Analisis Perbandingan PTES dan OWASP sebagai Acuan Penetration Testing dalam Mengidentifikasi dan Memitigasi Kerentanan Website

(Studi Kasus : Dinkominfo Banyumas)

1st Muhamad Gilang Herawan
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto
mugiher@student.telkomuniversity.ac.id

2nd Sandhy Fernandes *Direktorat Universitas Telkom Purwokerto*
Universitas Telkom Purwokerto
Purwokerto
sandhyf@telkomuniversity.ac.id

3rd Gunawan Wibisono
Direktorat Universitas Telkom Purwokerto
Universitas Telkom Purwokerto
Purwokerto
gunawanw@telkomuniversity.ac.id

***Abstrak** Website pemerintah memiliki peran strategis dalam menyediakan akses informasi dan interaksi digital kepada publik, termasuk yang dikelola oleh Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas. Namun, paparan terhadap internet meningkatkan kerentanannya terhadap berbagai serangan siber. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan keamanan pada website Dinkominfo Banyumas menggunakan dua pendekatan penetration testing, yaitu Penetration Testing Execution Standard (PTES) dan OWASP Top 10. Pengujian dilakukan melalui pemetaan port, identifikasi direktori, pengujian konfigurasi keamanan, serta eksploitasi kerentanan menggunakan tools seperti Nmap, ZAP, SQLMap, dan Burp Suite. Hasil penelitian menunjukkan bahwa OWASP lebih efektif dalam mengidentifikasi kerentanan pada lapisan aplikasi seperti injection, broken access control, dan misconfiguration, serta lebih efisien dari segi waktu karena mampu menghasilkan temuan dalam durasi yang lebih singkat. Sebaliknya, PTES menawarkan pendekatan yang lebih sistematis dan menyeluruh dari tahap perencanaan hingga pelaporan, namun memerlukan waktu pelaksanaan yang lebih panjang. Temuan ini menunjukkan bahwa OWASP lebih cocok diterapkan pada pengujian keamanan aplikasi web instansi pemerintah daerah, sedangkan PTES relevan untuk pengujian berskala besar dengan kebutuhan dokumentasi menyeluruh. Hasil penelitian ini diharapkan menjadi acuan strategis dalam memperkuat keamanan dan perlindungan data pada layanan digital pemerintahan.*

Kata kunci: Penetration Testing, OWASP Top 10, PTES, Keamanan Website, Efisiensi, Pemerintahan Daerah.

I. PENDAHULUAN

Di era digital, sistem informasi berbasis web telah menjadi fondasi utama layanan publik, termasuk di sektor pemerintahan. Website Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas memegang peran penting dalam penyampaian informasi, pelayanan publik, dan pengelolaan data internal. Namun, ketergantungan yang tinggi terhadap teknologi ini meningkatkan risiko serangan siber, sebagaimana tercermin dari berbagai insiden kebocoran data pada situs web instansi pemerintah di Indonesia. Pemilihan Dinkominfo Banyumas sebagai objek studi kasus didasarkan pada peran strategisnya dalam pengelolaan infrastruktur digital daerah dan minimnya publikasi terkait pengujian keamanan sistemnya. Berdasarkan observasi awal dan wawancara dengan kepala bidang APTIKA, ditemukan dugaan insiden kebocoran data internal yang menunjukkan adanya celah keamanan belum tertangani secara optimal. Fakta ini memperkuat urgensi pelaksanaan penetration testing secara metodologis guna mengidentifikasi serta memitigasi kerentanan sebelum berdampak lebih luas.

Penelitian [1] mengungkapkan enam kerentanan utama pada website Dinas Sosial Surabaya, seperti Browsable Web Directories dan Content Security Policy (CSP) Header Not Set, yang menunjukkan pentingnya penerapan penetration testing untuk mengidentifikasi dan mengatasi celah keamanan sebelum dimanfaatkan oleh pihak tidak bertanggung jawab. Sektor publik kerap menjadi target empuk serangan siber karena lemahnya sistem pertahanan dan minimnya audit keamanan berkala. Dampaknya bukan hanya kebocoran data pribadi, tetapi juga potensi disinformasi, gangguan layanan publik, hingga hilangnya kepercayaan masyarakat terhadap lembaga pemerintah. Bahkan, serangan semacam ini berpotensi melanggar UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Untuk itu, penetration testing menjadi langkah proaktif dalam mengidentifikasi kerentanan melalui simulasi serangan nyata. Keberhasilannya sangat bergantung pada metodologi yang tepat dan terstandarisasi. Dua framework yang umum digunakan adalah PTES (Penetration Testing Execution Standard) dan OWASP (Open Web Application Security Project). PTES menyusun pengujian menjadi tujuh tahap sistematis, mulai dari perencanaan hingga pelaporan, sedangkan OWASP lebih fokus pada sepuluh kerentanan aplikasi web paling umum melalui panduan OWASP Top 10 dan Testing Guide. Keduanya telah terbukti efektif dalam berbagai studi kasus dan mampu mengungkap celah keamanan kritis pada sistem informasi, khususnya di lingkungan instansi pemerintah.

Penelitian ini melakukan analisis perbandingan antara PTES dan OWASP pada sistem website Dinkominfo Banyumas untuk mengevaluasi efektivitas masing-masing kerangka kerja dalam mendeteksi kerentanan serta merumuskan rekomendasi strategis bagi instansi pemerintahan serupa. Mengingat kompleksitas dan sensitivitas data pada sistem informasi pemerintahan, pendekatan hybrid yang menggabungkan keunggulan kedua metodologi dinilai layak diterapkan. Beberapa studi menunjukkan bahwa kombinasi metode dapat meningkatkan cakupan deteksi kerentanan secara signifikan dibandingkan penggunaan framework tunggal. Temuan ini menegaskan pentingnya penelitian komparatif dalam mendukung penguatan kebijakan keamanan siber, khususnya di sektor publik yang semakin terdigitalisasi.[6]

II. KAJIAN TEORI

A. PTES

Penetration Testing Execution Standard (PTES) adalah metodologi sistematis untuk pengujian penetrasi yang terdiri dari tujuh tahapan: Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, dan Reporting. PTES memastikan pengujian dilakukan secara profesional

dan konsisten, mulai dari penyusunan ruang lingkup hingga pelaporan hasil dan rekomendasi mitigasi. Pendekatan ini memberikan kerangka kerja yang komprehensif dalam mendeteksi dan menangani kerentanan sistem secara efektif [12].

B. Keamanan Website

Keamanan aplikasi web merupakan aspek yang semakin vital di tengah perkembangan teknologi digital dan meningkatnya serangan siber yang mengeksploitasi celah keamanan. Penerapan langkah-langkah keamanan proaktif, termasuk pengujian penetrasi dan integrasi keamanan dalam siklus pengembangan perangkat lunak penting dilakukan untuk melindungi aplikasi web dari ancaman yang terus berkembang [13]

C. Penetration Testing

Penetration testing adalah metode untuk mengevaluasi kerentanan sistem informasi dengan mensimulasikan serangan, baik dari dalam maupun luar, guna mengidentifikasi celah keamanan yang tidak terdeteksi oleh pengujian standar. Pada aplikasi web pemerintah seperti LPSE Palembang mengungkap kerentanan serius seperti SQL Injection, XSS, dan RCE. Hal ini menunjukkan pentingnya uji penetrasi dalam melindungi sistem informasi instansi pemerintah. Di Dinkominfo Banyumas, penetration testing berperan penting dalam mencegah serangan siber, menjaga integritas data, dan meningkatkan kepercayaan publik terhadap layanan digital [17].

D. Konsep Dasar Kerentanan Website

Kerentanan website merupakan kelemahan dalam desain, implementasi, atau konfigurasi sistem yang dapat dieksploitasi oleh penyerang untuk mendapatkan akses tidak sah atau merusak sistem. Beberapa kerentanan umum yang sering ditemukan pada aplikasi web mencakup SQL Injection, Cross-Site Scripting (XSS), dan kesalahan konfigurasi keamanan. SQL Injection terjadi akibat kurangnya validasi input, memungkinkan penyisipan perintah SQL berbahaya untuk mengakses atau merusak data, yang dapat dicegah dengan penggunaan parameterized queries dan sanitasi input, terutama dalam aplikasi pemerintah seperti sistem milik Dinkominfo Banyumas [18]. XSS memungkinkan penyerang menyisipkan skrip berbahaya ke halaman web yang dijalankan oleh browser pengguna, berpotensi mencuri informasi sensitif seperti kredensial login; mitigasinya antara lain melalui penerapan Content Security Policy (CSP) dan encoding input [19]. Sementara itu, kesalahan konfigurasi (misconfiguration), seperti penggunaan kredensial default atau pengaturan server yang tidak aman, menjadi celah besar dalam keamanan, yang dapat mengakibatkan kebocoran data dan akses tidak sah. Dengan memperbaiki konfigurasi sistem secara menyeluruh, Dinkominfo Banyumas dapat meminimalkan risiko serangan dan meningkatkan kepercayaan publik terhadap layanan digital yang disediakan [20].

E. OWASP

OWASP (Open Web Application Security Project) Top 10 merupakan daftar sepuluh jenis kerentanan paling umum yang ditemukan pada aplikasi web, yang telah menjadi standar internasional bagi pengembang dan profesional keamanan dalam mengenali serta mengatasi risiko keamanan aplikasi [21]. Daftar ini mencakup ancaman kritis seperti SQL Injection, Cross-Site Scripting (XSS), dan Broken Access Control, yang berpotensi mengekspos data sensitif, merusak sistem, atau memungkinkan akses tidak sah ke aplikasi. Dengan menyediakan panduan prioritas terhadap risiko keamanan utama, OWASP Top 10 mendorong penerapan praktik pengembangan perangkat lunak yang lebih aman dan berorientasi pada mitigasi kerentanan sejak tahap awal pengembangan. Pembaruan daftar ini dilakukan secara berkala guna menyesuaikan dengan dinamika dan tren terbaru dalam lanskap ancaman keamanan siber [22].

E. Sistem Informasi Pemerintahan Berbasis Website

Sistem Informasi Pemerintahan berbasis web (e-Government) menjadi komponen penting dalam meningkatkan transparansi, efisiensi, dan akuntabilitas layanan publik melalui pemanfaatan teknologi informasi yang memungkinkan akses layanan secara cepat dan mudah bagi masyarakat. Salah satu implementasinya adalah sistem pelaporan di Dinas Komunikasi dan Informatika (Dinkominfo) Banyumas yang menangani laporan terkait penyimpangan oleh pejabat publik, di mana keberhasilan sistem ini sangat bergantung pada perlindungan dan pengelolaan data yang bersifat sensitif [26]. Meskipun e-Government di Indonesia terus berkembang, penerapannya masih menghadapi tantangan serius, seperti keterbatasan infrastruktur, kurangnya sumber daya manusia yang kompeten, serta ancaman terhadap keamanan informasi. Selain itu, hambatan dalam integrasi sistem dan manajemen informasi yang belum optimal turut menjadi kendala utama dalam mencapai efektivitas dan keberlanjutan implementasi e-Government secara menyeluruh [27].

F. Audit keamanan Dan Evaluasi Berkala Sistem

Audit keamanan dan evaluasi berkala terhadap sistem informasi merupakan langkah krusial dalam mengidentifikasi dan mengatasi kerentanan yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab, yang dapat mengancam integritas serta keamanan data yang dikelola. Menurut Rahman (2023), audit yang efektif dan komprehensif harus mencakup penilaian mendalam terhadap perlindungan data pribadi, terutama dalam konteks penerapan Sistem Pemerintahan Berbasis Elektronik (e-Government) yang semakin luas. Evaluasi ini meliputi aspek pengumpulan, penyimpanan, dan pemrosesan data masyarakat serta efektivitas mekanisme perlindungan privasi yang dijalankan, sesuai dengan standar dan regulasi keamanan data nasional maupun internasional. Dengan demikian, pelaksanaan audit keamanan yang tepat tidak hanya mampu melindungi sistem dari ancaman eksternal, tetapi juga menjamin tata kelola data sensitif yang patuh terhadap regulasi, sehingga dapat meningkatkan kepercayaan publik terhadap sistem e-Government [28].

G. Kali Linux

Kali Linux adalah distribusi berbasis Debian yang dikembangkan oleh Offensive Security untuk pengujian penetrasi dan forensik digital. Dilengkapi lebih dari 600 alat keamanan, Kali Linux mendukung analisis kerentanan, eksploitasi, dan investigasi forensik. Dengan komunitas aktif dan dokumentasi lengkap, distribusi ini menjadi standar industri dalam keamanan siber. Dalam konteks pengujian sistem, Kali Linux digunakan untuk mendeteksi kerentanan secara sistematis melalui tahapan seperti pengumpulan informasi, simulasi serangan, dan pelaporan, sehingga mendukung perlindungan data dan sistem informasi][30].

III. METODE

Penelitian ini menggunakan pendekatan penetration testing untuk menganalisis kerentanan pada website Dimassatria milik Dinkominfo Kabupaten Banyumas. Metode pengujian dilakukan dengan membandingkan dua framework, yaitu Penetration Testing Execution Standard

(PTES) dan Open Web Application Security Project (OWASP).

Penelitian ini menggunakan metode penetration testing dengan membandingkan dua framework keamanan, yaitu Penetration Testing Execution Standard (PTES) dan Open Web Application Security Project (OWASP), untuk menguji kerentanan website Dinkominfo Kabupaten Banyumas. PTES terdiri dari tujuh tahapan, yaitu Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, dan Reporting, yang bersifat menyeluruh dan formal. Sementara itu, OWASP berfokus pada pengujian kerentanan aplikasi web berbasis daftar OWASP Top 10 seperti SQL Injection (A03), Broken Access Control (A01), dan Security Misconfiguration (A05). Pengujian dilakukan menggunakan pendekatan black-box dan grey-box dengan bantuan enam tools utama, yakni Nmap, Dirsearch, SQLMap, Burp Suite, OWASP ZAP, dan XRAY.

Proses metodologis meliputi identifikasi sistem, perencanaan pengujian, pengumpulan data teknis, pelaksanaan eksploitasi aktif, serta analisis hasil berdasarkan klasifikasi risiko. Temuan dikategorikan berdasarkan standar OWASP dan dibandingkan efektivitasnya antara kedua framework. Hasil dari pengujian digunakan untuk merumuskan rekomendasi penguatan sistem, seperti penerapan parameterized queries, Content Security Policy (CSP), penguatan kontrol akses, serta kebijakan internal terkait keamanan data dan prosedur penanganan insiden guna meningkatkan ketahanan dan kepercayaan terhadap sistem informasi pemerintah daerah.

IV. HASIL PERCOBAAN DAN ANALISIS

Website resmi Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas merupakan portal layanan publik berbasis CMS PHP yang menggunakan web server Nginx serta protokol HTTP/HTTPS. Website ini memiliki peran strategis dalam transparansi dan layanan digital pemerintahan, sehingga membutuhkan perhatian serius terhadap keamanannya. Melalui proses fingerprinting menggunakan tools seperti Nmap, WhatWeb, dan banner grabbing, ditemukan bahwa website berjalan di atas sistem operasi Linux, menggunakan Nginx 1.20.1, PHP 8.0.12, dan PostgreSQL sebagai basis data. Ditemukan pula akun superuser ‘postgres’ yang berisiko tinggi jika tereksploitasi. Pengumpulan data dilakukan melalui observasi langsung, wawancara dengan pengelola sistem, serta pemanfaatan tools keamanan seperti Nmap, Dirsearch, OWASP ZAP, Burp Suite, SQLMap, dan XRAY. Dari proses ini teridentifikasi sejumlah port terbuka (80, 443, 8443, 2000, 5060, dan 8010), serta file sensitif seperti .git dan .env yang dapat diakses publik, mengindikasikan adanya kelemahan konfigurasi keamanan yang signifikan pada sistem.

A. Analisis Kerentanan berdasarkan PTES

Pengujian berdasarkan metode PTES (Penetration Testing Execution Standard) dilaksanakan untuk mengidentifikasi potensi kerentanan dalam sistem dan mengeksploitasi titik-titik lemah pada aplikasi yang diuji. PTES terdiri atas beberapa fase penting, yakni: Planning, Discovery, Attack/Penetration, dan Reporting. Setiap tahapan memberikan kontribusi terhadap pemahaman menyeluruh terhadap kondisi keamanan aktual dari sistem yang diuji.

Tabel 1. Temuan PTEST

No	Sumber Temuan	Ringkasan Temuan	Risiko
1	Nmap	Port non-standar dan service dev aktif	Tinggi
2	Dirsearch	File sensitif terekspos (.git, .env)	Tinggi
3	ZAP	Header keamanan tidak diterapkan	Sedang
4	SQLMap/XRAY	SQLi → Shell → manipulasi database	Sangat Tinggi
5	Burp Suite	Error log bocorkan struktur sistem	Tinggi
6	XRAY	RCE, Path Traversal, Auth Bypass (CVE)	Sangat Tinggi

Berdasarkan metode PTES yang mencakup tahapan perencanaan, pengumpulan data, eksploitasi, hingga pelaporan, pengujian keamanan pada website Dinkominfo Banyumas berhasil mengidentifikasi sejumlah kerentanan signifikan. Temuan utama mencakup port terbuka dan layanan pengembangan aktif (Nmap), file sensitif yang dapat diakses publik seperti .git dan .env (Dirsearch), serta absennya header keamanan seperti CSP dan X-Frame-Options (OWASP ZAP). Eksploitasi menggunakan SQLMap dan XRAY mengungkap celah SQL Injection yang memungkinkan akses shell dan manipulasi database, sementara Burp Suite mendeteksi kebocoran struktur direktori akibat kesalahan konfigurasi log. Selain itu, XRAY juga menemukan celah kritis seperti RCE, path traversal, dan auth bypass. Untuk mitigasi, disarankan menutup port tidak perlu, menghapus file sensitif, mengaktifkan header keamanan dan CSRF token, memvalidasi input dengan query aman, memperbarui sistem, serta memperkuat kontrol akses dan autentikasi. Seluruh hasil ini memberikan dasar strategis bagi penguatan sistem secara menyeluruh.

B. Analisis Kerentanan Berdasarkan OWASP

OWASP (Open Web Application Security Project) Top 10 merupakan standar global yang mendokumentasikan sepuluh jenis kerentanan paling kritis pada aplikasi web. Dalam penelitian ini, pendekatan OWASP digunakan untuk menganalisis keamanan website Dinkominfo Kabupaten Banyumas, dengan fokus pada risiko nyata yang sering dieksploitasi penyerang serta memberikan dasar mitigasi yang kuat. Proses pengujian dilakukan melalui tahapan metodologi OWASP, yaitu Reconnaissance, Scanning, Exploitation, dan Reporting.

Tabel 2. Temuan OWASP

Kode OWASP	Nama Risiko	Jumlah Temuan	Rincian Temuan
A05	Security Misconfiguration	5	- XRAY: RCE, Auth Bypass (CVE) - Burp Suite: Error log bocorkan struktur - Dirsearch: File sensitif (.git, .env) - ZAP: Header keamanan tidak diterapkan - Nmap: Port non-standar dan service dev aktif
A01	Broken Access Control	2	- SQLMap/XRAY: SQL Injection → Shell - XRAY: Path Traversal, Auth Bypass
A03	Injection	2	- SQLMap/XRAY: SQL Injection → Shell - XRAY: Path Traversal (Injection

			context)
A02	Cryptographic Failures	1	- Dirsearch: Ekspos file sensitif (.env)
A07	Identification & Authentication Failures	1	- ZAP: Header keamanan tidak diterapkan (CSRF protection tidak ada)

Hasil pengujian menunjukkan bahwa kategori OWASP A05: Security Misconfiguration mendominasi dengan lima temuan, seperti akses file sensitif dan absennya header keamanan. Diikuti A01: Broken Access Control dan A03: Injection, masing-masing dua temuan, termasuk bypass autentikasi dan celah SQL Injection. Sementara itu, A02: Cryptographic Failures dan A07: Identification & Authentication Failures muncul satu kali. Temuan ini menyoroti pentingnya perbaikan konfigurasi sistem, kontrol akses, dan mekanisme autentikasi.

C. Perbandingan Hasil Analisis Kerentanan

Setelah dilakukan pengujian menggunakan dua pendekatan, yaitu PTES dan OWASP Top 10, diperoleh hasil identifikasi kerentanan yang mencerminkan keunggulan masing-masing metodologi. PTES menawarkan pendekatan menyeluruh yang mencakup seluruh tahapan, mulai dari pra-engagement hingga post-exploitation, dengan fokus pada simulasi serangan nyata. Sementara itu, OWASP lebih terfokus pada sepuluh jenis kerentanan paling umum dalam aplikasi web, yang dijadikan standar global dalam keamanan aplikasi. Hasil pengujian terhadap website Dinkominfo Banyumas menunjukkan bahwa kedua pendekatan mampu mengidentifikasi kerentanan di berbagai lapisan sistem, namun terdapat perbedaan dalam cakupan dan kedalaman eksploitasi yang dilakukan, yang menjadi dasar dalam perbandingan efektivitas keduanya.

Tabel 3. Perbandingan Hasil Analisis Kerentanan

No	Aspek Pengujian	PTES	OWASP Top 10
1.	Pendekatan	Tahapan menyeluruh dari rekognisi hingga pelaporan	Klasifikasi kerentanan aplikasi web paling umum
2.	Fokus Utama	Infrastruktur, sistem operasi, layanan jaringan, aplikasi	Aplikasi web (front-end dan back-end)
3.	Tools Utama	Nmap, Dirsearch, SQLMap, Xray, manual testing	OWASP ZAP, BurpSuite, Dirsearch, browser console, dependency check
4.	Cakupan Kerentanan	Port terbuka, direktori sensitif, SQLi, RCE, akses shell, logging	CSRF, CSP, insecure headers, error disclosure, outdated JS
5.	Tingkat Eksploitasi	Mendalam hingga shell, manipulasi DB, privilege escalation	Umumnya pada permukaan aplikasi (web layer)
6.	Kerentanan Utama yang Terdeteksi	Broken Access Control, RCE, Path Traversal, SQL Injection	Misconfiguration, CSRF, XSS, Insecure Components
7.	Kategori OWASP yang Terdeteksi	A01, A03, A05, A06, A07	A01, A03, A05, A06, A07
8.	Kelebihan	Mampu meniru skenario serangan dunia nyata dengan eksploitasi penuh	Memberikan kerangka standar dan spesifik untuk aplikasi web
9.	Kekurangan	Butuh waktu dan keahlian tinggi, tidak terstandarisasi klasifikasinya	Tidak menjangkau aspek sistem operasi atau jaringan

Berdasarkan hasil pengujian, pendekatan PTES terbukti unggul dalam hal kedalaman eksploitasi dan cakupan sistem karena mampu menelusuri celah dari tahap pengumpulan informasi hingga pengambilalihan shell sistem, sehingga cocok diterapkan pada lingkungan kompleks seperti instansi pemerintah. Sementara itu, OWASP lebih unggul dalam klasifikasi risiko pada tingkat aplikasi web karena pendekatannya yang fokus, mudah diimplementasikan, dan didukung oleh tools otomatis. OWASP efektif dalam mengidentifikasi kerentanan umum seperti SQL Injection, Security Misconfiguration, dan Broken Access Control secara cepat. Meski PTES menawarkan proses menyeluruh dari perencanaan hingga pelaporan, metode ini membutuhkan lebih banyak waktu dan sumber daya. Dengan demikian, OWASP lebih cocok sebagai baseline evaluasi keamanan aplikasi, sedangkan PTES efektif untuk simulasi serangan kompleks. Kombinasi kedua pendekatan ini memberikan hasil yang lebih komprehensif, dan dapat menjadi strategi optimal dalam pengujian keamanan website seperti milik Dinkominfo Banyumas.

D. Perbandingan Waktu Temuan Kerentanan

Penelitian ini melakukan perbandingan terhadap kecepatan dua pendekatan pengujian keamanan, yaitu OWASP Top 10 dan Penetration Testing Execution Standard (PTES), dalam mendeteksi kerentanan pada sistem berbasis web. Pengukuran dilakukan berdasarkan waktu rata-rata yang diperlukan oleh masing-masing metode untuk mengidentifikasi dan memverifikasi kerentanan, dengan studi kasus pada website milik Dinkominfo Banyumas.

Tabel 4. Perbandingan waktu Temuan

No.	Jenis Kerentanan	Waktu Temuan (OWASP)	Waktu Temuan (PTES)	Selisih waktu	Keterangan
1	SQL Injection	10 menit	20 menit	10 menit	OWASP langsung mendeteksi dengan tools otomatis seperti SQLMap
2	Cross-Site Scripting (XSS)	15 menit	30 menit	15 menit	OWASP lebih cepat karena fokus pada kategori umum kerentanan
3	Broken Access Control	25 menit	35 menit	10 menit	PTES Membutuhkan proses lebih panjang karena melalui tahapan eksploitasi dan verifikasi
4	Server Misconfiguration	12 menit	25 menit	13 menit	OWASP mengidentifikasi melalui scanner, PTES melalui tahap reconnaissance

					& scanning
5	Insecure Deserialization	30 menit	40 menit	10 menit	PTES mengidentifikasi setelah threat modeling dan eksploitasi manual

Dari sisi efisiensi waktu, pendekatan OWASP lebih unggul karena bersifat langsung, praktis, dan fokus pada aplikasi web, serta didukung oleh tools otomatis seperti OWASP ZAP dan SQLMap yang memungkinkan proses identifikasi kerentanan dilakukan dalam 1–2 hari. Sebaliknya, PTES membutuhkan waktu lebih lama karena mencakup tahapan formal seperti pre-engagement hingga post-exploitation, dengan durasi pengujian yang bisa memakan waktu beberapa hari hingga minggu. Oleh karena itu, dalam konteks instansi pemerintahan daerah, OWASP dinilai lebih efisien untuk pelaksanaan pengujian keamanan berbasis waktu.

E. Penyusunan Rekomendasi Penguatan

Berdasarkan hasil analisis kerentanan pada website Dinas Komunikasi dan Informatika (Dinkominfo) Kabupaten Banyumas menggunakan pendekatan PTES dan OWASP Top 10, ditemukan sejumlah celah keamanan pada aspek jaringan, sistem operasi, konfigurasi server, dan aplikasi web. Untuk mengurangi risiko tersebut, diperlukan strategi mitigasi yang terstruktur, dengan rekomendasi yang disusun berdasarkan klasifikasi OWASP Top 10 serta temuan kritis dari tahapan pengujian PTES, dan disesuaikan dengan prinsip keamanan sistem informasi modern.

Tabel 5. Penyusunan Rekomendasi Penguatan

No	Kategori OWASP	Temuan Utama	Rekomendasi Teknis
1.	A01: Broken Access Control	Akses tidak sah ke Bitbucket, panel admin terbuka, shell access	- Terapkan autentikasi berbasis token atau Oauth - Gunakan IP whitelisting - Batasi akses ke endpoint admin dengan role-based access control
2.	A03: Injection	SQL Injection, RCE via pbocms dan ezoffice-documentedit	- Implementasi *prepared statements* - Validasi input secara ketat (whitelist) - Gunakan Web Application Firewall (WAF)
3.	A05: Security Misconfiguration	Port terbuka, direktori sensitif, error detail ditampilkan	- Tutup port tidak digunakan-Konfigurasi firewall dan header keamanan HTTP - Gunakan mode produksi tanpa menampilkan pesan error detail
4.	A06: Vulnerable Components	Komponen JS, Composer dan PHP usang	- Audit dependensi secara berkala menggunakan Snyk atau OWASP Dependency-Check - Update ke versi stabil terbaru
5.	A07: Identification Failures	Tidak adanya autentikasi pada XMPP dan SIP	- Aktifkan TLS dan autentikasi pada semua protokol komunikasi - Audit akses login dan nonaktifkan akun default
6.	Layanan Database dan RAC	User postgres memiliki privilege super dan shell access	- Ganti password default DB - Nonaktifkan shell akses DB user - Jalankan DB di sandbox dengan prinsip *least privilege*
7.	File Sensitif dan Directory Listing	.git, .env, .svn, /vendor/composer dapat diakses publik	- Blokir akses direktori melalui .htaccess atau konfigurasi server - Hindari menyimpan file rahasia di root path
8.	Error Handling dan Logging	Error 500 muncul 3.547 kali selama pengujian	- Terapkan logging internal yang tidak terekspos ke klien - Tampilkan custom error page tanpa detail teknis

Rekomendasi penguatan keamanan website Dinkominfo Banyumas difokuskan pada tiga aspek utama, yaitu: (1) penguatan infrastruktur dan konfigurasi sistem melalui penutupan port tidak perlu, pengamanan protokol komunikasi, serta pembatasan akses direktori sensitif; (2) peningkatan keamanan aplikasi web dengan prinsip secure coding, validasi input, penggunaan prepared statements, serta penerapan header keamanan seperti CSP, X-Frame-Options, dan HSTS; dan (3) manajemen akses berbasis peran (RBAC), autentikasi dua faktor, serta pembatasan akses IP. Selain itu, penguatan ini diarahkan untuk mendukung ketahanan jangka panjang melalui proses continuous hardening, pelatihan SDM, dan audit keamanan berkala guna memastikan efektivitas mitigasi yang diterapkan.

V. KESIMPULAN

Penelitian ini membandingkan dua framework penetration testing, yaitu Penetration Testing Execution Standard (PTES) dan OWASP Top 10, dalam mengidentifikasi dan memitigasi kerentanan aplikasi web pada website Dinkominfo Banyumas. Tujuan utama penelitian ini adalah untuk mendukung perlindungan

hukum data pribadi sesuai UU No. 27 Tahun 2022.

1. OWASP Top 10 terbukti lebih efektif dalam mendeteksi kerentanan pada aplikasi web karena fokus pada sepuluh jenis celah umum yang relevan dengan sistem pemerintahan. Pendekatannya yang praktis dan cepat menjadikannya lebih cocok untuk instansi daerah yang membutuhkan hasil uji cepat dan terfokus.
2. PTES menawarkan metodologi yang lebih menyeluruh dan mendalam, dari tahap perencanaan hingga pelaporan, namun memerlukan waktu dan sumber daya lebih besar. PTES lebih cocok untuk pengujian skala besar dan mendalam hingga ke tingkat sistem operasi.
3. Dari segi efisiensi waktu, OWASP lebih unggul karena memiliki tahapan yang lebih sederhana dan langsung mengarah pada kerentanan aplikasi web. Hal ini menjadikannya ideal untuk diterapkan pada instansi pemerintah daerah seperti Dinkominfo Banyumas.

REFERENSI

[1] B. A. Bagaskara, M. Idhom, and H. E. Wahanani, "Pengujian Website Dinas Sosial Surabaya Menggunakan Metode Penetration Testing dan OWASP Top 10
," vol. 8, no. 1, pp. 40–50, 2025.

[2] B. Kurniawan and I. Ruslianto, "Implementation of Penetration Testing on the Website Using the Penetration Testing Execution Standard (PTES) Method," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 8, no. 2, p. 518, 2023, doi: 10.24114/cess.v8i2.47096.

[3] M. F. Safitra, M. Lubis, and A. Widjajarto, "Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website," *ACM Int. Conf. Proceeding Ser.*, no. August, pp. 139–145, 2023, doi: 10.1145/3592307.3592329.

[4] I. D. G. G. Dharmawangsa, G. M. A. Sasmita, and I. P. A. E. Pratama, "Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X Website)," *JITTER J. Ilm. Teknol. dan Komput.*, vol. 4, no. 1, p. 1613, 2023, doi: 10.24843/jtrti.2023.v04.i01.p06.

[5] S. A. Nugroho and T. Rochmadi, "Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) Dan Information Systems Security Assessment Framework (ISSAF) Security Analysis Of Magelang Pusaka Information System Using Open Web Applicati," vol. 7, no. 1, pp. 56–61, 2024.

[6] R. M. Fauzi, R. Hermawan, D. R. Adhy, and S. Maesaroh, "Analisis Kerentanan Keamanan Web Menggunakan Metode Owasp Dan Ptes Di Web Pemerintahan Desa Xyz," *Power Elektron. J. Orang Elektro*, vol. 13, no. 2, pp. 225–231, 2024, doi: 10.30591/polektro.v13i2.6711.

[7] M. F. Yusuf, I. R. Hikmah, Amiruddin, and S. U. Sunaringtyas, "Security Testing of XYZ Website Application Using ISSAF and OWASP WSTG v4.2 Methods," *Teknika*, vol. 14, no. 1, pp. 66–77, Mar. 2025, doi: 10.34148/teknika.v14i1.1156.

[8] T. Revolino Syarif and D. Andri Jatmiko, "Comparison Analysis Of The Web Security Ptes, Issaf And Owasp In Diskominfo, Bandung City," *Elibrary Univ. Komput. Indones.*, no. May, 2019, [Online]. Available: https://elibrary.unikom.ac.id/880/13/21.10112427_TIO

[9] R. Ashar, "Analysis of Open Website Security Using OWASP and ISSAF Methods," *J. Inf. dan Teknol.*, vol. 4, no. 4, pp. 187–194, 2022, doi: 10.37034/jidt.v4i4.233.

[10] R. N. Dasmen, R. Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, "Pengujian Penetrasi Pada Website Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard)," *J. Komput. dan Inform.*, vol. 11, no. 1, pp. 91–95, 2023, doi: 10.35508/jicon.v11i1.9809.

[11] H. M. Adam, Widyawan, and G. D. Putra, "A Review of Penetration Testing Frameworks, Tools, and Application Areas," *Proc. - 2023 IEEE 7th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2023*, no. November 2023, pp. 319–324, 2023, doi: 10.1109/ICITISEE58992.2023.10404397.

[12] L. F. Burhani and D. Priyawati, "Analisis Pengujian Keamanan Website Pengelolaan Internet Desa Kragan Menggunakan Metode Penetration Testing Execution Standard (Ptes)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 9, no. 1, pp. 307–319, 2024, doi: 10.29100/jipi.v9i1.4455.

[13] S. Disawal and U. Suman, "Enhancing Security to Prevent Vulnerabilities in Web Applications," *Int. J. Eng. Trends Technol.*, vol. 72, no. 7, pp. 278–283, 2024, doi: 10.14445/22315381/IJETT-V72I7P130.

[14] D. Priyawati, S. Rokhmah, and I. C. Utomo, "Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP," *Int. J. Comput. Inf. Syst. Peer Rev. J.*, vol. 3, no. 3, pp. 143–147, 2022, doi: 10.29040/ijcis.v3i3.90.

[15] T. Ariyadi, A. P. Salsabila, and Y. P. Nugroho, "Implementasi Secure Code Pada Pengembangan Sistem Keamanan Website Teknik Komputer Universitas Bina Darma Menggunakan Penetration Testing dan OWASP ZAP," vol. 4, no. 1, 2025.

[16] J. P. Deviarinda, A. Budiyono, and A. Almaarif, "Analysis of Potential Security Issues in Regional Government X Website using Scanning Method in Kali Linux," *2nd Fac. Ind. Technol. Int. Congr.*, pp. 169–174, 2020.

[17] P. Raghu Vamsi, A. Ahmad, and V. Dwivedi, "Application for Simulating OWASP Vulnerabilities," no. January, pp.