Penerapan Metodologi NIST SP 800-115 dalam Pengujian Keamanan *Website* Disparbudpora Kabupaten Pacitan

Implementation of the NIST SP 800-115 Methodology in Security Testing of the Disparbudpora Pacitan District Website

Bayu Saputra[1], Andria[2], Hani Atun Mumtahana[3]
[1,2,3] Program Studi Sistem Informasi, Fakultas Teknik, Universitas PGRI Madiun
e-mail: [1]bayu_2105102003@mhs.unipma.ac.id, [2]andria@unipma.ac.id,
[3]hanimumtahana@unipma.ac.id

Abstrak **-** *Website* Dinas Pariwisata, Kebudayaan, Pemuda, dan Olahraga (Disparbudpora) Kabupaten Pacitan digunakan sebagai sarana penyampaian informasi publik. Penelitian ini bertujuan untuk menganalisis potensi kerentanan keamanan pada *website* tersebut menggunakan metode NIST SP 800-115. Pengujian dilakukan dengan pendekatan *white-box testing*. Hasil menunjukkan bahwa dari 38 temuan, sebanyak 10 (26,32%) dikategorikan sebagai kerentanan yang berpotensi membahayakan, dengan rata-rata skor CVSS v3.1 sebesar 6,4 (kategori sedang). Kerentanan utama yang ditemukan antara lain aktivasi *xmlrpc.php, potensi blind SQL injection*, dan eksposur akun melalui *REST API*. Beberapa tindakan mitigasi telah difokuskan pada penguatan konfigurasi sistem, penghapusan komponen yang tidak diperlukan, serta pembatasan akses terhadap endpoint sensitif. Sementara itu, perbaikan lanjutan terhadap aspek infrastruktur seperti DNS dan pembatasan direktori masih memerlukan dukungan dari administrator sistem.

Kata kunci – Keamanan *Website*; NIST SP 800-115; *Penetration Testing*; CVSS; *WordPress*

Abstract *- The website of the Pacitan Regency Tourism, Culture, Youth, and Sports Agency (Disparbudpora) is used as a means of conveying public information. This study aims to analyze potential security vulnerabilities on the website using the NIST SP 800-115 method. Testing was conducted using a white-box testing approach. The results showed that of the 38 findings, 10 (26.32%) were categorized as potentially dangerous vulnerabilities, with an average CVSS v3.1 score of 6.4 (moderate category). The main vulnerabilities found included xmlrpc.php activation, potential blind SQL injection, and account exposure via the REST API. Several mitigation measures have focused on strengthening system configuration, removing unnecessary components, and restricting access to sensitive endpoints. Meanwhile, further improvements to infrastructure aspects such as DNS and directory restrictions still require support from system administrators.*

Keywords – Website Security; NIST SP 800-115; Penetration Testing; CVSS; WordPress

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong transformasi digital di berbagai sektor, termasuk pariwisata. *Website* kini menjadi media strategis dalam penyebaran informasi dan promosi destinasi wisata karena mampu menjangkau audiens secara luas dan real-time[1] . Selain menyajikan konten promosi, *website* juga mendukung interaksi pengguna melalui fitur seperti galeri multimedia dan peta digital.

Namun, kemajuan teknologi juga disertai dengan meningkatnya ancaman keamanan siber[2]. *Website* publik sering menjadi target serangan seperti *SQL Injection, Cross-Site Scripting (XSS),* dan *Distributed Denial of Service (DDoS),* yang dapat menyebabkan kebocoran data, kerusakan sistem, atau bahkan manipulasi informasi[3]. Jika tidak ditangani secara serius, serangan ini dapat menurunkan kepercayaan publik terhadap layanan digital pemerintah.

Menurut data Badan Siber dan Sandi Negara (BSSN), pada tahun 2022 tercatat lebih dari 370 juta serangan siber terhadap Indonesia, meningkat drastis dari tahun sebelumnya. Sektor administrasi pemerintahan menjadi target utama, menunjukkan pentingnya perlindungan data dan sistem informasi, termasuk *website* instansi pemerintahan di bidang pariwisata.

Website Dinas Pariwisata, Kebudayaan, Pemuda, dan Olahraga (Disparbudpora) Kabupaten Pacitan merupakan sarana resmi publikasi dan layanan informasi wisata daerah. Meski memiliki fungsi strategis, hingga saat ini belum dilakukan pengujian keamanan secara menyeluruh terhadap sistem tersebut. Hal ini menjadi urgensi tersendiri mengingat tingginya risiko eksploitasi jika sistem tidak dilindungi dengan baik.

Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan keamanan pada *website* Disparbudpora Kabupaten Pacitan dengan metode NIST SP 800-115 dan pendekatan *white-box testing*. Dengan melakukan evaluasi melalui tahapan sistematis seperti *information gathering, scanning, vulnerability validation,* dan *simulated attack*, diharapkan temuan dalam penelitian ini dapat digunakan sebagai dasar rekomendasi mitigasi untuk memperkuat ketahanan *website* terhadap serangan siber yang semakin kompleks.

II. TINJAUAN TEORI

1. *Website*

   Website merupakan kumpulan halaman yang terorganisasi dan saling terhubung melalui tautan, dirancang untuk menyampaikan informasi dalam berbagai format seperti teks, gambar, suara, dan elemen multimedia lainnya. Halaman dapat bersifat statis maupun dinamis tergantung pada tujuan dan fungsinya[4].

2. *WordPress*

   WordPress adalah *CMS open-source* yang mendukung lebih dari 40% dari semua situs web di internet. Keamanan *WordPress* bergantung pada berbagai faktor termasuk pembaruan perangkat lunak penggunaan *Plugin* dan tema yang aman, serta konfigurasi yang tepat[5].

3. *Penetration testing*

   Penetration testing merupakan metode evaluasi keamanan sistem informasi dengan mengidentifikasi kerentanan, konfigurasi yang lemah, serta kelemahan perangkat keras dan lunak. Tujuannya adalah mengungkap seberapa rentan sistem terhadap serangan nyata dan memberikan dasar untuk perbaikan keamanan. Selain menguji infrastruktur teknis, pengujian ini juga dapat menilai efektivitas kebijakan keamanan dan kesiapan organisasi dalam menangani insiden[6].

4. NIST

   National Institute of Standards and Technology atau NIST adalah sebuah perusahaan keamanan informasi yang dikembangkan oleh pemerintah Amerika Serikat untuk membuat dan mendorong pengukuran, standar, dan teknologi. Pengujian keamanan dilakukan melalui empat langkah utama, yaitu *Planning, Discovery, Attack, dan Reporting*[7].

5. *Kali Linux*

   Kali Linux adalah distribusi *Linux* berbasis *Debian* yang berfokus pada pengujian penetrasi tingkat lanjut dan peretasan etis. *Linux* sendiri berisikan beberapa alat yang ditujukan untuk berbagai macam tugas keamanan informasi, seperti pengujian penetrasi, pemeriksaan keamanan, komputer forensik, dan rekayasa terbalik[8].

III. METODE

A. Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk memberikan gambaran menyeluruh mengenai proses dan hasil pengujian kerentanan keamanan pada *website* Disparbudpora Kabupaten Pacitan. Pengujian dilakukan berdasarkan standar NIST SP 800-115 dengan pendekatan *white-box testing*.

Identifikasi kerentanan dianalisis dengan menghitung persentase potensi kerentanan dari total temuan pengujian, menggunakan rumus:

$$\text{Tingkat Kerentanan (\%)} = (\text{Jumlah Potensi Kerentanan} / \text{Total Test Case}) \times 100\%$$

Selain itu, tingkat keparahan dari kerentanan yang ditemukan diukur menggunakan skor CVSS v3.1 untuk memperkuat analisis risiko dan merumuskan rekomendasi mitigasi.

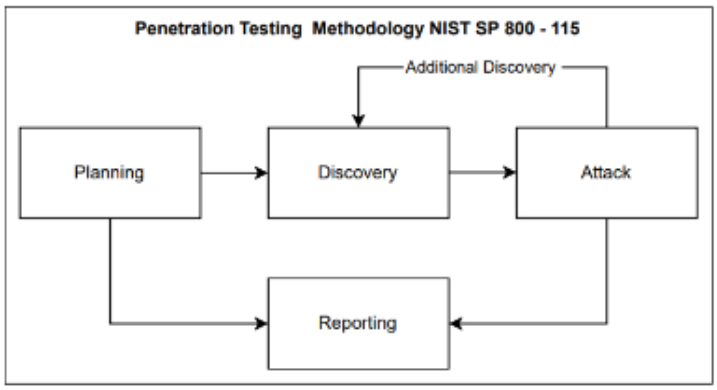
B. Metode Pengumpulan Data

Data diperoleh melalui tiga teknik utama:

a. Observasi langsung terhadap struktur dan konfigurasi *website*,
b. Pengumpulan data digital melalui alat bantu otomatis dan manual, serta
c. Dokumentasi hasil uji selama proses penetration testing berlangsung.

C. Metode Pengujian

Peneliti menggunakan NIST SP 800-115 sebagai metodologi pengujian dalam penelitian ini. NIST SP 800-115 adalah dokumen yang menunjukkan metode dan teknik yang digunakan untuk menguji kerentanan situs dalam *penetration testing* serta memberikan rekomendasi solusi dalam menangani kerentanan yang ditemukan. Pemilihan metode ini didasarkan pada keunggulannya dalam menyediakan pendekatan sistematis terhadap perencanaan, identifikasi kelemahan, eksploitasi, serta pelaporan hasil pengujian keamanan sistem. NIST SP 800-115 juga mendukung pendekatan *White Box*, yang memungkinkan pengujian dilakukan dengan akses dan pemahaman mendalam terhadap sistem target[7].



Gambar 1 Metode NIST SP 800-115

Berikut adalah penjelasan dari tahapan-tahapan metode *NIST*:

a. *Planning*

Dalam fase ini, penguji dan pihak organisasi menentukan ruang lingkup pengujian, tujuan, metodologi yang digunakan, serta batasan-batasan yang disepakati

b. *Discovery*

Pada tahap ini, dilakukan proses pengumpulan berbagai informasi terkait sistem target guna menemukan adanya celah keamanan.

c. *Attack*

Tahap *attack* merupakan fase eksekusi, di mana penguji mencoba mengeksploitasi kerentanan yang telah diidentifikasi. Tujuannya adalah untuk mensimulasikan serangan nyata, sehingga organisasi dapat memahami dampak potensial dari celah keamanan tersebut.

d. *Reporting*

Reporting adalah proses mendokumentasikan seluruh hasil dari pengujian keamanan (*penetration testing*), yang mencakup teknik yang digunakan, kerentanan yang ditemukan, analisis dampak, serta potensi risiko terhadap sistem atau aplikasi yang diuji.

IV. HASIL DAN PEMBAHASAN

Seperti yang telah dijelaskan sebelumnya, metode penetration testing yang disediakan di dalam NIST SP 800-115 terdiri dari 4 tahap yaitu Planning, Discovery, Attack dan Report. Setiap tahapan di dalam metode ini dimaksudkan untuk membantu penguji dalam melakukan pengujian terhadap domain *website*. Berikut langkah-langkah yang dilakukan dalam pengujian berdasarkan Metode NIST SP 800-115

1. Planning

   Tahap *planning* diawali dengan komunikasi resmi antara peneliti dan pihak Dinas Pariwisata, Kebudayaan, Pemuda, dan Olahraga (Disparbudpora) Kabupaten Pacitan. Diskusi ini bertujuan untuk menyusun ruang lingkup pengujian keamanan yang akan dilakukan dan menjamin bahwa aktivitas yang dilakukan berjalan sesuai dengan prinsip legalitas dan etika pengujian.

   Adapun hasil kesepakatan yang dicapai dalam tahap ini adalah sebagai berikut:

a). Identifikasi kontak peneliti dan perwakilan dari pihak Disparbudpora dan Diskominfo Pacitan sebagai penanggung jawab sistem.
b). Konfirmasi ruang lingkup pengujian, termasuk domain *website* yang diuji (*disparbudpora.pacitankab.go.id* dan *wisata.pacitankab.web.id*), serta pendekatan pengujian *white-box* yang digunakan.
c). Penjelasan metode pengujian berdasarkan standar NIST SP 800-115, yang meliputi tahapan *planning, discovery, attack, dan reporting*.
d). Persetujuan pengujian terhadap skenario eksploitasi terbatas, seperti *brute-force, user enumeration,* dan *directory listing*, tanpa melibatkan modifikasi sistem atau basis data.
e). Penyerahan data dan akses terbatas ke sistem, termasuk informasi struktur URL untuk mendukung proses pengujian secara realistis.
f). Komitmen dari peneliti untuk menyampaikan hasil analisis dan rekomendasi keamanan secara tertulis kepada pihak Disparbudpora setelah proses pengujian selesai dilakukan.

Dengan kesepakatan tersebut, maka tahap *planning* telah diselesaikan dan menjadi dasar pelaksanaan tahap selanjutnya dalam proses pengujian keamanan.

2. *Discovery*

Tahap Penemuan *(Discovery)* merupakan fase kedua dalam metodologi pengujian penetrasi berdasarkan standar NIST SP 800-115, yang dilakukan setelah tahap perencanaan *(planning)* selesai dilaksanakan. Fokus utama dari fase ini adalah mengumpulkan informasi sebanyak mungkin tentang sistem target serta mengidentifikasi potensi kerentanan guna memahami permukaan serangan *(attack surface)*. Proses *discovery* terbagi menjadi dua pendekatan, yaitu pengumpulan informasi secara pasif dan aktif, yang menjadi dasar dalam merancang langkah eksploitasi di tahap selanjutnya.

a. Pengumpulan informasi pasif

Pengumpulan informasi pasif dilakukan tanpa interaksi langsung dengan sistem target, sehingga mengurangi risiko terdeteksi oleh sistem pertahanan. Dalam penelitian ini, pendekatan pasif dilakukan terhadap dua domain milik Disparbudpora Kabupaten Pacitan, yaitu disparbudpora.pacitankab.go.id *(WordPress)* dan wisata.pacitankab.web.id *(Laravel)*. Tools seperti *WhatWeb* digunakan untuk mengidentifikasi *CMS, server*, dan *framework* yang digunakan. Hasilnya menunjukkan bahwa situs *WordPress* menggunakan Apache 2.4.62 di sistem operasi *Debian* dengan *WordPress* versi 6.8.1, sedangkan situs *Laravel* menggunakan struktur standar framework *Laravel* versi terbaru.

File *robots.txt* dianalisis untuk mencari direktori tersembunyi, namun tidak ditemukan entri penting. Selain itu, analisis metadata dan file publik default seperti *readme.html, license.txt,* dan *xmlrpc.php* pada *WordPress* menunjukkan bahwa beberapa file sensitif masih dapat diakses publik. Temuan ini menandakan bahwa *website* belum dikonfigurasi secara optimal untuk menyembunyikan informasi dasar yang berpotensi dimanfaatkan oleh penyerang.

b. Pengumpulan informasi aktif

Pengumpulan informasi aktif dilakukan dengan cara berinteraksi langsung dengan sistem target untuk mendapatkan informasi teknis yang lebih rinci. Dalam penelitian ini, dilakukan pemindaian port menggunakan *Nmap* yang mengidentifikasi bahwa layanan HTTP (port 80) dan HTTPS (port 443) aktif pada kedua domain. Selain itu, tools seperti *Gobuster* digunakan untuk mendeteksi direktori tersembunyi, dan ditemukan bahwa direktori seperti */wp-content/uploads/ (WordPress)* dan *public/storage/ (Laravel)* dapat diakses publik.

Pada *website WordPress*, pemindaian lanjutan dengan *WPScan* mengungkap sejumlah *plugin* yang belum diperbarui dan memiliki riwayat kerentanan, termasuk *plugin SEO* dan *page builder*. *REST API WordPress* juga ditemukan dalam kondisi terbuka tanpa autentikasi, yang memungkinkan dilakukannya *enumerasi* akun pengguna. File default seperti *readme.html, xmlrpc.php,* dan *license.txt* juga masih aktif.

Untuk domain *Laravel*, ditemukan potensi *directory listing* pada folder publik dan file konfigurasi yang mengekspos jalur direktori internal. Meskipun tidak ditemukan kerentanan kritis, celah-celah seperti *user enumeration, clickjacking, directory listing,* serta *endpoint login* yang tidak dilindungi dari *brute-force attack* tetap dinilai sebagai risiko sedang hingga tinggi.

Secara keseluruhan, meskipun tidak ditemukan eksploitasi yang menyebabkan *deface* atau akses tidak sah terhadap data sensitif, hasil *discovery* ini menunjukkan bahwa sistem memiliki permukaan serangan yang cukup terbuka dan dapat menjadi celah awal bagi penyerang dalam melakukan eskalasi akses. Temuan inilah yang menjadi dasar untuk dilanjutkannya proses uji eksploitasi secara terbatas pada tahap berikutnya.

3. *Attack*

Tahap serangan *(attack)* merupakan fase ketiga dalam metodologi NIST SP 800-115, yang bertujuan untuk menguji validitas dan dampak dari kerentanan yang telah diidentifikasi sebelumnya. Pengujian dilakukan secara terbatas, terkontrol, dan berlandaskan pada prinsip etis tanpa menyebabkan gangguan pada sistem target. Tujuan utama dari fase ini adalah mengukur sejauh mana potensi eksploitasi dapat terjadi dalam skenario dunia nyata.

Dalam penelitian ini, eksploitasi difokuskan pada 10 dari 38 temuan kerentanan yang dinilai memiliki tingkat risiko sedang hingga tinggi. Pada domain disparbudpora.pacitankab.go.id, dilakukan pengujian terhadap potensi *blind SQL injection* melalui halaman *login*, serta interaksi dengan *endpoint xmlrpc.php* untuk mendeteksi serangan berbasis *XML*. *REST API WordPress* yang terbuka tanpa autentikasi memungkinkan dilakukannya enumerasi pengguna, dan hasilnya mengungkap dua akun administrator secara eksplisit.

Salah satu temuan paling signifikan adalah adanya indikasi potensi *subdomain takeover* akibat entri DNS yang mengarah ke layanan eksternal yang tidak diklaim atau tidak lagi aktif. Meskipun tidak dilakukan eksploitasi penuh terhadap *subdomain* tersebut, konfigurasi DNS yang lemah menunjukkan bahwa penyerang berpotensi mengambil

alih *subdomain* jika tidak segera ditindaklanjuti, yang dapat dimanfaatkan untuk penyebaran *malware* atau *phishing*.

Selain itu, tidak ditemukannya header keamanan HTTP seperti *X-Frame-Options* dan *Content-Security-Policy* membuka kemungkinan terjadinya serangan *clickjacking* dan *content sniffing*. Pada domain wisata.pacitankab.web.id, ditemukan kelemahan berupa akses direktori publik tanpa pembatasan serta absennya proteksi *brute-force* pada halaman *login*.

4. *Reporting*

Tahap pelaporan bertujuan menyusun hasil pengujian secara sistematis dan dapat diverifikasi. Seluruh kerentanan yang ditemukan selama tahap *discovery* terdokumentasi dalam tabel berikut, yang mencakup nama kerentanan, domain, jenis kerentanan, dan ringkasan tingkat risiko awal berdasarkan analisis manual.

Tabel 1. Daftar Lengkap 38 Temuan Kerentanan

No	Informasi / Temuan
1	*Web Server* (Apache 2.4.62)
2	Sistem Operasi *(Debian)*
3	CMS *WordPress* 6.8.1
4	*Page Builder Elementor* 3.29.2
5	Bahasa *PHP* 8.2.28
6	*Frontend HTML5*
7	*jQuery* 3.7.1
8	Judul Halaman
9	*Header link, speculationrules*
10	*WordPress session cookies*
11	*IP Server* (103.138.10.12)
12	*Port* Terbuka (80, 443)
13	*Port* tertutup 113 (ident)
14	*Framework Golang net/http (Go-IPFS?)*
15	*SSL/TLS valid, wildcard*
16	File *robots.txt* terbuka
17	Meta generator *WordPress* terdeteksi
18	*Header X-Frame-Options* tidak tersedia
19	*Header Strict-Transport-Security* tidak tersedia
20	*Header X-Content-Type-Options* tidak tersedia
21	*Header X-Powered-By* terbuka
22	*Content-Encoding deflate*
23	*REST API /wp-json/* terbuka
24	*robots.txt*
25	*/wp-admin/* ditemukan
26	*/wp-login.php* ditemukan
27	*wp-config.php* ditemukan
28	*readme.html* ditemukan
29	*license.txt* ditemukan
30	*/admin/, /login/, admin/index.php, login.php*

No	Informasi / Temuan
31	*sitemap.xml* tersedia
32	*Indikasi blind SQL injection*
33	*Endpoint xmlrpc.php* aktif
34	*wp-cron.php* terbuka
35	Tema: *Inspiro* v2.0.7
36	Username *WordPress* terdeteksi (2 user)
37	*Plugin & tema* tidak bisa dianalisis karena tanpa API token
38	*Subdomain CNAME* tidak valid

Dari 38 temuan tersebut, dilakukan seleksi terhadap 10 kerentanan yang dianggap paling berpotensi membahayakan sistem berdasarkan aspek kemungkinan eksploitasi dan dampaknya. Pemilihan dilakukan secara kualitatif, mempertimbangkan vektor serangan, eksposur publik, serta jenis data yang dapat diakses atau dimanipulasi jika eksploitasi berhasil dilakukan.

Tabel 2. Sepuluh Kerentanan yang Diuji Lebih Lanjut

No	Kerentanan Ditemukan	Eksploitasi yang Dilakukan
1	xmlrpc.php aktif & *(Username 1 & Username 2)* terekspos	Brute-force login via xmlrpc.php menggunakan *WPScan* & wordlist terhadap 2 akun admin
2	wp-login.php mengindikasikan *Blind SQLi*	Eksploitasi *Blind SQL Injection* pada Parameter action=lostpassword di wp-login.php
3	File hello.php, readme.html dapat diakses	Eksploitasi File Terbuka untuk Pengungkapan Versi *WordPress*
4	wp-cron.php terbuka publik	Simulasi Serangan terhadap wp-cron.php untuk Menyebabkan Eksekusi Berulang
5	*REST API* /wp-json/ mengungkap data user	Enumerasi User *WordPress* melalui *REST API* wp-json
6	Tidak adanya *Header X-Frame-Options*	Eksploitasi *Clickjacking* Melalui Penyisipan Iframe ke Situs Target
7	Tidak adanya *Strict-Transport-Security (HSTS)*	Tidak dieksploitasi langsung, hanya dicatat sebagai temuan
8	Tidak adanya *X-Content-Type-Options*	Tidak dieksploitasi langsung, disarankan simulasi upload MIME attack

No	Kerentanan Ditemukan	Eksploitasi yang Dilakukan
9	Subdomain *CNAME* tidak valid	Identifikasi dan Eksploitasi Potensi *Subdomain Takeover*
10	Direktori & file admin/login terbuka (/admin, /login, /wp-admin)	Eksplorasi Direktori Sensitif untuk Potensi Bypass Autentikasi atau Enumerasi Struktur

Untuk mengukur tingkat keparahan kerentanan secara objektif, dilakukan penilaian menggunakan metode *Common Vulnerability Scoring System* versi 3.1 (CVSS v3.1). Evaluasi ini mempertimbangkan parameter teknis seperti vektor serangan *(Attack Vector)*, kompleksitas *(Complexity)*, hak akses yang dibutuhkan *(Privileges Required)*, dampak terhadap kerahasiaan, integritas, dan ketersediaan.

Tabel 3. Skor CVSS v3.1 pada 10 Kerentanan Utama

No	Kerentanan Ditemukan	Eksploitasi yang Dilakukan	Tingkat Kerentanan
1	xmlrpc.php aktif & *(Username 1 & Username 2)* terekspos	Brute-force login via xmlrpc.php menggunakan *WPScan* & wordlist terhadap 2 akun admin	7.5
2	wp-login.php mengindikasikan *Blind SQLi*	Eksploitasi *Blind SQL Injection* pada Parameter action=lostpassword di wp-login.php	8.6
3	File hello.php, readme.html dapat diakses	Eksploitasi File Terbuka untuk Pengungkapan Versi *WordPress*	5.3
4	wp-cron.php terbuka publik	Simulasi Serangan terhadap wp-cron.php untuk Menyebabkan Eksekusi Berulang	5.3
5	*REST API* /wp-json/ mengungkap data user	Enumerasi User *WordPress* melalui *REST API* wp-json	5.3
6	Tidak adanya *Header X-Frame-Options*	Eksploitasi *Clickjacking* Melalui	4.3

No	Kerentanan Ditemukan	Eksploitasi yang Dilakukan	Tingkat Kerentanan
		Penyisipan Iframe ke Situs Target	
7	Tidak adanya *Strict-Transport-Security (HSTS)*	Tidak dieksploitasi langsung, hanya dicatat sebagai temuan	5.4
8	Tidak adanya *X-Content-Type-Options*	Tidak dieksploitasi langsung, disarankan simulasi upload MIME attack	5.4
9	Subdomain *CNAME* tidak valid	Identifikasi dan Eksploitasi Potensi *Subdomain Takeover*	10.0
10	Direktori & file admin/login terbuka (/admin, /login, /wp-admin)	Eksplorasi Direktori Sensitif untuk Potensi Bypass Autentikasi atau Enumerasi Struktur	7.3
Total Score			64,4

Berdasarkan evaluasi tersebut, skor kumulatif dari seluruh kerentanan utama mencapai 64,4 dengan rata-rata 6,4, yang tergolong dalam kategori sedang (*medium*). Meskipun tidak tergolong kritis, skor ini menunjukkan adanya celah keamanan yang dapat dieksploitasi dalam skenario serangan nyata apabila tidak dilakukan mitigasi secara tepat dan cepat

5. Mitigasi

Setelah proses identifikasi kerentanan dilakukan, langkah selanjutnya adalah merancang strategi mitigasi yang tepat untuk mencegah potensi eksploitasi lebih lanjut. Tindakan mitigasi disusun berdasarkan jenis dan tingkat risiko dari masing-masing kerentanan. Tabel berikut merangkum daftar kerentanan yang ditemukan beserta rekomendasi mitigasinya:

Tabel 4. Rekomendasi Mitigasi

No.	Kerentanan Ditemukan	Rekomendasi Mitigasi
1	Endpoint xmlrpc.php aktif & *(Username 1 & Username 2)* terekspos	Nonaktifkan atau batasi akses xmlrpc.php jika tidak digunakan; gunakan *Plugin* keamanan; aktifkan rate-limiting.
2	wp-login.php mengindikasikan *Blind SQLi*	Validasi input secara ketat; gunakan prepared statement

No.	Kerentanan Ditemukan	Rekomendasi Mitigasi
		untuk semua query; aktifkan Web Application Firewall.
3	*File hello.php, readme.html* dapat diakses	Hapus *file default WordPress* yang tidak diperlukan; batasi akses publik via .htaccess.
4	wp-cron.php terbuka publik	Nonaktifkan akses eksternal ke wp-cron.php; gunakan cron job dari server langsung.
5	*REST API* /wp-json/ mengungkap data user	Batasi data user dari endpoint *REST API*; gunakan *Plugin* keamanan *REST API*.
6	Tidak adanya *Header X-Frame-Options*	Tambahkan *Header X-Frame-Options*: SAMEORIGIN di konfigurasi server.
7	Tidak adanya *Strict-Transport-Security* (HSTS)	Tambahkan *Header Strict-Transport-Security* untuk memastikan koneksi HTTPS.
8	Tidak adanya *X-Content-Type-Options*	Tambahkan *Header X-Content-Type-Options*: *nosniff* untuk mencegah *sniffing MIME-type.*
9	Subdomain *CNAME* tidak valid	Hapus atau benahi *CNAME* pada DNS zone; hindari *Subdomain Takeover*.
10	Direktori & file *admin/login* terbuka *(/admin, /login, /wp-admin)*	Batasi akses ke direktori admin; gunakan *reCAPTCHA, 2FA*, atau *Plugin* pemindah *login page* (*WPS Hide Login*).

Beberapa rekomendasi mitigasi pada tabel di atas dapat diimplementasikan dengan bantuan plugin keamanan yang tersedia di ekosistem *WordPress*. Untuk menonaktifkan akses *ke xmlrpc.php, plugin* seperti *Disable XML-RPC* atau *Wordfence Security* dapat digunakan. Pengamanan *endpoint login* dan *user enumeration* melalui *REST API* dapat dibantu dengan *plugin* seperti *WPS Hide Login, Limit Login Attempts Reloaded*, dan *Stop REST API*. Selain itu, *plugin Really Simple SSL* atau konfigurasi manual pada file *.htaccess* dapat digunakan untuk menambahkan *header* keamanan seperti *X-Frame-Options, Strict-Transport-Security,* dan *X-Content-Type-Options.* Penghapusan file default seperti *readme.html* dan *hello.php* juga dapat dilakukan secara manual atau melalui fitur-fitur yang disediakan oleh plugin seperti *WP Hardening.* Pemilihan dan penerapan *plugin* yang tepat tidak hanya mempermudah proses mitigasi, namun juga memperkuat lapisan keamanan *WordPress* secara keseluruhan

V. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa website Disparbudpora Kabupaten Pacitan masih memiliki sejumlah celah keamanan yang perlu diperhatikan. Melalui metode NIST SP 800-115

dengan pendekatan *white-box testing*, ditemukan 38 temuan teknis, di mana 10 di antaranya (26,32%) diklasifikasikan sebagai kerentanan dengan tingkat risiko yang dapat membahayakan sistem. Hasil pengukuran dengan CVSS v3.1 menunjukkan rata-rata skor keparahan sebesar 6,4 yang masuk dalam kategori sedang *(medium)*. Beberapa kerentanan utama yang teridentifikasi antara lain aktivasi xmlrpc.php, potensi blind SQL injection, eksposur akun melalui REST API, serta ketiadaan HTTP security headers penting. Fakta ini menunjukkan bahwa meskipun website menggunakan platform yang cukup umum seperti WordPress, risiko keamanan tetap tinggi apabila tidak dilakukan konfigurasi dan pengawasan yang tepat.

Sarannya diperlukan tindakan segera dari pihak pengelola untuk menerapkan mitigasi terhadap celah yang ditemukan, baik melalui konfigurasi plugin keamanan maupun pembatasan akses terhadap fitur-fitur rawan. Selain itu, audit keamanan website secara rutin harus dijadikan bagian dari kebijakan pengelolaan sistem informasi instansi. Penelitian selanjutnya disarankan untuk menerapkan metode pengujian lain seperti black-box atau kombinasi (gray-box) guna mendapatkan gambaran keamanan sistem yang lebih komprehensif, serta memperluas cakupan analisis hingga ke sisi server dan jaringan pendukung.

VI. DAFTAR PUSTAKA

[1] J. P. Atmaja, "Peran Teknologi Informasi Dalam Peningkatan Daya Saing Destinasi Pariwisata Di Indonesia," *J. Destin. Pariwisata*, vol. 11, no. 1, p. 151, 2023, doi: 10.24843/jdepar.2023.v11.i01.p20.

[2] F. Rahman Najwa, "Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia," *AL-BAHTS J. Ilmu Sos. Polit. dah Huk.*, vol. 2, no. 1, pp. 8–16, 2024, doi: 10.32520/albahts.v2i1.3044.

[3] S. E. Prasetyo, H. Haeruddin, and K. Ariesryo, "Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall," *Antivirus J. Ilm. Tek. Inform.*, vol. 18, no. 1, pp. 27–36, 2024, doi: 10.35457/antivirus.v18i1.3339.

[4] A. N. Annaufal, M. N. Ardhani, S. Bintang, and G. Abetnego, "Analisis Kerentanan pada Situs Buatinkamu . id dengan Pengujian Penetrasi Metode Black Box EXPLORE – Volume 15 No 1 Tahun 2025 Terakreditasi Sinta 5 SK No : 23 / E / KPT / 2019," vol. 15, no. 1, pp. 11–17, 2025.

[5] G. T. A. Ramadhani, M. R. R. Steyer, M. H. Maulidan, and A. Setiawan, "Analisis Kerentanan WordPress dengan WPScan dan Teknik Mitigasi," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 15, 2024, doi: 10.47134/pjise.v1i4.2613.

[6] A. Gustiyono, E. I. Alwi, and S. M. Abdullah, "Analisa Kerentanan Website Terhadap Serangan Cross-Site Scripting (XSS) Metode Penetration Testing Analyze Website Vulnerability To Cross-Site Scripting (XSS) Attacks Using Penetration Testing," vol. 7, no. 1, pp. 25–33, 2024.

[7] Karen Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology," *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2020, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800

[8] P. Farmadika, A. Widjajarto, and M. Fathinuddi, "Implementasi Dan Mitigasi Phishing Attack Menggunakan Metode Human- Based Pada Pt . Xyz," vol. 11, no. 6, pp. 7310–7320, 2024.