TUGAS AKHIR
SKEMA MAGANG

PENGUJIAN KEAMANAN APLIKASI WEB G-ENTRY TERHADAP SERANGAN SQL INJECTION DAN CROSS-SITE SCRIPTING (XSS) MENGGUNAKAN METODE PENETRATION TESTING

M. HAFIZ

NIM : 215410092

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

TUGAS AKHIR

SKEMA MAGANG

PENGUJIAN KEAMANAN APLIKASI WEB G-ENTRY TERHADAP SERANGAN SQL INJECTION DAN CROSS-SITE SCRIPTING (XSS) MENGGUNAKAN METODE PENETRATION TESTING

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

Disusun Oleh
M. HAFIZ
NIM : 215410092

PROGRAM STUDI INFORMATIKA
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
YOGYAKARTA
2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Pengujian Keamanan Aplikasi Web G-Entry Terhadap Serangan SQL Injection dan Cross-Site Scripting (XSS) Menggunakan Metode Penetration Testing
Nama	:	M. Hafiz
NIM	:	215410092
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, 13 Agustus 2025

Dosen Pembimbing

Ariesta Damayanti S.Kom,M.Cs
NIDN : 0020047801

HALAMAN PENGESAHAN

PENGUJIAN KEAMANAN APLIKASI WEB G-ENTRY TERHADAP SERANGAN SQL INJECTION DAN CROSS-SITE SCRIPTING (XSS) MENGGUNAKAN METODE PENETRATION TESTING

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

Gelar Sarjana Komputer

Program Studi Informatika

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Yogyakarta 13 Agustus 2025

Dewan Penguji	NIDN	Tandatangan
1. Badiyanto, S.Kom.,M.Kom.	0520066301	.....
2. Ariesta Damayanti S.Kom,M.Cs	0020047801	.....
3. Adiyuda Prayitna, S.T, M.T.	0506067901	.....

Mengetahui

Ketua Program Studi Program Studi

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 Sarjana Komputer 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, 10 Juli 2025

M. Hafiz
NIM: 215410092

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur kehadirat Allah Subhanahu Wa Ta'ala, saya persembahkan tugas akhir ini untuk ayah dan ibu tercinta, yang telah memberikan atas segala doa, dukungan, dan kasih saya yang tak terhingga. Serta Naja Ratu Bania yang senantiasa memberi doa, semangat, dan dukungan.

Yogyakarta, 10 Juli 2025

M. Hafiz

PRAKATA

Puji syukur penulis panjatkan ke hadirat Allah Subhanahu Wa Ta'ala atas segala rahmat, taufik, dan hidayah-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Shalawat dan salam semoga senantiasa tercurah kepada junjungan Nabi Muhammad Shallallahu 'Alaihi Wasallam, beserta keluarga, sahabat, dan seluruh umat beliau. Tugas Akhir ini disusun untuk memenuhi salah satu syarat kelulusan pada Program Studi Informatika, Universitas Teknologi Digital Indonesia. Penulis menyadari bahwa penyusunan laporan ini tidak terlepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Ibu Sri Redjeki, S.Si., M.Kom., Ph.D., selaku Rektor Universitas Teknologi Digital Indonesia.
2. Ibu Dini Fakta Sari, S.T., M.T., selaku Ketua Program Studi Informatika.
3. Ibu Ariesta Damayanti, S.Kom., M.Cs., selaku Dosen Pembimbing, atas segala bimbingan, arahan, dan motivasi selama proses penyusunan Tugas Akhir.
4. Seluruh keluarga besar PT. Sekuriti Siber Indonesia, yang telah memberikan kesempatan, bimbingan, dan wawasan di bidang keamanan siber.
5. Ayah dan bunda tercinta, yang selalu memberikan doa, semangat, dan dukungan tiada henti.
6. Naja Ratu Bania, yang senantiasa memberikan dukungan moril, semangat, dan motivasi selama proses penulisan Tugas Akhir ini.
7. Teman-teman seperjuangan, Wahyu, Rama, Mahendra, serta rekan-rekan lainnya yang selalu memberikan dukungan dan kebersamaan.
8. Seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah membantu dalam bentuk apa p

Penulis menyadari bahwa Tugas Akhir ini masih memiliki keterbatasan, sehingga kritik dan saran yang membangun sangat diharapkan demi penyempurnaan di masa mendatang. Semoga laporan ini dapat bermanfaat bagi pembaca dan pihak-pihak yang memerlukan, khususnya di bidang keamanan aplikasi web**.**

INTISARI

PT. Sekuriti Siber Indonesia adalah perusahaan konsultan keamanan siber yang menyediakan layanan profesional di bidang Penetration Testing, SOC Monitoring, dan Kepatuhan terhadap Standar Keamanan Informasi. Dalam rangka mendukung edukasi praktis di bidang keamanan aplikasi web, perusahaan ini menginisiasi studi pembelajaran dengan fokus pada pengujian keamanan terhadap aplikasi Web *G-Entry*. Permasalahan umum dalam pengembangan aplikasi web adalah kurangnya penerapan kontrol keamanan sejak awal, yang dapat menyebabkan kerentanan terhadap serangan siber. Salah satu contoh nyata ditemukan pada aplikasi web G-Entry, yang berfungsi sebagai media pencatatan pesan pengguna namun belum dilengkapi sistem validasi input yang memadai. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis potensi celah keamanan pada aplikasi tersebut, khususnya terhadap serangan SQL Injection dan Cross-Site Scripting (XSS). Solusi yang diterapkan dalam penelitian ini adalah pengujian keamanan menggunakan metode penetration testing berbasis pendekatan greybox testing, dengan bantuan tools seperti Burp Suite dan SQLMap. Pengujian difokuskan pada form input yang menerima data dari pengguna, seperti login, registrasi, dan pengisian buku tamu. Hasil pengujian menunjukkan bahwa aplikasi rentan terhadap serangan XSS dan SQL Injection. Hal ini dibuktikan dengan keberhasilan penyisipan skrip berbahaya dan bypass autentikasi menggunakan payload SQL. Temuan ini menjadi dasar dalam menyusun rekomendasi teknis sebagai langkah mitigasi risiko, serta menjadi bukti pentingnya penerapan validasi input, penggunaan prepared statement, dan filter karakter sebagai upaya membangun sistem aplikasi yang aman sejak tahap pengembangan.

Kata kunci: Cross-Site Scripting(XSS), G-Entry, Keamanan Aplikasi Web, Penetration Testing, PT Sekuriti Siber Indonesia, SQL Injection.

ABSTRACT

PT. Sekuriti Siber Indonesia is a cybersecurity consulting firm that provides professional services in the fields of Penetration Testing, SOC Monitoring, and Compliance with Information Security Standards. In order to support practical education in the field of web application security, the company initiated a learning study focused on security testing of the G-Entry Web application. A common problem in web application development is the lack of implementation of security controls from the start, which can lead to vulnerability to cyber attacks. One real-world example is found in the G-Entry web application, which functions as a medium for recording user messages but is not equipped with an adequate input validation system. This study aims to identify and analyze potential security vulnerabilities in the application, specifically against SQL Injection and Cross-Site Scripting (XSS) attacks. The solution implemented in this study is security testing using a penetration testing method based on the greybox testing approach, with the help of tools such as Burp Suite and SQLMap. The testing focused on input forms that receive data from users, such as login, registration, and filling in the guest book. The test results showed that the application is vulnerable to XSS and SQL Injection attacks. This was demonstrated by the successful insertion of malicious scripts and authentication bypass using SQL payloads. These findings form the basis for developing technical recommendations for risk mitigation and demonstrate the importance of implementing input validation, prepared statements, and character filters to build secure application systems from the development stage.

***Keywords**: Cross-Site Scripting (XSS), G-Entry, Web Application Security, Penetration Testing, PT Sekuriti Siber Indonesia, SQL Injection.*

DAFTAR ISI

Hal

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal