INDOTECH
INDONESIAN JOURNAL OF EDUCATION AND COMPUTER SCIENCE

Indonesian Journal of Education And Computer Science

Vol. 3, No. 2, Agustus 2025
Hal 51-65

E-ISSN : 2987-2650
P-ISSN : 2987-7644

Site : https://jurnal.intekom.id/index.php/indotech

Analisis Kerentanan Keamanan *Website* Menggunakan *Open Web Application Security Project* (Owasp) Top-10 Studi Kasus *(web.bnpb.go.id)*

Arfan Dwi Madya[1], Rakhmat Purnomo[2], Nurfiyah[3]
[1,2,3] Fakultas Ilmu Komputer , Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Article Info

Article history:

Received July 14, 2025
Revised Agustus19, 2025
Accepted Agustus 31, 2025

Kata Kunci:

Keamanan Web,
OWASP Top 10,
Pengujian Keamanan,
Situs Pemerintah,
NIST SP 800-115

Keywords:

Web Security,
OWASP Top 10,
Security Testing,
Government Website,
NIST SP 800-115

ABSTRAK

Pemanfaatan situs web instansi pemerintah di Indonesia terus meningkat seiring dengan kebutuhan layanan publik berbasis digital. Namun, perkembangan tersebut diikuti oleh meningkatnya ancaman keamanan siber yang berpotensi mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Penelitian ini berfokus pada analisis kerentanan keamanan pada subdirektori PPID situs resmi Badan Nasional Penanggulangan Bencana (BNPB), dengan mengacu pada standar OWASP Top 10 tahun 2025 serta metodologi NIST SP 800-115 untuk pengujian penetrasi. Proses pengujian dilakukan menggunakan berbagai tools keamanan, di antaranya OWASP ZAP dan Nmap, yang mampu mengidentifikasi celah pada aplikasi web. Hasil pengujian menunjukkan adanya beberapa kerentanan signifikan, seperti akses direktori terbuka, brute-force login, SQL injection, serta konfigurasi header keamanan yang lemah. Temuan ini mengindikasikan bahwa meskipun situs telah berfungsi optimal dalam menyediakan layanan informasi, masih terdapat risiko eksploitasi yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Oleh karena itu, penelitian ini merekomendasikan peningkatan konfigurasi keamanan server, penerapan kebijakan proteksi yang lebih ketat, serta pengujian keamanan berkala guna meminimalkan potensi ancaman. Dengan demikian, diharapkan hasil penelitian ini dapat menjadi rujukan dalam upaya memperkuat keamanan sistem informasi pemerintah di era transformasi digital.

ABSTRACT

The use of government agency websites in Indonesia continues to increase in line with the need for digital-based public services. However, this development is accompanied by increasing cybersecurity threats that have the potential to compromise the privacy, integrity, and availability of information. This study focuses on analyzing security vulnerabilities in the PPID subdirectory of the official website of the National Disaster Management Agency (BNPB), with reference to the OWASP Top 10 2025 standard and the NIST SP 800-115 methodology for penetration testing. The testing process was conducted using various security tools, including OWASP ZAP and Nmap, which are capable of identifying vulnerabilities in web applications. The test results revealed several significant vulnerabilities, such as open directory access, brute-force login, SQL injection, and weak security header configurations. These findings indicate that although the site is functioning optimally in providing information services, there is still a risk of exploitation that can be exploited by irresponsible parties. Therefore, this study recommends improving server security configurations, implementing stricter protection policies, and regular security testing to minimize potential threats. Thus, it is hoped that the results of this study can serve as a

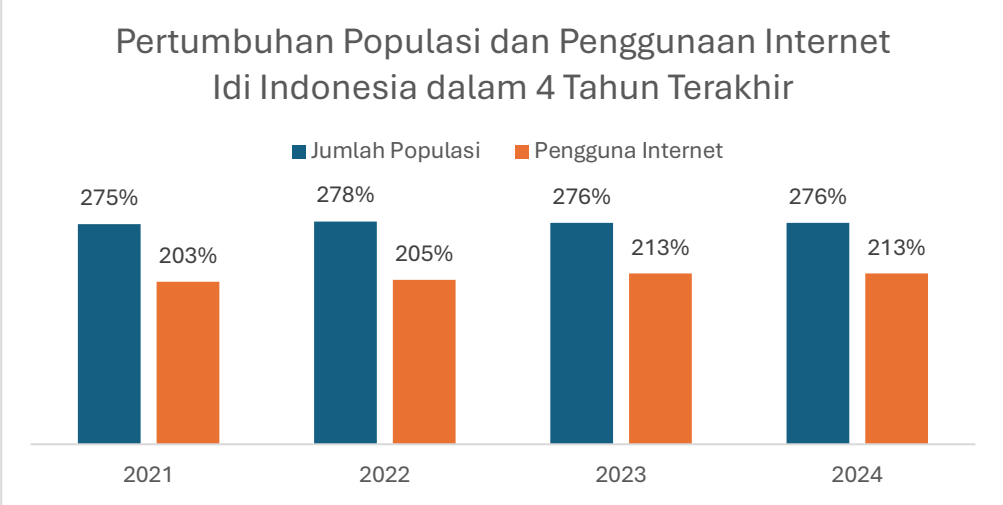
reference in efforts to strengthen the security of government information systems in the era of digital transformation.

Corresponding Author:

Arfan Dwi Madya
Fakultas Ilmu Komputer , Universitas Bhayangkara Jakarta Raya,
Jakarta, Indonesia
Email: 02110715156@mhs.ubharajaya.ac.id

1. PENDAHULUAN

Perkembangan informasi teknologi saat ini berlangsung sangat cepat dan dinamis. Hal ini terlihat dari meningkatnya jumlah pengguna situs web untuk berbagai keperluan, mulai dari lembaga pemerintahan, pendidikan, organisasi, hingga kebutuhan pribadi [1]. Dalam perkembangan ini, keamanan menjadi hal yang sangat penting untuk diperhatikan. Semakin banyak pengguna yang terhubung ke internet, semakin tinggi pula risiko kejahatan siber yang bisa terjadi akibat ulah oknum yang tidak bertanggung jawab [2].



Gambar 1. Pertumbuhan Populasi dan Penggunaan Internet di Indonesia dalam 4 Tahun Terakhir

Menurut laporan digital yang dibuat oleh We Are Social (Hootsuite), penggunaan internet di Indonesia dalam 4 tahun terakhir mengalami kenaikan 1% di mana pada tahun 2021 mencapai 275%, di 2022 mencapai 278%, dan di tahun 2023 mencapai 276%, akan tetapi jika dilihat dari data tersebut penggunaan internet pada bulan Januari 2024 sudah mencapai 276 juta pengguna, sehingga dapat dipastikan pada awal Januari 2025 mendatang jumlah populasi dan penggunaan internet di Indonesia terus mengalami kenaikan angka yang signifikan [3]. Dengan semakin bertambahnya penggunaan internet di Indonesia, menandakan bahwa kini masyarakat Indonesia lebih banyak mendapatkan informasi melalui internet. Website merupakan salah satu tujuan utama bagi pengguna internet khususnya dalam memanfaatkan untuk melakukan aktivitas baik untuk keperluan bisnis maupun mengakses sebuah informasi [4].

Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024, serangan siber terhadap instansi pemerintahan di Indonesia mengalami peningkatan yang signifikan. Salah satu ancaman yang paling umum adalah web defacement, di mana peretas mengubah tampilan halaman website untuk

menyebarkan propaganda atau mencuri data sensitif [5]. Selain itu, ancaman lain seperti SQL Injection, Cross-Site Scripting (XSS), dan Broken Authentication juga menjadi tantangan utama dalam menjaga keamanan sistem informasi berbasis web [6],[7].

Dari observasi terhadap domain web.bnpb.go.id melalui situs zone-h.com—yang memuat daftar laporan kerentanan—peneliti menemukan kasus penyusupan pada domain web.bnpb.go.id/ppid selama dua tahun terakhir [8]. Dan peneliti mendapatkan hasil berupa adanya kasus yang terjadi pada domain *web.bnpb.go.id/ppid* yang telah terjadi sejak dua tahun terakhir ini seperti yang tersaji pada gambar 1.


Total notifications: **1** of which **1** single ip and **0** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Time	Notifier	H	M	R	L	★	Domain	OS	View
2021/01/06	0x666cx					★	web.bnpb.go.id/hukum/artikel/d...	Linux	mirror

1

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Gambar 2. Hasil observasi kerentanan domain target menggunakan [20]

Dengan adanya data catatan kasus di atas, perlu dilakukan langkah antisipasi melalui pengujian sistem keamanan aplikasi berbasis website. Hal ini menjadi sangat penting untuk mencegah ancaman serangan siber yang semakin marak terjadi dalam beberapa tahun terakhir [9],[10]. Seiring dengan pesatnya perkembangan aplikasi berbasis web, jumlah kasus kejahatan siber juga meningkat dengan berbagai teknik serangan yang semakin canggih [11],[12].

Dengan adanya data catatan kasus di atas, perlu dilakukan langkah antisipasi melalui pengujian sistem keamanan aplikasi berbasis website. Hal ini menjadi sangat penting untuk mencegah ancaman serangan siber yang semakin marak terjadi dalam beberapa tahun terakhir [9],[10]. Seiring dengan pesatnya perkembangan aplikasi berbasis web, jumlah kasus kejahatan siber juga meningkat dengan berbagai teknik serangan yang semakin canggih [11],[12].

Oleh karena itu, diperlukan penelitian yang komprehensif untuk mengidentifikasi, menganalisis, dan memberikan solusi terhadap potensi kerentanan yang ada. Hasil penelitian ini diharapkan dapat menjadi referensi yang bermanfaat bagi para pengembang (developer) dalam mengimplementasikan langkah-langkah keamanan yang lebih baik guna melindungi sistem website dari berbagai ancaman siber [15]. Dengan pendekatan yang tepat, keamanan aplikasi web dapat ditingkatkan secara signifikan, sehingga memberikan perlindungan optimal bagi pengguna dan data yang dikelola oleh sistem tersebut [20].

Sejak diterbitkannya Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, informasi menjadi satu hal wajib yang harus disediakan oleh seluruh badan publik di Indonesia. Undang-Undang ini menjamin warga negaranya memperoleh informasi dan juga merupakan jawaban dari kebutuhan masyarakat akan informasi. Informasi bukan lagi menjadi satu hal yang rahasia atau ditutupi tetapi menjadi hal yang wajib dibuka karena menutupi suatu informasi berarti menyalahi Undang-Undang Keterbukaan Informasi Publik [16]. Salah satu bagian penting dari domain web.bnpb.go.id/ppid adalah direktori/ppid atau layanan pejabat pengelolah informasi dan dokumentasi yang berfungsi sebagai pintu informasi publik dan memiliki elemen autentikasi pengguna. Oleh karena itu direktori ini menjadi fokus utama dalam proses pengujian..

Untuk mengidentifikasi dan mengevaluasi tingkat kerentanan keamanan pada website web.bnpb.go.id, penelitian ini menggunakan standar Open Web Application Security Project (OWASP)

Top 10 sebagai referensi utama. OWASP Top 10 tahun 2024 merupakan daftar terbaru yang berisi sepuluh jenis ancaman keamanan web yang paling umum dan berbahaya. Dengan mengacu pada standar ini, penelitian akan melakukan uji penetrasi (penetration testing) untuk mengidentifikasi celah keamanan serta memberikan rekomendasi mitigasi guna meningkatkan ketahanan sistem terhadap serangan siber [18],[19]. Dikarenakan banyaknya subdomain yang ada, penulis dalam pengujian ini hanya memfokuskan pada tiga subdomain berdasarkan hasil pencarian informasi dan proses vulnerability scanner yang telah dilakukan sebelum penyusunan laporan skripsi ini, ketiga subdomain tersebut dianggap bermasalah dan perlu untuk dilakukan pengujian serta memberikan rekomendasi yang dapat digunakan oleh BNPB dalam meningkatkan keamanan website mereka.

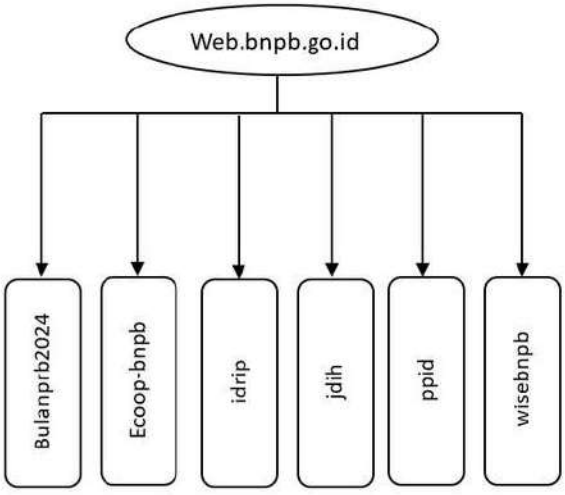
2. METODE

2.1 Objek dan Tempat Penelitian

Objek utama dalam penelitian ini adalah sistem aplikasi berbasis web milik Badan Nasional Penanggulangan Bencana (BNPB), yang dapat diakses melalui domain web.bnpb.go.id. Fokus utama yang diuji dalam penelitian ini adalah halaman e-PPID pada URL: https://web.bnpb.go.id/ppid. Subdirektori ini merupakan bagian dari website BNPB yang digunakan untuk pengelolaan informasi publik dan pelayanan keterbukaan informasi sebagaimana praktik PPID pada instansi pemerintah di Indonesia, yang secara kelembagaan dan layanan semakin dimatangkan dalam beberapa tahun terakhir [14], [16].

Dari sisi tata kelola dan kebijakan, e-PPID berada dalam ekosistem e-Government/SPBE yang bertujuan meningkatkan transparansi, akuntabilitas, dan kualitas layanan publik, sehingga pengujian dan perbaikan berkelanjutan pada kanal layanan informasi publik menjadi relevan [16], [17].

Dari sisi keamanan aplikasi web, pengujian akan mengacu pada kerangka OWASP Top 10 dan praktik uji kerentanan terkini (mis. OWASP ZAP) yang terbukti efektif pada studi mutakhir untuk mendeteksi celah seperti injection, security misconfiguration, dan kelemahan header keamanan pada situs pemerintah [13], [14]. Oleh karena itu, *https://web.bnpb.go.id/ppid* ditetapkan sebagai fokus utama pengujian kerentanan, yang dimana terlempir pada gambar di bawah ini :



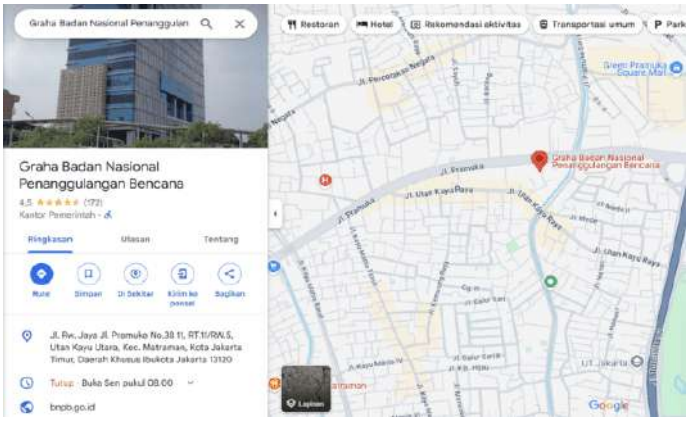
Gambar 3. Struktur Subdomain dan Informasi Keamanan *Web.bnpb.go.id*

Semua subdomain menggunakan *port* 443 (HTTPS). Sertifikat SSL *valid*, namun dalam beberapa kasus tidak cocok dengan *host* name, menimbulkan potensi peringatan *browser* beberapa *header* yang tidak diaktifkan:

1. X-*Frame-Options* : Rentan terhadap *clickjacking*.
2. *Strict-Transport-Security* : Rentan terhadap *downgrade attack*.

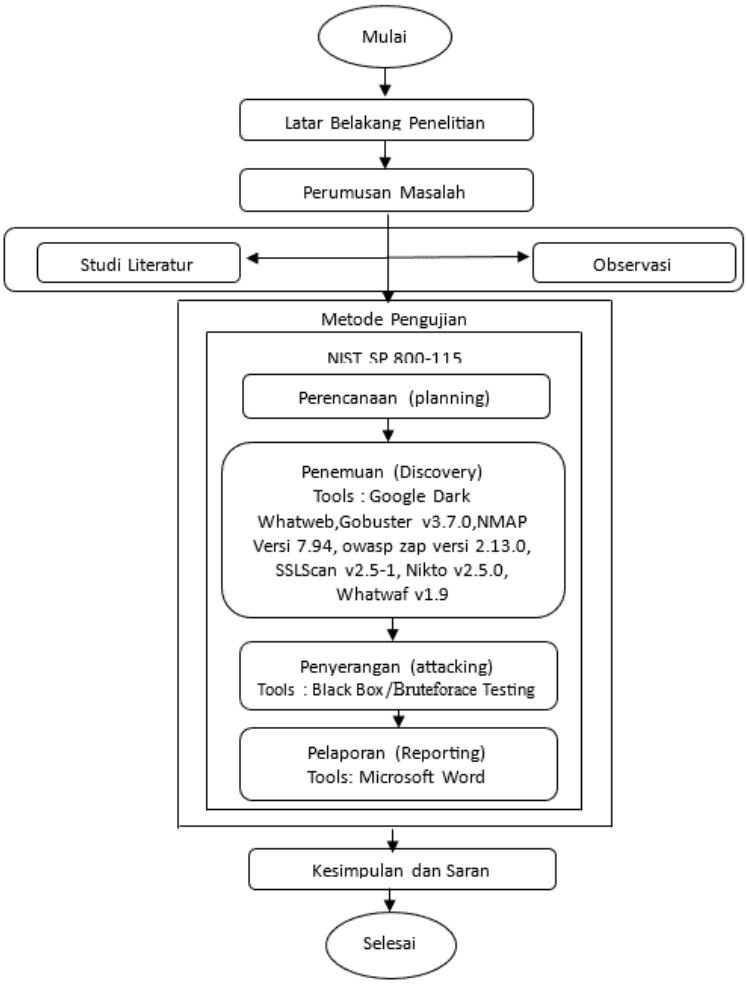
3. X-*Content-Type-Options* : Rentan terhadap serangan MIME *sniffing*.

Tempat pelaksanaan penelitian dilakukan secara *remote* yang telah disiapkan oleh peneliti menggunakan mesin *virtual* berbasis Kali Linux, mengingat objek penelitian berupa sistem web yang dapat diakses melalui jaringan internet. Penelitian ini dilaksanakan dalam rentang waktu satu minggu, dimulai dari tanggal 30 Juni 2025 , dengan tahapan kerja meliputi perencanaan, pengumpulan informasi, pengujian kerentanan, serta dokumentasi hasil pengujian.



Gambar 4. Lokasi Penelitian

2.2 Kerangka Penelitian



Gambar 5. Kerangka Penelitian

2.3 Metode Pengumpulan Data

Dalam melakukan pengujian pada penelitian pengumpulan data dilakukan dengan menggunakan metode studi pustaka dan observasi, adapun untuk penjelasannya sebagai berikut:

2.4 Penelitian Serupa

Penelitian serupa digunakan sebagai penyusun kerangka teori penelitian dan perbandingan hasil penelitian sebelumnya. Adapun studi literatur yang dilakukan pada penelitian ini bersumber dari beberapa refrensi antara lain melalui jurnal, *proceeding*, buku, tugas akhir, dan juga media *digital* seperti internet maupun *website.*

2.5 Observasi

Dalam observasi penelitian ini, peneliti melakukan Observasi yang berlangsung sejak 30 Juni 2025 hingga waktu penelitian selesaisaat ini. Observasi dilakukan untuk melakukan pengumpulan data dan informasi sebagai dasar penelitian terkait uji kerentanan pada *website* yang tentunya terkait dari studi kasus pada penelitian ini yaitu pada *website* domain *bnpb.go.id/ppid* Observasi dilakukan dengan cara mencari informasi terkait permasalahan kerentanan apa saja yang terjadi pada domain *bnpb.go.id/ppid* melalui media *internet* berupa *situs website* terkait.

2.6 Metode Analisis

Penelitian ini menerapkan metodologi NIST SP 800-115, yang merupakan standar dalam pengujian keamanan informasi. Metodologi ini terdiri dari empat tahapan utama sebagai berikut:

1. Perencanaan *(Planning)*
   a. Menentukan ruang lingkup pengujian, termasuk subdomain target.
   b. Menyusun jadwal pengujian dan mengidentifikasi alat yang akan digunakan.
   c. Mempersiapkan lingkungan pengujian, seperti konfigurasi *Oracle* VM *VirtualBox* dan Kali Linux versi 2025.1c.
   d. Mendapatkan izin resmi dari pihak yang berwenang untuk melaksanakan pengujian.
2. Penemuan *(Discovery)*
   a. Menggunakan teknik *Google Dork* untuk menemukan informasi sensitif yang mungkin terekspos di internet.
   b. Melakukan pemindaian jaringan dengan NMAP versi 7.97 untuk mengidentifikasi layanan, sistem operasi, dan *port* yang terbuka.
   c. Menggunakan *WhatWeb* untuk mengidentifikasi teknologi web seperti CMS, *server*, dan *framework* yang digunakan.
   d. Menggunakan SSLScan v3.7.0 untuk memeriksa konfigurasi SSL/TLS dan mendeteksi *cipher* atau protokol yang tidak aman.
   e. Menggunakan *Gobuster* v2.1.5-1 untuk menemukan direktori atau file tersembunyi melalui *brute-force* berbasis *wordlist*.
   f. Memanfaatkan OWASP ZAP versi 2.16.1 dan Nikto versi 2.5.0 untuk mendeteksi kerentanan aplikasi web berdasarkan OWASP Top-10.
3. Penyerangan *(Attacking)*
   a. Menguji eksploitasi kerentanan yang ditemukan pada tahap *discovery.*
   b. Melakukan simulasi serangan menggunakan pendekatan *Black Box* / *Bruteforace Testing*, yaitu pengujian tanpa pengetahuan internal tentang sistem.
   c. Mencatat hasil eksploitasi untuk dianalisis lebih lanjut.
4. Pelaporan *(Reporting)*
   a. Mencatat semua temuan terkait jenis kerentanan dan tingkat risikonya.

b. Menyusun laporan yang mencakup deskripsi kerentanan, dampak potensial, dan rekomendasi mitigasi.
c. Menyajikan hasil pengujian kepada pihak yang berwenang untuk evaluasi lebih lanjut.

2.7 Analisis Kebutuhan Sistem

Tujuan dari analisis kebutuhan sistem merupakan tahap mencari tahu apa saja yang dibutuhkan di dalam mengembangkan sistem seperti perangkat keras dan perangkat lunak.

1. Kebutuhan Perangkat keras *(Hardware)*
   Perangkat keras merupakan alat yang digunakan peneliti yang berfungsi dalam pengumpulan dan pengembangan sistem sebagai berikut:
   a. Laptop : MacBook Pro 13-inch, M1,2020
   b. Chip : Apple M1
   c. Prosesor : MacOS Sequoia
   d. RAM : 8 GB
   e. Storage : 245 GB
2. Kebutuhan Perangkat Lunak *(Sofeware)*
   Perangkat lunak yang digunakan dalam penelitian ini sebagai berikut :
   a. *Oracle* VM VirtualBox-amd64 Versi 7.18
   b. Google Hacking
   c. NMAP Versi 7.97
   d. *WhatWeb*
   e. SSLScan v3.7.0
   f. *Gobuster* v2.1.5-1
   g. OWASP ZAP Versi 2.16.1
   h. Nikto Versi 2.5.0
   i. Whatwaf
   j. Bruteforace

3. HASIL DAN PEMBAHASAN

Pengujian keamanan pada direktori/ppid dari domain *web.bnpb.go.id* dilakukan menggunakan pendekatan *black-box testing* berbasis OWASP Top 10 serta *tools* seperti OWASP ZAP, SQLMap, dan Nikto. Berdasarkan hasil analisis, ditemukan sejumlah temuan penting:

1. Kerentanan SQL *Injection* muncul pada formulir *input login*. Saat *payload injeksi* dimasukkan, sistem merespons dengan tanda-tanda adanya *query* manipulasi. Namun, saat eksploitasi lanjutan dilakukan, permintaan diblokir oleh *Web Application Firewall* (WAF), yang menunjukkan bahwa sistem sudah memiliki pertahanan awal tetapi belum cukup untuk mencegah teknik *bypass*.
2. *Sensitive* Data *Exposure* terjadi melalui keberhasilan serangan *brute-force login* menggunakan username valid yang berhasil diidentifikasi. Sistem tidak memiliki CAPTCHA, *rate limiting*, ataupun *two-factor* authentication (2FA), yang membuka peluang *login* tanpa proteksi tambahan.
3. *Directory Listing* ditemukan aktif di beberapa path seperti *upload* dan *assets*, yang memungkinkan pengguna tak sah melihat file dan struktur folder yang seharusnya disembunyikan.
4. Konfigurasi header HTTP tidak aman, seperti tidak adanya *X-Frame-Options , Strict-Transport-Security* , dan X-*Content-Type-Options*, menunjukkan sistem belum mengimplementasikan *best practice* dalam hardening aplikasi web.
5. *Cookie* keamanan, terutama Set-*Cookie*, tidak mengaktifkan *flag Secure* dan *HttpOnly*, yang memungkinkan pencurian sesi melalui serangan seperti *cross-site scripting* (XSS).

Secara keseluruhan, direktori/ppid memiliki kerentanan serius yang dapat dimanfaatkan oleh penyerang dengan teknik dasar hingga menengah.

Tabel 1. Rekapitulasi Hasil Pemindaian Kerentanan

Tingkat Resiko	Jumlah Temuan	Penjelasan
Tinggi	3	Terdeteksi SQL *Injection, Directory Listing* aktif, *Login bruteforce* berhasil
Sedang	5	Tidak adanya konfigurasi CSP, *header* keamanan, dan tidak adanya CAPTCHA
Rendah	9	*Cookie* tanpa *HttpOnly*, informasi versi server terbuka (*Apache*, PHP)
Informasional	4	Komentar mencurigakan pada kode HTML, struktur folder terbuka

Tabel 2. Ringkasan Hasil Pengujian Berdasarkan OWASP TOP 10-2025

No	OWASP Top 10 2025	Celah Kerentanan	Penjelasan
1	A1: *Broken Access Control*	*Directory Listing*	Folder /*upload* dan /*assets* dapat diakses langsung tanpa autentikasi
2	A2: *Cryptographic Failures*	*Sensitive* Data *Exposure*	*Login* berhasil dengan serangan *brute-force*, tanpa 2FA atau *rate-limiting*
3	A3: *Injection*	SQL *Injection*	Indikasi *query* manipulatif terdeteksi, diblokir oleh WAF (*Cloudflare*)
4	A5: *Security Misconfiguration*	*Header* Keamanan Tidak Aktif	X-*Frame-Options, Strict-Transport-Security* tidak terdeteksi
5–10	-	-	Tidak ada temuan signifikan lainnya (XSS, SSRF, API *issues*, dll.)

3.1 Hasil Pengujian SQL *Injection*

SQL *Injection* adalah salah satu jenis serangan terhadap aplikasi web yang terjadi ketika penyerang dapat menyisipkan perintah SQL berbahaya ke dalam *field input*, yang kemudian dijalankan oleh *serve*r basis data. Tujuan utama dari serangan ini adalah untuk membaca, memodifikasi, atau menghapus data yang seharusnya tidak dapat diakses oleh pengguna biasa. Pada pengujian ini, peneliti menggunakan *tools* otomatis seperti SQLMap untuk mendeteksi potensi celah SQL *Injection* pada parameter URL atau *form input* dari salah satu subdomain situs *web.bnpb.go.id/ppid.* Beberapa teknik pengujian yang digunakan antara lain:

1. *Error-Based Injection*
2. *Union-Based Injection*
3. *Boolean-Based Blind Injection*

3.1.1 Hasil Pengujian

1. Sistem menunjukkan respon yang mengindikasikan potensi kerentanan terhadap SQL *Injection* pada salah satu parameter.
2. memberikan respons yang menunjukkan kemungkinan manipulasi *query*. SQLMap mengindikasikan bahwa parameter rentan terhadap SQL *Injection* (*union-based* dan *boolean-based*). Namun, ketika dilakukan eksploitasi lanjutan untuk dump database, koneksi ditolak dengan error 403 *Forbidden*, menunjukkan bahwa *firewall* seperti *Cloudflare* atau proteksi *ModSecurity* aktif.
3. Tidak ditemukan akses langsung ke database karena perlindungan aktif dari WAF.

3.2 Hasil Pengujian *Sensitive* Data Exposure

Pengujian *sensitive* data exposure dilakukan dengan dua pendekatan:

1. *Brute-force Login*: Penyerang mencoba berbagai kombinasi *username* dan *password*. Salah satu username valid berhasil digunakan untuk *login* ke halaman e-PPID. Hal ini sangat berbahaya karena:

a. Tidak ada *rate-limiting* (bisa mencoba login berulang-ulang)
b. Tidak ada CAPTCHA
c. Tidak ada 2FA

2. Eksposur Informasi di *Source Code*: Kode HTML dan *JavaScript* pada halaman/ppid mengandung komentar seperti:

$$html$$
$$< ! - - T0D0 : disable\ debug\ for\ producation\ - ->$$

Ini menunjukkan adanya kelalaian penghapusan elemen pengujian sebelum *deployment.*

3. HTTPS memang aktif, namun *header* keamanan seperti *Strict-Transport-Security* tidak aktif, sehingga tidak memaksa *browser* untuk selalu menggunakan koneksi aman.

3.3 Hasil Pengujian *Directory Listing*

Penelusuran dilakukan secara manual dan menggunakan *tools* seperti Nikto dan *Gobuster*. Beberapa URL yang ditemukan dapat diakses tanpa autentikasi:

1. *https://web.bnpb.go.id/ppid/.git/*

Folder tersebut semestinya tidak diekspos ke publik. *Server* tidak menggunakan aturan konfigurasi seperti:

$$apache$$
$$0ptions\ -\ Indexes$$

yang diperlukan untuk menonaktifkan tampilan isi direktori. Hal ini membuka peluang bagi *attacker* untuk melakukan fingerprinting, path *traversal*, dan *enumeration file* konfigurasi penting.

3.4 Laporan Akhir

Setelah proses eksploitasi dilakukan, disusun sebuah ringkasan untuk mempermudah identifikasi keseluruhan kerentanan yang muncul, serta untuk mengelompokkan kerentanan berdasarkan dampaknya terhadap aspek *Confidentiality, Integrity,* dan *Availability* (CIA). Selain itu, ringkasan ini juga bertujuan untuk menentukan prioritas penanganan terhadap kerentanan yang memiliki tingkat risiko tertinggi, disertai dengan rekomendasi langkah-langkah mitigasi yang sesuai.

3.5 Hasil Pengujian *https://web.bnpb.go.id/ppid*

Hasil Pengujian Kerentanan *https://web.bnpb.go.id/ppid* dari Kegagalan *confidentiality*

Tabel 3. Hasil pengujian dari aspek confidentiality

No	*Vulnerabilities*	Dampak Serangan	Hasil Pengujian	Skor	Kualitatif	Rekomendasi
1	*Sensitive* Data *Exposure*	File PDF yang menampilkan NIP	Subdomain e-*ppid.bnpb.go.id* menampilkan data pribadi	7.5	*High*	Terapkan *Access Control*, HTTPS penuh, dan masking data
2	*Directory Listing Enabled*	Penyerang bisa menelusuri semua file direktori	Akses ke /upload/ memperlihatkan daftar file	6.2	Medium	Nonaktifkan *directory listing*, gunakan *Options - Indexes*
3	*Leaked Server* Info *Headers*	Info server membantu merancang serangan	*Header: Apache*/2.4.29, PHP/7.2.24 terdeteksi	5.4	*Low*	Konfigurasi server: *ServerTokens Prod*, *ServerSignature Off*

Berdasarkan hasil pengujian aspek *Confidentiality*, ditemukan tiga kerentanan yang dapat membahayakan keamanan informasi pada sistem yang diuji, *Sensitive* Data *Exposure* (Skor: 7.5 – *High*): Teridentifikasi adanya file PDF yang memuat informasi pribadi (NIP) pada subdomain tertentu. Hal ini berpotensi mengakibatkan kebocoran data sensitif. *Directory Listing Enabled* (Skor: 6.2 – *Medium*): Ditemukan bahwa direktori dapat diakses secara terbuka, sehingga memungkinkan pihak tidak berwenang menelusuri dan mengakses seluruh file dalam direktori tersebut. Untuk mengatasi hal ini, perlu dinonaktifkan fitur *directory listing* dengan mengkonfigurasi opsi *Options -Indexes, Leaked Server* Info *Headers* (Skor: 5.4 – *Low*): Informasi mengenai versi server dan aplikasi (seperti Apache dan PHP) terdeteksi melalui HTTP *headers*. Informasi ini dapat dimanfaatkan oleh penyerang untuk merancang serangan yang lebih spesifik. Rekomendasi perbaikannya adalah melakukan konfigurasi ulang pada *server* dengan mengaktifkan *ServerTokens Prod* dan *ServerSignature Off.*

3.6 Hasil Pengujian Kerntanan *https://web.bnpb.go.id/ppid* dari Kegagalan *Integrity*

Tabel 4. Hasil Pengujian dari Aspek *Integrity*

No	Vulnerabilities	Dampak Serangan	Hasil Pengujian	Skor	Kualitatif	Rekomendasi
1	SQL *Injection*	Modifikasi/hapus data database	SQL *Injection* berhasil disimulasikan	8.0	*High*	Gunakan *prepared* statements dan validasi input
2	Parameter Tampering	Modifikasi parameter untuk akses data lain	ID URL dapat dimanipulasi untuk akses data lain	6.7	Medium	Validasi parameter di sisi server, otorisasi berbasis *role*
3	*Insecure Deserialization*	Penyusupan *payload* objek	Tidak ditemukan bukti deserialisasi aman	6.0	Medium	Gunakan format aman (JSON), *whitelist class*, validasi objek

Hasil pengujian menunjukkan adanya tiga kerentanan keamanan, yaitu SQL *Injection* (Skor: 8.0 – *High*) yang memungkinkan modifikasi atau penghapusan data dan perlu ditangani dengan *prepared statements* serta validasi input, Parameter Tampering (Skor: 6.7 – *Medium*) yang memungkinkan manipulasi ID URL dan membutuhkan validasi sisi *server* serta otorisasi berbasis *role*, serta *Insecure* Deserialization (Skor: 6.0 – *Medium*) yang meskipun belum dieksploitasi, tetap memerlukan penggunaan format aman seperti JSON, pembatasan kelas (*whitelist class*), dan validasi objek untuk mencegah penyusupan *payload*.

3.7 Hasil Pengujian https://web.bnpb.go.id/ppid dari Kegagalan *Availability*

Tabel 5. Hasil Pengujian dari Aspek *Availability*

No	*Vulnerabilities*	Dampak Serangan	Hasil Pengujian	Skor	Kualitatif	Rekomendasi
1	*Bruteforce Login*	Sistem *down* karena percobaan *login* berulang	Tidak ada rate *limiting* atau CAPTCHA di halaman *login*	7.0	*High*	CAPTCHA, lockout policy, blok IP, delay waktu login
2	*DoS - Resource Exhaustion*	*Server overload*	Tidak ada proteksi trafik abnormal	6.5	Medium	Gunakan WAF, CDN, monitoring trafik server
3	*No Failover Mechanism*	Sistem tidak punya backup bila server gagal	Tidak ditemukan konfigurasi *failover/load balancing*	5.8	Medium	Terapkan *load balancer*, DNS *failover*, server cadangan

Berdasarkan hasil pengujian, ditemukan tiga kerentanan utama yang berdampak pada ketersediaan sistem: *Bruteforce Login* (skor 7.0), DoS - *Resource Exhaustion* (6.5), dan *No Failover Mechanism* (5.8). Ketiganya menunjukkan kurangnya proteksi terhadap serangan berulang, trafik abnormal, dan kegagalan *server*. Diperlukan penerapan CAPTCHA, WAF, serta konfigurasi *failover* untuk meningkatkan keamanan dan keandalan sistem.

3.8 Skor Akhir Tingkat Kerentanan *web.bnpb.go.id*

Tabel 6. Skor Akhir Tingkat Kerentanan *web.bnpb.go.id/ppid*

No	Web	*Confidentiality*	*Integrity*	*Availability*	Rata-rata / Peringkat Kualitatif
1	web.bnpb.go.id/ppid	6.5	6.9	6.4	6.6 / Medium *to High*

Hasil analisis terhadap tingkat kerentanan pada situs *web.bnpb.go.id/ppid* menunjukkan bahwa skor rata-rata dari tiga aspek utama, yaitu *Confidentiality* (6.5), *Integrity* (6.9), dan *Availability* (6.4), berada pada kisaran 6.6. Skor ini termasuk dalam kategori Medium *to High*, yang mengindikasikan bahwa *website* tersebut memiliki tingkat risiko keamanan yang cukup signifikan.

Dengan nilai *Integrity* yang paling tinggi (6.9), dapat disimpulkan bahwa potensi gangguan atau perubahan data menjadi salah satu risiko utama. Oleh karena itu, perlu dilakukan peningkatan mekanisme pengamanan data dan validasi integritas untuk meminimalisir dampak yang mungkin ditimbulkan oleh potensi serangan. Secara keseluruhan, meskipun tidak berada dalam kategori risiko tertinggi, situs web ini tetap memerlukan perhatian dan tindakan mitigasi untuk menurunkan tingkat kerentanannya, khususnya dalam aspek integritas dan kerahasiaan data.

Validasi Skor dan Konsistensi Tabel

Perhitungan :

$$\frac{7.5 + 6.2 + 5.4}{3} = \frac{19.1}{3} = 6.4$$

Tabel 7. *Confidentiality*

Detail Skor	Nilai
Skor Individual	7.5, 6.2, 5.4
Rata-rata	6.4

$$\frac{8.0 + 6.7 + 6.0}{3} = \frac{20.7}{3} = 6.9$$

Tabel 8. *Integrity*

Detail Skor	Nilai
Skor Individual	8.0, 6.7, 6.0
Rata-rata	6.9

$$\frac{7.0 + 6.5 + 5.8}{3} = \frac{19.3}{3} \approx 6.4$$

Tabel 9. *Availability*

Detail Skor	Nilai
Skor Individual	7.0, 6.5, 5.8
Rata-rata	6.4

$$\frac{6.4 + 6.9 + 6.4}{3} = \frac{19.7}{3} \approx 6.6$$

Tabel 10. Rata-rata Skor Akhir

Detail Skor	Nilai
Skor Individual	6.4, 6.9, 6.4
Rata-rata	6.6

1. Score individual berasal dari penilaian masing-masing jenis kerentanan hyang mdempengaruhi aspek *Confidentiality, Integrity*, dan *Availability*
2. Rata-rata akhir digunakan sebagai indikator tingkat resiko keseluruhan, yang dapat dikategorikan:
   a. 0.0 - 3.9 = Low
   b. 4.0 – 6.9 = Medium
   c. 7.0 – 8.9 = High
   d. 9.0 – 10.0 = Critical

4. KESIMPULAN

Website web.bnpb.go.id/ppid masih memiliki sejumlah kerentanan krusial, khususnya dalam aspek kontrol akses, proteksi terhadap *injeksi* perintah SQL, eksposur data sensitif, konfigurasi server, dan penggunaan komponen usang. Berdasarkan hasil *skoring Confidentiality* (6.4), *Integrity* (6.9), dan *Availability* (6.4), diperoleh rata-rata nilai risiko sebesar 6.6, yang termasuk kategori Medium *to High Risk.* Temuan teknis utama dalam pengujian mencakup:

a. SQL *Injection*: Sistem mengindikasikan kelemahan pada validasi input di *form login. Payload* standar seperti (' OR '1'='1 --) memberikan respons anomali, meskipun akhirnya diblok oleh *Web Application Firewall* (WAF).
b. Sensitive Data *Exposure*: Proses *brute-force* terhadap *form login* berhasil mengakses akun pengguna tanpa adanya mekanisme pembatasan percobaan login ataupun CAPTCHA. Tidak ditemukan dukungan *two-factor authentication (*2FA).
c. *Directory Listing*: Direktori /*upload*/ dan /*assets*/ dapat diakses publik dan menampilkan *file internal* seperti gambar struktur organisasi dan dokumen PDF, tanpa proteksi *Options -Indexes*.
d. Security Misconfiguration: Absennya *header* keamanan penting (X-*Frame-Options, Strict-Transport-Security*, X-*Content-Type-Options*) serta terlihatnya informasi versi *server* (*Apache*/2.4.56, PHP/8.1.12) pada *header* HTTP *response.*
e. Komponen Usang: Ditemukan penggunaan *jQuery* versi 1.7.2 yang memiliki beberapa kerentanan XSS berdasarkan CVE publik, namun masih digunakan dalam struktur *front-end.*

Dari 10 kategori OWASP Top 10, setidaknya 5 kategori teridentifikasi aktif pada sistem /ppid, yaitu: A01 (*Broken Access Control*), A02 (*Cryptographic Failures*), A03 (*Injection*), A05 (*Security Misconfiguration*), dan A06 (*Vulnerable & Outdated Components*).

Pengujian ini menunjukkan bahwa pendekatan sistematis berbasis OWASP Top 10 sangat relevan untuk mengidentifikasi potensi celah keamanan dan dapat digunakan sebagai dasar evaluasi keamanan sistem web publik yang beroperasi di bawah institusi pemerintahan.

REFERENSI

[1] O. Ben Fredj, O. Cheikhrouhou, M. Krichen, *et al.*, "An OWASP Top Ten driven survey on web application protection methods," in *Proc. Int. Conf. Secure Software Technol.*, Nov. 2020.
[2] E. Altulaihan, A. Alismail, and M. Frikha, "A survey on web application penetration testing," *Electronics*, vol. 12, no. 3, Mar. 2023, doi: 10.3390/electronics12030580.
[3] R. Ventura, D. J. Franco, and O. K. Akram, "A novel VAPT algorithm: Enhancing web application security through OWASP Top 10 optimization," *arXiv preprint arXiv:2311.10450*, Nov. 2023, doi: 10.48550/arXiv.2311.10450.
[4] J. R. Tadhani, V. Vekariya, V. Sorathiya, S. Alshathri, and W. El-Shafai, "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," *Sci. Rep.*, vol. 14, art. 1803, Jan. 2024, doi: 10.1038/s41598-023-48845-4.
[5] R. Bakır, "UniEmbed: A novel approach to detect XSS and SQL injection attacks leveraging multiple feature fusion with machine learning techniques," *Arab. J. Sci. Eng.*, Jan. 2025, doi: 10.1007/s13369-024-09916-4.
[6] S. Sharma, "A study of vulnerability scanners for detecting SQL injection and XSS attack in websites," *Artif. Intell. Appl.*, vol. 1, no. 4, May 2023, doi: 10.47852/bonviewAIA3202754.

[7] "Automating SQL injection and cross-site scripting vulnerability detection and remediation (CARES)," *MDPI Security and Informatics*, vol. 3, no. 1, 2024, doi: 10.3390/si3010002.
[8] L. K. Shar, C. M. Poskitt, K. J. Shim, and L. Y. L. Wong, "XSS for the masses: Integrating security in a web programming course using a security scanner," *arXiv preprint arXiv:2204.12416*, Apr. 2022, doi: 10.48550/arXiv.2204.12416.
[9] N. Nedeljković, N. Vugdelija, and N. Kojić, "Use of 'OWASP Top 10' in web application security," *J. Cybersecur. Educ. Res.*, Feb. 2025.
[10] "Vulnerabilities of web applications: Good practices and new trends," *Appl. Cybersecurity Internet Governance*, vol. 3, no. 2, Dec. 2024, doi: 10.60097/ACIG/199521.
[11] "Cross-site scripting attacks and defensive techniques," *J. Comput. Prog.*, vol. 12, no. 9, 2024, doi: 10.4236/jcp.2024.119069.
[12] "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," *Sci. Rep.*, 2024, doi: 10.1038/s41598-023-48845-4.
[13] A. A. Fanani, A. S. Indrawan, and F. Fadlillah, "Analisis kerentanan website menggunakan OWASP ZAP," *RESTIA: J. Inf. Technol. Res.*, vol. 3, no. 1, pp. 36–50, 2025, doi: 10.28880/restia.v3i1.561.
[14] S. D. Hilda, N. Heryana, and A. A. Ridha, "Analisis keamanan website pemerintah desa Curug menggunakan OWASP," *JITET: J. Inform. Tek. Elektro Terap.*, vol. 12, no. 3S1, 2024, doi: 10.23960/jitet.v12i3S1.5236.
[15] A. Pandiangan, "PPID institutions and services in regional apparatus of Central Jawa province government," *J. Komun. Media*, vol. 5, no. 2, pp. 87–105, 2025, doi: 10.24167/jkm.v5i2.13561.
[16] A. Kennedy, W. H. Surya, and F. X. Wartoyo, "Tantangan dan solusi penerapan e-government di Indonesia," *J. Terap. Pemerintahan Minangkabau*, vol. 4, no. 2, pp. 134–147, Dec. 2024, doi: 10.33701/jtpm.v4i2.4459.
[17] E. T. Simanjuntak and S. Sukri, "Penerapan e-government pada sektor pelayanan publik," *Pena Bangsa*, vol. 1, no. 1, 2025. [Online]. Available: https://ejurnal.teraskampus.id