TUGAS AKHIR
MAGANG MBKM MANDIRI

PENETRASI TESTING KEAMANAN WEBSITE MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS

ZAKI NEDHIANSYAH

NIM : 215410141

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

TUGAS AKHIR
MAGANG MBKM MANDIRI

PENETRASI TESTING KEAMANAN WEBSITE MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS

Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada
Program Sarjana
Program Studi Informatika
Fakultas Teknologi Informasi
Universitas Teknologi Digital Indonesia

Disusun Oleh
ZAKI NEDHIANSYAH
NIM : 215410141

PROGRAM STUDI INFORMATIKA
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Penetrasi testing keamanan website menggunakan teknik SQL Injection dan XSS
Nama	:	Zaki Nedhiansyah
NIM	:	215410141
Program Studi	:	Informatika
Program	:	Sarjana
Semester	:	Semester 8
Tahun Akademik	:	Genap (2024/2025)

Telah diperiksa dan disetujui untuk diujikan
di hadapan Dewan Penguji Tugas Akhir

Yogyakarta, 23 Juli 2025

Dosen Pembimbing,

Dini Fakta Sari, S.T, M.T.
NIDN : 0507108401

HALAMAN PENGESAHAN

PENETRASI TESTING KEAMANAN WEBSITE MENGGUNAKAN TEKNIK SQL INJECTION DAN XSS

Telah dipertahankan di depan Dewan Penguji dan dinyatakan diterima untuk memenuhi sebagian persyaratan guna memperoleh

Gelar Strata Satu

Program Studi Informatika

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Yogyakarta, 29 Juli 2025

Dewan Penguji	NIDN	Tandatangan
1. Indra Yatini Buryadi, S.Kom., M.Kom.	0511046702	.....
2. Dini Fakta Sari, S.T., M.T.	0507108401	.....
3. Yudhi Kusnanto, S.T., M.T.	0531127002	.....

Mengetahui

Ketua Program Studi Informatika

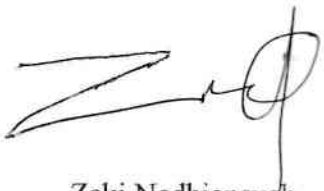
Dini Fakta Sari, S.T., M.T.,

NIDN : 0507108401

PERNYATAAN KEASLIAN TUGAS AKHIR

Dengan ini saya menyatakan bahwa naskah Tugas Akhir ini belum pernah diajukan untuk memperoleh gelar Strata Satu di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 19 Agustus 2025



Zaki Nedhiansyah
NIM: 215410141

HALAMAN PERSEMBAHAN

Puji dan syukur saya panjatkan atas kehadiran Allah SWT, yang telah memberikan kesehatan, rahmat dan hidayah, sehingga saya dapat menyelesaikan tugas akhir ini sebagai syarat memperoleh gelar sarjana. Walaupun tugas akhir ini masih memiliki kekurangan dan jauh dari kata sempurna namun saya bangga dapat menyelesaikan nya dengan tepat waktu.

Tugas akhir ini saya persembahkan kepada orang orang yang selalu memberikan dukungan:

1. Kedua orang tua saya yang selalu memberikan kasih sayang, doa yang tak pernah putus, dan dukungan yang tak ternilai sepanjang hidup saya.
2. Dosen pembimbing Ibu Dini yang selalu memberikan ilmu, bimbingan, serta arahan yang berharga selama proses penyusunan tugas akhir ini
3. Teman-teman magang di PT Sekuriti Siber Indonesia yang menjadi teman diskusi dari awal penyusunan hingga selesainya tugas akhir saya.

PRAKATA

Puji dan syukur saya panjatkan atas kehadirat Allah SWT, karena berkat rahmat dan hidayahNya penyusunan tugas akhir yang berjudul “Penetrasi Testing Keamanan Website Menggunakan teknik SQL Injection dan XSS” ini dapat diselesaikan guna memenuhi salah satu persyaratan dalam menyelesaikan pendidikan strata satu pada jurusan Informatika Universitas Teknologi Digital Indonesia Yogyakarta.

INTISARI

SQL Injection (SQLI) dan Cross Site Scripting (XSS) merupakan dua metode serangan siber yang umum digunakan untuk mengeksploitasi kelemahan pada aplikasi web. Teknik ini memungkinkan penyerang untuk mengakses, memanipulasi, atau mencuri data dari basis data dengan menyisipkan skrip berbahaya ke dalam input yang disediakan oleh aplikasi. Celah semacam ini umumnya ditemukan pada fitur yang menerima masukan dari pengguna, seperti formulir login, registrasi, dan komentar, terutama apabila tidak terdapat validasi karakter secara ketat.

Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan terhadap serangan SQLI dan XSS pada sebuah situs web forum diskusi melalui metode penetration testing. Pengujian dilakukan secara langsung pada elemen-elemen input yang dianggap berisiko dengan menggunakan payload tertentu yang merepresentasikan serangan SQLI dan XSS. Berdasarkan hasil pengujian, ditemukan sebanyak empat titik kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan serangan terhadap sistem.

Kata Kunci: Penetrasi Testing, SQLI, XSS, Website.

ABSTRACT

SQL Injection (SQLI) and Cross-Site Scripting (XSS) are two common cyberattack methods used to exploit vulnerabilities in web applications. These techniques allow attackers to access, manipulate, or steal data from databases by inserting malicious scripts into the input provided by the application. These vulnerabilities are commonly found in features that accept user input, such as login, registration, and comment forms, especially when strict character validation is lacking.

This research aims to identify potential vulnerabilities to SQLI and XSS attacks on a discussion forum website through penetration testing. Testing was conducted directly on input elements deemed at risk using specific payloads representing SQLI and XSS attacks. Based on the test results, four vulnerabilities were identified that could be exploited by malicious parties to attack the system.

Keywords: Penetration Testing, SQLI, XSS, Website.

DAFTAR ISI

Hal

DAFTAR GAMBAR

DAFTAR TABEL

Hal