ANALISIS KERENTANAN KEAMANAN *WEB*SITE DENGAN METODE UJI PENETRASI MENGGUNAKAN FRAMEWORK ISSAF PADA *WEB*SITE XYZ (STUDI KASUS : PT.XYZ)

1st Rivaldo Dava Abimanyu
Fakultas Rekayasa Industri
Telkom University
Surabaya, Indonesia
rivaldodava@student.telkomuniveristy.ac.id

2nd Muhamad Nasrullah
Fakultas Rekayasa Industri
Telkom University
Surabaya, Indonesia
emnasrul@telkomuniversity.ac.id

3rd Rizky Fenaldo Maulana
Fakultas Informatika
Telkom University
Surabaya, Indonesia
rizkyfenaldo@telkomuniversity.ac.id

***Abstrak* — Keamanan informasi adalah aspek kritis yang harus dijaga, terutama pada sistem yang menyimpan data sensitif. Jika diabaikan, peretas dapat mengeksploitasi celah keamanan dan merusak informasi. Beberapa serangan umum meliputi virus, pencurian kartu kredit, dan peretasan server. Penelitian ini mengevaluasi keamanan situs web Xyz, platform donasi online di bawah PT.Xyz, yang mengelola data pengguna, laporan keuangan, dan riwayat transaksi. Evaluasi menggunakan Metodologi ISSAF (Information Systems Security Assessment Framework) dengan 9 tahapan pengujian penetrasi. Analisis awal mengidentifikasi infrastruktur situs yang dikelola oleh DigitalOcean, LLC dengan IP 157.xxx.xx.xxx. Pengujian menggunakan Nessus dan OWASP ZAP menemukan ancaman seperti DNS Server Spoofed Request Amplification DDoS dan Cache Poisoning. Meski demikian, pengujian lanjutan dengan sqlmap, Hydra, dan Metasploit menunjukkan sistem keamanan cukup baik dengan mekanisme seperti pembatasan login, sanitasi input, dan pengelolaan cookie aman. Untuk meningkatkan keamanan, direkomendasikan pembaruan perangkat lunak, perbaikan konfigurasi server, serta implementasi Web Application Firewall (WAF) dan Intrusion Detection System (IDS). Hasil penelitian ini memberikan rekomendasi konkret kepada PT.Xyz untuk meningkatkan keamanan platform dalam melindungi data pengguna dan transaksi donasi.**

***Kata kunci*— website, Penetration Testing, Framework ISSAF.**

I. PENDAHULUAN

Perkembangan teknologi yang semakin canggih telah menjadikan situs web sebagai media baru dalam penyebaran informasi, termasuk dalam konteks pendidikan dan sosial. Salah satu implementasinya adalah platform Xyz yang merupakan anak perusahaan dari PT.Xyz, sebuah Lembaga Amil Zakat Nasional yang dikukuhkan oleh Menteri Agama Republik Indonesia. Platform ini berfungsi sebagai crowdfunding berbasis web yang bertujuan menghimpun dana masyarakat dalam bentuk zakat, infaq, dan sedekah. Mengingat platform ini menangani data sensitif seperti informasi pengguna, laporan keuangan, detail program, penerima donasi, dan riwayat transaksi, keamanan menjadi faktor yang sangat krusial. Untuk memastikan keamanan sistem, diperlukan Penetration Testing dengan framework ISSAF (The Information System Security Assessment Framework) menggunakan metode Black Box testing. Pendekatan ini melibatkan pemindaian sistem untuk menemukan kelemahan yang ada, serta eksploitasi sistem untuk menguji seberapa rentan terhadap serangan. Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan keamanan pada situs Xyz dan memberikan rekomendasi perbaikan untuk meningkatkan keamanan sistemnya.

II. KAJIAN TEORI

Kajian teori mencakup asumsi, postulat, tesis, hipotesis, proposisi, serta konsep yang terhubung dengan lingkungan alam atau kehidupan sosial masyarakat. Dasar teori disusun dengan teratur dan melibatkan variabel-variabel yang relevan.

A. PT.Xyz

PT.Xyz adalah lembaga yang bergerak di bidang sosial dan kemanusiaan, yang fokus pada pengelolaan zakat, infak, sedekah, dan wakaf untuk mendukung berbagai program pemberdayaan masyarakat di Indonesia.PT.Xyz dikenal sebagai pelopor dalam pengelolaan dana umat secara profesional dan transparan.

B. *Website* Xyz

Website Xyz adalah platform berbasis website yang berfokus pada kegiatan donasi dan penggalangan dana secara online. *Website* ini memungkinkan pengguna untuk melakukan donasi atau menggalang dana untuk berbagai tujuan sosial dan kemanusiaan.

C. Sistem Informasi

Sistem informasi adalah suatu sistem dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan informasi yang diperlukan untuk pengambilan keputusan[1].

D. Keamanan Sistem Informasi

Segala tindakan yang dilakukan untuk memastikan bahwa data dalam suatu sistem dilindungi dari ancaman seperti *hacking*, *virus*, atau *malware* disebut keamanan sistem informasi. Tujuan keamanan sistem informasi adalah untuk mencegah, mengatasi, dan melindungi berbagai sistem informasi dari tindakan ilegal[2].

E. Penetration Lifecycle

Siklus uji penetrasi (*Penetration Testing lifecycle*), adalah serangkaian tindakan yang dimaksudkan untuk menemukan dan memperbaiki masalah keamanan dalam sistem, jaringan, atau aplikasi[3].

F. Penetration Testing

Penetration Testing adalah teknik yang digunakan untuk menguji sistem dengan mencari kerentanan, melacak *bug*, menemukan konfigurasi yang salah, dan mengidentifikasi kelemahan teknis baik pada perangkat keras maupun perangkat lunak dari sistem yang sedang diuji[4].

G. Kali Linux

Kali Linux merupakan plat*form* uji penetrasi yang paling terkemuka dan powerful di dunia yang digunakan oleh para profesional keamanan dalam berbagai bidang, termasuk uji penetrasi, forensik, rekayasa balik, dan evaluasi kerentanan[5].

H. Oracle VM Virtualbox

Oracle VM VirtualBox adalah aplikasi virtualisasi yang dapat diinstal pada komputer fisik dengan arsitektur Intel atau AMD. Penggunaan mesin virtual merupakan solusi efisien untuk mengurangi jumlah *server* yang digunakan dalam lingkungan perusahaan[6].

I. Nmap

Nmap adalah alat yang memungkinkan pengguna untuk melakukan pemindaian jaringan, mengeksplorasi infrastruktur dengan memeriksa *port*, mengenali perangkat yang terhubung, dan menemukan layanan yang sedang berjalan[7].

III. METODE

A. *Black Box Testing*

Metode *Black Box Testing* melibatkan seorang penguji yang tidak diberitahu tentang apa yang sedang diuji. Mereka mengandalkan pengetahuan dan pengalaman mereka untuk menemukan kelemahan dalam sistem keamanan tanpa informasi sebelumnya.

B. ISSAF *(Information Systems Security Assessment Framework)*

ISSAF merupakan sebuah pendekatan yang digunakan untuk menilai keamanan dari sistem informasi, jaringan komputer, dan juga potensi kelemahan dalam program aplikasi. Dalam kerangka kerja ISSAF, terdapat tiga tahapan evaluasi: perencanaan dan persiapan, penilaian, serta pelaporan dan proses pembersihan serta penghapusan jejak yang dilakukan setelahnya[8]. Adapun tahapan dari metode ISSAF:

1. Tahap pertama: *Planning and Preparation*

Di fase awal ini, pihak yang melakukan uji penetrasi dan pihak yang akan diuji dikenalkan dan disesuaikan. Langkah-langkah meliputi pertukaran informasi, perencanaan, dan persiapan uji[4]

2. Tahap kedua: *Assessment*

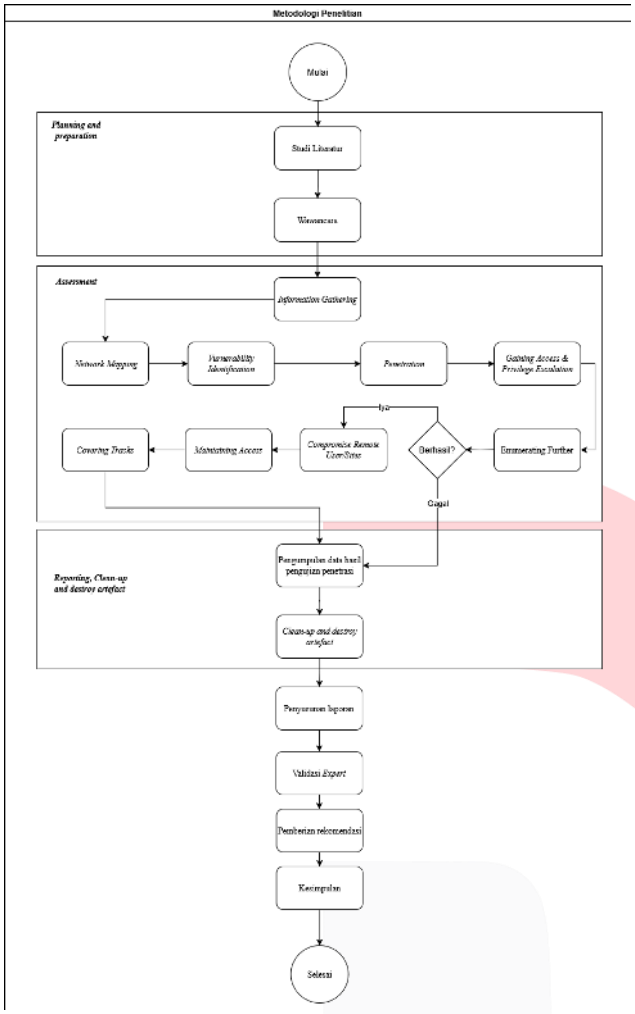
Fase ini adalah saat uji penetrasi dilakukan. Proses di setiap tahap meliputi; pengumpulan informasi, pemetaan jaringan, identifikasi kerentanan, penetrasi, memperoleh akses & eskalasi hak akses, mengidentifikasi lebih lanjut, mengompromi pengguna/situs jarak jauh, menjaga akses, dan menghilangkan jejak[4]

3. Tahap ketiga: *Reporting, Clean Up and Destroy Artefats*

Fase terakhir dari uji penetrasi. Di sini, laporan hasil uji penetrasi dibuat. Setelah uji dilakukan, *log* harus segera dihapus karena dapat membahayakan sistem jika digunakan oleh pihak lain.[4]

C. Alur Penelitian

Alur pada penelitian dengan judul "ANALISIS KERENTANAN KEAMANAN WEBSITE DENGAN METODE UJI PENETRASI MENGGUNAKAN FRAMEWORK ISSAF PADA WEBSITE Xyz (STUDI KASUS : PT.Xyz)" dapat dilihat pada gambar di bawah.



GAMBAR 1
(Alur Penelitian)

Penelitian dimulai dengan studi literatur tentang pengujian yang akan dilakukan, serta melakukan wawancara dan diskusi dengan Divisi IT PT.Xyz tentang perizinan. Selanjutnya, Penetration Testing dilakukan menggunakan tahap Assessment pada framework ISSAF. Setelah pengujian tersebut selesai, tahap terakhir adalah membuat rekomendasi berdasarkan hasil pengujian Penetration Testing menggunakan framework ISSAF dan menghapus semua jejak yang terkait dengan serangan. Pada penelitian ini menggunakan rangkaian metode penelitian yang dimulai dengan Planning and Preparation dimana informasi awal dikumpulkan dan rencana serta persiapan untuk pengujian dibuat, termasuk studi literatur dan wawancara dengan Divisi IT PT.Xyz. Tahap Assessment merupakan tahap inti yang terdiri dari Information Gathering untuk mengumpulkan informasi umum tentang situs web target, Network Mapping untuk memperoleh informasi spesifik tentang jaringan, Vulnerability Identification untuk menemukan kerentanan keamanan, Penetration untuk simulasi serangan, Gaining Access and Privilege Escalation untuk menguji dan meningkatkan akses ke sistem target, Enumerating Further untuk mencari informasi tambahan, Compromise Remote User/Sites untuk menggunakan celah yang ditemukan, Maintaining Access untuk menjaga akses melalui penanaman backdoor, dan Covering Tracks untuk menghilangkan jejak serangan. Setelah itu dilakukan Reporting, Clean Up and Destroy Artefats untuk menghapus semua data yang telah dikumpulkan, termasuk pengumpulan data hasil pengujian dan pembersihan artefak. Terakhir dilakukan penyusunan laporan hasil pengujian dan pemberian rekomendasi untuk memperbaiki kerentanan keamanan, memperkuat pertahanan sistem, serta mengurangi potensi risiko yang dapat timbul[9].

IV. HASIL DAN PEMBAHASAN

Pada bagian ini, akan dijelaskan pembahasan terkait tahapan yang dilakukan beserta hasil penelitian terhadap objek, kemudian dari hasil yang didapat dibuatkan lampiran serta rekomendasi berdasarkan hasil pengujian untuk perbaikan system kedepannya dengan menggunakan metode testing *black box testing* serta *framework* ISSAF.

A. *Planning and Preparation*

Pada tahap ini dilakukanna perencanaan dan persiapan untuk melakukan perizinan dan pengelolaan awal dari web yang akan diuji.

TABEL 1
(Informasi Studi Kasus)

No.	Studi Kasus	Informasi
1.	*Web* yang digunakan pada studi ini	*Web Xyz*
2.	IP Addres dari *web*	IP 15x.xx5.5x.2x4.
3.	Waktu pengetesan *web*	Dimulai dari 1 oktober 2024 sampai 30 oktober 2024
4.	Perizinan	Diizinkan oleh perusahaan untuk melakukan penelitian.

B. *Assessment*

1. Information Gathering

Pada tahapan ini dilakukan agar mendapatkan informasi *web* yang akan dianalisa menggunakan *tools* whois[10].

TABEL 2
(Hasil *Information Gathering)*

No	Teknik Pengujian	Hasil Informasi
1.	Pencarian IP *Address*	IP 15x.xx5.5x.2x4.
2.	Pencarian data informasi tentang domain	Menggunakan domain dengan hosting DigitalOcean, LLC.
3.	Pencarian IP Address dan server	Perintah nslookup menunjukkan bahwa domain Xyz terhubung ke IP 15x.xx5.5x.2x4.melalui server DNS 192.xxx.xx.x.
4.	Pencarian Teknologi yang digunakan	Website ini menggunakan Facebook Pixel dan Google Analytics untuk analisis, reCAPTCHA untuk keamanan, CDN untuk konten, Apache 2.4.41 di Ubuntu, Firebase 8.0.1 sebagai basis data, jQuery

No	Teknik Pengujian	Hasil Informasi
		3.5.1, Moment.js, Swiper, Bootstrap 4/5, Font Awesome, Google Font API, Popper, Open Graph, dan Google Tag Manager.

2. *Network Mapping*

Hasil dari *network mapping* pada pedulibaik.id menunjukkan IP *Address* 15x.xx5.5x.2x4.dengan 3 port yaitu, *port* 22, 80, 443 dan *port* 33406[11].

3. *Vulnerability Identification*

Berikut hasil pengujian Vulnerability Identification menggunakan dua tools yaitu nessus dan owasp zap yang dapat dilihat pada tabel 3[12].

Teknik Pengujian	Tools	Hasil Pengujian
Vulnerability Identification	Nessus	Terdapat kelemahan protokol, kerentanan aplikasi web, dan risiko spoofing serta pemalsuan data pada DNS.
	Owasp Zap	Miskonfigurasi server web mengekspos informasi sensitif, berisiko menyebabkan serangan siber seperti SQL injection dan DDoS, sehingga perlu mitigasi melalui rekonfigurasi, pemutakhiran, dan penerapan Web Application Firewall..

4. *Penetration*

Pada tahap *Penetration Testing*, penguji akan melakukan uji keamanan sistem secara menyeluruh. Pada langkah ini, berbagai kerentanan dalam sistem pedulibaik.id akan diidentifikasi dan diperiksa menggunakan dua alat, yaitu sqlmap dan xss[13].

Teknik Pengujian	Tools	Hasil Pengujian	Status
Penetration Testing	Sqlmap	Melakukan uji SQL *Injection*	Gagal
		pada halaman *login*	
	Burpsuite	Melakukan uji XSS pada halaman search bar dengan *payload stored* XSS	Gagal

Dari tabel 4 pengujian dinyatakan tidak berhasil, dengan sqlmap melaporkan bahwa tidak ada kerentanan SQL *Injection* yang ditemukan, dan mencatat bahwa versi alat yang digunakan sudah usang.[14]

5. *Gaining Access and Privilege Escalation*

Berikut hasil *Gaining Access* dan *Privilege Escalation* menggunakan *tools Hydra, Burp Suite* dan *Metasploit* yang dapat dilihat pada tabel 5[15]

Teknik Pengujian	Tools	Hasil Pengujian	Status
Gaining Access and Privilege Escalation	*Hydra, Burpsuite*	Melakukan pengujian *brute force Attack* pada halaman *login* pedulibaik.id	Gagal
	Metasploit	Melakukan pengujian pada *port* 22, 80, 443 dan *port* 33406	Gagal

Berdasarkan tabel pengujian keamanan yang dilakukan, terdapat dua jenis pengujian yang telah dilaksanakan. Pengujian pertama adalah upaya Gaining Access dan Privilege Escalation menggunakan tools Hydra dan Burpsuite untuk melakukan brute force attack pada halaman login website xyz, namun upaya ini tidak berhasil. Pengujian kedua dilakukan menggunakan tool Metasploit untuk menguji kerentanan pada port 22, 80, 443, dan 33406, dan hasilnya juga menunjukkan tidak ditemukan celah keamanan karena pengujian tersebut gagal dilakukan.

6. *Enumerating Further*

Pada tahap *Enumerating Further dilakukan dengan* menggunakan *2 tools yaitu Wireshark dan Cookie Manager.*

Teknik Pengujian	Tools	Hasil Pengujian	Status
Enumerating Further	*Wireshark*	Melakukan rekam data untuk mendapatkan data yang *sensitive*	Gagal

Teknik Pengujian	Tools	Hasil Pengujian	Status
	Cookie Manager	Melakukan pengecekan *cookie* yang tersimpan untuk menemukan data yang *sensitive*	Gagal

Berdasarkan tabel pengujian keamanan tersebut, telah dilakukan dua jenis pengujian dalam kategori Enumerating Further. Pengujian pertama menggunakan tool Wireshark untuk merekam dan menganalisis lalu lintas data dengan tujuan mendapatkan data sensitif, namun hasilnya tidak berhasil menemukan informasi yang dapat dieksploitasi. Pengujian kedua dilakukan menggunakan Cookie Manager untuk memeriksa cookie yang tersimpan dalam upaya menemukan data sensitif, tetapi pengujian ini juga tidak berhasil mengidentifikasi adanya kerentanan keamanan pada cookie yang dapat dimanfaatkan.

7. *Compromise Remote User/Sites*

Pada tahap ini, upaya dilakukan untuk memperoleh hak akses istimewa ke dalam jaringan dengan mengeksploitasi kelemahan pengguna atau situs *web* target. Tujuannya adalah untuk mengambil alih kendali pengguna atau situs jarak jauh agar dapat mengakses jaringan internal dengan hak akses yang lebih tinggi. Namun, upaya ini tidak berhasil karena sistem pada situs Pedulibaik.id telah menerapkan mekanisme keamanan yang membatasi jumlah percobaan *login*, sehingga dapat mencegah serangan *brute force.*

8. *Maintaining Access*

Pada tahap ini, berbagai metode digunakan untuk mempertahankan akses yang telah diperoleh dengan mengeksploitasi kerentanan yang ada dan menanam *backdoor* guna mendapatkan akses jangka panjang secara tersembunyi agar tidak terdeteksi oleh sistem keamanan. Namun, pemasangan *backdoor* sangat tidak disarankan karena dapat menimbulkan dampak serius, seperti kerusakan sistem, kebocoran data sensitif secara permanen, dan dalam skenario terburuk, kerusakan tersebut tidak dapat diperbaiki. Tahap ini pun tidak dapat dicapai karena sistem keamanan pada situs Pedulibaik.id telah dikonfigurasi dengan sangat baik untuk mencegah upaya tersebut.

9. *Covering Tracks*

Pada tahap ini, dilakukan upaya untuk menghilangkan jejak agar aktivitas tidak terdeteksi oleh sistem keamanan, salah satunya dengan menghapus *log* pada sistem. Penghapusan *log* bertujuan agar serangan yang telah dilakukan sebelumnya tidak dapat dilacak oleh sistem keamanan. Namun, upaya ini tidak berhasil karena kegagalan pada tahap-tahap sebelumnya. Hal tersebut terjadi karena sistem keamanan pada situs Pedulibaik.id telah dikonfigurasi dengan baik sehingga mampu mencegah akses lebih lanjut dan menahan upaya penyusupan.

V. KESIMPULAN

Penelitian keamanan pada situs web xyz menggunakan metode ISSAF yang terdiri dari 9 tahapan sistematis, mulai dari pengumpulan informasi hingga pemeliharaan akses. Melalui pengujian yang komprehensif, penelitian berhasil mengidentifikasi beberapa kerentanan kritis seperti DNS Server Spoofed Request Amplification DDoS dan DNS Server Recursive Query Cache Poisoning, serta miskonfigurasi server web yang berpotensi mengekspos metadata cloud menggunakan berbagai tools seperti Nikto, Whois, Nslookup, Nmap, dan OWASP ZAP. Meski ditemukan beberapa kerentanan, sistem keamanan web xyz terbukti telah dirancang dengan baik dan efektif dalam mencegah berbagai serangan umum seperti SQL Injection, XSS, session hijacking, dan Privilege Escalation, yang dibuktikan dengan gagalnya upaya eksploitasi menggunakan tools seperti sqlmap, Hydra, Metasploit, dan Burp Suite. Untuk meningkatkan keamanan lebih lanjut, disarankan untuk melakukan pembaruan perangkat lunak, memperbaiki konfigurasi server, dan menerapkan mekanisme keamanan tambahan seperti Web Application Firewall (WAF) dan Intrusion Detection System (IDS).

REFERENSI

[1] G. Oktavianti, “Pengantar Sistem Informasi,” 2019. [Online]. Available: https://www.researchgate.net/publication/331672535

[2] L. Kestina and G. Widi Nurcahyo, “Penanganan Celah Keamanan Website dengan Ethical Hacking dan Issaf Menggunakan Acunetix Vulnerability (Studi Kasus di Bkpsdmd Kabupaten Kerinci)”.

[3] Borislav Kiprin, “The 5 Penetration Testing Phases,” Veracode.

[4] L. Costaner and dan Musfawati, “Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF DAN OWASP (Studi Kasus OJS Universitas Lancang Kuning).”

[5] R. R. Asaad, “Penetration Testing: Wireless Network Attacks Method on Kali Linux OS,” *Academic Journal of Nawroz University*, vol. 10, no. 1, pp. 7–12, Feb. 2021, doi: 10.25007/ajnu.v10n1a998.

[6] A. A. Lubis, J. Pinem, M. Agus, S. Lubis, and D. Kiswanto, “Attribution-ShareAlike 4.0 International Some rights reserved Cient Server Implementasi Roundcube pada Mail Server untuk Lingkungan Program Studi Ilmu Komputer UNIMED”, doi: 10.12345/10.56211/blendsains.v1i3.163.

[7] R. Ashar, “Jurnal Informasi dan Teknologi Analisis Keamanan Open Website Menggunakan Metode OWASP dan ISSAF,” vol. 4, pp. 187–194, 2022, doi: 10.37034/jsisfotek.v4i4.233.

[8] N. Kade *et al.*, “Evaluation Security Web-Based Information System Application Using ISSAF Framework (Case Study: SIMAK-NG Udayana University),” 2020.

[9] M. Yunus, “Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework OWASP Versi 4,”

Jurnal Ilmiah Informatika Komputer, vol. 24, no. 1, pp. 37–48, 2019, doi: 10.35760/ik.2019.v24i1.1988.

[10] P. P. Anggraeni and Z. Pertahanan, "Security Analysis on Website Using the Information System Assessment Framework (ISSAF) and Open Web Application Security Version 4 (OWASPv4) Using the Penetration Testing Method," vol. 8, no. 3, pp. 2549–9459, 2022, doi: 10.33172/jp.v8.

[11] T. Revolino Syarif and D. Andri Jatmiko, "Analisis Perbandingan Metode Web Security PTES, ISSAF DAN OWASP di Dinas Komunikasi dan informasi Kota Bandung."

[12] T. D. H. Abdul Fattah Hasibuan, "Analisis Keretanan Website Dengan Aplikasi Owasp Zap," *JIRSI*, May 2023.

[13] S. Andriyani, M. Fajar Sidiq, and B. Parga Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," 2023.

[14] S. Utoro *et al.*, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard."

[15] M. A. Z. Risky and Y. Yuhandri, "Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS," *Jurnal Sistim Informasi dan Teknologi*, pp. 215–220, Aug. 2021, doi: 10.37034/jsisfotek.v3i4.68.