

TUGAS AKHIR

MAGANG BERSERTIFIKAT KAMPUS MERDEKA

IMPLEMENTASI TEKNIK PENETRATION TESTING

UNTUK MENGIDENTIFIKASI RESIKO

KEAMANAN PADA INFRASTRUKTUR WEBSITE MYAPP

(STUDI KASUS : PENETRATION TESTING WEBSITE MYAPP)



SATRIA MATAHARI SAMPURNA

NIM : 215410020

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

TUGAS AKHIR
MAGANG BERSERTIFIKAT KAMPUS MERDEKA
IMPLEMENTASI TEKNIK PENETRATION TESTING
UNTUK MENGIDENTIFIKASI RESIKO
KEAMANAN PADA WEBSITE MYAPP
(STUDI KASUS : PENETRATION TESTING WEBSITE MYAPP)

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



Disusun Oleh :

SATRIA MATAHARI SAMPURNA

NIM : 215410020

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

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul : Impelementasi Teknik Penetratin Testing Untuk
Mengidentifikasi Keamanan Pada Website MyApp
(Studi Kasus : Penetration Testing Website MyApp)

Nama : Satria Matahari Sampurna

NIM : 215410020

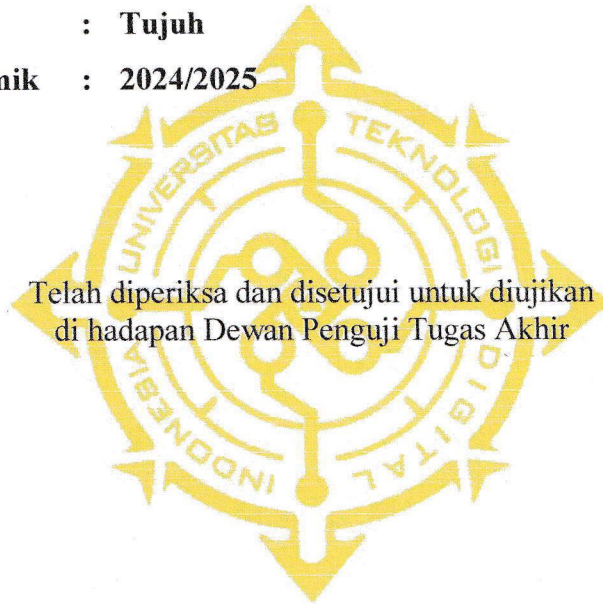
Program Studi : Informatika

Program : Sarjana

Semester : Tujuh

Tahun Akademik : 2024/2025

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



Yogyakarta, 23 Januari 2025

Dosen Pembimbing,

Indra Yatini Buryadi, S.Kom., M.Kom.

NIDN : 0511046702




HALAMAN PENGESAHAN

IMPLEMENTASI TEKNIK PENETRATION TESTING UNTUK MENGIDENTIFIKASI RESIKO KEAMANAN PADA WEBSITE MYAPP

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, 23 Januari 2025

Dewan Penguji	NIDN	Tandatangan
1. <u>Indra Yatini Buryadi, S.Kom., M.Kom.</u>	0511046702	
2. <u>Dr. L.N. Harnaningrum, S.Si., M.T.</u>	0513057101	
3. <u>Dini Fakta Sari, S.T., M.T.</u>	0507108401	

Mengetahui

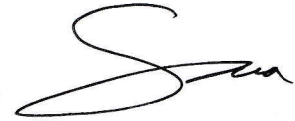
Ketua Program Studi Informatika


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 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, 23 Januari 2025



Satria Matahari Sampurna
NIM: 215410020

HALAMAN PERSEMBAHAN

Puji Syukur penulis panjatkan kepada Allah SWT, yang telah memberikan kesehatan, rahmat dan hidayah, sehingga penulis masih diberikan kesempatan untuk menyelesaikan Tugas Akhir ini sebagai salah satu syarat untuk mendapatkan gelar kesarjanaan. Shalawat serta salam semoga tetap tercurahkan kepada Nabi Muhammad SAW yang telah membawa kita dari zaman kebodohan menuju zaman yang modern seperti saat ini. Akhirnya terselesaikan juga tugas akhir ini dan untuk itu penulis ingin mempersembahkannya untuk orang-orang yang penulis cintai dan sayangi, yaitu :

1. Allah SWT yang telah melimpahkan rahmat dan nikmat-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Keluarga tercinta, bapak, ibu, adik yang telah memberikan doa dan menjadi sumber semangat penulis dalam menyusun Tugas Akhir ini.
3. Ibu Indra Yatini Buryadi, S.Kom., M.Kom. selaku dosen pembimbing dan yang telah memberikan dukungan dan pengarahan dalam penyusunan Tugas Akhir ini.
4. Universitas Teknologi Digital Indonesia yang telah memberikan tempat untuk menambah ilmu, pengalaman, dan teman sehingga membantu dalam penyusunan Tugas Akhir ini.
5. PT Sekuriti Siber Indonesia yang telah memberikan tempat untuk menambah ilmu, pengalaman, dan teman sehingga membantu dalam penyusunan Tugas Akhir ini.
6. Seluruh dan rekan kerja di PT Sekuriti Siber Indonesia yang telah memberikan masukan dan dukungan untuk menyelesaikan Tugas Akhir ini.

7. Keluarga besar HIMAFORKA UTDI yang telah memberikan pengalaman, pelajaran, dan teman selama perkuliahan.

Yogyakarta, 23 Januari 2025

Satria Matahari Sampurna

NIM: 215410020

PRAKATA

Segala syukur dan puji hanya kepada Tuhan Yang Maha Esa atas anugerah Nya yang melimpah, sehingga penulis dapat menyelesaikan penulisan skripsi ini guna memenuhi salah satu persyaratan dalam mencapai Gelar Sarjana Komputer di Fakultas Teknologi Informasi Universitas Teknologi Digital Indonesia Yogyakarta.

Selesainya Skripsi ini tidak terlepas dari bantuan, bimbingan serta dukungan dari berbagai pihak, oleh karena itu melalui kesempatan ini dengan segala kerendahan hati penulis mengucapkan banyak terimakasih 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. dan Ibu Femi Dwi Astuti, S.Kom., M.Cs. , Ketua dan Sekretaris Program Studi Informatika Universitas Teknologi Digital Indonesia.
3. Ibu Indra Yatini Buryadi, S.Kom., M.Kom selaku dosen pembimbing yang telah memberikan bimbingan selama pengerjaan skripsi.
4. Keluarga tercinta, bapak, ibu, adik yang telah memberikan doa dan menjadi sumber semangat penulis dalam menyusun Tugas Akhir ini.
5. PT Sekuriti Siber Indonesia yang telah memberikan tempat untuk menambah ilmu, pengalaman, dan teman sehingga membantu dalam penyusunan Tugas Akhir ini.
6. Teman-teman dan seluruh dan rekan kerja di PT Sekuriti Siber Indonesia yang telah memberikan dukungan untuk menyelesaikan Tugas Akhir ini.
7. Keluarga besar HIMAFORKA UTDI yang telah memberikan pengalaman, pelajaran, dan teman selama perkuliahan.

INTISARI

Penetration testing adalah salah satu metode untuk mengidentifikasi dan mengevaluasi celah keamanan dalam aplikasi ataupun *website*. Tugas akhir ini berfokus pada pengembangan *website* MyApp dan pengujian keamanan melalui *penetration testing* menggunakan berbagai *tools*. Penelitian ini dilakukan untuk mengetahui potensi ancaman keamanan pada MyApp dan memberikan solusi pencegahan untuk meningkatkan perlindungan data pengguna.

Penelitian ini diawali dengan pengembangan *website* MyApp yang memiliki fitur yang sudah ditentukan dari tempat magang seperti chat, top-up dan transaksi antar pengguna. Selanjutnya, dilakukan *penetration testing* yang mencakup tahapan scanning, exploitation, dan post-exploitation. *Tools* seperti *Burp Suite* dan *SQL Map* digunakan untuk mendeteksi celah keamanan. Setelah itu, dibuat laporan hasil temuan yang mencakup deskripsi celah, tingkat risiko, serta langkah eksploitasi yang berhasil dilakukan.

Hasil penelitian menunjukkan beberapa celah keamanan yang signifikan, seperti *SQL Injection*, *HTML Injection*, *IDOR (Insecure Direct Object References)*. Berdasarkan temuan tersebut, rekomendasi diberikan untuk memperbaiki kelemahan yang telah ditemukan dari hasil *Penetration testing*. Rekomendasi ini bertujuan untuk memitigasi risiko keamanan dan meningkatkan ketahanan sistem.

Penelitian ini diharapkan memberikan kontribusi dalam memahami pentingnya pengujian keamanan pada aplikasi web serta membantu pengembang dalam merancang sistem yang lebih aman.

Kata kunci: *Penetration Testing*, *MyApp*, *Kemanan*, *Burp Suite*, *SQL Map*

ABSTRACT

Penetration testing is a method for identifying and evaluating security gaps in applications or websites. This final project focuses on developing the MyApp website and security testing through penetration testing using various tools. This research was conducted to determine potential security threats to MyApp and provide preventative solutions to increase user data protection.

Next, penetration testing is carried out which includes scanning, exploitation and post-exploitation stages. Tools such as Burp Suite and SQL Map are used to detect security gaps. After that, a report on the findings is created which includes a description of the gap, level of risk, and successful exploitation steps.

The research results show several significant security gaps, such as SQL Injection, HTML Injection, IDOR (Insecure Direct Object References). Based on these findings, recommendations are given to improve weaknesses that have been found from the results of penetration testing. These recommendations aim to mitigate security risks and increase system resilience.

This research is expected to contribute to understanding the importance of security testing in web applications and help developers in designing more secure systems.

Keywords: Penetration Testing, MyApp, Security, Burp Suite, SQL Map

DAFTAR ISI

TUGAS AKHIR	1
HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR	2
HALAMAN PENGESAHAN	3
PERNYATAAN KEASLIAN TUGAS AKHIR	4
HALAMAN PERSEMBAHAN	5
PRAKATA	7
INTISARI	8
ABSTRACT	9
DAFTAR ISI.....	10
DAFTAR GAMBAR	12
DAFTAR TABEL.....	13
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Deskripsi Pekerjaan	2
1.3 Tujuan.....	3
1.4 Manfaat.....	4
BAB II PROFIL INSTANSI TEMPAT MAGANG.....	6
2.1. Sejarah PT Security Siber Indonesia (Nemo Security)	6
2.2. Struktur Organisasi PT Security Siber Indonesia (Nemo Security).....	7
2.3. Visi dan Misi PT Security Siber Indonesia (Nemo Security).....	9
2.4. Tugas Pokok dan Fungsi PT Security Siber Indonesia (Nemo Security)	10
BAB III DESKRIPSI KEGIATAN	11
3.1 Persoalan.....	11
3.2 Deskripsi Produk	13
3.3 Analisis dan Rancangan.....	15
3.4 Jadwal Kerja	18
BAB IV HASIL DAN PEMBAHASAN.....	22
4.1 Hasil.....	23
4.2 Uji coba	26
4.3 Pembahasan	42
BAB V PENUTUP	49
5.1 Simpulan.....	49
5.2 Saran.....	51

LAMPIRAN.....	53
1. Transkrip/Penilaian dari tempat magang	53
2. Sertifikat magang	54
3. Dokumentasi/foto kegiatan.....	54
4. Log Activity Kegiatan Magang program MBKM	56
DAFTAR PUSTAKA	80

DAFTAR GAMBAR

Gambar 2. 1 Sturktur Organisasi PT Sekurity Siber Indonesi (Nemo Security).....	7
Gambar 3. 1 Diagram Alir Penetration Testing.....	16
Gambar 4. 1 Halaman BurpSuite dan Login MyApp	27
Gambar 4. 2 POC halaman login dan hasil request dari burpsuite	27
Gambar 4. 3 POC repeter burpsuite dan hasil celah SQL Injection.....	28
Gambar 4. 4 POC hasil eksploitasi menggunakan SQL Map menampilkan database	29
Gambar 4. 5 POC hasil scanning SQL Map menampilkan database MyApp.....	29
Gambar 4. 6 POC hasil eksploitasi SQL Map menampilkan tabel user MyApp	30
Gambar 4. 7 POC login menggunakan database dari hasil eksploitasi	30
Gambar 4. 8 POC payload di halaman registrasi.....	34
Gambar 4. 9 hasil eksploitasi dari penyusupan payload	34
Gambar 4. 10 POC mengirimkan payload berbahaya	36
Gambar 4. 11 Hasil eksploitasi dari payload	37
Gambar 4. 12 POC melakukan transaksi antar user	39
Gambar 4. 13 POC hasil request dari burpsuite dan ekpoitasi.....	40
Gambar 4. 14 Hasil dari eksploitasi data	40
Gambar 4. 15 Program yang menyebabkan celah HTML Injection pada registrasi	44
Gambar 4. 16 Program yang menyebabkan celah HTML Injection pada chat	45
Gambar 4. 17Program yang menyebabkan celah HTML Injection pada chat	45
Gambar 4. 18 Program yang menyebabkan celah IDOR pada transfer	46
Gambar 4. 19 potongan program terhindar dari eksploitasi.....	47

DAFTAR TABEL

Tabel 3. 1 penjabaran jadwal kerja.....	18
Tabel 4. 1 Rangkuman Celah Pada Website MyApp	24
Tabel 4. 2 Hasil report dari Penetration Testing halaman login MyApp	32
Tabel 4. 3 Hasil report dari Penetration Testing halaman register MyApp.....	35
Tabel 4. 4 Hasil report dari Penetration Testing halaman chat MyApp.....	38
Tabel 4. 5 Hasil report dari Penetration Testing halaman Transfer MyApp	41