

***Penetration Testing* pada Sistem ABC dan Sistem XYZ**
Universitas Pendidikan Ganesha



OLEH
KETUT WAWAN ARIMBAWA
1915101015

PROGRAM STUDI ILMU KOMPUTER
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA
SINGARAJA

2023

***Penetration Testing* pada Sistem ABC dan Sistem XYZ
Universitas Pendidikan Ganesha**

SKRIPSI

Diajukan Kepada

Universitas Pendidikan Ganesha

Untuk Memenuhi Salah Satu Persyaratan dalam Menyelesaikan

Program Sarjana Program Studi Ilmu Komputer



Oleh

KETUT WAWAN ARIMBAWA

1915101015

PROGRAM STUDI ILMU KOMPUTER

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK DAN KEJURUAN

UNIVERSITAS PENDIDIKAN GANESHA

SINGARAJA

2023

SKRIPSI

**DIAJUKAN UNTUK MELENGKAPI TUGAS
DAN MEMENUHI SYARAT-SYARAT UNTUK
MENCAPAI GELAR SARJANA KOMPUTER**

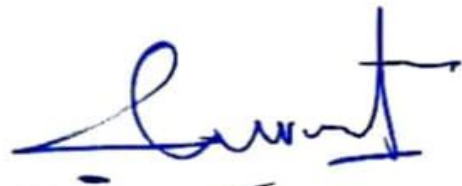
Menyetujui

Pembimbing I,



I Ketut Resika Arthana, S.T., M.Kom.
NIP. 198412012012121002

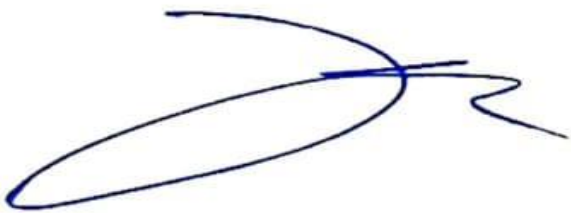
Pembimbing II,



I Ketut Purnamawan, S.Kom., M.Kom.
NIP. 197905112006041004

Skripsi oleh Ketut Wawan Arimbawa ini
telah di pertahankan di depan dewan penguji
pada tanggal 17 Juli 2023

Dewan Penguji,



I Ketut Resika Arthana, S.T., M.Kom.
NIP. 198412012012121002

(Ketua)



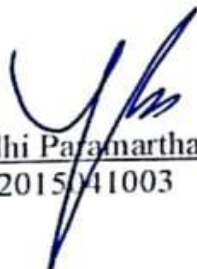
I Ketut Purnamawan, S.Kom., M.Kom.
NIP. 197905112006041004

(Anggota)



I Nyoman Saputra Wahyu Wijaya, S.Kom., M.Cs.
NIP. 198910262019031004

(Anggota)



A.A. Gede Yudhi Paramartha, S.Kom., M.Kom.
NIP. 198806222015041003

(Anggota)

Diterima oleh Panitia Ujian Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha
Guna memenuhi syarat-syarat untuk mencapai gelar sarjana

Pada:

Hari : Senin.....

Tanggal : 17 Juli 2023

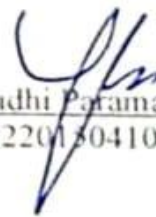
Mengetahui,

Ketua Ujian,



Prof. Dr. Ketut Agustini, S.Si., M.Si.
NIP. 197408012000032001

Sekretaris Ujian,



A.A. Gede Yudhi Paramartha, S.Kom., M.Kom.
NIP. 198806222013041003

Mengesahkan,

Wakil Rektor I Bidang Akademik dan Kerja Sama



Prof. Dr. Gede Rasben Dantes, S.T., M.T.I.
NIP. 197502212003121001

PERNYATAAN

Dengan ini saya menyatakan bahwa karya tulis yang berjudul "*Penetration Testing* pada Sistem ABC dan Sistem XYZ Universitas Pendidikan Ganesha " beserta keseluruhan isinya adalah benar-benar hasil karya sendiri dan tidak melakukan penjiplakan dan pengutipan dengan cara yang tidak sesuai dengan etika yang berlaku pada buku pendoman skripsi. Jika dikemudian hari ditemukan adanya pelanggaran saya siap menanggung resiko atau sanksi yang di jatuhkan kepada saya.

Singaraja, 17 Juli 2023

Yang membuat pernyataan,



Ketut Wawan Arimbawa

NIM. 1915101015

PRAKATA

Puji syukur peneliti panjatkan ke hadapan Ida Sang Hyang Widhi Wasa/Tuhan Yang Maha Esa karena berkat rahmat-Nya lah sehingga memungkinkan peneliti menyelesaikan skripsi dengan judul "**Penetration Testing pada Sistem ABC dan Sistem XYZ Universitas Pendidikan Ganesha**" sebagai salah satu syarat untuk memperoleh gelar sarjana Ilmu Komputer di Universitas Pendidikan Ganesha. Dalam menyelesaikan skripsi ini, peneliti banyak mendapatkan motivasi dan bantuan baik berupa moral maupun material dari berbagai pihak. Untuk itu dalam kesempatan ini peneliti mengucapkan rasa terima kasih kepada:

1. Ibu Dr. Luh Joni Erawati Dewi, ST., M.Pd., selaku Ketua Jurusan Teknik Informatika atas motivasi dan fasilitas yang diberikan sehingga peneliti dapat menyelesaikan studi ini dengan tepat waktu.
2. Bapak A.A. Gede Yudhi Paramartha, S.Kom.,M.Kom. selaku Kaprodi Ilmu Komputer atas motivasi dan fasilitas yang diberikan kepada peneliti dalam penyelesaian skripsi ini.
3. Bapak I Ketut Resika Arthana, S.T., M.Kom. selaku pembimbing I serta pembimbing akademik yang telah membimbing peneliti selama kurang lebih 8 semester dan selalu memberikan arahan selama peneliti menjalani studi. yang telah memberikan banyak motivasi, bimbingan, arahan, petunjuk skripsi, dengan penuh kesabaran kepada peneliti dalam menyelesaikan skripsi ini sehingga peneliti dapat menyelesaikan skripsi dengan tepat waktu.
4. Bapak I Ketut Purnamawan, S.Kom., M.Kom. selaku pembimbing II yang telah banyak memberikan motivasi, semangat, bimbingan, arahan dengan penuh kesabaran kepada peneliti dalam menyelesaikan skripsi ini sehingga peneliti dapat menyelesaikan skripsi dengan tepat waktu.
5. Bapak Gede Arna Jude Saskara, S.T.,M.T Selaku ketua divisi infrastuktur, jaringan, dan keamanan Unit Penunjang Akademik Teknologi, Informasi dan Komunikasi (UPT-TIK) Universitas Pendidikan Ganesha yang

memfasilitasi penelitian serta sudah seperti pembimbing ke-3 yang memberikan masukan selama melakukan penelitian.

6. Seluruh staf dosen di lingkungan Jurusan Teknik Informatika/ Program Studi Ilmu Komputer yang telah memberikan ilmu, pengalaman, motivasi, serta semangat selama menjalani studi di Universitas Pendidikan Ganesha.
7. Kepada orang tua peneliti Ketut Sumara dan Luh Reniti yang telah mendukung, membimbing, melatih memarahi, serta memberikan dukungan finansial kepada putranya Ucapan terima kasih seumur hidup peneliti tidak akan pernah cukup untuk seluruh jasa mereka yang luar biasa.
8. Untuk seluruh teman – teman prodi Ilmu Komputer Angkatan 2019 yang telah memberikan berbagai pengalaman dan kebersamaan selama peneliti menempuh pendidikan di Universitas Pendidikan Ganesha.
9. Seluruh pihak yang tidak bisa di sebutkan satu persatu yang telah membantu peneliti dalam penyusunan skripsi sehingga dapat selesai tepat waktu.

Semoga Ida Sang Hyang Widhi Wasa/Tuhan Yang Maha Esa senantiasa memberikan karunianya dan membantu peneliti dalam menyelesaikan skripsi ini. Peneliti menyadari sepenuhnya bahwa apa yang disajikan dalam skripsi ini masih jauh dari kata sempurna mengingat keterbatasan peneliti. Peneliti mengharapkan segala masukan, kritik dan saran yang bersifat membangun dari berbagai pihak. Peneliti berharap apa yang dibuat oleh peneliti dapat bermanfaat dan berharga bagi kita semua, khususnya untuk mengembangkan dunia pendidikan

Singaraja, 17 Juli 2023

Peneliti

DAFTAR ISI

PRAKATA.....	i
ABSTRAK.....	iii
DAFTAR ISI.....	v
DAFTAR TABEL.....	viii
DAFTAR GAMBAR.....	ix
DAFTAR LAMPIRAN.....	x
BAB I PENDAHULUAN.....	1
1.1 Latar belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan.....	3
1.4 Batasan Masalah.....	4
1.5 Manfaat.....	4
BAB II KAJIAN TEORI.....	6
2.1 Sistem Informasi.....	6
2.1.2 Karakteristik Informasi.....	7
2.2 Konsep Dasar Keamanan Sistem Informasi.....	8
2.2.1 Pengertian Keamanan Sistem Informasi.....	8
2.2.2 Ancaman dalam Keamanan Sistem Informasi.....	9
2.3 Kerentanan Sistem.....	11
2.4 Kali Linux.....	12
2.5 OWASP.....	12
2.5.1 OWASP TOP 10.....	13
2.6 <i>Vulnerability Assessment</i>	16
2.7 <i>Penetration Testing</i>	17
2.8 Penelitian Sejenis.....	17
BAB III METODE PENELITIAN.....	19
3.1 Metode Pengumpulan Data.....	19
3.1.1 Observasi.....	20

3.1.2	Wawancara.....	20
3.1.3	Studi Literatur	20
3.2	Teknik Pengujian dan Kebutuhan Informasi.....	21
3.3	Skenario Identifikasi Kerentanan dan Uji Penetrasi.....	22
3.4	Skenario Ancaman pada Sistem ABC.....	22
3.4.1	<i>Sensitive Information Disclosure (A04:2021-Insecure Design)</i>	23
3.4.2	<i>Cloud metadata potentially exposed (A05:2021-Security Misconfiguration)</i>	24
3.4.3	<i>Hidden file found (A05:2021-Security Misconfiguration)</i>	26
3.4.4	<i>Sql Injection (A03:2021-Injection)</i>	27
3.5	Skenario Ancaman pada Sistem XYZ.....	29
3.5.1	<i>Cross Site Scripting Reflected (A03:2021-Injection)</i>	29
3.5.2	<i>Cloud Metadata Potentially Exposed (A03:2021-Injection)</i>	30
3.5.3	<i>Sql injection (A03:2021-Injection)</i>	32
3.5.4	<i>Hidden file found (A05:2021-Security Misconfiguration)</i>	33
3.5.5	<i>Arbitrary File Upload (A08:2021-Software and Data Integrity Failures)</i>	35
3.6	Metode Analisis dan Penilaian Risiko Kerentanan	36
BAB IV HASIL DAN PEMBAHASAN		39
4.1	Hasil Pengujian (Proof of concept/PoC) Eksploitasi Celah Keamanan pada Sistem ABC.....	39
4.1.1	<i>Sensitive Information Disclosure (A04:2021-Insecure Design)</i>	40
4.1.2	<i>Cloud metadata potentially exposed (A05:2021-Security Misconfiguration)</i>	42
4.1.3	<i>Hidden file found (A05:2021-Security Misconfiguration)</i>	44
4.1.4	<i>Sql Injection (A03:2021-Injection)</i>	45
4.2	Hasil Pengujian (Proof of concept/PoC) Eksploitasi Celah Keamanan pada Sistem XYZ.....	47
4.2.1	<i>Cross Site Scripting Reflected (A03:2021-Injection)</i>	48
4.2.2	<i>Cloud Metadata Potentially Exposed (A05:2021-Security Misconfiguration)</i>	51

4.2.3	<i>SQL injection (A03:2021-Injection)</i>	52
4.2.4	<i>Hidden file found (A05:2021-Security Misconfiguration)</i>	53
4.2.5	<i>Arbitrary File Upload (A08:2021-Software and Data Integrity Failures)</i>	54
4.3	Pembahasan Kerentanan pada Sistem ABC.....	56
4.3.1	<i>Sensitive Information Disclosure</i>	56
4.3.2	<i>Cloud metadata potentially exposed</i>	57
4.3.3	<i>Hidden file found</i>	57
4.3.4	<i>Sql Injection</i>	58
4.4	Pembahasan Kerentanan pada Sistem XYZ.....	58
4.4.1	<i>Cross Site Scripting Reflected</i>	59
4.4.2	<i>Cloud metadata potentially exposed</i>	59
4.4.3	<i>Sql injection</i>	60
4.4.4	<i>Hidden file found</i>	60
4.4.5	<i>Arbitrary File Upload</i>	61
4.5	Pengukuran Nilai Kerentanan	61
BAB V PENUTUP.....		68
5.1	Kesimpulan.....	68
5.2	Saran.....	69
DAFTAR PUSTAKA		70
LAMPIRAN.....		72
RIWAYAT HIDUP.....		77

DAFTAR TABEL

Tabel 2.1 Penelitian sejenis.....	17
Tabel 3.1 Tool untuk melakukan pengintaian dan uji penetrasi	21
Tabel 3.2 likelihood and impact level	37
Tabel 3.3 Likelihood	37
Tabel 3.4 Impact.....	37
Tabel 3.5 Tingkat Risiko Kerentanan	38
Tabel 4. 1 Hasil pengumpulan informasi dari sistem ABC	39
Tabel 4. 2 Informasi dan hasil kerentanan sensitive information disclosure	41
Tabel 4. 3 Informasi terkait kerentanan cloud metadata potentially exposed.....	42
Tabel 4. 4 Informasi terkait kerentanan hidden file found.....	44
Tabel 4. 5 Informasi terkait kerentanan Sql Injection.....	45
Tabel 4. 6 Hasil pengumpulan informasi dari sistem XYZ	47
Tabel 4. 7 Informasi terkait kerentanan cross site scripting reflected.....	49
Tabel 4. 8 Informasi terkait kerentanan cloud meta data potentially exposed.....	51
Tabel 4. 9 Informasi terkait kerentanan Sql Injection.....	52
Tabel 4. 10 Informasi terkait kerentanan hidden file found.....	54
Tabel 4. 11 Informasi terkait kerentanan arbitrary file upload.	54
Tabel 4. 12 likelihood kerentanan sensitive information disclosure.....	63
Tabel 4. 13 Impact kerentanan sensitive information disclosure	63
Tabel 4. 14 likelihood kerentanan Hidden file found	63
Tabel 4. 15 Impact kerentanan Hidden file found.....	63
Tabel 4. 16 likelihood kerentanan Sql Injection	64
Tabel 4. 17 Impact kerentanan Sql Injection	64
Tabel 4. 18 likelihood kerentanan arbitrary file upload.....	64
Tabel 4. 19 Impact kerentanan arbitrary file upload	64
Tabel 4. 20 likelihood kerentanan cross site scripting reflected	65
Tabel 4. 21 Impact kerentanan cross site scripting reflected	65
Tabel 4. 22 likelihood kerentanan hidden file found	65
Tabel 4. 23 Impact kerentanan hidden file found	65
Tabel 4. 24 Pengukuran nilai kerentanan sistem ABC	66
Tabel 4. 25 Pengukuran kerentanan pada sistem XYZ.....	66

DAFTAR GAMBAR

Gambar 2.1 <i>Top 10 Web Application Security Risks</i> 2017 ke 2021.....	13
Gambar 3.1 Jaringan Publik/Eksternal.....	22
Gambar 3.2 Jaringan <i>Private/Internal</i>	22
Gambar 4. 1 Hasil pemindaian DNSdumpster.....	39
Gambar 4. 2 Hasil pemindaian dari whois.....	40
Gambar 4. 3 Hasil pemindaian nmap.....	40
Gambar 4. 4 Dokumentasi RESTful API.....	41
Gambar 4. 5 Data pribadi mahasiswa.....	42
Gambar 4. 6 Mengubah <i>request header</i> dan response melalui <i>burp suite</i>	43
Gambar 4. 7 Hasil pengujian metadata <i>cloud</i>	43
Gambar 4. 8 File info.php.....	45
Gambar 4. 9 Tampilan awal sebelum dimasukkan skrip.....	46
Gambar 4. 10 Urutan data menjadi berubah.....	46
Gambar 4. 11 Hasil pemindaian dnsdumpster.....	47
Gambar 4. 12 Hasil pemindaian whois.....	48
Gambar 4. 13 Hasil pemindaian nmap.....	48
Gambar 4. 14 Menambahkan skrip <code></code> pada parameter <i>draw</i> menggunakan <i>burp suite</i>	50
Gambar 4. 15 Respon yang terjadi pada kerentanan <i>XSS reflected</i>	50
Gambar 4. 16 Melakukan <i>intercept</i> menggunakan <i>burp suite</i>	51
Gambar 4. 17 Hasil pengujian metadata <i>cloud</i>	52
Gambar 4. 18 Menambahkan skrip 2-2 pada parameter <code>order[0][column]</code> menggunakan <i>burp suite</i>	53
Gambar 4. 19 Respon yang terlihat pada web.....	53
Gambar 4. 20 <i>Response body</i> dari hasil eksekusi kerentana <i>hidden file found</i>	54
Gambar 4. 21 Tampilan dari jquery.filer.....	55
Gambar 4. 22 Tampilan halaman ketika file berhasil di <i>upload</i>	55
Gambar 4. 23 Tampilan dari <i>shell backdoor</i> yang berhasil di akses.....	56

DAFTAR LAMPIRAN

Lampiran 1. Surat Izin penelitian.....	73
Lampiran 2. Hasil <i>vulnerability scanning</i> sistem ABC	73
Lampiran 3. Hasil <i>vulnerability scanning</i> sistem XYZ	75
Lampiran 4. Wawancara dengan ketua divisi infrastuktur, jaringan, dan keamanan pemilik sistem	76

