TUGAS AKHIR
SKEMA MAGANG

Implementasi dan Analisis Metode Pentesting pada Website Perusahaan XYZ untuk Meningkatkan Keamanan Aplikasi Web

MUHAMMAD RIDWAN NUR IHSAN

NIM : 215410074

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

TUGAS AKHIR

SKEMA MAGANG

Implementasi dan Analisis Metode Pentesting pada Website Perusahaan XYZ untuk Meningkatkan Keamanan Aplikasi Web

Diajukan sebagai salah satu syarat untuk menyelesaikan studi pada

Program Sarjana

Program Studi Informatika

Fakultas Teknologi Informasi

Universitas Teknologi Digital Indonesia

Disusun Oleh

MUHAMMAD RIDWAN NUR IHSAN

NIM : 215410074

PROGRAM STUDI INFORMATIKA

PROGRAM SARJANA

FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR

Judul	:	Implementasi dan Analisis Metode Pentesting pada Website Perusahaan XYZ untuk Meningkatkan Keamanan Aplikasi Web
Nama	:	Muhammad Ridwan Nur Ihsan
NIM	:	215410074
Program Studi	:	Informatika
Program	:	Sarjana
Semester	:	7
Tahun Akademik	:	2025

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

Yogyakarta, 23 Januari 2025

Dosen Pembimbing,

Dr. L.N. Harnaningrum, S.Si., M.T.

NIDN : 0513057101

HALAMAN PENGESAHAN

Implementasi dan Analisis Metode Pentesting pada Website Perusahaan XYZ untuk Meningkatkan Keamanan Aplikasi Web

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, 14 Februari 2025

Dewan Penguji	NIDN	Tandatangan
1. Thomas Edyson Tarigan, S.Kom., M.Cs.	0023107402	.....
2. Dr. L.N. Harnaningrum, S.Si., M.T.	0513057101	.....
3. M. Agung Nugroho, S.Kom., M.Kom.	0507078501	.....

Mengetahui

Ketua Program Studi Informatika

Ibu 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, 26 Januari 2025

Muhammad Ridwan Nur Ihsan

NIM: 215410074

HALAMAN PERSEMBAHAN

Dengan penuh rasa syukur atas berkat, rahmat, serta kasih karunia Allah SWT, serta doa, kebaikan, dan dukungan dari orang-orang di sekitar, penulis akhirnya dapat menyelesaikan laporan tugas akhir ini. Oleh karena itu, laporan tugas akhir ini penulis persembahkan kepada:

1. Ibu tercinta, yang senantiasa memberikan kasih sayang, dukungan, dan doa tanpa henti. Ibu tetap menjadi sumber semangat dan inspirasi di setiap langkah penulis.
2. Bapak tercinta, yang selalu memberikan dukungan, nasihat, dan semangat hidup yang menjadi pedoman berharga bagi penulis dalam menjalani perjalanan ini.
3. Dosen pembimbing dan seluruh pengajar, yang telah memberikan bimbingan, ilmu, dan dukungan akademis yang sangat berarti selama proses penyusunan laporan tugas akhir ini.
4. Rekan-rekan seperjuangan, yang senantiasa memberikan dukungan, motivasi, serta kerja sama selama masa studi.
5. Sahabat-sahabat terbaik saya—Maul, Azis, Ilham—yang selalu ada di sisi penulis, memberikan dorongan, berbagi tawa, dan semangat dalam setiap keadaan.
6. Semua pihak yang telah berkontribusi namun tidak dapat disebutkan satu per satu. Penulis mengucapkan terima kasih yang sebesar-besarnya. Semoga Allah SWT membalas segala kebaikan kalian semua.

PRAKATA

Segala puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan tugas akhir dengan judul "Implementasi dan Analisis Metode Pentesting pada Website Perusahaan XYZ untuk Meningkatkan Keamanan Aplikasi Web". Tugas akhir ini disusun sebagai bagian dari persyaratan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Teknologi Digital Indonesia.

Dalam proses penyusunan tugas akhir ini, penulis menyadari bahwa penyelesaian karya ini tidak akan mungkin tanpa bantuan, arahan, serta dukungan dari berbagai pihak. Oleh karena itu, dengan penuh rasa hormat dan terima kasih, penulis ingin menyampaikan penghargaan setinggi-tingginya kepada:

1. Ibu Sri Redjeki, S.Si., M.Kom., Ph.D., selaku Rektor Universitas Teknologi Digital Indonesia.
2. Bapak Dr. Bambang Purnomosidi DP, S.E. Akt., S.Kom., MMSI., selaku Dekan Fakultas Teknologi Informasi.
3. Ibu Dini Fakta Sari, S.T., M.T., selaku Ketua Program Studi Informatika Universitas Teknologi Digital Indonesia.
4. Dr. L.N. Harnaningrum, S.Si., M.T., selaku dosen pembimbing yang dengan penuh kesabaran telah memberikan bimbingan, arahan, serta dukungan hingga terselesaikannya tugas akhir ini.
5. Keluarga tercinta, yang selalu memberikan doa, dukungan, dan motivasi kepada penulis selama masa perkuliahan hingga penyelesaian laporan tugas akhir ini.
6. Teman-teman sejawat yang selalu mendampingi selama masa studi, serta memberikan semangat dan motivasi dalam menyelesaikan laporan ini.
7. Kekasih tersayang, yang senantiasa memberikan dukungan moral,

semangat, serta dorongan motivasi untuk menyelesaikan tugas akhir ini.

8. Seluruh dosen dan staf Universitas Teknologi Digital Indonesia yang telah membantu dalam berbagai hal selama masa studi.
9. Semua pihak yang turut berkontribusi, baik secara langsung maupun tidak langsung, yang tidak dapat disebutkan satu per satu.

Penulis menyadari bahwa tugas akhir ini masih memiliki kekurangan dan jauh dari kesempurnaan. Oleh karena itu, penulis sangat terbuka untuk menerima kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga tugas akhir ini dapat memberikan manfaat, baik bagi penulis maupun para pembaca, serta menjadi kontribusi yang positif dalam pengembangan ilmu pengetahuan.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang telah mendukung, dan semoga Tuhan Yang Maha Esa senantiasa melimpahkan rahmat dan berkah-Nya kepada kita semua.

Yogyakarta, 26 Januari 2025

Muhammad Ridwan Nur Ihsan

NIM : 215410074

INTISARI

Penelitian ini berfokus pada penerapan metode *penetration testing* (pentesting) untuk mengidentifikasi dan menganalisis kerentanan keamanan pada aplikasi web. Dalam upaya meningkatkan pemahaman dan keterampilan dalam keamanan siber, proyek ini dilakukan dengan mengembangkan sebuah *website dummy* yang menyerupai aplikasi perusahaan *XYZ*, dilengkapi dengan kerentanan umum seperti *SQL Injection, Cross-Site Scripting (XSS), security misconfiguration*, dan *exposed sensitive data*.

Metode pentesting dilakukan secara manual dan otomatis menggunakan tools seperti, *Burp Suite*, *SQLMap*, dan *Nmap*. Prosesnya mencakup identifikasi kerentanan, eksploitasi kerentanan, dan dokumentasi hasil. Standar *OWASP Top 10* digunakan sebagai referensi utama dalam menganalisis kerentanan yang ditemukan.

Hasil penelitian menunjukkan berbagai kerentanan yang dapat dieksploitasi untuk mengakses data sensitif, mengubah data, atau menyerang pengguna aplikasi. Analisis kerentanan dilakukan untuk mengevaluasi dampak terhadap keamanan aplikasi, serta memberikan rekomendasi mitigasi seperti validasi input, penerapan kebijakan keamanan, dan pengamanan data sensitif.

Proyek ini membuktikan pentingnya pengujian keamanan terhadap aplikasi web dalam mencegah ancaman siber yang semakin kompleks. Proses dan hasil dokumentasi yang disusun dapat menjadi referensi bagi perusahaan untuk meningkatkan keamanan aplikasi mereka.

Kata kunci: *keamanan siber, OWASP Top 10, penetration testing, website dummy, XSS.*

ABSTRACT

This research focuses on implementing penetration testing (pentesting) methods to identify and analyze security vulnerabilities in web applications. To enhance knowledge and skills in cybersecurity, this project involves developing a dummy website resembling the application used by XYZ company. The dummy website is equipped with common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), security misconfiguration, and exposed sensitive data.

The pentesting process is conducted both manually and using automated tools such as Burp Suite, SQLMap, and Nmap. The process includes vulnerability identification, exploitation, and documentation. The OWASP Top 10 standard serves as the primary reference for analyzing the vulnerabilities discovered.

The results reveal several vulnerabilities that can be exploited to access sensitive data, alter information, or attack application users. Vulnerability analysis evaluates the impact on application security and provides mitigation recommendations such as input validation, implementing security policies, and securing sensitive data.

This project demonstrates the importance of conducting security testing on web applications to prevent increasingly complex cyber threats. The documented processes and results can serve as references for companies to improve the security of their applications.

Keywords: cybersecurity, OWASP Top 10, penetration testing, dummy website, XSS.

DAFTAR ISI

TUGAS AKHIR 1
HALAMAN PERSETUJUAN UJIAN TUGAS AKHIR ii
HALAMAN PENGESAHAN iii
PERNYATAAN KEASLIAN TUGAS AKHIR iv
HALAMAN PERSEMBAHAN v
PRAKATA vi
INTISARI viii
ABSTRACT ix
DAFTAR ISI x
DAFTAR GAMBAR xii
DAFTAR TABEL xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Deskripsi Pekerjaan 2
1.3 Tujuan 5
1.4 Manfaat 7
BAB II PROFIL INSTANSI TEMPAT MAGANG 10
2.1 Sejarah 10
2.2 Visi dan Misi 11
2.3 Struktur Organisasi 12
BAB III DESKRIPSI KEGIATAN 18
3.1 Persoalan 18
3.2 Deskripsi Produk 20
3.3 Analisis dan Rancangan 22
3.3.1 Analisis Sistem 26
3.3.2 Rancangan Sistem 28
3.3.3 Penjelasan Rancangan Sistem 29
3.3.4 Alur Proses 31
3.3.5 Rancangan Pengujian 31
3.3.6 Metode Pengujian 32
3.4 Jadwal Kerja 33

BAB IV HASIL DAN PEMBAHASAN 37
4.1 Hasil 38
4.2 Uji coba 42
4.3 Pembahasan 57
BAB V PENUTUP 64
5.1 Simpulan 64
5.2 Saran 65
LAMPIRAN 67
1. Transkrip/Penilaian dari tempat magang 67
2. Sertifikat magang 68
3. Dokumentasi/foto kegiatan 68
4. Log Activity Kegiatan Magang program MBKM 71
5. Kriteria, Catatan, dan Keputusan Tugas Akhir 94
6. Persetujuan Dosen Penguji dan Pembimbing 95
7. Surat Keterangan Persetujuan Publikasi 96
DAFTAR PUSTAKA 97

DAFTAR GAMBAR

Gambar 1 Struktur Organisasi 11
Gambar 2 Diagram Alir Penetration Testing 22
Gambar 3 Rancangan Sistem 29
Gambar 4 POC Tabel 4 Form Login 44
Gambar 5 POC Tabel 4 Burp Suite Intercept Pada Form Login 44
Gambar 6 POC Tabel 4 Hasil Request Intercept Pada Form Login 45
Gambar 7 POC Tabel 4 Uji SQL Injection Menggunakan Tools SQLMap 45
Gambar 8 POC Tabel 4 Menggunakan perintah dump dengan SQLMap 46
Gambar 9 POC Tabel 4 Hasil dari perintah dump 46
Gambar 10 POC Tabel 5 Form Register 48
Gambar 11 POC Tabel 5 Hasil Dari Payload HTML Injection 48
Gambar 12 POC Tabel 5 Hasil Dari Payload HTML Injection didatabase 48
Gambar 13 POC Tabel 6 Fitur Chat 50
Gambar 14 POC Tabel 6 Hasil Dari Payload XSS 50
Gambar 15 POC Tabel 7 Fitur Transaksi 52
Gambar 16 POC Tabel 7 Burp Suite Request dari Fitur Transaksi 52
Gambar 17 POC Tabel 7 Setelah Memodifikasi Parameter Username 53
Gambar 18 POC Tabel 7 Hasil dari Kerentanan IDOR 53
Gambar 19 POC Tabel 7 Kerentanan XSS pada Fitur Transaksi 54
Gambar 20 POC Tabel 8 Form Edit User 55
Gambar 21 POC Tabel 9 Hasil Dari Delete User 57
Gambar 22 Transkip Nilai Dari Tempat Magang 67
Gambar 23 Sertifikat Magang 68
Gambar 24 Dokumentasi Diskusi Pekerjaan 68
Gambar 25 Dokumentasi Pergantian Shift 69
Gambar 26 Dokumentasi Latihan Pentesting 69
Gambar 27 Dokumentasi Diskusi Incident 70
Gambar 28 Dokumentasi Pemantauan Server 70

DAFTAR TABEL

Table 1 Jadwal Kerja 34
Table 2 Report Hasil Kerentanan 39
Table 3 Grafik Tingkat Keparahan Kerentanan 42
Table 4 Report Kerentanan SQL Injection 43
Table 5 Report Kerentanan HTML Manipulation 47
Table 6 Report Kerentanan XSS 49
Table 7 Report Kerentanan IDOR 51
Table 8 Report Rekomendasi Fitur Edit User 54
Table 9 Report Rekomenedasi Fitur Delete User 56
Table 10 Rangkuman Seluruh Hasil Kerentanan 63
Table 11 Log Activity Program MBKM Magang Mandiri UTDI 71