



Daftar Isi

Halaman Pengesahan	ii
Pernyataan	iii
Prakata.....	iv
Daftar Isi.....	v
Daftar Gambar.....	viii
Daftar Tabel	ix
Intisari	x
Abstract	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
BAB II TINJAUAN PUSTAKA.....	5
BAB III LANDASAN TEORI.....	10
3.1 Sistem Informasi.....	10
3.2 Keamanan Informasi	11
3.3 Prinsip dan Fundamental Keamanan Informasi	11
3.4 Ancaman dan Serangan Siber.....	13
3.4.1 Broken Access Control	14
3.4.2 Injection.....	14
3.4.3 Malware.....	15
3.5 Tindakan dan Teknologi Keamanan.....	15
3.5.1 Kontrol Akses	15
3.5.2 Autentikasi	15
3.5.3 Otorisasi	16
3.6 Uji Penetrasi	16
3.6.1 Planning	17



3.6.2	Discovery	17
3.6.3	Attacking.....	18
3.6.4	Reporting.....	18
3.7	Perangkat Lunak dan <i>Tools</i> Keamanan	18
3.7.1	Nmap.....	19
3.7.2	Wireshark	19
3.7.3	OWASP Zap & Burp Suite	19
3.8	Studi Kasus dan Contoh Dunia Nyata.....	20
BAB IV METODOLOGI PENELITIAN		21
4.1	Deskripsi Penelitian.....	21
4.2	Alat dan Bahan Penelitian	22
6.2.1	Perangkat Keras	22
6.2.2	Perangkat Lunak.....	22
4.3	Tahapan Penelitian	23
4.4	Pengumpulan dan Penelitian Data.....	24
4.3.1	Studi Pustaka.....	24
4.3.2	Studi Kasus	24
4.4	Skenario Pengujian.....	24
4.4.1	Tahap Perencanaan (Planning).....	25
4.4.2	Tahap Penemuan (Discovery).....	26
4.4.3	Tahap Penyerangan (Attacking).....	26
4.4.4	Tahap Pelaporan (Reporting)	27
BAB V IMPLEMENTASI.....		28
5.1	Implementasi Skenario Pengujian	28
5.2	Implementasi Planning	28
5.3	Implementasi Discovery.....	29
5.3.1	Ping	29
5.3.2	Whois dan Whatweb	30
5.3.3	Nmap.....	31
5.3.4	Wireshark	32



5.3.5	ZAP	33
5.3.6	Burp Suite	34
5.4	Implementasi Kode.....	35
5.4.1	Skrip Nmap	35
5.4.2	Skrip Wireshark	37
5.4.3	Skrip XSS.....	39
BAB VI HASIL PENELITIAN DAN PEMBAHASAN		42
6.1	Hasil Discovery	42
6.1.1	Ping	42
6.1.2	Whois	43
6.1.3	Whatweb	44
6.1.4	Nmap.....	44
6.1.5	Wireshark	46
6.1.6	OWASP ZAP	50
6.1.7	Burp Suite	52
6.2	Hasil Attacking.....	53
6.2.1	Server-Side Request Forgery	53
6.2.2	Cross Site Scripting.....	54
6.2.3	Insecure <i>Cookies</i>	57
6.2.4	Big Redirect Detected (Potential Sensitive Information Leak).....	58
6.2.5	Cross-Domain JavaScript Source File Inclusion.....	58
6.2.6	Server Leaks Version Information via "Server" HTTP Response Header Field	59
6.2.7	Strict-Transport-Security Header Not Set.....	59
6.2.8	Rangkuman Tingkat Kerentanan.....	59
BAB VII KESIMPULAN		62
7.1	Kesimpulan.....	62
7.2	Saran.....	62
DAFTAR PUSTAKA		62