Penetration Testing Pada Domain xyz.ac.id Menggunakan OWASP 10

Prawira Zamal Mustofa*[1], Yusuf Sumaryana[2], Ruuhwan[3]
[1,2,3]Universitas Perjuangan; Jl. Peta No.177, (0265) 326058 [1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Perjuangan
e-mail: *[1]2003010058@unper.ac.id, [2]yusufsumaryana@unper.ac.id, [3]ruuhwan@unper.ac.id

ABSTRAK

Perkembangan teknologi informasi, khususnya internet, telah mengubah paradigma kehidupan manusia dengan memudahkan akses informasi dan komunikasi. Namun, penggunaan teknologi ini tanpa kebijaksanaan juga membawa dampak negatif yang signifikan, seperti penyebaran ujaran kebencian, berita palsu, dan kejahatan online. Di Indonesia, dengan populasi internet yang signifikan, kebijakan dan perilaku bijak dalam penggunaan internet masih menjadi tantangan. Survei Digital Civility Index menunjukkan bahwa tingkat kesopanan online di Indonesia masih rendah, tercermin dari masalah seperti penipuan, ujaran kebencian, dan diskriminasi. Penelitian ini menyoroti keamanan informasi di lingkungan akademik, khususnya Universitas Perjuangan Tasikmalaya, yang menghadapi risiko akses tidak sah dan penyalahgunaan informasi. Melalui analisis sistem dengan pendekatan penetration testing berbasis OWASP Top 10, penelitian ini bertujuan untuk mengidentifikasi kelemahan keamanan dan menawarkan solusi yang dapat meningkatkan ketahanan sistem terhadap serangan. Dengan demikian, penelitian ini memberikan kontribusi penting dalam memperkuat keamanan informasi di lingkungan pendidikan tinggi dan membangun kesadaran akan risiko keamanan yang terkait dengan penggunaan teknologi informasi.

***Kata Kunci**: Pengujian Penetrasi, OWASP 10, Informasi Keamanan*

ABSTRACT

The development of information technology, especially the internet, has changed the paradigm of human life by making it easier to access information and communication. However, the use of this technology without discretion also has significant negative impacts, such as the spread of hate speech, fake news and online crime. In Indonesia, with a significant internet population, wise policies and behavior in internet use are still a challenge. The Digital Civility Index survey shows that the level of online civility in Indonesia is still low, reflected in problems such as fraud, hate speech and discrimination. This research highlights information security in the academic environment, especially Universitas Perjuangan Tasikmalaya, which faces the risk of unauthorized access and misuse of information. Through system analysis using a penetration testing approach based on the OWASP Top 10, this research aims to identify security weaknesses and offer solutions that can increase the system's resistance to attacks. Thus, this research makes an important contribution to strengthening information security in higher education environments and building awareness of the security risks associated with the use of information technology.

***Keywords:** Penetration Testing, OWASP 10, Security Information*

1. PENDAHULUAN

Perkembangan teknologi informasi, khususnya internet, memberikan kemudahan namun juga membawa dampak negatif seperti ujaran kebencian, penyebaran berita bohong, dan kejahatan internet. Penggunaan internet tanpa kebijaksanaan dapat berpotensi menciptakan masalah besar, termasuk kekerasan di ruang maya. Meskipun internet mempercepat pekerjaan dan memberikan informasi real-time, dampak negatifnya perlu diwaspadai karena informasi yang tersebar dapat memengaruhi tindakan manusia. Oleh karena itu, penting bagi individu untuk secara kritis menilai informasi yang diterima agar tidak menjadi korban atau pelaku kekerasan online[1].

Pada tahun 2022, penduduk Indonesia mencapai 275.773 juta jiwa, dengan 215.636 juta individu terkoneksi internet, atau 78,19% dari total populasi. Sekitar 60,4% dari total populasi aktif di media sosial. Mayoritas pengguna internet Indonesia berusia 18 hingga 34 tahun, namun kesadaran akan penggunaan internet yang bijak masih rendah. Indonesia menempati peringkat 29 dari 32 negara dalam Digital Civility Index 2020 oleh Microsoft, menunjukkan rendahnya tingkat kesopanan dalam perilaku online, yang dipengaruhi oleh penipuan, berita palsu, ujaran kebencian, dan diskriminasi online[2].

Keamanan informasi menggambarkan usaha untuk melindungi computer dan non peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab. Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi dalam suatu perusahaan. Keamanan Sistem informasi terdiri atas perlindungan harian, yang disebut keamanan informasi (information security) dan persiapan-persiapan operasional. Tujuan penulisan artikel ini guna membangun hipotesis pengaruh antar variabel untuk digunakan pada riset selanjutnya. Hasil artikel literature review ini adalah:[3].

1) Keamanan Informasi berpengaruh terhadap Keamanan Sistem Informasi;
2) Teknologi Informasi berpengaruh terhadap Keamanan Sistem Informasi;
3) Network berpengaruh terhadap Keamanan Sistem Informasi.

OWASP (Open Web Application Security Project) adalah komunitas terbuka yang mendedikasikan untuk membuat sebuah organisasi yang bertujuan untuk mengembangkan, membeli, dan memelihara aplikasi yang terpercaya. Di OWASP pengunjung akan menemukan semua gratis dan terbuka. Seluruh tools, dokumen, forum, dan cabang OWASP bebas dan terbuka bagi semua orang yang tertarik memperbaiki aplikasi keamanan. OWASP mendukung pendekatan keamanan aplikasi sebagai masalah perseorangan, proses, dan masalah teknologi karena pendekatan paling efektif terhadap keamanan aplikasi membutuhkan perbaikan diseluruh area. OWASP adalah jenis organisasi baru yang bebas dari tekanan komersial sehingga memungkinkan untuk memberikan informasi terkait keamanan aplikasi yang tidak biasa, praktis, dan efektif biaya. OWASP tidak terafiliasi dengan perusahaan teknologi manapun, meskipun OWASP mendukung penggunaan teknologi keamanan komersial. Serupa dengan banyak proyek software open-source, OWASP menghasilkan beragam jenis materi dengan cara kolaborasi dan terbuka. Yayasan OWASP merupakan lembaga non-profit yang memastikan kesuksesan jangka panjang proyek. Hampir semua yang terasosiasi dengan OWASP adalah sukarelawan [4].

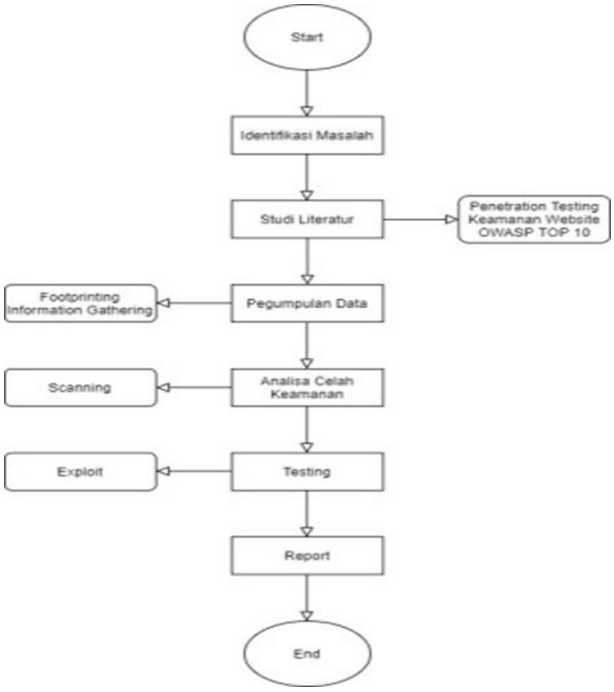
Menurut OWASP terdapat beberapa tahap untuk menentukan dan mengkombinasikan besarnya resiko yang ditimbulkan akibat eksploitasi kelemahan yang terdapat pada suatu aplikasi web, Berikut tahapan OWASP *Risk Rating Methodology yaitu Identifying a Risk, Factors for Estimating Impact, Determining the Severity of the Risk, Deciding What to Fix, Customizing the Risk Rating Model* [5]. Adapun beberapa penelitian sebelumnya yang menjadi sebuah referensi pembeda bagi penulis untuk mengimplementasikan *Penetration Testing* sebagai berikut ini:

1) Pengujian Penetrasi Web Server Diva Karaoke dan Analisis Keamanan [6].
2) Pengujian Penetrasi dan Peningkatan Keamanan Website CV Rental Mobil Merdeka Auto Rental melalui Teknik *SQL Injection (SQLI)* dan *Cross-Site Scripting (XSS)* [7].
3) Peningkatan Keamanan Aplikasi Webserver Pelaporan Pajak Regional melalui Pengujian Penetrasi [8].
4) Pengujian Keamanan Sistem *Open Journal System* (*OJS*) di Universitas Lancang Kuning Menggunakan Metode ISSAF dan OWASP [9].

Analisis Keamanan Website Institusi Pendidikan Tinggi di Indonesia Menggunakan Teknik *Footprinting* dan *Vulnerability Scanning* [10].

2. METODE PENELITIAN

Dalam melakukan penelitian pentest terhadap web yang ber-subdomain xyz.ac.id ini terdapat beberapa tahap dalam pengumpulan data. Tahapan yang dilakukan dalam pengumpulan data ini terdapat beberapa sumber antara lain melalui literatur seperti jurnal, paper ilmiah, tugas akhir atau dari media digital seperti internet. Selain dari itu informasi juga didapatkan melalui hasil analisis pada infrastruktur sistem web Universitas Perjuagan dan melakukan diskusi dengan pihak pengelola jaringan Universitas Perjuangan dan ahli dalam bidang keamanan informasi atau uji pentest.



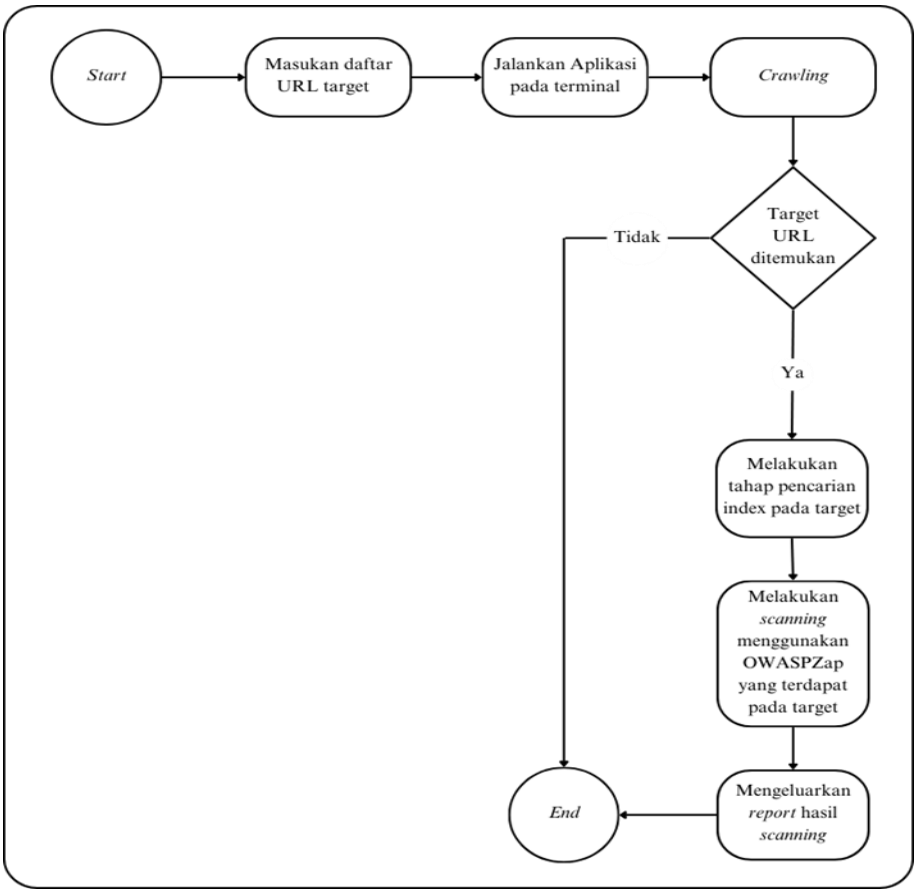
Gambar 1. Diagram Alur Penelitian

3. HASIL DAN PEMBAHASAN

3.1 Otomatisasi OWASP Zap

Aplikasi otomatisasi OWASPZap yang dikembangkan oleh pihak OWASP untuk membantu dalam proses pentest ini memiliki alur diagram (flowchart) seperti pada Gambar 2. Pada Gambar 2. hal pertama yang dilakukan adalah memasukan daftar nama-nama web yang akan dijadikan target, kemudian user menjalankan aplikasi pada terminal. Selanjutnya aplikasi akan melakukan proses crawling terhadap daftar target yang telah ditentukan. Setelah target ditemukan aplikasi akan melakukan proses pencarian terhadap semua index yang terdapat dalam web target.

Setelah semua index terdeteksi aplikasi akan melakukan scanning terhadap index target guna mencari celah keamanan setelah proses selesai aplikasi akan mengeluarkan report hasil scanning dan selanjutnya aplikasi akan melakukan pengecekan apakah daftar target sudah selesai dieksekusi dan sudah tidak terdapat daftar target lagi maka aplikasi akan berhenti namun jika masih ada target aplikasi akan mengulang proses seperti sebelumnya hingga semua daftar target selesai dieksekusi.



Gambar 2. *Flowchart* aplikasi Otomatisasi OWASPZap

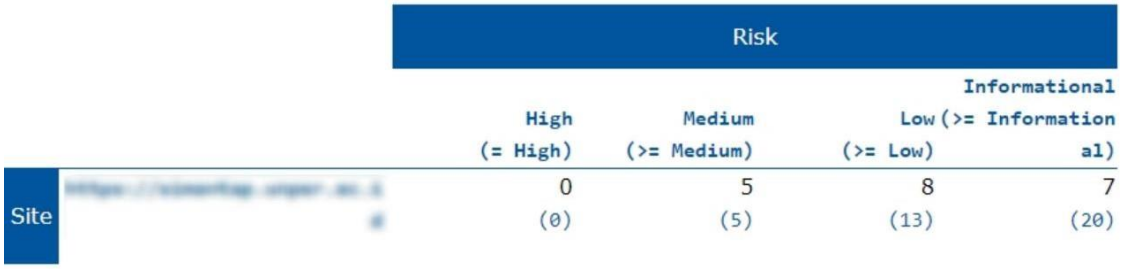
3.2 Hasil

Dari proses scanning yang telah dilakukan didapat hasil kemungkinan terdapat celah keamanan pada web target yang berdomain xyz.ac.id diantara seperti pada Tabel 1. dan Gambar 3. Celah keamanan pada sub domain abc.xyz.ac.id

Tabel 1. Celah keamanan pada sub domain abc.xyz.ac.id

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	24 (120.0%)
Hidden File Found	Medium	4 (20.0%)
Missing Anti-clickjacking Header	Medium	22 (110.0%)
Vulnerable JS Library	Medium	1 (5.0%)
XSLT Injection	Medium	8 (40.0%)
Big Redirect Detected(Potential Sensitive Information Leak)	Low	5 (25.0%)
Cookie No HttpOnly Flag	Low	67 (335.0%)
Cookie Without SecureFlag	Low	134 (670.0%)
Cookie without SameSite Attribute	Low	134 (670.0%)
Server Leaks Version Information via "Server"HTTP Response HeaderField	Low	91 (455.0%)
Strict-Transport-Security Header Not Set	Low	89 (445.0%)
Timestamp Disclosure -Unix	Low	59 (295.0%)
Content-Type HeaderMissing	Informational	2 (10.0%)
Information Disclosure - Suspicious Comments	Informational	16 (80.0%)
Modern Web Application	Informational	11 *(55.0%)*
Re-examine Cache-control Directives	Informational	65 *(325.0%)*
Session Management Response Identified	Informational	269 *(1,345.0%)*
User Agent Fuzzer	Informational	384

		(1,920.0%)
User Controllable HTML *Element Attribute(Potential XSS)*	Informational	7 *(35.0%)*
Total		**20**



		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Information al)
Site	[illegible]	0 (0)	5 (5)	8 (13)	7 (20)

Gambar 3. Hasil *scanning* Otomatisasi OWASPZap

3.3 Hasil Analisis

Dari hasil scanning yang telah dilakukan pada proses sebelumnya ditemukan web target telah menggunakan Debian Linux versi 2.4.25 dan terdapat beberapa celah keamanan yang dapat membahayakan keamanan web yang dikelola oleh UPT TIK Univeritas Perjuangan sehingga perlu segera dilakukan tindakan pencegahaan lebih dini dan rata-rata kemungkinan celah keamanan yang ditemukan pada hasil scanning menggunakan aplikasi VulnX dan otomatisasi OWASPZap yang terdeteksi. Beberapa plugin belum dilakukan pembaruan oleh pengelola sehingga terdapat query tertentu yang terindikasi sebagai celah keamanan oleh aplikasi scanning akan tetapi web target yang memiliki domain xyz.ac.id tertolong dengan firewall yang di miliki karena serangan yang dilakukan terhadap celah keamanan yang ditemukan terhalang dan dapat langsung di cegah oleh firewall. Dari hasil scanning menggunakan VulnX dan otomatisasi OWASPZap juga terdapat false positive dimana peringatan keamanan yang ditemukan tidak terbukti atau palsu hal ini terjadi karena aplikasi mendeteksi query yang mungkin menjadi ciri-ciri dari sebuah celah keamanan sehingga aplikasi memberikan peringatan. Selain itu juga perlu dilakukan konfigurasi kembali terhadap web target karena terdapat celah keamanan yang cukup sensitive karena terdapat token yang mungkin berupa berbagai jenis informasi, seperti token autentikasi, token CSRF (Cross-Site Request Forgery), atau token lain yang digunakan dalam komunikasi antara klien dan server. Dari semua proses yang telah dilakukan pada tahap sebelumnya penulis memiliki beberapa rekomendasi dari berhasilnya menemukan token dan celah keamanan hasil scanning aplikasi otomatisasi OWASPZap dengan kategori tingkat ancaman menengah (medium) antara lain :

Tabel 2. Solusi dari celah keamanan yang ditemukan.

Celah Keamanan	Solusi
Insecure Direct Object References (IDOR)" atau *"Missing Function Level Access Control*	Melakukan pengecekan otorisasi yang tepat sebelum memberikan akses ke sumber daya atau fungsi tertentu.
Content Security Policy (CSP) HeaderNot Set	Pastikan server web, server aplikasi, penyeimbang beban, dll. Anda dikonfigurasi untuk menyetel header Kebijakan Keamanan Konten.

Missing Anti-clickjacking Header	Browser Web modern mendukung header HTTP Content-Security-Policy dan X-Frame-Options. Pastikan salah satunya disetel di semua halaman *web*.
Vulnerable JS Library	Meningkatkan ke versi terbaru moment.js.
Celah Keamanan	**Solusi**
XSLT Injection	Analisis setiap masukan pengguna yang datang dari sisi klien mana pun.
Hidden File Found	Mempertimbangkan apakah komponen tersebut benar-benar diperlukan dalam produksi atau tidak, jika tidak maka nonaktifkan. Jika ya, pastikan akses ke sana memerlukan autentikasi dan otorisasi yang sesuai, atau batasi paparan ke sistem internal atau IP sumber tertentu.

4. KESIMPULAN

Dalam melakukan uji penetration testing menggunakan metode OWASP10 tahun 2021 yang bertujuan untuk menguji tingkat keamanan pada sistem web yang berdomain xyz.ac.id yang di miliki oleh Universitas Perjuangan berdasarkan dari seluruh kegiatan yang dilakukan maka dapat diambil beberapa kesimpulan yang antara lain sebagai berikut:

1. Metode OWASP10 tahun 2021 masih sangat cocok dijadikan sebagai dasar dalam melakukan uji penetration testing pada web yang berdomain xyz.ac.id. Karena masih ditemukan beberapa celah keamanan yang sesuai dengan daftar OWASP10 tahun 2021
2. Keamanan sistem pada web target yang memiliki domain xyz.ac.id mempunyai celah keamanan tingkat menengah (medium) dan tidak memiliki tingkat celah keamanan yang tinggi (high). Hal tersebut dapat dilihat dari hasil scanning menggunakan aplikasi otomatisasi OWASPZap. Sehingga mengurangi tingkat resiko exploitasi.
3. Domain xyz.ac.id memiliki firewall yang cukup bisa diandalkan dalam menanggulangi serangan-serangan oleh orang yang tidak bertanggung jawab.
4. Meskipun berhasil mendapatkan token yang mungkin berupa berbagai jenis informasi, seperti token autentikasi, token CSRF (Cross-Site Request Forgery), atau token lain yang digunakan dalam komunikasi antara klien dan server namun token tersebut mempunyai algoritma yang sulit untuk dipecahkan, sehingga sulit untuk menggunakan token tersebut.

DAFTAR PUSTAKA

[1] Paramitha, D. I., & Tyas, I. K. D. (2022). Sosialisasi media sosial sebagai sarana membangun budaya damai di kalangan generasi z di Kota Samarinda. Dalam Pemberdayaan Masyarakat (Vol. 7, Issue 10, pp. 1716–1722). https://doi.org/10.31603/ce.7235

[2] Karmila, P., & Budimansyah, D. (2022). Rasisme Digital: Bentuk Rasisme Baru, Ancaman Keutuhan Bangsa. Prosiding Konferensi Pendidikan Kewarganegaraan Tahunan (ACEC 2021), 636(Acec 2021), 296–301. https://doi.org/10.2991/assehr.k.220108.054

[3] Nurul, S., Shynta Anggrainy and Siska Aprelyani (2022) "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE SIM)", Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), pp. 564-573. doi: 10.31933/jemsi.v3i5.992

[4] Owasp.org. (2021). Tentang OWASP - OWASP Top 10:2021. [online] Available at: https://owasp.org/Top10/id/A00-about-owasp/

[5] Rifainstitute.com. (2023). View of ANALISIS KERENTANAN KEAMANAN WEBSITE MENGGUNAKAN METODE OWASP (OPEN WEB APPLICATION SECURITY PROJECT) PADA DINAS TENAGA KERJA. [online] https://fusion.rifainstitute.com/index.php/fusion/article/view/53/48

[6] Marzuki Hasibuan and Andi Marwan Elhanafi (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. sudo Jurnal Teknik Informatika, [online] 1(4)pp.171–177. doi:https://doi.org/10.56211/sudo.v1i4.160.

[7] Muhammad and Y Yuhandri (2021). Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS. Jurnal Sistim Informasi dan Teknologi, [online] pp.215–220. doi:https://doi.org/10.37034/jsisfotek.v3i4.68.

[8] Yosua Ade Pohan, Yunus, Y. and Sumijan Sumijan (2021). Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar. Jurnal Sistim Informasi dan Teknologi, [online] pp.1–6. doi:https://doi.org/10.37034/jsisfotek.v3i1.36.

[9] Guntoro Guntoro, Loneli Costaner and Musfawati Musfawati (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 Pembelajaran Informatika), [online] 5(1), pp.45–45.doi:https://doi.org/10.29100/jipi.v5i1.1565.

[10] Erick Irawadi Alwi, Herdianti Herdianti and Umar, F. (2020). Analisis Keamanan Website Menggunakan Teknik Footprinting dan Vulnerability Scanning. Informal: informatics journal, [online] 5(2), pp.43–43. doi:https://doi.org/10.19184/isj.v5i2.18941.