

**ANALISIS KERENTANAN *WEBSITE* DENGAN
PENDEKATAN *PENETRATION TESTING*
MENGUNAKAN METODE *OWASP*
(Studi Kasus: SMK Taruna Bangsa)**

SKRIPSI

**Oleh:
Zidhanifa Asshada
202110715063**



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

LEMBAR PERSETUJUAN PEMBIMBING

Judul Tugas Akhir : Analisis Kerentanan *Website* dengan Pendekatan *Penetration Testing* Menggunakan Metode *OWASP* (Studi Kasus: SMK Taruna Bangsa)

Nama Mahasiswa : Zidhanifa Asshada

Nomor Pokok Mahasiswa : 202110715063

Program Studi/Fakultas : Informatika / Ilmu Komputer

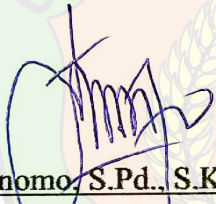
Tanggal Lulus Ujian Tugas Akhir : 25 Juli 2025

Jakarta , 11 Juli 2025

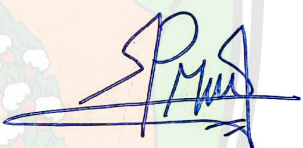
MENYETUJUI

Pembimbing I

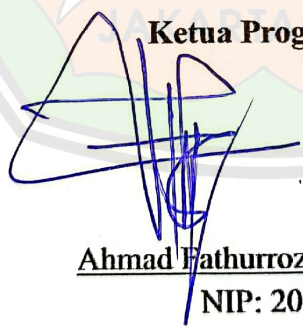
Pembimbing II


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

NIDN: 0322108201


Prio Kustanto, S.T., M.Kom.

NIDN: 0309047701


Ketua Program Studi

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 *Website* dengan Pendekatan *Penetration Testing* Menggunakan Metode *OWASP* (Studi Kasus: SMK Taruna Bangsa)

Nama Mahasiswa : Zidhanifa Asshada

Nomor Pokok Mahasiswa : 202110715063

Program Studi/Fakultas : Informatika / Ilmu Komputer

Tanggal Lulus Ujian Tugas Akhir : 25 Juli 2025

Jakarta, 01 Agustus 2025

MENGESAHKAN,

Ketua Tim Penguji : Sugiyatno, S.Kom., M.Kom.

NIDN: 0313077206

Penguji I : Muhammad Yasir, S.Si., M.Kom.

NIDN: 0317129002

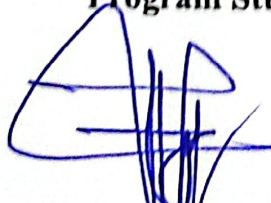
Penguji II : Rakhmat Purnomo, S.Pd., S.Kom., M.Kom.

NIDN: 0322108201

MENGETAHUI,

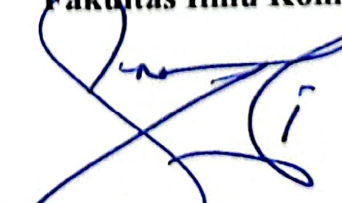
Ketua

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 : Zidhanifa Asshada
NPM : 202110715063
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Analisis Kerentanan *Website* dengan Pendekatan *Penetration Testing* Menggunakan Metode *OWASP* (Studi Kasus: SMK Taruna Bangsa)

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri 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, 01 Agustus 2025

Penulis



Zidhanifa Asshada

ABSTRAK

Zidhanifa Asshada, 202110715063. Analisis Kerentanan *Website* dengan Pendekatan *Penetration Testing* Menggunakan Metode *OWASP* (Studi Kasus: SMK Taruna Bangsa). Bekasi: Fakultas Ilmu Komputer. Universitas Bhayangkara Jakarta Raya. 2025

Website kini menjadi salah satu media utama bagi institusi pendidikan dalam menyampaikan informasi dan menyediakan layanan digital. Namun, meningkatnya penggunaan *website* juga membawa ancaman terhadap aspek keamanannya, terutama bagi institusi yang belum memiliki sistem perlindungan yang memadai. Penelitian ini bertujuan untuk mengevaluasi tingkat kerentanan keamanan pada *website* SMK Taruna Bangsa dengan menggunakan *penetration testing* berdasarkan standar *OWASP* (*Open Web Application Security Project*). Proses penelitian dilakukan melalui empat tahapan utama *OWASP*, yaitu perencanaan, pengumpulan informasi, serangan, dan pelaporan. Berbagai tools seperti *Acunetix*, *Greenbone*, *Nuclei*, dan *Nikto* digunakan untuk mengidentifikasi potensi kerentanan, didukung pula oleh teknik manual seperti *Google Dorking* dan *Wayback Machine* untuk memperoleh data awal. Hasil pengujian menunjukkan adanya beberapa celah keamanan dengan tingkat risiko sedang hingga tinggi, antara lain *Cross-Site Scripting* (*XSS*), *Clickjacking*, konfigurasi direktori yang tidak aman, serta tidak adanya header keamanan seperti *HSTS* dan *CSP*. Selain itu, juga ditemukan indikasi kebocoran jalur internal dan file konfigurasi yang dapat diakses publik, yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Berdasarkan hasil tersebut, penelitian ini memberikan sejumlah saran teknis dan prosedural untuk meningkatkan keamanan *website*, seperti penguatan konfigurasi server, implementasi header keamanan, serta pelaksanaan audit dan pemantauan sistem secara berkala. Studi ini diharapkan dapat berkontribusi dalam meningkatkan kesadaran serta penguatan keamanan digital di lingkungan pendidikan.

Kata Kunci: *Penetration Testing*, *OWASP*, Keamanan *Website*, Kerentanan, SMK Taruna Bangsa.

ABSTRACT

Zidhanifa Asshada. 202110715063. Website Vulnerability Analysis Using Penetration Testing Approach with OWASP Method (Case Study: SMK Taruna Bangsa). Bekasi: Faculty Of Computer Science. Jakarta Raya Bhayangkara University. 2025

Websites have become one of the primary platforms for educational institutions to deliver information and provide digital services. However, the increasing use of websites also brings potential security threats, especially for institutions that lack adequate protection systems. This research aims to evaluate the security vulnerabilities of the SMK Taruna Bangsa website by conducting penetration testing based on the OWASP (Open Web Application Security Project) methodology. The research follows four main OWASP stages: planning, information gathering, attacking, and reporting. Several tools, including Acunetix, Greenbone, Nuclei, and Nikto, were used to identify potential vulnerabilities, supported by manual techniques such as Google Dorking and the Wayback Machine for preliminary information gathering. The testing results revealed several security flaws with medium to high risk levels, such as Cross-Site Scripting (XSS), Clickjacking, insecure directory configurations, and the absence of essential security headers like HSTS and CSP. Additionally, indications of internal path disclosure and publicly accessible configuration files were found, which could potentially be exploited by unauthorized parties. Based on these findings, the study provides several technical and procedural recommendations to enhance website security, including improving server configurations, implementing security headers, and conducting regular audits and system monitoring. This research is expected to contribute to increasing awareness and strengthening digital security within educational institutions.

Keywords: Penetration Testing, OWASP, Website Security, Vulnerability, SMK Taruna Bangsa

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik universitas bhayangkara jakarta raya, saya yang bertanda tangan dibawah ini:

Nama : Zidhanifa Asshada
NPM : 202110715063
Program Studi : Informatika
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 Website dengan Pendekatan Penetration Testing Menggunakan Metode OWASP (Studi Kasus: SMK Taruna Bangsa)

beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-ekslusif 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 ijin 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 sebenarnya.

Dibuat di : Bekasi
Pada tanggal : 01 Agustus 2025

Yang Menyatakan



Zidhanifa Asshada

KATA PENGANTAR

Alhamdulillah, segala puji bagi Allah *Subhanahu wa Ta'ala* atas rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi berjudul “**Analisis Kerentanan Website dengan Pendekatan Penetration Testing Menggunakan Metode OWASP (Studi Kasus: SMK Taruna Bangsa)**” Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Informatika di Universitas Bhayangkara Jakarta Raya, dengan dukungan dan bantuan dari berbagai pihak yang penulis haturkan terima kasih.

1. Bapak Irjen Pol (Purn.) Prof. Dr. Drs. Bambang Karsono, S.H., M.M., 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, S.E., M.M.S.I. selaku Ketua Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya.
4. Bapak Rakhmat Purnomo, S.Pd., S.Kom., M.Kom. selaku Dosen Pembimbing I pada penelitian ini.
5. Bapak Prio Kustanto, S.T., M.Kom. selaku Dosen Pembimbing II pada penelitian ini.
6. Bapak Mayadi, S.Kom., M.Kom. selaku Dosen Pembimbing Akademik.
7. Kedua orang tua tercinta, yang mendoakan tiada henti kepada penulis hingga dapat menyelesaikan skripsi ini dengan lancar.

8. Kepada Bapak Koderi, S.T. yang sudah membantu terkait surat izin penelitian pada SMK Taruna Bangsa, sehingga proses penyusunan skripsi berjalan dengan baik hingga selesai.
9. Teman-teman seperjuangan, khususnya keluarga besar grup MGG atas segala bentuk bantuan, dukungan, serta fasilitas tempat yang telah diberikan selama proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, segala kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa mendatang.

Bekasi, 25 Juli 2025



Zidhanifa Asshada

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING.....	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN BUKAN PLAGIASI.....	iv
ABSTRAK.....	v
<i>ABSTRACT</i>	vi
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI.....	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian	5
1.6 Batasan Masalah.....	6
1.7 Sistematika Tugas Akhir	7
BAB II TINJAUAN PUSTAKA	9
2.1 Penelitian Terdahulu.....	9
2.2 Landasan Teori	12

2.2.1	Information System Security	13
2.2.2	CIA Triad.....	13
2.2.3	<i>Website</i>	15
2.2.4	Vulnerability.....	15
2.2.5	Vulnerability Assessment	16
2.2.6	Penetration Testing.....	16
2.2.7	<i>VAPT Lifecycle</i>	16
2.2.8	<i>OWASP</i>	19
2.2.9	<i>Common vulnerability scoring system (CVSS)</i>	22
BAB III METODOLOGI PENELITIAN		28
3.1	Objek Penelitian dan Tempat Penelitian	28
3.1.1	Visi	28
3.1.2	Misi	28
3.2	Metode Pengumpulan Data.....	29
3.2.1	Observasi.....	29
3.2.2	Wawancara	29
3.2.3	Studi Literatur	31
3.3	Analisis Kebutuhan Sistem	31
3.3.1	Kebutuhan Perangkat Keras.....	31
3.3.2	Kebutuhan Perangkat Lunak	31
3.3.3	Kerangka Penelitian dan Skenario Pengujian	34
BAB IV HASIL DAN PEMBAHASAN		37
4.1	Hasil Pengujian	37
4.1.1	<i>Planning and Scoping</i>	37
4.1.2	<i>Information Gathering</i>	39

4.1.3	<i>Vulnerability Assessment</i>	53
4.1.4	<i>Gaining Access</i>	59
4.1.5	<i>Maintaining Access</i>	65
4.2	<i>Analisis dan Pembahasan</i>	65
4.2.1	<i>Analisis Kerentanan Berdasarkan OWASP Top 10</i>	65
4.2.2	Hasil perhitungan Manual <i>CVSS V3.0</i>	68
4.2.3	Rekomendasi Perbaikan	76
BAB V PENUTUP		78
5.1	Kesimpulan	78
5.2	Saran.....	79
DAFTAR PUSTAKA		80
LAMPIRAN		82



DAFTAR TABEL

Tabel 2. 1 <i>State of the art</i>	12
Tabel 2. 2 <i>Score Base CVSS</i>	25
Tabel 2. 3 <i>Tabel Base Metrics (v3.0 / v3.0)</i>	25
Tabel 3. 1 Hasil Wawancara	30
Tabel 4. 1 List <i>URL Website</i>	46
Tabel 4. 2 Hasil <i>Vulnerability Scanning</i>	54
Tabel 4. 3 Kerentanan temuan dengan <i>Greenbone</i>	57
Tabel 4. 4 Hasil Perhitungan CVSS.....	67
Tabel 4. 5 Perhitungan <i>CVSS Vulnerability Directory</i>	68
Tabel 4. 6 Perhitungan <i>CVSS Vulnerability XSS via Outdated jQuery</i>	69
Tabel 4. 7 Perhitungan <i>CVSS Clickjacking</i>	71
Tabel 4. 8 Perhitungan <i>CVSS Host Header Injection</i>	73
Tabel 4. 9 Perhitungan <i>CVSS Internal Path Disclosure</i>	74
Tabel 4. 10 Rekomendasi dan perbaikan	76

DAFTAR GAMBAR

Gambar 2. 1 <i>CIA Triad</i>	13
Gambar 2. 2 <i>VAPT Process</i>	17
Gambar 2. 3 <i>OWASP Top 10</i>	20
Gambar 2. 4 <i>OWASP Top 10 2021</i>	21
Gambar 3. 1 <i>Lokasi SMK Taruna Bangsa</i>	29
Gambar 3. 2 <i>Kerangka Penelitian</i>	34
Gambar 4. 1 <i>Black-box Testing</i>	38
Gambar 4. 2 <i>Hasil Whatweb</i>	40
Gambar 4. 3 <i>Hasil ffuf</i>	41
Gambar 4. 4 <i>Hasil Subfinder</i>	42
Gambar 4. 5 <i>Hasil dnsX</i>	43
Gambar 4. 6 <i>Hasil dirsearch</i>	45
Gambar 4. 7 <i>Directory asset</i>	46
Gambar 4. 8 <i>Penemuan File index Directory</i>	47
Gambar 4. 9 <i>Hasil query google dorking</i>	48
Gambar 4. 10 <i>Pengujian Wayback Machine</i>	49
Gambar 4. 11 <i>Script Python</i>	49
Gambar 4. 12 <i>Pengujian menggunakan Script Python</i>	50
Gambar 4. 13 <i>gitigner pada website SMK Taruna Bangsa</i>	51
Gambar 4. 14 <i>Directory Internal server</i>	52
Gambar 4. 15 <i>Vulnerability scanning Acunetix</i>	54
Gambar 4. 16 <i>Vulnerability Assessment Greenbone</i>	57
Gambar 4. 17 <i>Nuclei Scanning</i>	58
Gambar 4. 18 <i>Teknik Inframe Injection</i>	59
Gambar 4. 19 <i>Pengujian clickjacking</i>	60
Gambar 4. 20 <i>Inspect Element</i>	61
Gambar 4. 21 <i>Inspect element</i>	62
Gambar 4. 22 <i>File jQuery</i>	62
Gambar 4. 23 <i>Script Python Simple HTTP Server</i>	63

Gambar 4. 24 Hasil <i>XSS jQuery</i>	63
Gambar 4. 25 Proses validasi menggunakan <i>Burp Suite</i>	64
Gambar 4. 26 Hasil <i>Base Score CVSS Vulnerability Directory Listening</i>	69
Gambar 4. 27 Hasil <i>Base Score CVSS Vulnerability XSS via Outdated</i>	71
Gambar 4. 28 Hasil <i>Base Score CVSS Clickjacking</i>	72
Gambar 4. 29 Hasil <i>Base Score CVSS Host Header Injection</i>	74
Gambar 4. 30 Hasil <i>Base Score CVSS Internal Path Disclosure</i>	76



DAFTAR LAMPIRAN

Lampiran 1 Hasil Cek Plagiarisme

Lampiran 2 Biodata Mahasiswa

Lampiran 3 Kartu Konsultasi Bimbingan Pembimbing I

Lampiran 4 Kartu Konsultasi Bimbingan Pembimbing II

Lampiran 5 Rekomendasi Pembimbing I

Lampiran 6 Rekomendasi Pembimbing II

Lampiran 7 Surat Bakas Permohonan Izin Penelitian

