

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR ORISINALITAS	iii
ABSTRAK	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR.....	vi
UCAPAN TERIMA KASIH	vii
DAFTAR ISI.....	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN	xv
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan dan Manfaat	3
1.4. Batasan Masalah	4
1.5. Metode Penelitian.....	4
BAB 2 TINJAUAN PUSTAKA.....	6
2.1. Tinjauan Pustaka	6
2.2. Landasan Teori	12
2.2.1. Keamanan <i>Website</i>	12
2.2.2. <i>Web Security Testing Guide (WSTG)</i>	12
2.2.3. <i>Penetration Testing</i>	12
2.2.4. <i>Open Web Security Application Project (OWASP)</i>	13
2.2.5. <i>Website</i>	13

2.2.6.	Keamanan Informasi	14
2.2.7.	Kali Linux	14
2.2.8.	<i>Cyber Attack</i>	15
2.2.9.	<i>Burp Suite</i>	15
2.2.10.	<i>Nmap</i>	15
2.2.11.	<i>SQL Injection</i>	16
2.2.12.	<i>Distributed Denial of Service</i>	16
2.2.13.	<i>Low Orbit Ion Cannon</i>	16
2.2.14.	<i>Slow Loris</i>	17
2.2.15.	<i>Nikto</i>	17
2.2.16.	<i>OWASP DirBuster</i>	18
2.2.17.	<i>OWASP ZAP</i>	18
2.2.18.	<i>Nessus</i>	18
BAB 3 METODE PENELITIAN		20
3.1.	Subjek dan Objek Penelitian	20
3.2.	Alat dan Bahan Penelitian	20
3.2.1.	Alat	20
3.2.2.	Bahan	24
3.3.	Diagram Alir Penelitian	24
3.3.1.	Identifikasi Masalah dan Studi Literatur	24
3.3.2.	<i>Information Gathering</i>	25
3.3.3.	<i>Vulnerability Analysis</i>	27
3.3.4.	<i>Exploitation</i>	28
3.3.5.	<i>Reporting</i>	30
BAB 4 HASIL & PEMBAHASAN		31

4.1. Information Gathering.....	31
4.1.1. Conduct Search Engine Discovery Reconnaissance for Information Leakage (WSTG-INFO-01)	31
4.1.2. Fingerprint Web Server (WSTG-INFO-02)	32
4.1.3. Review Webserver Metafiles for Information Leakage (WSTG-INFO-03)	34
4.1.4. Enumerate Applications on Webserver (WSTG-INFO-04).....	35
4.1.5. Review Web Page Content for Information Leakage (WSTG-INFO-05)	37
4.1.6. Identify Application Entry Points (WSTG-INFO-06).....	38
4.1.7. Map Execution Paths Through Application (WSTG-INFO-07) 40	
4.1.8. Fingerprint Web Application Framework dan Web Application (WSTG-INFO-08 & WSTG-INFO-09)	42
4.1.9. Map Application Architecture (WSTG-INFO-10)	43
4.2. Vulnerability Analysis	45
4.2.1. Analisis Temuan dari OWASP ZAP.....	45
4.2.2. Analisis Temuan dari WPScan.....	48
4.3. Exploitation	49
4.3.1. Testing for Reflected Cross Site Scripting (WSTG-INPV-01)....	50
4.3.2. Testing for Clickjacking (WSTG-CLNT-09)	51
4.3.3. Testing for SQL Injection (WSTG-INPV-05)	53
4.3.4. Distributed Denial of Service (DDoS)	54
4.3.5. Testing for Weak Lockout Mechanism (WSTG-ATHN-03)	55
4.4. Reporting	57
4.5. Evaluasi dan Tindak Lanjut oleh Mitra.....	59
BAB 5 KESIMPULAN & SARAN	62

5.1	Kesimpulan	62
5.2	Saran.....	63
DAFTAR PUSTAKA.....		65
LAMPIRAN.....		68