

PENGUJIAN PENETRASI APLIKASI WEB XXX DAN YYY MENGUNAKAN METODOLOGI OWASP WEB APPLICATION SECURITY TESTING

MUHAMMAD ZAHRAN



**PROGRAM STUDI SARJANA ILMU KOMPUTER
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2026**

@Hak cipta milik IPB University

IPB University



IPB University
Bogor Indonesia

- Hak Cipta Dilindungi Undang-undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

Perpustakaan IPB University

PERNYATAAN MENGENAI SKRIPSI DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa skripsi dengan judul “Pengujian Penetrasi Aplikasi Web XXX dan YYY Menggunakan Metodologi OWASP Web Application Security Testing” adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Juni 2026

Muhammad Zahran
G6401211074

ABSTRAK

MUHAMMAD ZAHRAN. Pengujian Penetrasi Aplikasi Web XXX dan YYY Menggunakan Metodologi OWASP Web Application Security Testing. Dibimbing oleh SRI WAHJUNI dan MUSHTHOFA.

Seiring dengan banyaknya bisnis yang menggunakan internet untuk menawarkan produk dan layanan mereka, aplikasi berbasis web telah menjadi tulang punggung masyarakat digital modern kita. Namun, ketergantungan terhadap aplikasi web menarik perhatian dari pelaku jahat untuk menyelipkan ke dalam sistem demi keuntungan pribadi. Pada tahun 2024, aplikasi web menjadi vektor aksi kebocoran data yang paling banyak digunakan oleh penyerang. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis kerentanan pada aplikasi XXX dan YYY, yang merupakan sistem informasi penting di lingkungan suatu perguruan tinggi. Pendekatan yang digunakan adalah pengujian penetrasi dengan metode OWASP Web Application Security Testing (WAST) berdasarkan panduan OWASP Web Security Testing Guide (WSTG). Hasil pengujian menunjukkan adanya kelemahan mendasar pada manajemen identitas dan kontrol akses, yang memungkinkan manipulasi *role* pengguna menjadi admin, serta inkonsistensi dalam implementasi *role-based access control*. Kerentanan XSS tersimpan memperparah keadaan karena memperluas permukaan serangan dengan lebih memungkinkan seorang pengguna biasa mendapatkan identitas pengguna lain sehingga dapat melakukan aksi di luar wewenangnya. Dan di luar kelemahan-kelemahan mendasar tersebut, ditemukan kerentanan yang paling fatal, yaitu kerentanan tingkat kritis berupa *remote command execution* yang memungkinkan seorang pengguna mengambil alih server sepenuhnya.

Kata kunci: aplikasi web, OWASP, pengujian penetrasi

ABSTRACT

MUHAMMAD ZAHRAN. Penetration Testing of XXX dan YYY Web Applications Using the OWASP Web Application Security Testing Methodology. Supervised by SRI WAHJUNI and MUSHTHOFA.

As more businesses rely on the internet to offer their products and services, web-based applications have become the backbone of modern digital society. However, this dependence on web applications has also attracted malicious actors seeking to infiltrate systems for personal gain. In 2024, web applications became the most commonly exploited vector in data breach incidents. This study aims to identify and analyze vulnerabilities in the XXX dan YYY applications, which are critical information system within a higher education institution. The approach used in this research is penetration testing based on the OWASP Web Application Security Testing (WAST) methodology from the OWASP Web Security Testing Guide (WSTG). The testing results revealed fundamental weaknesses in identity management and access control, allowing users to manipulate their roles into administrator privileges, as well as inconsistencies in the implementation of role-based access control. Stored XSS vulnerabilities further worsen the situation by expanding the attack surface, enabling ordinary users to obtain other users' identities and perform actions beyond their authorized privileges. Beyond these

fundamental weaknesses, the most severe finding was a critical remote command execution vulnerability that allowed a user to fully compromise the server.

Keywords: OWASP, penetration testing, web application

@Hak cipta milik IPB University

IPB University





@Hak cipta milik IPB University

IPB University



IPB University
Bogor Indonesia

- Hak Cipta Dilindungi Undang-undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
 2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

© Hak Cipta milik IPB, tahun 2026¹
Hak Cipta dilindungi Undang-Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah, dan pengutipan tersebut tidak merugikan kepentingan IPB.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apa pun tanpa izin IPB.



PENGUJIAN PENETRASI APLIKASI WEB XXX DAN YYY MENGUNAKAN METODOLOGI OWASP WEB APPLICATION SECURITY TESTING

MUHAMMAD ZAHRAN

Skripsi
sebagai salah satu syarat untuk memperoleh gelar
Sarjana pada
Program Studi Ilmu Komputer

**PROGRAM STUDI SARJANA ILMU KOMPUTER
SEKOLAH SAINS DATA, MATEMATIKA, DAN INFORMATIKA
INSTITUT PERTANIAN BOGOR
BOGOR
2026**



@Hak cipta milik IPB University

IPB University

Tim Penguji pada Ujian Skripsi:

1 Endang Purnama Giri S.Kom., M.Kom.



IPB University
— Bogor Indonesia —

Hak Cipta Dilindungi Undang-undang

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
 - b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

Perpustakaan IPB University



Judul Skripsi : Pengujian Penetrasi Aplikasi Web XXX dan YYY Menggunakan Metodologi OWASP Web Application Security Testing

Nama : Muhammad Zahran

NIM : G6401211074

@Hak cipta milik IPB University

Disetujui oleh

Pembimbing 1:

Dr. Ir. Sri Wahjuni, M.T.

Pembimbing 2:

Dr. Mushthofa, S.Kom., M.Sc.

Diketahui oleh

Ketua Program Sarjana Ilmu Komputer:

Dr. Sony Hartono Wijaya, S.Kom., M.Kom.

NIP 19810809 200812 1 002

Tanggal Ujian:

10 Juni 2026

Tanggal Lulus:

PRAKATA

Puji dan syukur penulis panjatkan kepada Allah subhanaahu wa ta'ala atas segala karunia-Nya sehingga karya ilmiah ini berhasil diselesaikan. Tema yang dipilih dalam penelitian yang dilaksanakan sejak bulan Maret 2025 sampai bulan Mei 2026 ini ialah pengujian penetrasi aplikasi web, dengan judul “Pengujian Penetrasi Aplikasi Web XXX dan YYY Menggunakan Metodologi OWASP Web Application Security Testing”.

Penelitian ini dapat diselesaikan dengan baik tentunya dengan bantuan dari banyak pihak. Maka dari itu penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

- a. Ibu Dr. Ir. Sri Wahjuni, M.T. dan Bapak Dr. Mushtofa, S.Kom., M.Sc., selaku dosen pembimbing skripsi, atas segala bimbingan, arahan, dan saran yang sangat berharga selama proses penelitian ini.
- b. Bapak Endang Purnama Giri S.Kom., M.Kom, selaku dosen penguji, atas masukan dan arahnya yang membangun.
- c. Tim ICT pihak klien pengujian penetrasi yang telah banyak membantu dalam memastikan kelancaran penelitian ini.
- d. Kedua orang tua tercinta, para abang, kakak, dan adik yang senantiasa memberikan doa dan kekuatan dalam setiap langkah penulis.
- e. Teman-teman seperjuangan dari Ilmu Komputer angkatan 58

Semoga karya ilmiah ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Juni 2026

Muhammad Zahran



DAFTAR ISI

DAFTAR TABEL	xi
DAFTAR GAMBAR	xi
DAFTAR LAMPIRAN	xi
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Manfaat	3
1.5 Ruang Lingkup	3
II TINJAUAN PUSTAKA	4
2.1 Penetration Testing Execution Standard	4
2.2 Open Web Application Security Project	4
2.3 OWASP Web Security Testing Guide	5
2.4 OWASP Web Application Security Testing	5
2.5 Common Vulnerability Scoring System	5
III METODE	12
3.1 Peralatan Penelitian	12
3.2 Tahapan Penelitian	12
IV HASIL DAN PEMBAHASAN	15
4.1 Interaksi Prapengujian	15
4.2 Pengumpulan Informasi	15
4.3 Pengujian Penetrasi	16
4.4 Analisis dan Pelaporan	26
V SIMPULAN DAN SARAN	33
5.1 Simpulan	33
5.2 Saran	33
DAFTAR PUSTAKA	34
LAMPIRAN	35
RIWAYAT HIDUP	54

Hak cipta milik IPB University

Hak Cipta Dilindungi Undang-undang
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik atau tinjauan suatu masalah
b. Pengutipan tidak merugikan kepentingan yang wajar IPB University.
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin IPB University.

DAFTAR TABEL

1	Metrik-metrik basis pada CVSS 4.0	6
2	Pemetaan kategori keparahan kerentanan CVSS	7
3	Subkelompok metrik pada CVSS 4.0	8
4	Pengumpulan informasi pada OWASP WAST	13
5	Jenis-jenis pengujian pada OWASP WAST	14
6	<i>Response header</i> dari aplikasi XXX dan YYY	16
7	Nilai metrik CVSS kerentanan 1	18
8	Nilai metrik CVSS kerentanan 6	19
9	Nilai metrik CVSS kerentanan 3	20
10	Nilai metrik CVSS kerentanan 2	21
11	Nilai metrik CVSS kerentanan 4	22
12	Nilai metrik CVSS kerentanan 5	23
13	Nilai metrik CVSS kerentanan 6	23
14	Nilai metrik CVSS kerentanan 9	24
15	Nilai metrik CVSS kerentanan 8	25
16	Temuan kerentanan	25
17	Matrik kerentanan	26

DAFTAR GAMBAR

1	Visualisasi jarak keparahan antara dua vektor CVSS	10
2	Tahapan penelitian	12
3	<i>Remote command execution</i> dari webshell pada aplikasi XXX	17
4	Kalkulator CVSS 4.0	18
5	Peringatan <i>browser</i> dari input HTML yang diselipkan kode JavaScript	19

DAFTAR LAMPIRAN

1	Penentuan nilai EQ1	36
2	Penentuan nilai EQ2	37
3	Penentuan nilai EQ3	38
4	Penentuan nilai EQ4	39
5	Penentuan nilai EQ5	40
6	Penentuan nilai EQ6	41
7	Gabungan penentuan nilai EQ3 dan EQ6	42
8	Pemetaan nilai akhir dari setiap kemungkinan kombinasi EQ	43
9	Visualisasi gabungan makrovektor EQ3 = 0 dan EQ6 = 1	49
10	Contoh perhitungan skor akhir CVSS 4.0	50
11	Kode-kode pengujian yang dilakukan pada aplikasi XXX dan YYY	52
12	Temuan kerentanan pada aplikasi XXX dan YYY beserta vektor CVSS-nya	53