

DAFTAR ISI

ABSTRAK	ii
<i>ABSTRACT</i>	iii
LEMBAR PENGESAHAN	iv
LEMBAR PERNYATAAN ORISINALITAS	v
Kata Pengantar	vi
Daftar Isi.....	viii
Daftar Gambar.....	xi
Daftar Istilah.....	xii
Daftar Tabel	xiii
Daftar Lampiran	xiv
Bab I Pendahuluan	1
I.1 Latar Belakang	1
I.2 Perumusan Masalah.....	5
I.3 Tujuan Penelitian.....	5
I.4 Batasan Penelitian	5
I.5 Manfaat Penelitian.....	6
I.6 Sistematika Penulisan.....	6
Bab II Tinjauan Pustaka	8
II.1 <i>Website</i>	8
II.2 <i>Website XYZ</i>	9
II.3 NIST 800-115.....	10
II.4 VirtualBox	11
II.5 Kali Linux.....	11

II.6	Metode <i>Black Box</i>	12
II.7	<i>SQL Injection</i>	13
II.8	<i>Penetration Testing</i>	14
II.9	Nmap	15
II.10	OWASP Zed Attack Proxy (ZAP).....	15
II.11	Burp Suite	15
II.12	Foxyproxy	16
II.13	Penelitian Terdahulu	17
Bab III	Metodologi Penelitian.....	18
III.1	Pengembangan Model Konseptual	18
III.2	Sistematika Penelitian	19
III.2.1	Tahap Awal	20
III.2.2	Pengujian.....	20
III.2.3	Analisis.....	20
III.2.4	Tahap Akhir	20
Bab IV	Rancangan PENGUJIAN.....	21
IV.1	<i>Planning</i>	21
IV.1.1	Spesifikasi <i>Hardware</i>	21
IV.1.2	Spesifikasi <i>Software</i>	21
IV.2	<i>Discovery</i>	22
IV.2.1	<i>Information Gathering</i>	22
IV.2.2	<i>Vulnerability analysis</i>	23
IV.3	<i>Attack</i>	24
IV.3.1	Skenario penggunaan Burp Suite	25
IV.4	<i>Reporting</i>	25
Bab V	HASIL PENGUJIAN DAN ANALISIS	26

V.1	Analisis Terhadap Hasil <i>Scanning</i> Nmap.....	26
V.2	Analisis Terhadap Hasil Scanning OWASP ZAP.....	27
V.3	Analisis Terhadap Hasil Eksploitasi Burp Suite.....	28
V.3.1	Isi <i>Database</i>	29
V.3.2	<i>Direktori Website XYZ</i>	30
V.4	Analisis Hasil dan Rekomendasi	30
V.4.1	Menggunakan <i>Firewall</i>	33
V.4.2	Melakukan Implementasi Kueri Berparameter	33
V.4.3	Mengaitkan Daftar Validasi dengan <i>Access-Control-Allow-Origin</i> yang Mengidentifikasi <i>Domain</i> Secara Spesifik yang Dapat Mengakses Data <i>Website</i> . 33	
V.4.4	Memastikan Menggunakan <i>Library</i> Paling Akhir	33
V.4.5	Menggunakan <i>Framework</i> OWASP CSRFGuard	33
V.4.6	Melakukan <i>Setting Header</i> Menjadi <i>Settingan No-Chace</i>	34
V.4.7	Menambahkan <i>Helmet Middleware</i>	34
V.4.8	Melakukan <i>Enkripsi</i> Menggunakan MIME	34
Bab VI	KESIMPULAN DAN SARAN	35
VI.1	Kesimpulan.....	35
VI.2	Saran	36
	DAFTAR PUSTAKA	37
	Lampiran	39