Analisis Keamanan Jaringan Server Ujian Sman 20 Bandung Menggunakan Standar Penetration Testing Execution Standard (Ptes)

1st Dafin Dafwatul Yudha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
dayudhaa@student.telkomuniversity.ac.id

2nd RD Rohmat Saedudin
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

3rd Muhammad Fathinuddin
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
muhammadfathinuddin@telkomuniversity.ac.id

***Abstrak*—Perkembangan sistem informasi mendorong lembaga pendidikan untuk mengadopsi website sebagai media ujian daring. SMAN 20 Bandung merupakan salah satu institusi yang telah mengimplementasikan sistem ujian berbasis web. Penelitian ini bertujuan untuk mengidentifikasi, menguji, dan merekomendasikan perbaikan terhadap potensi celah keamanan yang ada pada sistem ujian tersebut.**

***Metode yang digunakan mengacu pada Penetration Testing Execution Standard (PTES) dengan tiga alat bantu utama: Burpsuite, OWASP ZAP, dan Nessus. Dari ketiga alat tersebut ditemukan total 160 kerentanan yang diklasifikasikan berdasarkan tingkat severity, mulai dari informational hingga critical. Seluruh temuan kemudian dianalisis menggunakan pendekatan vulnerability analysis, di mana proses eliminasi dilakukan berdasarkan tiga kriteria utama: tingkat severity, keberulangan antar tools, dan efisiensi mitigasi.**

Tujuh kerentanan prioritas dipilih dan diuji melalui tahapan eksploitasi, yang kemudian diikuti dengan perancangan mitigasi baik pada sisi konfigurasi server maupun kode aplikasi. Pengujian ulang pasca mitigasi menunjukkan bahwa sebagian besar kerentanan berhasil diminimalisasi secara signifikan. Namun, beberapa isu seperti Content Security Policy (CSP) dan token CSRF masih membutuhkan penanganan lanjutan di tingkat pengembangan aplikasi. Penelitian ini memberikan gambaran menyeluruh terhadap keamanan website ujian SMAN 20 Bandung dan menjadi pijakan awal dalam peningkatan keamanan sistem secara berkelanjutan.

Kata kunci— Keamanan website, eksploitasi, mitigasi.

I. PENDAHULUAN

Teknologi informasi terus berkembang pesat, mendorong berbagai sektor termasuk pendidikan untuk beradaptasi dengan solusi digital. *Website*, yang pada awalnya hanya berfungsi sebagai sarana penyajian informasi satu arah, kini berkembang menjadi *platform* interaktif yang mendukung pembelajaran daring dan sistem evaluasi seperti ujian berbasis komputer (CBT) [1][2]. Transformasi tersebut meningkatkan efisiensi penyelenggaraan ujian, namun juga membuka peluang terhadap risiko keamanan informasi.

Penerapan CBT pada institusi pendidikan perlu diiringi dengan perlindungan terhadap data sensitif seperti akun siswa, nilai, dan soal ujian. Ancaman terhadap sistem digital kini semakin kompleks, sebagaimana tercermin dalam laporan tahunan BSSN yang mencatat lebih dari 403 juta anomali dan serangan siber di Indonesia sepanjang tahun 2023 [3].

GAMBAR 1
Trafik Anomali tistik Trafik Anomali dan Serangan Cyber di Indonesia selama Tahun 2023

Risiko ini berlaku tidak hanya untuk sistem berskala besar, tetapi juga server lokal yang dibuka publik secara terbatas selama ujian berlangsung.

SMAN 20 Bandung, sebagai salah satu sekolah yang telah mengadopsi CBT, menggunakan server ujian berbasis Bitnami WAMP Stack yang belum terdokumentasi dan belum pernah diuji keamanannya secara menyeluruh. Mengingat pentingnya kerahasiaan dan integritas data, pengujian keamanan menjadi kebutuhan yang mendesak. Penelitian ini dilakukan menggunakan pendekatan *Penetration Testing Execution Standard* (PTES) untuk mengevaluasi potensi kerentanan serta memberikan rekomendasi penguatan keamanan sistem.

II. KAJIAN TEORI

A. Sistem Informasi

Sistem informasi merupakan gabungan antara manusia, teknologi, dan prosedur yang bekerja bersama untuk mengelola data menjadi informasi yang mendukung pengambilan keputusan dalam organisasi [4]. Dalam konteks pendidikan, sistem ini banyak dimanfaatkan untuk mengelola data siswa, materi pembelajaran, hingga pelaksanaan ujian berbasis komputer.

B. Keamanan Sistem Informasi

Keamanan sistem informasi menjadi aspek krusial yang menjamin kerahasiaan, integritas, dan ketersediaan informasi [5]. Ketiga prinsip ini dikenal sebagai konsep *Confidentiality*, *Integrity*, dan *Availability* (CIA), yang harus dijaga secara seimbang untuk memastikan sistem dapat berfungsi secara

andal dan terlindungi dari gangguan maupun penyalahgunaan.

C. Website

Website sendiri, bukan hanya merupakan media penyajian informasi, tetapi juga dapat difungsikan sebagai sarana komunikasi, publikasi, hingga transaksi digital yang kompleks [1]. Dalam penelitian ini, *website* ujian SMAN 20 Bandung memiliki peran sentral sebagai sistem yang memfasilitasi pelaksanaan evaluasi pembelajaran, sehingga keberadaan kerentanan dalam sistem tersebut dapat menimbulkan implikasi serius terhadap keamanan data siswa maupun integritas sistem akademik.

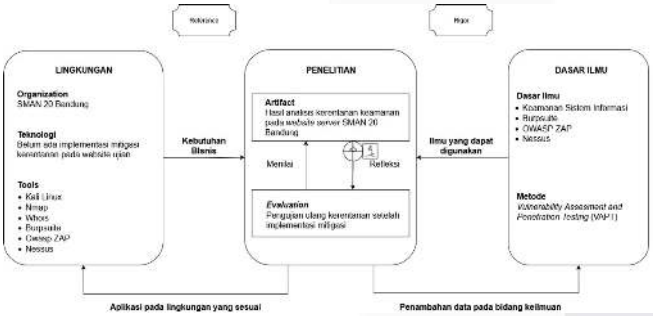
D. Penetration Testing Execution Standard (PTES)

PTES terdiri dari tujuh tahapan utama: *Pre-Engagement Interactions*, *Intelligence Gathering*, *Threat Modeling*, *Vulnerability Analysis*, *Exploitation*, *Post Exploitation*, dan *Reporting*. Standar ini banyak diterapkan dalam pengujian keamanan karena menyajikan alur yang sistematis dan dapat disesuaikan dengan konteks sistem yang diuji [6].

III. METODOLOGI PENELITIAN

A. Model Konseptual

Model konseptual dalam penelitian ini berfungsi sebagai kerangka pemikiran untuk menjelaskan hubungan antara elemen-elemen utama yang mendasari proses pengujian keamanan *website* ujian di SMAN 20 Bandung. Model ini dirancang berdasarkan pendekatan penelitian dari Hevner (2010), yang memetakan keterkaitan antara lingkungan penelitian, proses pengembangan, dan landasan keilmuan yang digambarkan pada gambar 2.

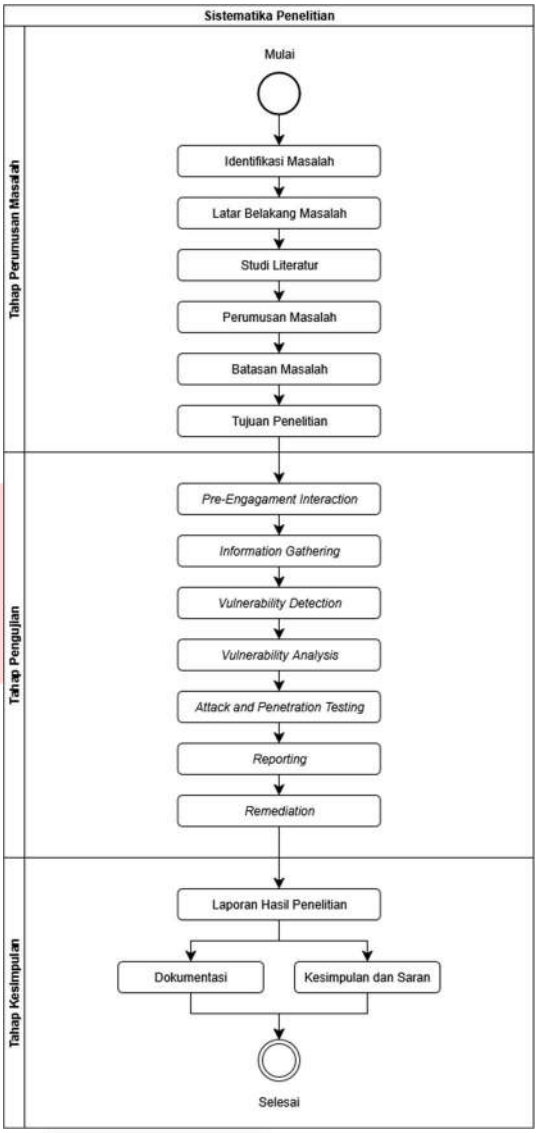


GAMBAR 2
Model Konseptual

Sistematika penyelesaian masalah yang digambarkan dalam penelitian ini berisi tahapan yang dilakukan selama penelitian. Tahapan yang digunakan dijabarkan dalam tiga tahap yaitu tahap perumusan masalah, tahap pengujian, dan tahap kesimpulan seperti yang di gambarkan pada Gambar 3.

B. Sistematika Penulisan

Penelitian ini disusun secara sistematis untuk menggambarkan alur langkah yang ditempuh dalam proses analisis keamanan *website* ujian di SMAN 20 Bandung. Penulisan dibagi ke dalam tiga bagian utama, yaitu perumusan masalah, pelaksanaan pengujian, serta penarikan kesimpulan dan rekomendasi. Pada Gambar 3 menjelaskan 3 tahapan utama yaitu: Tahap perumusan masalah, Tahap Pengujian, dan Tahap Kesimpulan.



GAMBAR 3
Sistematika Penulisan

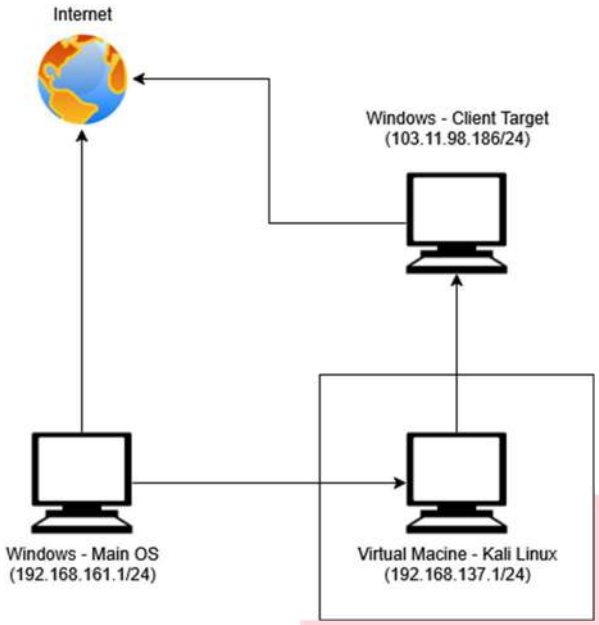
IV. PERANCANGAN DAN IMPLEMENTASI

A. Perancangan Pengujian

Tahap awal dimulai dengan melakukan proses *cloning repository website* ujian SMAN 20 Bandung oleh penulis. Sistem target sebelumnya telah menerapkan secara lokal oleh pihak sekolah menggunakan Bitnami WAMP *Stack*. Langkah *cloning* ini bertujuan untuk menyediakan lingkungan pengujian yang identik dengan server asli, tanpa mengganggu sistem produksi yang sedang berjalan. Setelah berhasil dijalankan secara stabil, proses pengujian keamanan terhadap *website* tersebut dapat dilakukan secara menyeluruh.

B. Platform Pengujian

Platform pengujian merupakan lingkungan terkontrol yang dirancang untuk menjalankan seluruh proses uji keamanan terhadap sistem target tanpa mengganggu operasional sistem produksi. *Platform* ini terdiri dari perangkat *host* sebagai pengelola *virtual machine*, satu mesin *virtual* Kali Linux sebagai *attacker*, serta satu *client* target yang merepresentasikan server ujian SMAN 20 Bandung. Struktur topologi dan hubungan antar komponen dijelaskan pada Gambar 4.



GAMBAR 4
Platform Pengujian

C. Perancangan Sistem

Pengujian dilakukan dengan dukungan perangkat keras dan perangkat lunak yang dikonfigurasi untuk menunjang seluruh tahapan pengujian keamanan. Daftar lengkap spesifikasi perangkat keras dan perangkat lunak yang digunakan dapat dilihat pada Tabel 1 dan Tabel 2.

TABEL 1
Spesifikasi Perangkat Keras

Nama Komponen	Informasi Spesifikasi	
Komputer Host	Computer Name	LAPTOP-EIF3SGMH
	Processor	AMD Ryzen™ 7 8845HS @5,1Ghz (8 Core 16 Threads) ~5,1GHz
	Memory	32768 MB RAM
	Storage	474 GB
	System Type	64-bit Operating System
	Operating System	Microsoft Windows 11 Home Single Language 64-bit (Version 10.0.22631, Build 22631)
Virtual Machine	Computer Name	Kali Linux 2025.1
	Processor	AMD Ryzen™ 7 8845HS @5,1Ghz (8 Core 16 Threads) ~5,1GHz
	Memory	8196 MB
	Storage	40 GB
	System Type	64-bit Operating System
	Operating System	Kali GNU / Linux Rolling
Client Target	Computer Name	DESKTOP-5U96S24
	Processor	Intel(R) Core(TM) i7-6700 CPU @3.40GHz, 3408 Mhz, 4 Core(s), 8 Logical Processor(s)
	Memory	16384MB
	Storage	118GB
	System Type	64-bit Operating System
	Operating System	Microsoft Windows 10 Pro N (Version 10.0.19045 Build 19045)

TABEL 2
Spesifikasi Perangkat lunak

Nama Komponen	Perangkat Lunak
Operating System	Kali Linux 2024.4 Kali-rolling
Virtual Machine	VMware® Workstation 17 Pro 17.5.0 build-22583795
Scanning Tools	Nmap Version 7.94SVN
	WOIS 5.5.23
Vulnerability Scanning and Analysis Tools	Burp Suite Professional v2025.1.4
	ZAP Version 2.16.1
	Nessus Essentials 10.8.4 (#28) Linux Version

V. HASIL DAN PEMBAHASAN

A. Information Gathering

Pada tahap ini, dilakukan pengumpulan informasi terhadap target sistem untuk memperoleh gambaran umum struktur layanan serta potensi celah awal. Pengujian diawali dengan menggunakan *tool* Nmap untuk melakukan pemindaian terhadap port terbuka dan layanan aktif pada IP target. Setelah itu, digunakan *tool* WHOIS untuk mendapatkan informasi administratif dan registrasi domain dari alamat IP yang sama.

Hasil dari proses *information gathering* ini menjadi dasar dalam menyusun strategi pengujian selanjutnya, termasuk dalam menentukan *tools* dan skenario eksploitasi. Rangkuman hasil pengumpulan informasi disajikan dalam Tabel 3 dan Tabel 4.

TABEL 3
Hasil Information Gathering menggunakan NMAP

Spesifikasi	Keterangan
IP Address	103.11.98.186
Nama Domain	dnxip-186.bapenda.jabarprov.go.id
Status Host	Host aktif dengan latensi 0.055 detik
Durasi Pengujian	2870.38 detik
Port	21, 22,23,25,53,80,110,135, 139, 143,443,445, 3306. 3389, 5900, 8080, 8888, 8443,1025, 33060

TABEL 4
Hasil Information Gathering menggunakan WHOIS

Informasi	Keterangan
Nama Organisasi	PT Skyline Semesta
Alamat	Jl Terusan Mulyasari No. 8, Bandung
Lokasi	Bandung, Jawa Barat, Indonesia
Email Teknis	hostmaker@skyline.net.id

Email Abuse	abuse@skyline.net.id
Nomor Telepon	+62-22-82009555

B. Vunlerability Detenction

Vulnerability detection merupakan tahap identifikasi awal terhadap berbagai potensi celah keamanan pada sistem, baik dari sisi aplikasi web maupun konfigurasi infrastruktur. Tiga *tools* utama digunakan dalam tahap ini, yaitu Burpsuite, OWASP ZAP, dan Nessus.

Burpsuite dan OWASP ZAP digunakan untuk mendeteksi kerentanan dari sisi aplikasi, seperti kelemahan pada *input form*, kontrol sesi, serta celah *client-side* yang umum terjadi pada sistem berbasis web. Sementara itu, Nessus digunakan dalam mode *advanced scan* untuk melakukan pemindaian lebih komprehensif terhadap konfigurasi server, layanan jaringan, serta celah keamanan yang dikenal berdasarkan database CVE (*Common Vulnerabilities and Exposures*) terbaru.

Setiap alat digunakan dengan konfigurasi yang disesuaikan dengan struktur target dan fokus pengujian. Hasil dari tahap ini belum dianalisis secara mendalam, namun memberikan fondasi awal dalam memahami permukaan serangan dan prioritas risiko yang akan dikaji lebih lanjut pada tahap analisis kerentanan. Rangkuman hasil pemindaian ditampilkan dalam Tabel 5, Tabel 6, dan Tabel 7.

TABEL 5
Hasil Kerentanan yang Terdeteksi oleh Burpsuite

Jenis Kerentanan	CVE/CWE	Severity, Confidence
Client-side desync	CWE-444	High, Firm
TLS cookie without secure flag set	CWE-614	Medium, Firm
TLS certificate	CWE-295, CWE-326, CWE-327	Medium, Certain
Vulnerable JavaScript dependency	CVE-2018-20676, CVE-2018-14042, CVE-2018-20677, CVE-2018-14041	Low, Tentative
Cookie without HttpOnly flag set	CWE-16	Low, Firm
Unencrypted communications	CWE-326	Low, Certain
Strict transport security not enforced	CWE-523	Low, Certain
Cross-site request forgery (CSRF)	CWE-352	Informational, Tentative
Input returned in response (reflected)	-	Informational, Certain

TABEL 5
Hasil Kerentanan yang Terdeteksi oleh OWASP ZAP

Jenis Kerentanan	CVE/CWE	Risk, Confidence
Content Security Policy (CSP) Header Not Set	CWE-693	Medium, High
Vulnerable JS Library	CWE-1395	Medium, Medium
Absence of Anti-CSRF Tokens	CWE-319	Medium, Low
Strict-Transport-Security Header Not Set	CWE-1004	Low, High
Cookie No HttpOnly Flag	CWE-614	Low, Medium
Cookie Without Secure Flag	CWE-1004	Low, Medium
Cookie without SameSite Attribute	CWE-1275	Low, Medium
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	CWE-497	Low, Medium
X-Content-Type-Options Header Missing	CWE-693	Low, Medium
Authentication Request Identified	-	Infomational, High
Information Disclosure - Suspicious Comments	CWE-615	Informational, Medium
Session Management Response Identified	-	Informational, Medium

TABEL 6
Hasil Kerentanan yang Terdeteksi oleh Nessus

Jenis Kerentanan	CVE/CWE	Severity
PHP Unsupported Version Detection	CVE-2021-34798, CVE-2021-39275	Critical
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability	CVE-2019-11043	Critical
PHP 7.2.x < 7.2.14 Multiple vulnerabilities	CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024	Critical
PHP 7.2.x < 7.2.16 Multiple vulnerabilities	CVE-2019-9637, CVE-2019-9638, CVE-2019-9639, CVE-2019-9640, CVE-2019-9641	Critical
PHP 7.2.x < 7.2.17 Multiple Vulnerabilities	CVE-2019-11034, CVE-2019-11035	Critical
Apache 2.4.x < 2.4.60 Multiple Vulnerabilities	CVE-2024-38475, CVE-2024-38476, CVE-2024-38477, CVE-2024-39573	Critical
Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF	CVE-2021-44224, CVE-2021-44790	Critical
Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow	CVE-2021-44790	Critical
Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	CVE-2023-25690, CVE-2023-27522	Critical
Apache < 2.4.49 Multiple Vulnerabilities	CVE-2021-40438	Critical
OpenSSL 1.1.1 < 1.1.1p Vulnerability	CVE-2022-2068	Critical
OpenSSL 1.1.1 < 1.1.1o Vulnerability	CVE-2022-1292	Critical
OpenSSL 1.1.1 < 1.1.1l Multiple Vulnerabilities	CVE-2021-3711, CVE-2021-3712	Critical
OpenSSL 1.1.1 < 1.1.1za Vulnerability	CVE-2024-5535	Critical
OpenSSL 1.1.1 < 1.1.1w Vulnerability	CVE-2023-4807	High

DNS Server Spoofed Request Amplification DDoS	CVE-2006-0987	High
Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	CVE-2019-0215, CVE-2019-0217, CVE-2019-0220	High
DNS Server Recursive Query Cache Poisoning Weakness	CVE-1999-0024	Medium
PHP 7.2.x < 7.2.10 Transfer-Encoding Parameter XSS Vulnerability	CWE-693	Medium
TLS Version 1.0 Protocol Detection	CWE-327	Medium

C. Vulnerability Analysis

Tahap analisis kerentanan merupakan fondasi penting dalam pengujian keamanan karena menjadi dasar dalam menentukan arah eksploitasi dan perancangan mitigasi. Pemindaian yang dilakukan menggunakan tiga *tools* utama, yaitu Burpsuite, OWASP ZAP, dan Nessus, menghasilkan total sekitar 160 temuan kerentanan. Burpsuite mencatat sembilan kerentanan terkait pengelolaan sesi pengguna, validasi *input*, dan pengaturan *header* keamanan. OWASP ZAP mendeteksi dua belas kerentanan, sebagian besar serupa dengan Burpsuite terutama dalam aspek perlindungan sisi klien dan kebijakan HTTP. Nessus memberikan hasil terbanyak dengan 139 temuan yang mencakup beragam tingkat risiko, mulai dari informasi sistem hingga kelemahan kritis pada perangkat lunak server seperti Apache, PHP, dan OpenSSL.

Menghadapi jumlah temuan yang besar, dilakukan proses eliminasi secara bertahap untuk menyaring kerentanan yang paling relevan dan memiliki dampak signifikan terhadap sistem. Pada tahap awal, kerentanan berisiko rendah dan bersifat informasional dikecualikan. Selanjutnya, dilakukan pengelompokan terhadap entri yang memiliki akar teknis serupa. Sebanyak 17 temuan terkait Apache HTTP Server dikonsolidasikan karena berasal dari versi 2.4.41 yang sama dan menunjukkan pola kelemahan berulang, seperti *bypass* autentikasi dan eksekusi kode. Pada PHP, ditemukan 25 entri dari berbagai versi lawas yang seluruhnya mengarah pada kerentanan seperti eksekusi kode jarak jauh, *buffer overflow*, dan kebocoran informasi. OpenSSL menyumbang 22 entri, namun sebagian besar bersifat pasif, tidak divalidasi oleh *tools* lain, serta tidak ditemukan kondisi eksploitasi langsung, sehingga tidak dimasukkan dalam fokus utama.

Pengelompokan juga dilakukan terhadap kerentanan yang menunjukkan kesamaan pola risiko. Misalnya, absennya *header* keamanan seperti CSP, HSTS, dan X-Content-Type-Options dikelompokkan sebagai isu perlindungan *browser*. Temuan terkait pengaturan atribut *cookie* seperti *Secure* HttpOnly, dan SameSite disatukan sebagai risiko terhadap keamanan sesi pengguna. Selain itu, isu seperti tidak tersedianya token CSRF yang dilaporkan dengan istilah berbeda oleh Burp dan ZAP digabung karena berasal dari akar masalah autentikasi yang sama.

Melalui proses penyaringan ini, jumlah kerentanan berhasil dipadatkan dari sekitar 160 menjadi 15 kelompok kerentanan teknis utama. Dari hasil akhir tersebut, ditetapkan tujuh kerentanan paling signifikan yang menjadi fokus eksploitasi lanjutan dan dasar dalam perancangan mitigasi sistem. Daftar lengkap ketujuh kerentanan disajikan pada Tabel 7.

TABEL 7
List Vulnerability

Jenis Kerentanan	CVE/CWE	Severity
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	CVE-2020-11984, CVE-2020-11993, CVE-2020-9490	Critical
PHP 7.2.x < 7.2.14 Multiple vulnerabilities	CVE-2016-10166, CVE-2018-19935, CVE-2019-6977, CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024	Critical
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Exec	CVE-2019-11043	Critical
DoS via exif_thumbnail_extract	CVE-2018-14883	High
Client-side desync	CWE-444	High
Absence of Anti-CSRF Tokens	CWE-352	Medium
Content Security Policy (CSP) Header Not Set	CWE-693	Medium

D. Penetration Testing

Tahapan *penetration testing* bertujuan untuk memvalidasi sejauh mana kerentanan yang telah teridentifikasi dapat dieksploitasi dalam lingkungan nyata serta mengevaluasi dampak aktual yang mungkin terjadi. Dari total tujuh kerentanan prioritas yang telah diseleksi melalui tahap analisis, lima di antaranya dipilih untuk diuji lebih lanjut secara langsung. Dua sisanya, yaitu kelemahan versi Apache dan PHP lawas, tidak diuji eksplisit karena merupakan representasi dari kelompok kerentanan versi perangkat lunak yang secara umum dapat ditangani melalui pembaruan sistem.

Kelima kerentanan yang diuji dieksekusi dengan pendekatan manual dan semi-otomatis menggunakan *tools* seperti Burpsuite, phuip-fpizdam, dan teknik eksploitasi berbasis *payload* langsung. Hasil eksploitasi menunjukkan adanya indikasi keberhasilan pada tiga kerentanan, satu kerentanan dinyatakan sebagai *false positive*, dan satu kerentanan tidak valid secara lingkungan.

Tabel 8 berikut merangkum hasil dari pengujian eksploitasi terhadap lima kerentanan utama yang diuji dalam penelitian ini.

TABEL 8
Hasil Penetration Testing

Jenis Kerentanan	Tools	Indikasi Eksploitasi	Dampak Potensial
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Exec	phuip-fpizdam (manual)	Koneksi berhasil, tetapi payload gagal	Tidak valid karena target gunakan mod_php
DoS via exif_thumbnail_extract	Manual	Gambar EXIF rusak berhasil disimpan tanpa crash	False positive, sistem tidak terdampak
Client-side desync	Burpsuite Repeater	Server merespons struktur request tidak lazim	Potensi manipulasi cache atau pembajakan sesi

Absence of Anti-CSRF Tokens	Manual	Script dijalankan, muncul alert	Potensi session hijacking, manipulasi data admin
Content Security Policy (CSP) Header Not Set	Burp ClickBandit	Halaman termuat dalam iframe tanpa proteksi	Clickjacking, pemalsuan klik, pengalihan konten

E. Remediasi

Remediasi merupakan tahapan akhir dalam siklus pengujian keamanan yang bertujuan untuk memperbaiki celah keamanan yang telah ditemukan dan divalidasi sebelumnya. Pada konteks website ujian SMAN 20 Bandung, langkah ini dilaksanakan berdasarkan tujuh kerentanan prioritas yang ditentukan melalui seleksi risiko, validasi silang, dan efisiensi mitigasi.

Proses remediasi mencakup perancangan langkah perbaikan yang menyesuaikan karakteristik tiap kerentanan, mulai dari penguatan konfigurasi server, pembaruan perangkat lunak, hingga peningkatan kebijakan keamanan sisi klien. Setelah mitigasi diterapkan, dilakukan verifikasi ulang menggunakan *tools* yang sama untuk memastikan efektivitas tindakan dan mengamati perubahan status tiap kerentanan. Rangkuman strategi mitigasi dan hasil pemindaian pasca mitigasi dijabarkan pada Tabel 9 dan Tabel 10.

TABEL 9
Perancangan Mitigasi

Jenis Kerentanan	Tahapan Perbaikan
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	Memperkuat konfigurasi keamanan pada file httpd.conf. Konfigurasi meliputi pembatasan ukuran dan jumlah header untuk mencegah HTTP Request Smuggling dan header overflow: LimitRequestFields 40 LimitRequestFieldSize 4094 Kemudian menonaktifkan fitur proxy: <IfModule mod_proxy.c> ProxyRequests Off </IfModule> Serta pembatasan metode HTTP yang diizinkan untuk mencegah eksploitasi metode yang tidak sah pada .htaccess : <LimitExcept GET POST> Require all denied </LimitExcept>
PHP 7.2.x < 7.2.14 Multiple vulnerabilities	Melakukan, penguatan konfigurasi keamanan PHP sebagai langkah mitigasi dari berbagai vulnerabilities pada versi PHP 7.2.x < 7.2.14, Tindakan ini meliputi: Menonaktifkan tampilan versi PHP di header HTTP agar tidak terekspos pada sisi client: expose_php = Off Dan juga menonaktifkan allow_url_fopen untuk mencegah eksploitasi berbasis remote file inclusion: allow_url_fopen = Off
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Exec	Berdasarkan hasil pengujian menggunakan script eksploitasi phuip-fpizdam.py, tidak ditemukan gejala atau eksekusi perintah yang berhasil. Lingkungan server tidak menggunakan PHP-FPM sehingga eksploitasi dinyatakan tidak valid atau false positive.
DoS via exif_thumbnail_extract	Walaupun tidak ditemukan dampak signifikan saat pengujian, untuk mencegah potensi serangan DoS melalui fitur exif, dilakukan penonaktifan ekstensi exif secara keseluruhan. Perubahan dilakukan dengan menambahkan tanda ; (komentar) pada baris berikut di file php.ini: ;extension=php_exif.dll
Client-side desync	Menambahkan konfigurasi pencegahan di httpd dan .htaccess untuk membatasi permintaan yang dapat menyebabkan desinkronisasi interpretasi antara client dan server: Konfigurasi pada httpd: LimitRequestFields 40 LimitRequestFieldSize 4094 Konfigurasi pada.htaccess: RequestHeader unset Transfer-Encoding
Absence of Anti-CSRF Tokens	Karena framework dan struktur CBT belum menyediakan token CSRF secara default, maka belum dapat diterapkan pada tahap ini. Namun, dapat dilakukan penguatan sisi browser dengan menambahkan header berikut untuk meminimalkan risiko XSS yang sering berkaitan dengan CSRF dengan konfigurasi pada .htaccess : Header always set X-XSS-Protection "1; mode=block"
Content Security Policy (CSP) Header Not Set	Menambahkan header CSP minimum melalui konfigurasi file .htaccess untuk membatasi pemuatan sumber daya dari domain yang tidak dikenal, dengan mengkonfigurasi: <IfModule mod_headers.c> Header always set Content-Security-Policy "default-src 'self';" Header always set X-Content-Type-Options "nosniff" </IfModule>

TABEL 10
Hasil Analisis Pasca Mitigasi

Vulnerability Scanning Pra Mitigasi	Vulnerability Scanning Pasca Mitigasi	Tahapan Perbaikan
Apache 2.4.x < 2.4.46 Multiple Vulnerabilities (Critical)	-	Mitigasi telah dilakukan melalui penyesuaian konfigurasi httpd.conf dan .htaccess serta menonaktifkan modul proxy.
PHP 7.2.x < 7.2.14 Multiple vulnerabilities (Critical)	-	Mitigasi telah dilakukan dengan penguatan pada konfigurasi php.ini
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11	-	Mitigasi dilakukan melalui analisis Vulnerability dan

Remote Code Exec (Critical)		dinyatakan false positive karena target tidak menggunakan PHP-FPM
DoS via exif_thumbnail_extract (Critical)	-	Mitigasi telah dilakukan dengan menonaktifkan ekstensi exif pada php.ini
Client-side desync (High, Firm)	-	Mitigasi dilakukan melalui pengaturan pembatasan header di .htaccess
Absence of Anti-CSRF Tokens (Medium, Low)	Absence of Anti-CSRF Tokens (Medium, Low)	Mitigasi terbatas telah dilakukan namun belum menyeluruh. Diperlukan implementasi token acak pada setiap form serta validasi token di sisi server.
Content Security Policy (CSP) Header Not Set (Medium, High)	Content Security Policy (CSP) Header Not Set (Medium, High)	Mitigasi awal telah diterapkan melalui .htaccess.

Hasil analisis menunjukkan bahwa sebagian besar kerentanan berhasil ditangani melalui pendekatan teknis pada sisi server. Namun, beberapa celah seperti absennya token anti-CSRF dan *header* CSP masih memerlukan tindak lanjut dari sisi pengembangan aplikasi.

VI. KESIMPULAN

Berdasarkan hasil penelitian terhadap sistem *website* ujian SMAN 20 Bandung menggunakan pendekatan *Penetration Testing Execution Standard* (PTES), diperoleh beberapa kesimpulan utama sebagai berikut:

1. Tahapan deteksi kerentanan berhasil mengidentifikasi sebanyak 160 celah keamanan dengan rincian 139 dari Nessus, 9 dari Burpsuite, dan 12 dari OWASP ZAP. Kerentanan yang ditemukan mencakup berbagai aspek, mulai dari konfigurasi perangkat lunak server yang belum diperbarui, hingga kelemahan sisi klien seperti absennya *header* keamanan dan validasi *input*. Setelah proses normalisasi data, penggabungan entri duplikat, serta klasifikasi berdasarkan tingkat risiko dan kemiripan teknis, jumlah temuan valid disaring menjadi 83. Dari jumlah tersebut, tujuh kerentanan utama dipilih sebagai fokus eksploitasi dan mitigasi berdasarkan tingkat keparahan, kemunculan lintas perangkat uji, dan efektivitas penanganan.
2. Pengujian eksploitasi terhadap tujuh kerentanan menunjukkan bahwa lima di antaranya dapat dimanfaatkan secara langsung untuk menyerang sistem, seperti manipulasi permintaan tanpa token, desinkronisasi HTTP, dan *clickjacking* akibat ketiadaanya kebijakan keamanan *header*. Dua kerentanan lainnya, yaitu eksekusi perintah jarak jauh dan serangan DoS berbasis metadata gambar, tidak menunjukkan indikasi eksploitasi aktif karena konfigurasi sistem tidak sesuai dengan prasyarat teknisnya. Proses mitigasi dilakukan dengan memperkuat konfigurasi Apache dan PHP, serta menambahkan kebijakan keamanan seperti *Content Security Policy*. Hasil pemindaian ulang pasca mitigasi menunjukkan penurunan signifikan pada jumlah kerentanan, meskipun masih terdapat kelemahan residual pada sisi aplikasi yang memerlukan intervensi pengembang secara langsung. Hal ini menegaskan pentingnya kolaborasi antara tim teknis dan pengembang dalam mewujudkan sistem yang aman secara menyeluruh.

REFERENSI

[1] N. Ashri, "Studi literatur: Analisis perkembangan website pada lingkup komunikasi," *Media Bina Ilmiah*, vol. 16, no. 6, pp. 3–4, 2022. [Online]. Tersedia: http://ejurnal.binawakya.or.id/index.php/MBI/article/view/1454

[2] M. T. Hidayatullah, M. Asbari, M. I. Ibrahim, dan A. Hadidtia, "Urgensi aplikasi teknologi dalam pendidikan di Indonesia," *Journal of Information Systems and Management (JISMA)*, vol. 2, no. 6, pp. 70–73, 2023, doi: 10.4444/jisma.v2i6.785.

[3] Badan Siber dan Sandi Negara, *Lanskap Keamanan Siber Indonesia 2023*. Jakarta: BSSN, 2023. [Online]. Tersedia: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[4] L. Abdurrahman dan A. F. Santoso, *Pengantar Sistem Informasi*. Bandung: Tel-U Press, 2023. [Online]. Tersedia: https://openlibrary.telkomuniversity.ac.id/home/catalog/id/205331

[5] M. F. Safitra, "Analisis kerentanan keamanan terhadap website pemerintahan daerah XYZ menggunakan Penetration Testing Execution Standard (PTES)," Skripsi, Universitas Telkom, 2022. [Online]. Tersedia: https://openlibrary.telkomuniversity.ac.id/home/catalog/id/180246

[6] The Penetration Testing Execution Standard, "Main Page," 2014. [Online]. Tersedia: http://www.pentest-standard.org/index.php/Main_Page