

**ANALISIS KEAMANAN JARINGAN WEB UNIVERSITAS
BHAYANGKARA JAKARTA RAYA DENGAN METODE
PENETRATION TESTING MENGGUNAKAN
OWASP (Studi Kasus: skripsifasilkom.id)**

SKRIPSI

**Oleh:
Karina Nuraini
202110715199**



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

LEMBAR PERSETUJUAN PEMBIMBING
(DIGUNAKAN UNTUK TUGAS AKHIR)

Judul Proposal Tugas Akhir : Analisis Keamanan Jaringan Web Universitas Bhayangkara Jakarta Raya dengan Metode Penetration Testing Menggunakan OWASP (Studi Kasus: skripsifasilkom.id)

Nama Mahasiswa : Karina Nuraini

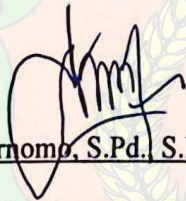
Nomor Pokok Mahasiswa : 202110715199

Program Studi/Fakultas : Informatika/Ilmu Komputer

Tanggal Lulus Ujian Skripsi : 28 Juli 2025

Bekasi, 11 Juli 2025
MENYETUJUI,

Pembimbing I



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

NIDN: 0322108201

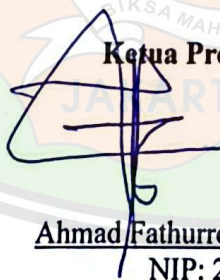
Pembimbing II



Agus Hidayat, S.Kom., M.Si.

NIDN: 0304088303

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 Keamanan Web Universitas
Bhayangkara Jakarta Raya dengan Metode
Penetration Testing Menggunakan OWASP
(Studi Kasus: skripsifasilkom.id)

Nama Mahasiswa : Karina Nuraini

Nomor Pokok Mahasiswa : 202110715199

Program Studi/Fakultas : Informatika/Ilmu Komputer

Tanggal Lulus Ujian Skripsi : 28 Juli 2025

Jakarta, 4 Agustus 2025

MENGESAHKAN,

Ketua Tim Penguji : Sugiyatno, S.Kom., M.Kom
NIDN: 0313077206



Penguji I : Asep Ramdhani Mahbub, S.Kom., M.Kom
NIDN: 0329087703

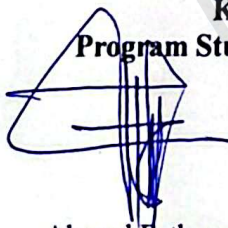


Penguji II : Rakhmat Purnomo, S.Pd., S.Kom., M.Kom
NIDN: 0322108201



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 : Karina Nuraini
NPM : 202110715199
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Analisis Keamanan Jaringan Web Universitas Bhayangkara Jakarta Raya dengan Metode Penetration Testing Menggunakan OWASP (Studi Kasus: skripsifasilkom.id).

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 mana pun.

Bekasi, 04 Agustus 2025

Penulis,



Karina Nuraini

ABSTRAK

Karina Nuraini. 202110715199. Analisis Keamanan *Web* Universitas Bhayangkara Jakarta Raya dengan Metode *Penetration Testing* Menggunakan OWASP (Studi Kasus: skripsifasilkom.id). Bekasi: Fakultas Ilmu Komputer. Universitas Bhayangkara Jakarta Raya. 2025.

Perkembangan teknologi informasi yang pesat meningkatkan risiko serangan siber, termasuk pada *website* institusi pendidikan seperti Universitas Bhayangkara Jakarta Raya. *Website* skripsifasilkom.id sebagai platform akademik berpotensi menjadi target serangan yang dapat mengganggu integritas data dan layanan. Penelitian ini bertujuan untuk menganalisis keamanan *website* tersebut dengan fokus pada kerentanan SQL Injection pada form login, menggunakan metode *penetration testing* berbasis standar OWASP Top 10. Pengujian dilakukan melalui beberapa tahapan, yaitu perencanaan, pengumpulan informasi, eksploitasi, identifikasi kerentanan, analisis risiko, dan pelaporan, dengan menggunakan *tools* WebCheck, OWASP ZAP, BurpSuite, SQLMap, serta perhitungan risiko menggunakan metode CVSS v3.1. Hasil pengujian menunjukkan bahwa tidak ditemukan kerentanan SQL Injection pada form login. Namun, OWASP ZAP berhasil mengidentifikasi beberapa kerentanan lain dengan tingkat risiko rendah hingga sedang, seperti tidak adanya *header* keamanan, penggunaan *library* JavaScript yang rentan, dan konfigurasi *cookie* yang kurang aman. Skor CVSS terhadap temuan yang teridentifikasi berkisar antara 3.1 hingga 6.5, yang menunjukkan bahwa kerentanan tersebut bersifat minor namun tetap perlu diperbaiki untuk meningkatkan ketahanan sistem. Penelitian ini diharapkan dapat memberikan kontribusi dalam peningkatan keamanan aplikasi *web* serta sebagai referensi bagi pengembangan kebijakan keamanan siber di lingkungan akademik..

Kata Kunci: Keamanan *Web*, *Penetration Testing*, OWASP, SQL Injection, OWASP ZAP, BurpSuite.

ABSTRACT

Karina Nuraini. 202110715199 *Security Analysis Of Bhayangkara Jakarta Raya University Web With Penetration Testing Method Using OWASP (Case Study: skripsifasilkom.id). Bekasi: Faculty of Computer Science. University Of Bhayangkara Jakarta Raya. 2025.*

The rapid development of information technology has increased the risk of cyberattacks, including on educational institution websites such as Universitas Bhayangkara Jakarta Raya. The skripsifasilkom.id website, as an academic platform, has the potential to become a target of attacks that could compromise data integrity and service availability. This study aims to analyze the security of the website by focusing on SQL Injection vulnerabilities on the login form using penetration testing methods based on the OWASP Top 10 standard. The testing process includes planning, information gathering, exploitation, vulnerability identification, risk analysis, and reporting, utilizing tools such as WebCheck, OWASP ZAP, BurpSuite, SQLMap, and risk scoring with the CVSS v3.1 method. The results showed that no SQL Injection vulnerability was found on the login form. However, OWASP ZAP successfully identified several other potential vulnerabilities with low to medium risk levels, including missing security headers, the use of vulnerable JavaScript libraries, and insecure cookie configurations. The CVSS scores of the identified issues range from 3.1 to 6.5, indicating that while the vulnerabilities are minor, they still require mitigation to enhance overall system resilience. This research is expected to contribute to the improvement of web application security and serve as a reference for cybersecurity policy development in academic environments..

Keywords: *Web Security, Penetration Testing, OWASP, SQL Injection, OWASP ZAP, BurpSuite.*

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

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

Nama : Karina Nuraini
NPM : 202110715199
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 Keamanan *Web* Universitas Bhayangkara Jakarta Raya dengan Metode *Penetration Testing* Menggunakan *OWASP* (Studi Kasus: skripsifasilkom.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 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 : 04 Agustus 2025

Yang Menyatakan



Karina Nuraini

KATA PENGANTAR

Segala puji bagi kehadiran Allah SWT. yang telah memberikan rahmat serta karunia-Nya sehingga saya dapat menyelesaikan tugas akhir yang berjudul “Analisis Keamanan *Web* Universitas Bhayangkara Jakarta Raya Dengan Metode *Penetration Testing* Menggunakan OWASP (Studi Kasus: skripsifasilkom.id)”. Banyak pihak yang telah memberikan dukungan dan bantuan selama proses penyelesaian penelitian ini. Oleh karena itu sudah sepantasnya, dengan penuh hormat mengucapkan terima kasih dan mendoakan semoga Allah SWT memberikan balasan terbaik pada mereka.

1. Bapak Irjen Pol (Purn) Prof. Dr. Drs. H. Bambang Karsono, S.H., M.M., Ph.D., D.Crim(Hc) 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 Tugas Akhir Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
5. Bapak Agus Hidayat, S.Kom., M.Si selaku Dosen Pembimbing II Tugas Akhir dan Pembimbing Akademik Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.

6. Kedua orang tua, atas kasih sayang, doa, dukungan moral, dan semangat yang tiada henti dalam setiap langkah, serta menjadi sumber kekuatan selama proses studi dan penyusunan tugas akhir ini.
7. Tia Aulia sebagai teman, sahabat, dan adik, atas waktu, support, kebersamaan, canda tawa, dan segala bantuan yang telah diberikan. Terima kasih telah menemani di masa-masa sulit maupun senang selama mengenal penulis.
8. Teman-teman “Princess A5” dan “Cemara” yang selalu mendukung selama perkuliahan dan penyusunan tugas akhir ini.
9. Idola penulis, Stray Kids khususnya 3Racha yang secara tidak langsung memberikan support, inspirasi, dan menemani dalam masa perkuliahan maupun masa pengerjaan tugas akhir.

Dalam penulisan dan penyusunan laporan tugas akhir ini disadari masih jauh dari kata sempurna. Hal itu karena terbatasnya pengetahuan dan pengalaman yang dimiliki. Oleh karena itu, diharapkan segala bentuk saran dan masukan yang membangun agar dapat menjadi lebih baik lagi. Semoga tugas akhir skripsi ini dapat bermanfaat khususnya bagi penyusun dan bagi para pembaca lain pada umumnya.

Jakarta, 04 Agustus 2025

Hormat Saya



Karina Nuraini

202110715199

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iv
ABSTRAK	v
ABSTRACT	vi
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL	xiii
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian	4
1.5.1 Bagi Peneliti	4
1.5.2 Bagi Fakultas Ilmu Komputer	4
1.5.3 Bagi Pembaca.....	5
1.6 Batasan Masalah.....	5
1.6.1 Metode	5
1.6.2 Tools	5
1.6.3 Proses	6
1.7 Sistematika Tugas Akhir	6
BAB II TINJAUAN PUSTAKA.....	9
2.1 Kajian Literatur	9
2.2 Keamanan Informasi	13
2.3 CIA Triad.....	15
2.4 Ethical Hacking.....	17

2.5	<i>Vulnerability Analysis</i>	18
2.6	<i>SQL Injection</i>	20
2.7	Oracle VM VirtualBox	23
2.8	Kali linux.....	23
2.9	WEBCHECK	24
2.10	SQLMAP	25
2.11	OWASP	27
2.12	BurpSuite	31
2.13	<i>CVSS Calculator</i>	34
BAB III METODOLOGI PENELITIAN		39
3.1	Objek dan Tempat Penelitian	39
3.2	Profil Institusi.....	40
3.2.1	Universitas Bhayangkara Jakarta Raya.....	40
3.2.2	Visi	40
3.2.3	Misi	40
3.2.4	Struktur Organisasi.....	41
3.3	Kerangka Penelitian	42
3.4	Metode Pengumpulan Data.....	43
3.4.1	Penelitian Serupa.....	43
3.4.2	Observasi.....	43
3.4.3	Pengujian <i>Penetration Testing</i>	43
3.5	Pengujian dan Analisis	44
3.5.1	<i>Roadmap</i> Penelitian	44
3.5.2	<i>Planning and Scoping</i>	45
3.5.3	<i>Information Gathering</i>	45
3.5.4	<i>Vulnerability Identification</i>	46
3.5.5	<i>Exploitation</i>	46
3.5.6	<i>Reporting</i>	46
3.6	Analisis Kebutuhan Sistem	46
3.6.1	Kebutuhan <i>hardware</i>	46
3.6.2	Kebutuhan <i>Software</i>	47
BAB IV HASIL DAN PEMBAHASAN.....		48

4.1	Pembahasan.....	48
4.1.1	<i>Planning and Scoping</i>	48
4.1.2	<i>Information Gathering</i>	50
4.1.3	<i>Vulnerability Identification</i>	54
4.1.4	<i>Exploitation</i>	55
4.1.5	Analisis dan Evaluasi	59
4.1.6	<i>Reporting</i>	60
4.2	Uji Validitas Pengujian.....	63
BAB V KESIMPULAN DAN SARAN		65
5.1	Kesimpulan	65
5.2	Saran.....	66
DAFTAR PUSTAKA.....		68
LAMPIRAN.....		72



DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	10
Tabel 3. 1 Roadmap Penelitian.....	44
Tabel 4. 1 Hasil Pemindaian WebCheck	51
Tabel 4. 2 Hasil Pemindaian OWASP ZAP	52
Tabel 4. 3 Vulnerability Identification	54
Tabel 4. 4 Hasil Uji BurpSuite	57
Tabel 4. 5 Perbandingan Tools Pengujian	59
Tabel 4. 6 Ringkasan Laporan Kerentanan	61



DAFTAR GAMBAR

Gambar 2. 1 <i>CIA TRIAD</i>	16
Gambar 2. 2 Parkerian Hexad	17
Gambar 2. 3 SQLMAP.....	25
Gambar 2. 4 Metrik Utama CVSS	35
Gambar 2. 5 Security Rating CVSS.....	38
Gambar 3. 1 Objek Penelitian	39
Gambar 3. 2 Struktur Organisasi Ubhara Jaya.....	42
Gambar 3. 3 Kerangka Penelitian	42
Gambar 4. 1 Hasil Pemindaian WebCheck	50
Gambar 4. 2 Hasil Pemindaian OWASP ZAP.....	52
Gambar 4. 3 Hasil Pengujian BurpSuite bypass username.....	56
Gambar 4. 4 Hasil Pengujian BurpSuite bypass username dan password	57
Gambar 4. 5 Pengujian SQLMAP.....	58

DAFTAR LAMPIRAN

Uji Plagiasi

Biodata Mahasiswa

Kartu Konsultasi Bimbingan

Kartu Bimbingan Skripsi Dosen Pembimbing I

Kartu Bimbingan Skripsi Dosen Pembimbing II

Rekomendasi Dari Pembimbing I Untuk Tugas Akhir

Rekomendasi Dari Pembimbing II Untuk Tugas Akhir

Bukti Submit Artikel

