TUGAS AKHIR
SKEMA MAGANG

PENGUJIAN PENETRASI UNTUK MENGIDENTIFIKASI DAN MEMPERBAIKI KERENTANAN CROSS-SITE SCRIPTING (XSS) PADA WEBSITE PEMESANAN HOTEL TRIUPASEDANAN DI PT. SEKURITI SIBER INDONESIA

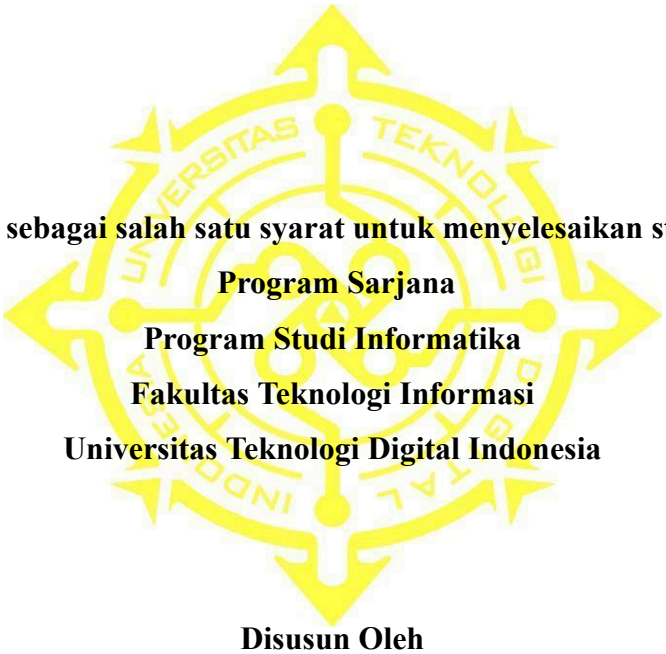
I DEWA GEDE AGUSTINA DHARMA PUTRA
NIM : 225410061

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

TUGAS AKHIR

SKEMA MAGANG

PENGUJIAN PENETRASI UNTUK MENGIDENTIFIKASI DAN MEMPERBAIKI KERENTANAN CROSS-SITE SCRIPTING (XSS) PADA WEBSITE PEMESANAN HOTEL TRIUPASEDANAN DI PT. SEKURITI SIBER INDONESIA



Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada

Program Sarjana

Program Studi Informatika

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Disusun Oleh

I DEWA GEDE AGUSTINA DHARMA PUTRA

NIM : 225410061

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Pengujian Penetrasi Untuk Mengidentifikasi Dan Memperbaiki Kerentanan Cross-Site Scripting (XSS) Pada Website Pemesanan Hotel Triupasedanan Di PT. Sekuriti Siber Indonesia
Nama	:	I Dewa Gede Agustina Dharma Putra
NIM	:	225410061
Program Studi	:	Informatika
Program	:	Sarjana
Semester	:	Semester Genap
Tahun Akademik	:	2024/2025

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

Yogyakarta, Agustus 2025

Dosen Pembimbing,

Adiyuda Prayitna, S.T, M.T.
NIDN : 0506067901

HALAMAN PENGESAHAN

PENGUJIAN PENETRASI UNTUK MENGIDENTIFIKASI DAN MEMPERBAIKI KERENTANAN CROSS-SITE SCRIPTING (XSS) PADA WEBSITE PEMESANAN HOTEL TRIUPASEDANAN DI PT. SEKURITI SIBER INDONESIA

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, 25 juli 2025 (tgl Ujian)

Dewan Penguji	NIDN	Tandatangan
1. Dini Fakta Sari, S.T., M.T.	0507108401	.....
2. Adiyuda Prayitna, S.T, M.T.	0506067901	.....
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 penulis menyatakan bahwa naskah Tugas Akhir ini belum pernah diajukan untuk memperoleh gelar Sarjana Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan penulis 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, 11 Juli 2025

I Dewa Gede Agustina Dharma Putra
NIM: 225410061

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur, tugas akhir ini saya persembahkan kepada orang tua tercinta yang selalu setia menanyakan perkembangan tugas akhir dan menjadi sumber kekuatan di setiap langkah saya, serta saudara saya yang terus mengingatkan dengan pertanyaan sederhana “kapan lulus?” namun bermakna sebagai dorongan untuk segera menyelesaikan proses ini. Ucapan terima kasih juga saya sampaikan kepada teman-teman seperjuangan di PT. Sekuriti Siber Indonesia, khususnya rekan-rekan magang batch 2, atas semangat, kebersamaan, dan kerja sama selama menjalani proses magang. Rasa terima kasih yang mendalam juga saya tujukan kepada para mentor di PT. Sekuriti Siber Indonesia atas bimbingan, arahan, dan ilmu yang telah diberikan. Tak lupa, untuk semua sahabat, teman dan semua yang tidak dapat saya sebutkan satu per satu, terima kasih atas dukungan dan doa yang telah membantu saya hingga sampai pada tahap ini.

PRAKATA

Puji syukur saya panjatkan ke hadirat Ida Sang Hyang Widhi Wasa, Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, sehingga saya dapat menyelesaikan tugas akhir ini yang berjudul "Pengujian Penetrasi Untuk Mengidentifikasi Dan Memperbaiki Kerentanan Cross-Site Scripting (XSS) Pada Website Pemesanan Hotel Triupasedanan Di PT. Sekuriti Siber Indonesia". Tugas akhir ini disusun sebagai salah satu syarat untuk meraih gelar Sarjana pada Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia.

INTISARI

TriUpasedanan adalah aplikasi web yang dikembangkan sebagai lab simulasi untuk pembelajaran serangan Cross-Site Scripting (XSS). Tujuannya membantu peserta magang memahami cara serangan XSS bekerja dan potensi ancaman akibat kurangnya validasi masukkan pengguna. PT. Sekuriti Siber Indonesia (SSI) memberikan bimbingan teknis melalui magang di Security Operation Center (SOC), di mana peserta mempelajari teknik pengujian penetrasi dengan menyisipkan payload seperti `<script>alert('XSS')</script>` dan mensimulasikan pencurian cookie session admin menggunakan XSS.Report. PT. Sekuriti Siber Indonesia juga mengajarkan mitigasi serangan dengan menggunakan fungsi htmlspecialchars() dan teknik perbaikan lainnya. Setelah perbaikan, peserta diminta untuk melakukan pengujian ulang untuk memastikan kerentanannya tertutup.

Hasil kegiatan ini menunjukkan bahwa tanpa validasi masukkan pengguna yang baik, serangan XSS dapat menyebabkan pencurian sesi admin. Namun, dengan mitigasi yang tepat, celah tersebut berhasil ditangani, dan aplikasi dapat menampilkan masukkan secara aman. Kegiatan ini memberikan pengalaman nyata dalam praktik keamanan aplikasi web, menekankan pentingnya simulasi langsung dalam meningkatkan pemahaman dan kesadaran terhadap ancaman siber.

Kata kunci: TriUpasedanan, PT. Sekuriti Siber Indonesia, XSS, Web Aplikasi, Keamanan Siber, Penetration Testing, XSS.Report.

ABSTRACT

TriUpasedanan is a web application developed as a simulation lab for learning about Cross-Site Scripting (XSS) attacks. Its goal is to help internship participants understand how XSS attacks work and the potential threats posed by insufficient user input validation. PT. Sekuriti Siber Indonesia (SSI) provides technical guidance through an internship at the Security Operation Center (SOC), where participants learn penetration testing techniques by injecting payloads like `<script>alert('XSS')</script>` and simulate admin session cookie theft using XSS.Report. SSI also teaches mitigation techniques using functions like htmlspecialchars() and other security fixes. After making improvements, participants are asked to perform retesting to ensure vulnerabilities are closed.

The results of this activity show that without proper user input validation, XSS attacks can lead to admin session theft. However, with the correct mitigations in place, the vulnerability was successfully addressed, and the application was able to securely display user input. This activity provided real-world experience in web application security practices, emphasizing the importance of hands-on simulations to enhance understanding and awareness of cybersecurity threats.

Keywords: TriUpasedanan, PT. Sekuriti Siber Indonesia, XSS, Web Application, Cybersecurity, Penetration Testing, XSS.Report

DAFTAR ISI

DAFTAR GAMBAR