ANALISIS RISIKO KEAMANAN WEBSITE SIMULASI BERBASIS DVWA MENGGUNAKAN PENETRATION TESTING DAN EVALUASI CVSS V4.0 (STUDI KASUS INSTANSI DAERAH XYZ)

LAPORAN TUGAS AKHIR

YUSUF ABDUL ROZAK
41520010161

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025

ANALISIS RISIKO KEAMANAN WEBSITE SIMULASI BERBASIS DVWA MENGGUNAKAN PENETRATION TESTING DAN EVALUASI CVSS 4.0 (STUDI KASUS INSTANSI DAERAH XYZ)

LAPORAN TUGAS AKHIR

YUSUF ABDUL ROZAK
41520010161

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2025

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama	:	Yusuf Abdul Rozak
NIM	:	41520010161
Program Studi	:	Teknik Informatika
Judul Proposal Penelitian	:	Analisis Risiko keamanan Webstite Simulasi Berbasis Dvwa Menggunakan Penetration Testing dan Evaluasi Cvss v4.0 (Studi Kasus Instansi Daerah XYZ)

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Jakarta, 28 Juli 2025

Yusuf Abdul Rozak

HALAMAN PENGESAHAN

Laporan Skripsi ini diajukan oleh:

Nama	:	YUSUF ABDUL ROZAK
NIM	:	41520010161
Program Studi	:	Teknik Informatika
Judul Proposal Penelitian	:	Analisis Risiko Keamanan Website Simulasi Berbasis Dvwa Menggunakan Penetration Testing Dan Evaluasi Cvss v4.0 (Studi Kasus Instansi Daerah XYZ)

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing	:	Dr. Nungky Awang Chandra, S.Si, M.TI	( )
NIDN	:	0306117303	
Ketua Penguji	:	Dr. Hadi Santoso, S.Kom., M.Kom	( )
NIDN	:	0225067701	
Penguji 1	:	Umniy Salamah, S.T.,MMSI	( )
NIDN	:	0306098104	
Penguji 2	:	Ida Farida, ST,M.Kom	( )
NIDN	:	0324018301	

Jakarta, 4 Agustus 2025

Mengetahui,

Dekan	Ketua Program Studi
Dr. Bambang Jokonowo, S.Si., MTI	Dr. Hadi Santoso, S.Kom., M.Kom
NIDN : 0320037002	NIDN : 0225067701

KATA PENGANTAR

Puji syukur kehadirat Tuhan yang Maha Esa, atas segala rahmat dan ridha-Nya sehingga penulis dapat menyelesaikan proposal penelitian yang merupakan salah satu persyaratan kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana.

Penulis menyadari bahwa proposal penelitian ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Oleh karena itu, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Bapak Dr. Nungky Awang Chandra, S.Si, M.TI.selaku dosen pembimbing MPTI dan Ibu Dr. Afiyati, S.Si, MT selaku dosen pengampu MPTI yang keduanya telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan proposal penelitian ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mensuport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, 15 Juni 2025

Yusuf Abdul Rozak

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Mercu Buana, saya yang bertanda tangan di bawah ini:

Nama	:	YUSUF ABDUL ROZAK
NIM	:	41520010161
Program Studi	:	Teknik Informatika
Judul Proposal Penelitian	:	Analisis Risiko Keamanan Website Simulasi Berbasis Dvwa Menggunakan Penetration Testing Dan Evaluasi Cvss v4.0 (Studi Kasus Instansi Daerah XYZ)

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (*Non-exclusive Royalty-Free Right)*** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Laporan Magang/Skripsi/Tesis/Disertasi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian Pernyataan ini saya buat dengan sebenarnya.

Jakarta, 28 Juli 2025

Yusuf Abdul Rozak

ABSTRAK

Nama	:	YUSUF ABDUL ROZAK
NIM	:	41520010161
Program Studi	:	Teknik Informatika
Judul Proposal Penelitian	:	Analisis Risiko Keamanan Website Simulasi Berbasis Dvwa Menggunakan Penetration Testing Dan Evaluasi Cvss v4.0 (Studi Kasus Instansi Daerah XYZ)
Dosen Pembimbing	:	Dr. Nungky Awang Chandra, S.Si, M.TI.

Penerapan digitalisasi suatu instansi khususnya pemerintahan daerah telah membawa perkembangan aplikasi web sebagai platform utama dalam pelayanan publik. namun, peningkatan belum sepenuhnya optimal dalam penguatan system keamanan. Berdasarkan laporan Lembaga BSNN tahun 2024 mencatat bahwa sektor pemerintahan rentan dengan serangan siber melalui celah keamanan dalam aplikasi web. Penelitian ini bertujuan untuk analisis risiko keamanan dalam website simulasi berbasis Damn Vulnerable Web App (DVWA).

Penelitian ini menggunakan metode penetration testing dengan pendekatan Black-Box, untuk mengidentifikasi dan mengeksploitasi kelemahan seperti SQL Injection, Cross Site Scripting, Command Injection dan File Upload. Setiap hasil eksploitasi dievaluasi dan diperbaiki dengan cara modifikasi pada kode sumber. Evaluasi tingkat risikonya menggunakan standar CVSS versi 4.0.

Hasil penelitian menunjukkan bahwa kerentanan bisa dimanfaatkan, dengan skor CVSS mulai dari 6.1 (tingkat sedang) hingga 9.1 (tingkat kritis). Semua proses eksploitasi dan evaluasi akan didokumentasikan dengan rapi untuk memberikan gambaran konkret tentang potensi ancaman dan solusi teknis yang bisa diterapkan. Penelitian ini memberikan kontribusi melalui studi kasus yang lengkap, mencakup eksploitasi, penanganan teknis, dan evaluasi risiko berdasarkan simulasi terhadap sistem informasi daerah.

Kata kunci: Keamanan Web, Penetration Testing, DVWA, CVSS v4.0, SQL Injection, XSS, Command Injection, File Upload

ABSTRACT

Nama	:	YUSUF ABDUL ROZAK
NIM	:	41520010161
Program Studi	:	Teknik Informatika
Judul Proposal Penelitian	:	Analisis Risiko Keamanan Website Simulasi Berbasis DVWA Menggunakan Penetration Testing dan Evaluasi Cvss v4.0 (Studi Kasus Instansi Daerah XYZ)
Dosen Pembimbing	:	Dr. Nungky Awang Chandra, S.Si, M.TI.

The implementation of digitization of an agency, especially local government, has brought the development of web applications as the main platform for public services. However, the increase has not been fully optimal in strengthening the security system. Based on the BSNN Institute report in 2024, it was noted that the government sector is vulnerable to cyber attacks through security holes in web applications. This research aims to analyze the security risks in the Damn Vulnerable Web App (DVWA) based simulation website.

This research uses penetration testing method with Black-Box approach, to identify and exploit weaknesses such as SQL Injection, Cross Site Scripting, Command Injection and File Upload. Each exploit result is evaluated and fixed by modifying the source code. The risk level evaluation uses the CVSS version 4.0 standard.

The results show that the vulnerabilities can be exploited, with CVSS scores ranging from 6.1 (moderate level) to 9.1 (critical level). All exploitation and evaluation processes will be neatly documented to provide a concrete picture of potential threats and workable technical solutions. This research contributes through a complete case study, covering exploitation, technical countermeasures, and simulation-based risk evaluation of local information systems.

Kata kunci: Web Security, Penetration Testing, DVWA, CVSS v4.0, SQL Injection, XSS, Command Injection, File Upload

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN