

# DAFTAR ISI

<b>ABSTRAK</b> .....	ii
<b>ABSTRACT</b> .....	iii
<b>LEMBAR PENGESAHAN</b> .....	iv
<b>KATA PENGANTAR</b> .....	vi
<b>DAFTAR ISI</b> .....	viii
<b>DAFTAR GAMBAR</b> .....	xi
<b>DAFTAR TABEL</b> .....	xiii
<b>BAB I PENDAHULUAN</b> .....	1
<b>I.1 Latar Belakang</b> .....	1
<b>I.2 Rumusan Masalah</b> .....	3
<b>I.3 Tujuan dan Manfaat</b> .....	3
<b>I.4 Batasan Masalah</b> .....	3
<b>BAB II TINJAUAN PUSAKA</b> .....	5
<b>II.1 Penelitian Terdahulu</b> .....	5
<b>II.1.1 Kesimpulan Penelitian Terdahulu</b> .....	13
<b>II.2 Dasar Teori</b> .....	14
<b>II.2.1 Sistem Informasi</b> .....	14
<b>II.2.2 Profil Perusahaan</b> .....	14
<b>II.2.2 Keamanan Sistem Informasi</b> .....	15
<b>II.2.3 Open Web Application Security Project (OWASP) Top 10 2021</b> .....	15
<b>II.2.4 Cybercrime (Kejahatan Siber)</b> .....	16
<b>II.2.5 Cross Site Scripting (XSS)</b> .....	16
<b>II.2.6 SQL Injection</b> .....	17
<b>II.2.7 Penetration Testing</b> .....	17
<b>II.2.8 Zed Attack Proxy (ZAP)</b> .....	17
<b>II.2.9 WHOIS</b> .....	17
<b>II.2.10 Network Mapping (Nmap)</b> .....	18
<b>II.2.11 Name Server Lookup (Nslookup)</b> .....	18
<b>II.2.12 Burp Suite</b> .....	19
<b>II.2.13 Dirsearch</b> .....	19
<b>II.2.14 Dirb</b> .....	19

II.2.15 Xerosplit3.....	19
II.2.16 Paramspider .....	20
II.2.17 Clickjacking.....	20
II.2.18 Gobuster .....	20
II.2.19 SQL Map .....	20
II.2.20 Wappalyzer.....	20
II.2.21 Inspect Element.....	21
II.2.22 SSRF Map.....	21
II.2.23 Klasifikasi Resiko.....	21
<b>BAB III METODOLOGI PENELITIAN .....</b>	<b>23</b>
III.1 Alat dan Bahan Penelitian.....	23
III.2 Prosedur Penelitian.....	24
III.3 Jadwal Pelaksanaan.....	27
III.4 SKENARIO PENGUJIAN.....	30
III.4.1 Skenario Pengujian Tahapan Observasi.....	30
III.4.2 Skenario Pengujian Tahapan Metode OWASP Top 10 .....	33
<b>BAB IV IMPLEMENTASI DAN PENGUJIAN .....</b>	<b>45</b>
IV.1 Observasi dan Wawancara .....	45
IV.1.1 Hasil Wawancara.....	45
IV.1.2 Whois.....	47
IV.1.3 DNS Lookup .....	48
IV.1.4 ZAP.....	51
IV.1.5 Nmap.....	53
IV.2 Pengujian OWASP Top 10.....	56
IV.2.1 A01: Broken Access Control .....	57
IV.2.2 A02: Cryptographic Failures .....	61
IV.2.3 A03: Injection .....	65
IV.2.4 A04: Insecure Design .....	68
IV.2.5 A05: Security Misconfiguration.....	70
IV.2.6 A06: Vulnerable and Outdated Components .....	71
IV.2.7 A07: Identification and Authentication Failures .....	73
IV.2.8 A08: Software and Data Integrity Failures .....	77
IV.2.9 A09: Security Logging and Monitoring Failures .....	78
IV.2.10 A10: Server-Side Request Forgery (SSRF) .....	79

IV.3 Analisis.....	82
IV.4 Rekomendasi Perbaikan .....	82
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>84</b>
V.1 Kesimpulan.....	84
<b>DAFTAR PUSTAKA.....</b>	<b>86</b>
<b>LAMPIRAN.....</b>	<b>89</b>
<b>LAMPIRAN A – Perizinan .....</b>	<b>89</b>
Lampiran A.1 – Perizinan via chat whatsapp.....	89
Lampiran A.2 – Surat Pengantar Penelitian dan Pengambilan Data .....	90
Lampiran A.3 - Surat Pengantar Penelitian dan Pengambilan Data (2) .....	91
Lampiran A.4 - Surat Perizinan Penelitian.....	92
<b>LAMPIRAN B – Testing.....</b>	<b>93</b>
Lampiran B.1 – Cryptographic Failures.....	93
Lampiran B.2 – Vulnerable and Outdated Components .....	94
Lampiran B.3 – Server-Side Request Forgery (SSRF) .....	94
<b>Lampiran C – Wawancara .....</b>	<b>95</b>
Lampiran C.1 – Record wawancara dengan pihak PT. XYZ.....	95