

**ANALISIS KERENTANAN KEAMANAN *WEBSITE*
MENGUNAKAN *OPEN WEB APPLICATION
SECURITY PROJECT (OWASP) TOP-10*
STUDI KASUS (*web.bnpb.go.id*)**

SKRIPSI

**Oleh:
Arfan Dwi Madya
202110715156**



**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2025**

LEMBAR PERSETUJUAN PEMBIMBING

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

Nama Mahasiswa : Arfan Dwi Madya

Nomor Pokok Mahasiswa : 202110715156

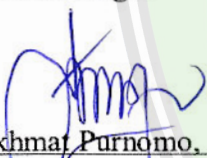
Program Studi/Fakultas : Informatika/Ilmu Komputer

Tanggal Lulus Ujian Skripsi : 29 Juli 2025

Jakarta, 5 Agustus 2025

MENYETUJUI,

Pembimbing I


Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.

NIDN. 0322108201

Pembimbing II


Nurfiyah, S.T., M.Kom.

NIDN. 0312079403

Ketua Program Studi Informatika


Ahmad Fathurrozi, S.E., M.M.S.I.

NIP. 2012486

**Program Studi Informatika
Fakultas Ilmu Komputer
Universitas Bhayangkara Jakarta Raya
2025**

LEMBAR PENGESAHAN

Judul Tugas akhir : Analisis Kerentanan Keamanan Website
Menggunakan Open Web Application
Security Project (Owasp) Top-10.
Studi Kasus (Web.bnpb.go.id)

Nama Mahasiswa : Arfan Dwi Madya

Nomor Pokok Mahasiswa : 202110715156

Program Studi/Fakultas : Informatika/Ilmu Komputer

Tanggal Lulus Ujian : 29 Juli 2025

Jakarta, 5 Agustus 2025

MENGESAHKAN,

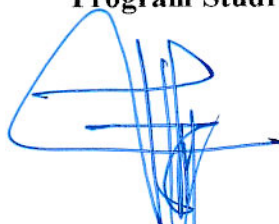
Ketua Tim Penguji : Ahmad Fathurrozi, S.E., M.M.S.I.
NIDN: 0327117402

Penguji I : Rasim, S.T., M.Kom
NIDN: 0415027301

Penguji II : Rakhmat Purnomo, S.Pd., S.Kom, M.kom
NIDN: 0322108201

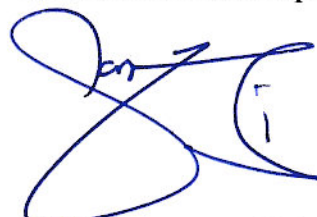
MENGETAHUI,

**Ketua
Program Studi Informatika**



Ahmad Fathurrozi, S.E., M.M.S.I
NIP. 2012486

**Dekan
Fakultas Ilmu Komputer**



Dr. Robertus Suraji, S.S., M.A.
NIP. 1904406



**UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA**

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini:

Nama : Arfan Dwi Madya
NPM : 202110715156
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Analisis Kerentanan Keamanan *Website* Menggunakan
Open Web Application Security Project (OWASP) Top-10.
Studi Kasus (web.bnpb.go.id)

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya sayasendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak manapun.

Bekasi, 05 Agustus 2025

Penulis



Arfan Dwi Madya

ABSTRAK

Arfan Dwi Madya. 202110715156. Analisis Kerentanan Keamanan *Website* Menggunakan *Open Web Application Security Project (OWASP) Top-10*: Studi Kasus *web.bnpb.go.id*. Bekasi: Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya. 2021.

Perkembangan teknologi informasi yang pesat mendorong pemanfaatan *website* sebagai sarana informasi publik, termasuk oleh instansi pemerintah. Namun peningkatan ini turut memunculkan ancaman keamanan siber yang semakin kompleks. Situs web milik Badan Nasional Penanggulangan Bencana (BNPB) menjadi salah satu target potensial, terutama pada subdirektori PPID yang berisi layanan informasi publik dan autentikasi pengguna. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada situs *web.bnpb.go.id*, dengan fokus pada direktori PPID, menggunakan acuan OWASP Top 10 tahun 2025 dan metodologi uji penetrasi dari NIST SP 800-115. Proses pengujian dilakukan melalui empat tahapan: perencanaan (*planning*), penemuan (*discovery*), penyerangan (*attacking*), dan pelaporan (*reporting*). *Tools* yang digunakan antara lain OWASP ZAP, Nmap, Gobuster, WhatWeb, SSLScan, dan Nikto. Hasil analisis menunjukkan terdapat beberapa kerentanan signifikan, seperti *directory listing*, *SQL injection*, *sensitive data exposure*, serta konfigurasi *header HTTP* dan *SSL/TLS* yang tidak aman. Melalui evaluasi berbasis CVSS v4.0, nilai rata-rata skor kerentanan menunjukkan tingkat risiko medium dengan potensi gangguan terhadap aspek *confidentiality*, *integrity*, dan *availability* dari sistem. Penelitian ini memberikan kontribusi dalam bentuk rekomendasi teknis guna meningkatkan keamanan sistem informasi web pemerintah. Temuan ini juga menekankan pentingnya audit keamanan berkala, konfigurasi sistem yang sesuai standar, serta penerapan kebijakan mitigasi risiko untuk mencegah eksploitasi oleh pihak tidak bertanggung jawab.

Kata Kunci: Keamanan *Web*, *OWASP Top 10*, NIST SP 800-115, CVSS, Uji Penetrasi

ABSTRACT

Arfan Dwi Madya. 202110715156. Website Security Vulnerability Analysis Using the Open Web Application Security Project (OWASP) Top-10: A Case Study of web.bnpb.go.id. Bekasi: Faculty of Computer Science, Bhayangkara University, Jakarta Raya. 2021.

The rapid development of information technology has encouraged the use of websites as a means of public information, including by government agencies. However, this increase has also given rise to increasingly complex cybersecurity threats. The website of the National Disaster Management Agency (BNPB) is a potential target, particularly the PPID subdirectory, which contains public information and user authentication services. This study aims to analyze security vulnerabilities on the website.bnpb.go.id, focusing on the PPID directory, using the OWASP Top 10 2025 reference and the NIST SP 800-115 penetration testing methodology. The testing process is carried out through four stages: planning, discovery, attack, and reporting. The tools used included OWASP ZAP, Nmap, Gobuster, WhatWeb, SSLScan, and Nikto. The analysis revealed several significant vulnerabilities, such as directory listing, SQL injection, sensitive data exposure, and insecure HTTP and SSL/TLS header configurations. Through a CVSS v4.0-based evaluation, the average vulnerability score indicated a medium risk level with potential compromises to the confidentiality, integrity, and availability of the system. This research contributes technical recommendations to improve the security of government web information systems. The findings also emphasize the importance of regular security audits, standardized system configuration, and the implementation of risk mitigation policies to prevent exploitation by malicious parties.

Keywords: Web Security, OWASP Top 10, NIST SP 800-115, CVSS, Penetration Testing

**LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK**

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini:

Nama : Arfan Dwi Madya
NPM : 202110715156
Program Studi : Informatik
Fakultas : Ilmu Komputer
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non- Eksklusif (Non-Exclusive Royalty-Free Right)**, atas karya ilmiah saya yang berjudul:

Analisis kerentanan keamanan *website* menggunakan *open web application security project (OWASP) Top-10*. Studi kasus (web.bnpb.go.id).

beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-eksklusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi.

Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Dibuat di : Indonesian Journal
of Education And
Computer Science

Pada tanggal : 14 Juli 2025

Yang Menyatakan



Arfan Dwi Madya

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Penyang, segala pujian dan terima kasih penulis panjatkan ke hadirat-Nya atas segala limpahan rahmat, hidayah, serta karunia-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul: "**Analisis Kerentanan Keamanan *Website* Menggunakan *Open Web Application Security Project (OWASP) Top-10 Studi Kasus *Web.bnpb.go.id****".

Skripsi ini disusun sebagai bagian dari menyediakan persyaratan untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya.

Penyusunan tugas akhir ini tentu tidak lepas dari dukungan, bimbingan, serta bantuan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, penulis ingin menyampaikan ucapan terima kasih dan penghargaan yang tulus kepada:

1. Bapak Irjen Pol. (Purn) Prof.Dr.Drs. H. Bambang Karsono, SH, MM, Ph.D., D.Crim (Honoris Causa), selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Bapak Dr. Robertus Suraji, S.S., M.A., selaku Dekan Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya.
3. Bapak Ahmad Fathurrozi, SE, MMSI, selaku Ketua Program Studi Informatika, yang telah memberikan dukungan dan kesempatan kepada penulis dalam menyelesaikan studi.

4. Bapak Rakhmat Purnomo, S.Pd., S.Kom., M.Kom., selaku Dosen Pembimbing I, yang telah memberikan bimbingan, motivasi, serta kritik yang membangun sepanjang proses penyusunan skripsi ini.
5. Ibu Nurfiyah, ST, M.Kom., selaku Dosen Pembimbing II, yang turut memberikan Arahan dan masukan yang sangat berarti dalam penyempurnaan penulisan skripsi ini.
6. Seluruh dosen dan staf Ilmu Komputer yang telah memberikan Fakultas ilmu dan pengalaman berharga selama masa kuliah.
7. Kedua orang tua tercinta, yang selalu menjadi sumber kekuatan melalui doa, kasih sayang, dan dukungan tanpa henti dalam segala aspek kehidupan penulis. Kakak Saya serta adik yang selalu memberikan dorongan dalam penyusunan proposal tugas akhir ini
8. Teman-teman seperjuangan, khususnya dari Program Studi Informatika angkatan tahun 2021, yang telah menjadi bagian dari proses belajar, berbagi, dan bertumbuh bersama.
9. Serta seluruh pihak yang tidak dapat penulis sebutkan satu per satu, namun ikut berperan dalam mendukung dan membantu penulis hingga skripsi ini dapat diselesaikan.

Penulis menyadari sepenuhnya bahwa masih terdapat kekurangan dalam penulisan skripsi ini, baik dari segi isi, metode, maupun teknik penyajiannya. Hal tersebut disebabkan oleh keterbatasan pengetahuan dan pengalaman penulis. Namun demikian, penulis berharap karya ilmiah ini dapat memberikan kontribusi

dan menjadi referensi bagi pembaca, khususnya mahasiswa yang tertarik pada bidang keamanan sistem informasi dan analisis kerentanan web.

Akhir kata, penulis mengucapkan terima kasih yang sebesar-besarnya atas segala bentuk dukungan, dan semoga semua kebaikan yang telah diberikan kepada penulis mendapat balasan terbaik dari Allah SWT.

Wassalamu'alaikum warahmatullahi wabarakatuh.



Bekasi, 15 Juli 2025

Arfan Dwi Madya

202110715156

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN BUKAN PLAGIASI .Error! Bookmark not defined.	
ABSTRAK	v
<i>ABSTRACT</i>	vi
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xv
DAFTAR GAMBAR.....	xviii
DAFTAR LAMPIRAN	xix
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah.....	5
1.3 Rumusan Masalah.....	5
1.4 Batasan Masalah	6
1.5 Tujuan Penelitian	6
1.6 Manfaat Penelitian	7

1.6.1	Bagi Peneliti	7
1.6.2	Bagi Universitas	7
1.6.3	Bagi Pembaca	8
1.7	Sistematika Penelitian	8
BAB 2	TINJAUAN PUSTAKA	10
2.1	Penelitian Terdahulu	10
2.2	Landasan Teori	12
2.2.1	Keamanan Informasi	12
2.2.2	Kerentanan Sistem (<i>vulnerability</i>)	15
2.2.3	Definisi <i>Website</i>	16
2.2.4	OSI (<i>Open System Interconnection</i>) <i>Layer</i>	18
2.2.5	<i>Penetration Testing</i> (Uji Penetrasi)	22
2.2.6	NIST SP 800-115 <i>Penetration Testing Methodology</i>	24
2.2.7	Tahapan NIST SP 800-115	24
2.2.8	OWASP (<i>Open Web Application Security Project</i>) TOP 10	25
2.2.9	Whatweb	29
2.2.10	Gobuster	31
2.2.11	SSLScan	32
2.2.12	<i>Wordpress</i>	33
2.2.13	<i>Open source intelligence</i> (OSINT)	34
2.2.14	Port	36
2.2.15	Kali Linux Tools	40

2.2.16 Komparasi OWASP Top 10 dan NIST SP 800-115 dalam Keamanan Aplikasi Web	47
2.2.17 <i>Common Vulnerability Scoring System (CVSS)</i>	50
BAB 3 METODOLOGI PENELITIAN	98
3.1 Objek dan Tempat Penelitian.....	98
3.2 Kerangka Penelitian.....	100
3.3 Metode Pengumpulan Data.....	101
3.3.1 Penelitian Serupa.....	101
3.3.2 Observasi.....	101
3.4 Metode Analisis	101
3.5 Analisis Kebutuhan Sistem.....	103
BAB 4 HASIL DAN PEMBAHASAN	105
4.1 Tahap <i>Planning</i>	105
4.1.1 Alat Kebutuhan Pengujian	105
4.1.2 Proses <i>Website</i> domain <i>bnpb.go.id</i> yang dijadikan target pengujian	
107	
4.2 Tahap <i>Discovery</i>	109
4.2.1 <i>Information Gathering</i>	109
4.2.2 <i>Network Mapping/Port Scanning</i>	121
4.2.3 <i>vulnerability scanning</i>	124
4.2.4 Analisis nilai kerentanan <i>https://bnpb.go.id/ppid</i>	136

4.3 Tahap <i>Attacking</i>	137
4.3.1 <i>Attacking SQL Injection</i>	138
4.3.2 <i>Attacking Directory Listing</i>	139
4.3.3 <i>Attacking Sensitive Data Exposure</i>	141
4.3.4 Ringkasan Hasil Temuan	143
4.3.5 Hasil Pengujian <i>SQL Injection</i>	147
4.3.6 Hasil Pengujian <i>Sensitive Data Exposure</i>	148
4.3.7 Hasil Pengujian <i>Directory Listing</i>	149
4.4 Laporan Akhir.....	150
4.4.1 Hasil Pengujian https://web.bn Timer pb.go.id/ppid	150
BAB 5 PENUTUP	158
5.1 Kesimpulan.....	158
5.2 Saran	159
DAFTAR PUSTAKA	162
LAMPIRAN	173

DAFTAR TABEL

Tabel 4. 1 Perangkat Lunak (Software) Penelitian	105
Tabel 4. 2 Perangkat keras (Hardware) Penelitian	106
Tabel 4. 3 Roadmap Penelitian	106
Tabel 4. 4 Website Target.....	109
Tabel 4. 5 hasil pencarian situs Dork.....	110
Tabel 4. 6 Hasil Enumerasi Direktori Menggunakan Gobuster.....	119
Tabel 4. 7 Hasil pencarian informasi website.....	122
Tabel 4. 8 Hasil Scanning dengan OWASP ZAP	124
Tabel 4. 9 Hasil Scanning pada website target menggunakan OWASP ZAP	125
Tabel 4. 10 Hasil Scanning dengan OWASP ZAP web.bnpb.go.id/ppid.....	127
Tabel 4. 11 Hasil Scanning pada website target menggunakan OWASP ZAP ...	127
Tabel 4. 12 Analisis Keamanan SSL/TLS web.bnpb.go.id	130
Tabel 4. 13 Hasil Pemindaian Nikto – web.bnpb.go.id/ppid.....	132
Tabel 4. 14 Hasil pencarian firewall menggunakan tools whatwaf.....	135
Tabel 4. 15 Pengukuran Nilai Kerentanan terhadap https://web.bnpb.go.id/ppid (CVSS v4.0)	137
Tabel 4. 16 Rekapitulasi Hasil Pemindaian Kerentanan.....	145
Tabel 4. 17 Ringkasan Hasil Pengujian Berdasarkan OWASP TOP 10-2025 ...	145
Tabel 4. 18 Hasil pengujian dari aspek confidentiality	150
Tabel 4. 19 Hasil Pengujian dari Aspek Integrity	152
Tabel 4. 20 Hasil Pengujian dari Aspek Availability	153
Tabel 4. 21 Skor Akhir Tingkat Kerentanan web.bnpb.go.id/ppid	155

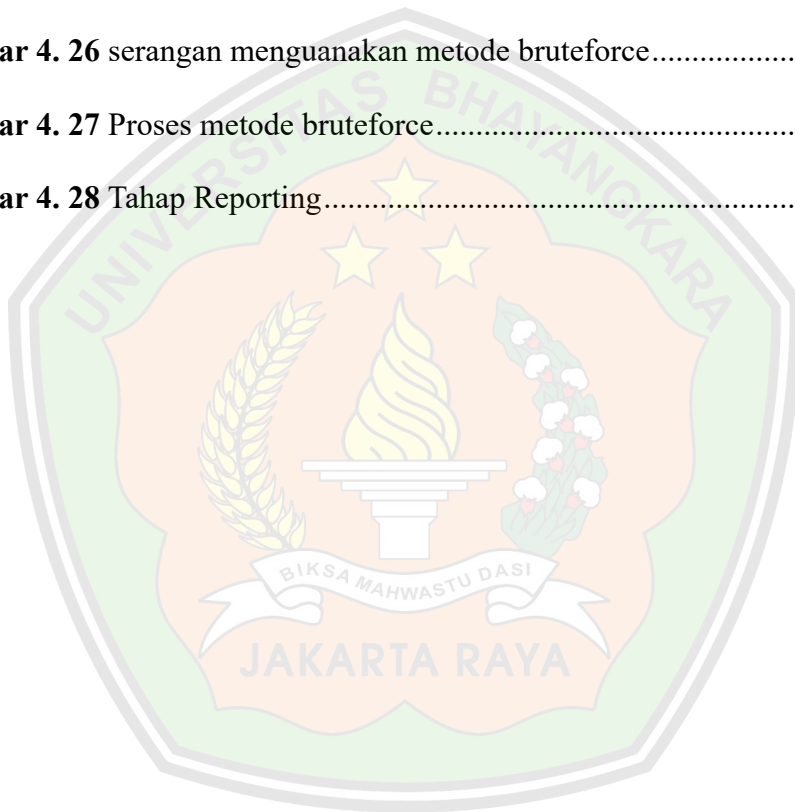
Tabel 4. 22 Confidentiality	156
Tabel 4. 23 Integrity.....	156
Tabel 4. 24 Availability.....	157
Tabel 4. 25 Rata-rata Skor Akhir	157



DAFTAR GAMBAR

Gambar 4. 1	Pencarian informasi domain dengan Google Dorking.....	108
Gambar 4. 2	Daftar dork wordpress dalam Google Hacking	110
Gambar 4. 3	Dorking WP-Login	112
Gambar 4. 4	Dorking WP-Slot	113
Gambar 4. 5	Dorking WP-Login	113
Gambar 4. 6	Wp admin.....	114
Gambar 4. 7	Wp content.....	114
Gambar 4. 8	404-redirection-manager.....	115
Gambar 4. 9	Dorking User WP-Json	115
Gambar 4. 10	Wp config	116
Gambar 4. 11	Imagemagick-engine.....	117
Gambar 4. 12	8-degree-notification-bar	117
Gambar 4. 13	Fingerprinting menggunakan WhatWeb	118
Gambar 4. 14	Pengujian Directory Enumeration Menggunakan Gobuster.....	119
Gambar 4. 15	Hasil TCP Scan	122
Gambar 4. 16	Hasil UDP Scan	123
Gambar 4. 17	Hasil Maimon Scan.....	123
Gambar 4. 18	OWASP ZAP v 2.16.1 (web.bnpb.go.id)	124
Gambar 4. 19	OWASP ZAP v 2.16.1 (web.bnpb.go.id/ppid).....	126
Gambar 4. 20	Analisis Keamanan SSL/TLS web.bnpb.go.id	130
Gambar 4. 21	Hasil Scanning menggunakan Nikto	132
Gambar 4. 22	Hasil pencarian web Application Firewall dengan whatwaf	135

Gambar 4. 23 Pengujian terhadap celah keamanan SQL Injection dengan tools SQLmap	139
Gambar 4. 24 penyerangan terhadap Directory Listing yang berhasil dilakukan	140
Gambar 4. 25 penemuan akun terhadap login e-PPID BNPB berhasil dilakukan	140
Gambar 4. 26 serangan menggunakan metode bruteforce.....	142
Gambar 4. 27 Proses metode bruteforce.....	142
Gambar 4. 28 Tahap Reporting.....	143



DAFTAR LAMPIRAN

Lampiran 1. 1 Hasil cek turnitin	174
Lampiran 1. 2 Biodata Mahasiswa.....	188
Lampiran 1. 3 Rekomendasi Pembimbing untuk Skripsi.....	189
Lampiran 1. 4 Lembar Bimbingan Skripsi Dengan Pembimbing I	191
Lampiran 1. 5 Lembar Bimbingan Skripsi Dengan Pembimbing II	192
Lampiran 1. 6 Surat Keterangan Penelitian di BNPB.....	193

