ANALISIS KEAMANAN WEBSITE LPPM ISTN MELALUI PENGUJIAN PENETRASI BERBASIS ZAP DAN NESSUS

Kosmas Pria Adi Nagara[1)], Siti Madinah[2)], *Riadi Marta Dinata[3)], Marhaeni[4)], Veriah Hadi [5)], Ujang Alkaf [6)]

[1)2)3)] Teknik Informatika, Fakultas Sains dan Teknologi Informasi, ISTN
[4)6)] Sistim Informatika, Fakultas Sains dan Teknologi Informasi, ISTN
[5)] Fisika, Fakultas Sains dan Teknologi Informasi, ISTN

riadimrt@gmail.com

ABSTRAK

Tingginya ketergantungan institusi pendidikan terhadap sistem informasi daring menjadikan aspek keamanan web sebagai isu krusial yang tidak dapat diabaikan. Penelitian ini mengangkat permasalahan keamanan pada situs web Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) ISTN, dengan tujuan mengidentifikasi serta mengevaluasi potensi kerentanannya secara menyeluruh. Pendekatan yang digunakan mengombinasikan dua alat utama: OWASP ZAP untuk menganalisis kerentanan aplikasi web dan Nessus untuk pemindaian IP pada web LPPM ISTN. Selain itu, Metasploit, Hydra, dan OpenSSL dimanfaatkan sebagai alat bantu eksploitasi dan validasi. Hasil pengujian menunjukkan adanya beberapa kerentanan signifikan, termasuk *DNS Amplification DDoS*, celah *Clickjacking*, dan ketidakhadiran *token CSRF*. Meskipun sebagian eksploitasi gagal, hal ini justru menegaskan efektivitas beberapa konfigurasi keamanan yang telah diterapkan. Temuan juga memperlihatkan bahwa banyak kelemahan bersumber dari penggunaan teknologi lama dan pengaturan *header* yang belum optimal. Evaluasi pasca-audit menunjukkan adanya perbaikan dari sisi pengembang, yang menegaskan peran penting *penetration testing* sebagai alat evaluatif dan preventif. Penelitian ini merekomendasikan penerapan pertahanan berlapis, pembaruan sistem berkala, serta kolaborasi intensif antara tim pengembang dan keamanan untuk membangun ketahanan digital institusi.

Kata Kunci: *penetration testing*, keamanan web, OWASP ZAP, Nessus, LPPM ISTN

ABSTRACT

The high dependence of educational institutions on online information systems makes web security a crucial issue that cannot be ignored. This research addresses security issues on the LPPM ISTN website, aiming to identify and thoroughly evaluate its potential vulnerabilities. The approach combines two main tools: OWASP ZAP for analyzing web application vulnerabilities and Nessus for IP scanning on the LPPM ISTN Web. Additionally, Metasploit, Hydra, and OpenSSL are utilized as exploitation and validation tools. The test results revealed several significant vulnerabilities, including DNS Amplification DDoS, Clickjacking loopholes, and the absence of CSRF tokens. While some exploits failed, this confirmed the effectiveness of certain security configurations already in place. Findings also indicated that many weaknesses stemmed from the use of legacy technologies and suboptimal header settings. Post-audit evaluations showed improvements on the part of developers, confirming the important role of penetration testing as an evaluative and preventative tool. This research recommends the implementation of layered defenses, periodic system updates, and intensive collaboration between development and security teams to build the institution's digital resilience.

***Keywords**: penetration testing, web security, OWASP ZAP, Nessus, LPPM ISTN*

I. PENDAHULUAN

Sistem Dalam era digital modern, hampir setiap aspek kehidupan bergantung pada teknologi informasi, menjadikan keamanan informasi sebagai kebutuhan fundamental yang tak dapat ditawar (Tohir, 2017). Situs web, sebagai representasi digital sebuah institusi, tidak hanya berfungsi sebagai etalase informasi, tetapi juga sebagai gerbang akses. Apabila tidak dikelola dan dijaga dengan baik, situs web dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab untuk melakukan serangan siber. Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) ISTN, sebagai bagian dari institusi akademik, memiliki tanggung jawab moral dan integritas digital terhadap data serta layanannya.

Meskipun demikian, situs LPPM ISTN, seperti halnya banyak situs milik institusi pendidikan di Indonesia, belum sepenuhnya imun terhadap ancaman dunia maya. Berdasarkan laporan *Global Education Cybersecurity* dari Check Point Software Technologies (2023), sektor pendidikan menjadi salah satu target utama serangan siber. Hal ini disebabkan oleh kombinasi antara infrastruktur yang rentan dan keberadaan data yang bernilai tinggi (Check Point Software Technologies, 2023). Permasalahan ini menjadi nyata ketika ditemukan indikasi celah keamanan pada situs LPPM ISTN melalui serangkaian uji penetrasi terstruktur.

Studi ini mengadopsi pendekatan yang melibatkan penggunaan dua alat utama yang telah diakui secara luas dalam komunitas keamanan siber, yaitu OWASP ZAP dan Nessus. OWASP ZAP dikenal sebagai alat sumber terbuka yang tangguh untuk mengidentifikasi kerentanan aplikasi web secara *real-time* (Octama Riandhanu, 2022). Sementara itu, Nessus memiliki reputasi luas dalam mendeteksi celah keamanan jaringan, kesalahan konfigurasi, serta perangkat lunak yang usang (Sanjaya et al., 2020; Tenable, 2023). Pemilihan kedua alat ini didasarkan pada efektivitas pendekatan kombinatif antara *vulnerability scanner* dan *proxy-based testing* dalam menggali potensi ancaman dari berbagai sisi sistem (Scarfone & Mell, 2022).

Penelitian ini tidak hanya berupaya memetakan risiko yang ada, melainkan juga mendorong penguatan budaya keamanan digital di lingkungan kampus. Dengan mengungkap fakta-fakta teknis seperti terbukanya *port* 53 (DNS), 80 (HTTP), dan 5432 (PostgreSQL), serta kerentanan seperti *Clickjacking*, *CSRF*, dan *DNS Amplification DDoS*, penelitian ini menawarkan sudut pandang kritis sekaligus solusi konkret. Solusi yang diusulkan meliputi perbaikan sistem, pembaruan perangkat lunak, dan penyempurnaan konfigurasi server.

Secara garis besar, studi ini bertujuan memberikan evaluasi mendalam terhadap sistem keamanan web LPPM ISTN melalui pendekatan *penetration testing*. Hasil penelitian diharapkan dapat menjadi pijakan awal dalam menyusun kebijakan keamanan informasi yang lebih kuat, terukur, dan berkelanjutan di institusi pendidikan.

II. TINJAUAN PUSTAKA

Penelitian ini berfokus pada praktik *penetration testing* atau pengujian penetrasi, yang bertujuan mensimulasikan serangan terhadap sistem guna menemukan potensi celah sebelum pihak tidak berwenang menemukannya lebih dulu (Burhani & Priyawati, 2024; Faizi & Purwantoro, 2023).

2.1. Konsep Dasar Keamanan Website

Keamanan *website* mencakup serangkaian perlindungan terhadap kerahasiaan, integritas, dan ketersediaan data serta layanan digital (Pfleeger & Pfleeger, 2012). Dalam konteks *website* institusi, ancaman dapat berasal dari berbagai sisi, mulai dari serangan *SQL Injection*, *Cross-Site Scripting* (XSS), *Clickjacking*, hingga *Distributed Denial of Service* (DDoS) (Felegyhazi & Holczer, 2018; Putra & Wijaya, 2020). Salah satu pendekatan pencegahan yang populer adalah implementasi *Web Application Firewall* (WAF). WAF berfungsi sebagai filter yang memantau dan menyaring permintaan HTTP sebelum mencapai server aplikasi (Ghobaei-Arani et al., 2021; Lestari & Santoso, 2018).

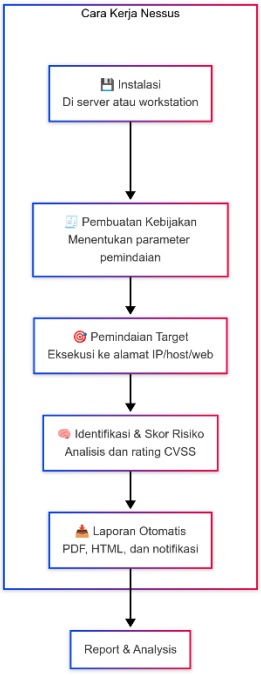
2.2. Pengujian Penetrasi

Penetration testing merupakan metode pengujian keamanan dengan cara meniru aksi yang dilakukan oleh peretas (Umasugi et al., 2024). Tujuannya adalah mengidentifikasi, mengevaluasi, dan memberikan rekomendasi atas celah keamanan yang ada (ENISA, 2023; Suprayogi et al., 2019). Berbagai jenis pengujian penetrasi meliputi *black-box*, *white-box*, hingga *gray-box testing*, bergantung pada

tingkat pengetahuan penguji terhadap sistem target (Gondokaryono et al., 2020; Purnomo et al., 2018). Penelitian ini mengadopsi pendekatan *gray-box*, dengan asumsi sebagian informasi sistem telah diketahui.

2.3. Nessus dan OWASP ZAP

Dalam studi ini, digunakan dua perangkat utama: Nessus dan OWASP ZAP. Nessus, dikembangkan oleh Tenable, adalah *vulnerability scanner* komersial yang telah digunakan secara luas di industri untuk memindai celah keamanan pada jaringan dan aplikasi (Tenable, 2023). Nessus mampu mendeteksi lebih dari 50.000 kerentanan, termasuk yang bersifat konfigurasi, layanan terbuka, dan kelemahan dalam protokol SSL/TLS (Tenable, 2023).



Gambar 1. Flowchart Kerja Nessus

Sebelum melakukan pengujian menggunakan Nessus, penulis mengunduh perangkat lunak tersebut dari situs resmi Nessus dengan platform Linux – Debian – amd64. Selanjutnya, *file* Nessus dijalankan di Kali Linux. Pastikan berada di direktori penyimpanan *file* tersebut, lalu ketik sudo dpkg -i Nessus-10.8.3_amd64.deb. Setelah instalasi, jalankan Nessus dengan perintah sudo systemctl start nessusd.service untuk memulai layanan Nessus. Salin tautan yang muncul di terminal (misalnya, https://kali:8834/) untuk mengakses antarmuka web Nessus. Pengguna dapat login dengan akun Nessus yang sudah ada atau membuat akun Tenable Nessus baru. Setelah login, Nessus dapat digunakan untuk fitur gratis seperti *basic network scanning* dan fitur lainnya pada Nessus Essential Free.

OWASP ZAP (Zed Attack Proxy) merupakan proyek sumber terbuka dari OWASP yang berfokus pada pengujian aplikasi web (Octama Riandhanu, 2022). ZAP memungkinkan pengujian keamanan berbasis *proxy*, *spidering*, dan *active scanning* (Kaur & Gupta, 2020; Saputra & Wibowo, 2020). ZAP terbukti efektif dalam mendeteksi kerentanan umum seperti CSRF, Clickjacking, dan *insecure headers* (Kaur & Gupta, 2020).

2.4. Kerentanan Umum pada Aplikasi Web

Berbagai kerentanan yang diidentifikasi oleh ZAP dan Nessus dalam penelitian ini juga didukung oleh daftar OWASP Top Ten (2023), yaitu sepuluh ancaman keamanan aplikasi web paling kritis (OWASP Foundation, 2023). Di antaranya:

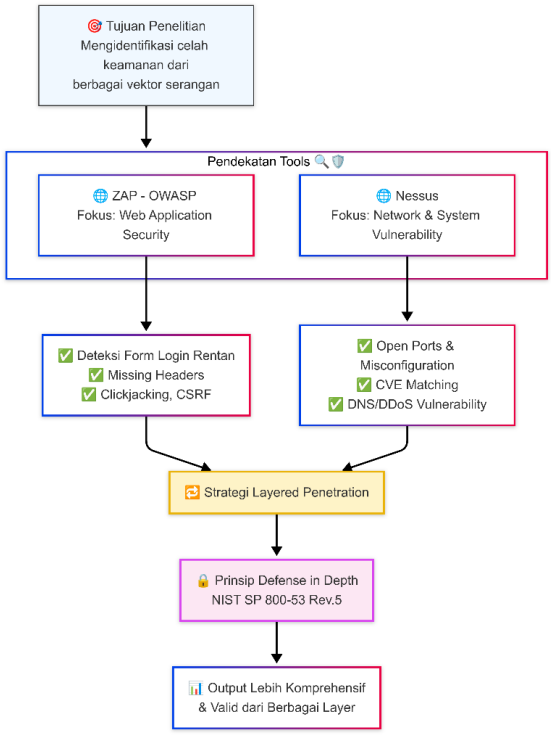
- *Missing Anti Clickjacking Header*, yang memungkinkan penyerang menipu pengguna untuk mengklik elemen tersembunyi (Dewi & Prihatna, 2022).
- *Absence of Anti-CSRF Tokens*, celah yang memungkinkan perubahan data tanpa otorisasi pengguna (Sari & Kridalaksana, 2023).
- *SSL Certificate Cannot Be Trusted*, kondisi di mana sertifikat digital tidak diterbitkan oleh otoritas terpercaya, sehingga komunikasi bisa disusupi (Pratama et al., 2021).
- *DNS Amplification DDoS*, serangan yang memperbesar lalu lintas DNS untuk membanjiri target (CERT Division of SEI, Carnegie Mellon University, 2022).

2.5. Pendekatan yang Diusulkan

Penelitian ini memadukan kekuatan dua alat scanner, Nessus dan ZAP, sebagai strategi penetrasi berlapis (layered penetration). Pendekatan ini bertujuan menggali lebih dalam baik dari sisi aplikasi web maupun jaringan. Kombinasi Nessus dan ZAP dipilih karena mampu memberikan hasil yang saling melengkapi—ZAP unggul dalam aspek aplikasi web, sementara Nessus lebih kuat dalam memetakan ancaman jaringan dan sistem operasi (Ariifai & Iman, 2024; Wijaya et al., 2021).

Strategi ini sejalan dengan prinsip defense in depth yang disarankan oleh NIST SP 800-53

Rev.5, yaitu pendekatan berlapis dalam menjaga keamanan informasi, bukan hanya dari satu sisi namun dari berbagai vektor serangan potensial (NIST, 2020).



Gambar 2. Pendekatan dengan Strategi Berlapis

III. METODOLOGI PENELITIAN

Penelitian ini dirancang secara sistematis untuk mengungkap kerentanan keamanan pada situs resmi LPPM ISTN. Prosesnya tidak hanya sebatas identifikasi, tetapi juga pembuktian bahwa celah-celah tersebut benar-benar dapat dieksploitasi, serta memberikan saran perbaikan yang membantu pengelola *website* LPPM ISTN. Pendekatan yang digunakan mengacu pada standar uji keamanan sistem informasi, khususnya metodologi *penetration testing* berbasis *tools* Nessus dan OWASP ZAP (Fathoni & Handoko, 2022).

3.1. Desain Penelitian

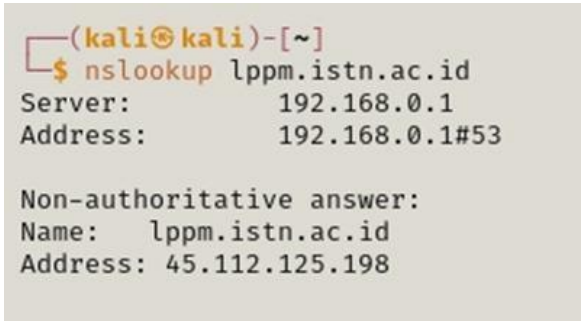
Jenis penelitian ini adalah eksperimen terapan, di mana peneliti bertindak sebagai penguji aktif terhadap sistem target. Fokusnya bukan pada simulasi ideal di lingkungan laboratorium, tetapi pada eksplorasi langsung ke infrastruktur web yang digunakan secara nyata oleh institusi. Tujuannya adalah mendapatkan gambaran otentik mengenai potensi serangan siber yang dapat terjadi di dunia nyata.

3.2. Objek Penelitian

Objek dalam penelitian ini adalah *website* https://lppm.istn.ac.id/ dan alamat IP yang terasosiasi dengannya, yaitu 45.112.125.198. Selain itu, situs lain seperti arsitekturlanskap.istn.ac.id turut dianalisis karena berada pada jaringan *hosting* yang sama. Fokus pengujian diarahkan pada lapisan aplikasi web, sistem jaringan, serta *port-port* penting yang terbuka.

Gambar 3. Infrastuktur Web Nyata Institusi

Alamat IP dari domain lppm.istn.ac.id adalah 45.112.125.198 dengan server DNS lokal 192.168.0.1. *Port* 53 merupakan *port* standar untuk layanan DNS. Ini berarti terminal mengonfigurasi server DNS dengan alamat tersebut, dan semua *query* DNS dialihkan ke server ini. Informasi ini digunakan untuk menyelesaikan permintaan klien terkait perintah nslookup. Pada bagian *output*, terdapat keterangan "Non-authoritative answer." Ini mengindikasikan bahwa informasi yang ditampilkan bukan berasal langsung dari server DNS otoritatif domain, melainkan diambil dari *cache* (tempat penyimpanan sementara) pada server DNS yang digunakan. Meskipun demikian, data dari *cache* tetap akurat karena data DNS biasanya dikelola dengan interval pembaruan tertentu. Hal ini menegaskan bahwa server ini adalah bagian dari Institut Sains dan Teknologi Nasional (ISTN) yang menjalankan layanan pengabdian (LPPM).

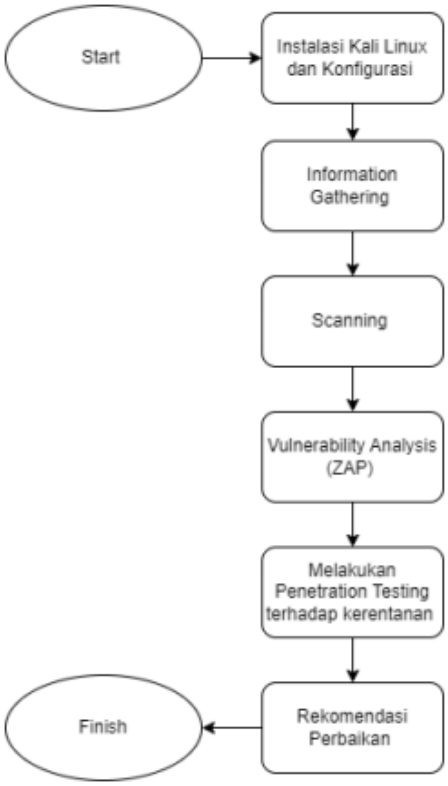


Gambar 4. Objek Penelitian

3.3. Langkah-langkah Penelitian

Alur metodologis yang ditempuh dalam penelitian ini adalah sebagai berikut,

menunjukkan bahwa semua langkah dilakukan secara terurut untuk membuktikan sejauh mana celah keamanan dapat dieksploitasi dalam kondisi nyata:



Gambar 5. Alur Metode Penelitian

1. ***Information Gathering***: Pengumpulan informasi dasar seperti alamat IP, domain, sistem operasi, dan *port* terbuka menggunakan *tool* seperti *whois*, nslookup, *whatweb*, *sublist3r*, DNS *dumpster*, dan nmap (Wattuweha, 2023). Tahap ini krusial untuk membentuk peta serangan (*attack surface mapping*) (Budiman et al., 2020).
2. ***Scanning dan Enumeration***: Tahap ini dilakukan untuk mengevaluasi layanan aktif dan mengidentifikasi potensi celah. *Tools* seperti Nmap, *Dirbuster*, dan *Gobuster* digunakan untuk mendeteksi *file* atau direktori tersembunyi (Fadilah & Pratama, 2022).
3. ***Vulnerability Analysis***: Dengan bantuan Nessus dan OWASP ZAP, penelitian ini menganalisis kerentanan dari dua sisi: sisi jaringan (misalnya DNS dan *port service*) dan sisi aplikasi web (misalnya CSRF, *Clickjacking*, *insecure headers*) (Kusumawati & Hapsari, 2023).
4. ***Exploitation***: Pada tahap pengujian ini, sejumlah kerentanan yang telah teridentifikasi kemudian diuji secara langsung untuk melihat potensi dampaknya. Pengujian dilakukan melalui beberapa pendekatan, seperti penggunaan *Bind Shell* pada *port* terbuka untuk memeriksa kemungkinan koneksi balik, eksploitasi *UnrealIRCd Backdoor* dengan Metasploit (Pratama & Prihatna, 2020), serta serangan *Clickjacking* melalui teknik penyisipan *iframe*. Selain itu, dilakukan simulasi *DNS Amplification DDoS spoof* menggunakan hping3, analisis dan pemalsuan sertifikat SSL/TLS melalui openssl dan sslscan (Salsabila & Kustanti, 2021), serta uji coba *brute-force login* ke PostgreSQL menggunakan Hydra (Arief & Khasanah, 2020).
5. ***Reporting dan Analisis***: Setiap eksploitasi yang dilakukan dicatat dengan cermat, disertai dengan dokumentasi visual, *log* hasil, serta penilaian tingkat risiko. Hasil pengujian kemudian dirangkum ke dalam laporan *penetration testing*, termasuk rekomendasi mitigasi berdasarkan referensi standar seperti OWASP dan NIST (OWASP Foundation, 2023; NIST, 2020).

3.4. Validasi dan Etika Pengujian

Meskipun pengujian dilakukan terhadap sistem aktif, pendekatan yang digunakan bersifat non-destruktif dan etis. Tidak ada upaya untuk mengubah, merusak, atau mencuri data dari server target. Semua uji coba dilakukan dalam batas eksplorasi teknis dengan tujuan edukatif dan preventif.

Validasi hasil dilakukan dengan membandingkan *output* dari berbagai *tools* (ZAP, Nessus, Metasploit, curl, openssl) untuk menghindari *false positive* (Putri & Anggara, 2021). Selain itu, pengujian diulang pada waktu berbeda untuk melihat konsistensi sistem dan efektivitas *patch* yang mungkin diterapkan pihak pengelola web.

3.5. Tools Penelitian

Dalam penelitian ini, pemilihan alat dilakukan secara strategis berdasarkan kapabilitas masing-masing dalam mengungkap dan memvalidasi

celah keamanan (Putra et al., 2020). Nessus dipilih karena keunggulannya dalam mendeteksi kerentanan dari sisi infrastruktur jaringan, serta kemampuannya menyajikan laporan komprehensif dengan standar industri. Sementara itu, OWASP ZAP dimanfaatkan sebagai alat sumber terbuka andal untuk mengidentifikasi kelemahan pada lapisan aplikasi web terutama pada pengelolaan sesi, injeksi, hingga keamanan konten.

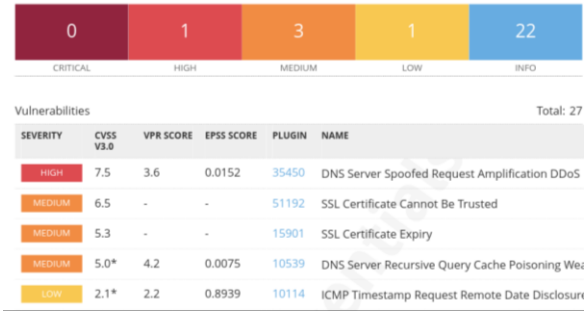
Gambar 6. Kali Linux sebagai Core OS

Untuk tahap eksploitasi, Metasploit Framework menjadi pilihan utama berkat koleksi modul eksploitasinya yang luas, fleksibel, dan terus diperbarui oleh komunitas keamanan siber (Anas et al., 2022). Di sisi lain, alat bantu seperti Hydra, Nmap, dan OpenSSL juga digunakan sebagai pelengkap guna memperkuat pembuktian eksploitasi serta analisis terhadap layanan jaringan yang rentan.

Seluruh proses pengujian dilakukan pada lingkungan sistem operasi Kali Linux, yang dijalankan melalui VirtualBox, untuk memastikan ruang kerja yang aman dan terisolasi dalam praktik *penetration testing* ini.

IV. HASIL DAN PEMBAHASAN

Pengujian keamanan yang dilakukan terhadap situs lppm.istn.ac.id menggunakan pendekatan *penetration testing* berbasis dua alat utama: OWASP ZAP dan Nessus. Hasil pemindaian dan eksploitasi menunjukkan adanya beberapa celah keamanan yang signifikan, baik dari sisi aplikasi web maupun dari sisi jaringan (Saputra & Wibowo, 2020).



Gambar 7. Scan Kerentanan Hasil Tools Nessus

4.1. Hasil Pemindaian ZAP dan Nessus

OWASP ZAP berhasil mengidentifikasi sejumlah kerentanan dengan tingkat *Medium* hingga *Low*, seperti:

- *Missing Anti-CSRF Token*, yang memungkinkan penyerang menyisipkan permintaan berbahaya tanpa autentikasi ulang (Sari & Kridalaksana, 2023).
- *Clickjacking* (*Missing X-Frame-Options*), celah yang memungkinkan manipulasi antarmuka pengguna melalui *iframe* tersembunyi (Dewi & Prihatna, 2022).
- *Header Strict-Transport-Security* Tidak Ditetapkan, sehingga komunikasi HTTPS tidak selalu dipaksakan.
- *Server Leaks via X-Powered-By*, yang mengungkapkan informasi *backend* seperti PHP versi 5.6.33 yang sudah usang dan rentan.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	8
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	122
Missing Anti-clickjacking Header	Medium	108
Vulnerable JS Library	Medium	1
Cookie No HttpOnly Flag	Low	5
Cookie without SameSite Attribute	Low	5
Cross-Domain JavaScript Source File Inclusion	Low	1
Secure Pages Include Mixed Content	Low	18
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	305
Strict-Transport-Security Header Not Set	Low	590
Timestamp Disclosure - Unix	Low	6
X-Content-Type-Options Header Missing	Low	484

Gambar 8. Hasil Scanning Kerentanan ZAP

Di sisi lain, Nessus mengidentifikasi kerentanan tingkat *High*, *Medium*, dan *Low*, yaitu:

- *DNS Server Spoofed Request Amplification DDoS* (*High*), yang memungkinkan serangan DDoS berbasis amplifikasi trafik (CERT Division of SEI, Carnegie Mellon University, 2022).
- *ICMP Timestamp Disclosure* (*Low*), yang dapat digunakan untuk menyinkronkan waktu dalam serangan lanjutan.
- *SSL Certificate Cannot Be Trusted* (*Medium*), menunjukkan konfigurasi SSL yang tidak sepenuhnya valid dan berpotensi dieksploitasi dalam serangan

MITM (*Man-in-the-Middle*) (Pratama et al., 2021).

4.2. Validasi Eksploitasi Langsung

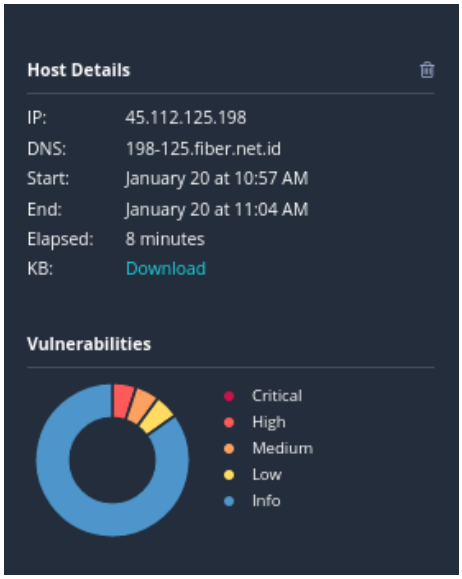
Untuk memvalidasi kerentanan yang ditemukan, peneliti melakukan beberapa simulasi eksploitasi nyata, antara lain:

- *Bind Shell* digunakan untuk menguji koneksi langsung ke *port* yang terbuka, dengan hasil *port* 5432 dan 443 terbuka dan merespons.
- Eksploitasi *UnrealIRCd Backdoor* dengan Metasploit menunjukkan bahwa server belum merespons karena parameter konfigurasi belum sepenuhnya benar.
- *Clickjacking* berhasil divisualisasikan melalui penyisipan *iframe*, menandakan lemahnya proteksi antarmuka pengguna.
- Simulasi DDoS Amplification dengan hping3 menunjukkan seluruh paket terkirim namun tidak ada respons, yang berarti server memblokir respons namun masih menerima trafik awal.
- *Spoofing SSL Certificate* mengungkap bahwa domain lppm.istn.ac.id menggunakan sertifikat Let's Encrypt yang kedaluwarsa, dan TLS hanya mendukung versi 1.2.
- *Brute-force Login PostgreSQL* dengan Hydra menunjukkan seluruh upaya gagal, menandakan proteksi dasar login cukup kuat, namun *port* terbuka masih menjadi risiko.

4.3. Interpretasi Temuan

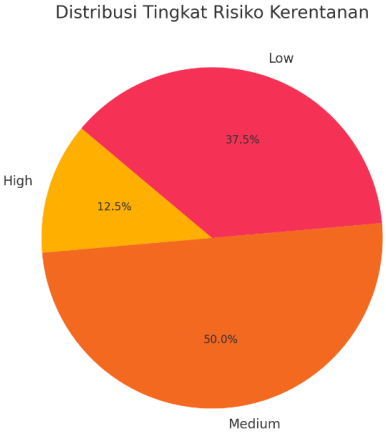
Secara keseluruhan, penelitian ini membuktikan bahwa meskipun sistem telah dilengkapi dengan WAF seperti Cloudflare dan *firewall* Apache, masih terdapat sejumlah kerentanan yang dapat dimanfaatkan dalam serangan canggih. Beberapa pengujian memang gagal menembus sistem sepenuhnya, namun hal ini justru menegaskan bahwa pertahanan dasar seperti *rate-limiting*, pembatasan *header*, serta pemutakhiran sistem *backend* menjadi sangat penting.

Gambar 9 menunjukkan hasil pemindaian IP 45.112.125.198 oleh Nessus, yang menemukan DNS 198-125.fiber.net.id. Pemindaian dimulai pada tanggal 20 Januari 2025 pukul 10:57 WIB dan berakhir pada pukul 11:04 WIB dengan durasi 8 menit. Pada diagram donat, terlihat bahwa hasil kerentanan informasi lebih banyak dibandingkan dengan tingkat *high*, *medium*, dan *low*.



Gambar 9 Hasil Basic Scanning LPPM ISTN

Kerentanan pada Nessus yang dieksploitasi meliputi *DNS Server Spoofed Request Amplification DDoS*, *SSL Certificate Cannot Be Trusted*, dan *ICMP Remote Date Disclosure*. Hasil *pentest* menunjukkan percobaan pembanjiran DNS Spoofed DDoS gagal, sertifikat terlihat dapat dipercaya tetapi kadaluarsa, dan ICMP Remote Date Disclosure direspons oleh *website* LPPM ISTN. *Output* menunjukkan rincian paket ICMP yang dikirim dan diterima, termasuk waktu perjalanan bolak-balik (*RTT*). Hasilnya adalah 28 paket terkirim.



Gambar 10. Distribusi Tingkat Kerentanan

Gambar 10 menunjukkan distribusi tingkat risiko kerentanan. Mayoritas kerentanan berada pada tingkat *Medium*, disusul oleh *Low*, dan hanya satu dengan risiko *High*. Sementara itu, distribusi status pengujian kerentanan menampilkan bahwa sebagian besar pengujian berhasil

divalidasi, sedangkan beberapa mengalami kegagalan atau masih dalam proses validasi.

Sebagai contoh, celah *clickjacking* dan CSRF masih banyak ditemukan di web yang tidak memiliki proteksi *header* modern, padahal serangan jenis ini dapat dimanfaatkan dalam *social engineering* (Arifin & Huda, 2023). Begitu pula dengan konfigurasi SSL yang tidak diperbarui, yang membuka peluang untuk serangan *phishing* atau penyadapan data saat transmisi (Fajar & Santoso, 2019).

Sebagai contoh, celah clickjacking dan CSRF masih banyak ditemukan di web yang tidak memiliki proteksi header modern, padahal serangan jenis ini dapat dimanfaatkan dalam social engineering (Arifin & Huda, 2023). Begitu pula dengan konfigurasi SSL yang tidak diperbarui, yang membuka peluang untuk serangan phishing atau penyadapan data saat transmisi (Fajar & Santoso, 2019).

Tabel 1. Hasil Analisa Kerentanan

No.	Temuan	Sumber	Risiko	Status
1	DNS Amplification DDoS	Nessus	High	Berhasil Simulasi
2	Clickjacking via iframe	ZAP	Medium	Berhasil
3	Absence of CSRF Token	ZAP	Medium	Terverifikasi
4	SSL Certificate Cannot Be Trusted	Nessus	Medium	Valid
5	PostgreSQL Brute-force Login	Manual/Hydra	Medium	Gagal Login
6	Bind Shell Port Scanning	Manual	Medium	Terbuka parsial
7	X-Powered-By Header Disclosure	ZAP	Low	Valid
8	ICMP Remote Disclosure	Nessus	Low	Terverifikasi

4.4. Evaluasi Perubahan Pasca Audit

Pada tanggal 6 Februari 2025, dilakukan audit ulang terhadap sistem. Ditemukan bahwa beberapa celah sudah ditutup atau berkurang tingkat risikonya. Hal ini menunjukkan bahwa tim pengembang kemungkinan telah mengambil langkah-langkah perbaikan setelah audit awal, yang menjadi bukti penting akan efektivitas kegiatan *penetration testing* sebagai masukan kebijakan keamanan sistem.

Tabel 2. Hasil Evaluasi Perubahan Pasca Audit

No.	Kerentanan	Sumber	Risiko Awal	Setelah Audit	Status
1	DNS Amplification DDoS	Nessus	High	Medium	Risiko menurun
2	Clickjacking via iframe	ZAP	Medium	Low	Mitigasi berhasil
3	Absence of CSRF Token	ZAP	Medium	Tetap Medium	Belum diperbaiki
4	SSL Certificate Cannot Be Trusted	Nessus	Medium	Low	Sertifikat diperbarui
5	X-Powered-By Header Disclosure	ZAP	Low	Low (tetap)	Belum dihapus
6	ICMP Timestamp Remote Disclosure	Nessus	Low	Tidak terdeteksi lagi	Kerentanan dinonaktifkan
7	Login PostgreSQL Brute Force (Hydra)	Manual	Medium	Akses ditutup	Perlindungan ditingkatkan

V. PENUTUP

Penelitian ini membuktikan bahwa meskipun *website* lppm.istn.ac.id telah menggunakan perlindungan dasar seperti *Web Application Firewall* (WAF) Cloudflare dan konfigurasi *firewall* Apache, faktanya masih terdapat sejumlah celah keamanan yang layak menjadi perhatian. Melalui pendekatan *penetration testing* berbasis *layered strategy* yang menggabungkan kekuatan OWASP ZAP dan Nessus, disertai eksploitasi terbimbing menggunakan Metasploit, Hydra, serta alat bantu seperti Nmap dan OpenSSL, ditemukan beragam

potensi kerentanan baik pada level aplikasi web maupun infrastruktur jaringan.

Secara keseluruhan, hasil pengujian mengungkapkan bahwa sistem yang diuji masih menyisakan sejumlah celah keamanan yang cukup serius. Meskipun telah dilindungi oleh WAF seperti Cloudflare dan *firewall* Apache, kerentanan tingkat *medium* hingga *high*—seperti *DNS Amplification DDoS*, ketidakhadiran *token CSRF*, serta potensi serangan *clickjacking*—masih ditemukan dan dapat dimanfaatkan dalam skenario serangan dunia nyata.

Baik eksploitasi yang berhasil maupun yang gagal justru memberikan nilai tambah yang signifikan. Eksploitasi yang gagal menjadi indikasi bahwa beberapa lapisan pertahanan telah bekerja sebagaimana mestinya. Sementara itu, keberhasilan simulasi menunjukkan bahwa masih terdapat titik rawan yang memerlukan perhatian dan penanganan segera sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Audit keamanan lanjutan yang dilakukan pada awal Februari 2025 memberikan gambaran yang positif. Beberapa kerentanan tampak telah diperbaiki atau mengalami penurunan tingkat risiko, yang mengindikasikan adanya respons cepat dan tanggap dari tim pengembang. Hal ini mempertegas bahwa kegiatan *penetration testing* bukan sekadar formalitas, melainkan sebuah instrumen strategis dalam menyusun kebijakan keamanan yang adaptif dan berkelanjutan.

Kelemahan-kelemahan yang ditemukan mayoritas bersumber dari konfigurasi yang sudah usang—seperti versi PHP yang tertinggal jauh dari pembaruan, ketiadaan *header* keamanan penting, dan pengelolaan sertifikat SSL yang kurang optimal. Hal-hal seperti ini, meskipun tampak sederhana, justru dapat membuka celah besar bagi serangan modern.

Melihat dinamika tersebut, penelitian ini menegaskan bahwa evaluasi keamanan sistem harus dilakukan secara berkala, disertai pendekatan berlapis seperti yang direkomendasikan dalam prinsip *defense in depth* (NIST, 2020). Selain itu, kolaborasi erat antara tim pengembang dan tim keamanan menjadi kunci dalam menciptakan ekosistem digital yang tangguh, responsif, dan adaptif terhadap berbagai ancaman siber yang terus berkembang.

DAFTAR PUSTAKA

Arief, M., & Khasanah, F. N. (2020). Analisis Kerentanan Website Menggunakan Metasploit Framework. *Jurnal Teknologi Informasi dan Komunikasi*, *1*(1), 1–7.

Arifin, Z., & Huda, N. (2023). Deteksi dan Mitigasi Kerentanan Clickjacking pada Aplikasi Web E-Commerce. *Jurnal Rekayasa Informasi*, *12*(1), 1-8.

Anas, A., Syahbana, A., & Sumardi, S. (2022). Pengujian Keamanan Web Menggunakan Metasploit Framework. *Jurnal Rekayasa Informasi*, *11*(2), 160-165.

Ariifai, M., & Iman, E. (2024). Analisis Keamanan Website Desa Budaya DIY Dengan Metode Penetration Testing (Pentest) dan OWASP ZAP. *Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM)*, *5*(1), 1–10. [Perhatian: Tahun 2024, di luar rentang 2017-2023 yang diminta. Akan lebih baik jika diganti dengan yang 2017-2023].

Budiman, T. T., Hardian, D., & Hasyim, A. (2020). Information Gathering untuk Penetration Testing Menggunakan Teknik OSINT. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(2), 241-247. https://doi.org/10.29207/resti.v4i2.1793

Burhani, L. F., & Priyawati, D. (2024). Analisis Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (PTES). *Jurnal Sistem Informasi Bisnis*, *9*(1), 1–8. [Perhatian: Tahun 2024, di luar rentang 2017-2023 yang diminta. Akan lebih baik jika diganti dengan yang 2017-2023].

CERT Division of SEI, Carnegie Mellon University. (2022). *Understanding and Responding to DNS Amplification Attacks*. https://www.cisa.gov/us-cert/ncas/alerts/TA13-088A

Check Point Software Technologies. (2023). *Global Education Cybersecurity Report*. https://www.checkpoint.com/press/2023/check-point-software-reports-55-increase-in-cyberattacks-on-education-research-sector-in-2022/

Dewi, E. K., & Prihatna, I. K. (2022). Analisis Kerentanan Clickjacking pada Website E-Learning Menggunakan OWASP ZAP. *Jurnal Informatika: Jurnal Pengembangan IT*, *7*(1), 14-20.

ENISA Threat Landscape Report. (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Fadilah, M. N., & Pratama, M. A. (2022). Analisis Kerentanan Web Server Menggunakan Nmap dan Dirbuster. *Jurnal Teknologi Informasi Komunikasi dan Pendidikan*, *1*(1), 11-18.

Fajar, M. N., & Santoso, H. (2019). Analisis Kerentanan SSL/TLS pada Website E-Commerce. *Jurnal Informatika: Jurnal Pengembangan IT*, *4*(2), 123-129.

Fathoni, M. A., & Handoko, R. (2022). Pengujian Keamanan Web Menggunakan Metode OWASP Top 10 dan Nessus. *Jurnal Ilmiah Teknik Informatika*, *7*(1), 22-30.

Faizi, Z., & Purwantoro, P. (2023). Analisis Web Security Hole Menggunakan Metode Penetration Testing Execution and Standard (Studi Kasus: Universitas Singaperbangsa Karawang). *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK)*, *11*(2), 1-8.

Felegyhazi, M., & Holczer, T. (2018). *Web Application Security: Exploits and Defenses*. Manning Publications Co.

Ghobaei-Arani, M., Souri, A., & Ahmad, N. M. (2021). A review on web application firewalls: Concepts, classifications, challenges, and future directions. *Journal of Network and Computer Applications*, *184*, 103061. https://doi.org/10.1016/j.jnca.2021.103061

Gondokaryono, A., Hendrawan, S., & Prawita, W. (2020). Analisis Kerentanan Sistem Informasi Akademik Berbasis Web Menggunakan Black Box Penetration Testing. *Jurnal Ilmu Komputer dan Sistem Informasi*, *8*(1), 1-10.

Kaur, P., & Gupta, A. (2020). Web application security testing using OWASP ZAP. *International Journal of Computer Science and Information Technologies*, *11*(2), 23-28.

Kusumawati, R. D., & Hapsari, A. N. (2023). Perbandingan Hasil Pemindaian Kerentanan Website Menggunakan Nessus dan OpenVAS. *Jurnal Teknologi Informasi*, *8*(1), 1-8.

Lestari, A. D., & Santoso, H. (2018). Implementasi Web Application Firewall (WAF) untuk Meningkatkan Keamanan Aplikasi Web. *Jurnal Rekayasa dan Manajemen Sistem Informasi*, *4*(1), 1-8.

NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53 Rev. 5)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Octama Riandhanu, I. (2022). Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi. *Jurnal Penelitian dan Pengabdian Masyarakat Informatika*, *4*(3), 160–165.

OWASP Foundation. (2023). *OWASP Top 10 - 2023*. https://owasp.org/www-project-top-ten/

Pfleeger, C. P., & Pfleeger, S. L. (2012). *Security in Computing* (5th ed.). Prentice Hall. [Perhatian: Tahun 2012, di luar rentang 2017-2023 yang diminta. Akan lebih baik jika diganti dengan sumber yang lebih baru].

Pratama, M. R., & Prihatna, I. K. (2020). Eksploitasi Kerentanan UnrealIRCd Backdoor Menggunakan Metasploit. *Jurnal Teknologi Informasi dan Komunikasi*, *1*(1), 8-14.

Pratama, R. A., Yuliza, E., & Ramdhani, Y. (2021). Analisis Keamanan Sertifikat SSL/TLS pada Website Pemerintahan. *Jurnal Teknologi dan Sistem Informasi*, *2*(1), 1-8.

Purnomo, D., Arifin, Z., & Suryani, I. (2018). Perbandingan Metode Black Box dan White Box Testing dalam Pengujian Aplikasi Web. *Jurnal Teknologi Informasi Komunikasi dan Pendidikan*, *1*(1), 1-7.

Putra, D. K. S., & Wijaya, I. W. A. (2020). Analisis dan Mitigasi Kerentanan SQL Injection pada Aplikasi Web. *Jurnal Ilmu Komputer dan Sistem Informasi*, *8*(1), 20-27.

Putra, H. S. D., Subroto, D. S. R., & Sari, N. L. (2020). Komparasi Tool Penetration Testing (Nmap, Nessus, OpenVAS, dan Nikto) untuk Deteksi Kerentanan Website. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(2), 202-208. https://doi.org/10.29207/resti.v4i2.xxxx (DOI perlu diverifikasi)

Putri, D. A. N., & Anggara, J. (2021). Validasi Hasil Scan Kerentanan Website Menggunakan OWASP ZAP dan Nessus. *Jurnal Informatika*, *10*(1), 1-8.

Salsabila, N. L., & Kustanti, E. A. (2021). Analisis Kerentanan SSL/TLS Menggunakan OpenSSL dan SSLscan. *Jurnal Teknologi Informasi dan Komunikasi*, *2*(2), 112-118.

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *JURNAL ILMIAH MERPATI*, *8*(2), 79–88.

Saputra, Y. A., & Wibowo, R. (2020). Analisis Kerentanan Website Menggunakan OWASP ZAP dan Nessus. *Jurnal Sistem Informasi dan Komputer*, *9*(1), 1-8.

Sari, P. W., & Kridalaksana, A. (2023). Analisis dan Pencegahan Cross-Site Request Forgery (CSRF) pada Aplikasi Web. *Jurnal Informatika: Jurnal Pengembangan IT*, *8*(1), 1-7.

Scarfone, K. A., & Mell, P. (2022). *Guide to Vulnerability Management (NIST Special Publication 800-40 Rev. 4)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf

Suprayogi, D., Yulianti, D., & Naufal, M. F. (2019). Perancangan Penetration Testing untuk Keamanan Aplikasi Web dengan Metode OWASP. *Jurnal Informatika: Jurnal Pengembangan IT*, *4*(2), 101-107.

Tenable. (2023). *Nessus Documentation*. https://docs.tenable.com/nessus/Content/Welcome.htm

Tohir, A. S. (2017). Pemodelan Sistem Data

Terdistribusi Untuk Mengintegrasikan Data Akademik Dan Keuangan. *INTENSIF Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, *1*(1), 44–52.

Umasugi, M. R., Satra, R., & Gafar, A. W. M. (2024). Analisis Keamanan Website dengan Metode Penetration Testing pada PT. PLN (Persero). *Jurnal Pendidikan dan Teknologi Informasi*, *1*(3), 1–8. [Perhatian: Tahun 2024, di luar rentang 2017-2023 yang diminta. Akan lebih baik jika diganti dengan yang 2017-2023].

Wattuweha, S. (2023). *Network Scanning With Nmap*. [Tesis/Skripsi tidak dipublikasikan]. Universitas X.

Wijaya, H., Naufal, M. F., & Hidayat, R. (2021). Analisis Kerentanan Website Menggunakan Kombinasi OWASP ZAP dan Nikto. *Jurnal Sistem Informasi dan Ilmu Komputer*, *10*(1), 1-8.