jist.v2i4.124.

[7] Sunardi, I. Riadi, and P. A. Raharja, "Vulnerability analysis of E-voting application using open web application security project (OWASP) framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 11, pp. 135–143, 2019, doi: 10.14569/IJACSA.2019.0101118.

[8] K. Nagendran, A. Adithyan, R. Chethana, P. Camillus, and K. B. Bala Sri Varshini, "Web application penetration testing," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 1029–1035, Aug. 2019, doi: 10.35940/ijitee.J9173.0881019.

[9] G. Guntoro, L. Costaner, and M. Musfawati, "ANALISIS KEAMANAN WEB SERVER OPEN JOURNAL SYSTEM (OJS) MENGGUNAKAN METODE ISSAF DAN OWASP (STUDI KASUS OJS UNIVERSITAS LANCANG KUNING)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, Jun. 2020, doi: 10.29100/jipi.v5i1.1565.

[10] O. Ben Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam, and A. Derhab, "An OWASP Top Ten Driven Survey on Web Application Protection Methods," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2021, vol. 12528 LNCS, pp. 235–252, doi: 10.1007/978-3-030-68887-5_14.