

## DAFTAR ISI

LEMBAR PENGESAHAN .....	iii
PERNYATAAN ORISINALITAS .....	iv
KATA PENGANTAR .....	v
ABSTRAK .....	vi
<i>ABSTRACT</i> .....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xii
DAFTAR TABEL.....	xiii
BAB 1 PENDAHULUAN.....	14
1.1 Latar Belakang .....	14
1.2 Rumusan Masalah.....	16
1.3 Tujuan dan Manfaat.....	16
1.4 Batasan Masalah.....	17
BAB 2 TINJAUAN PUSTAKA .....	18
2.1 Penelitian Terdahulu .....	18
2.2 Dasar Teori.....	22
2.2.1 <i>Website</i> .....	22
2.2.2 Keamanan Sistem Informasi .....	22
2.2.3 <i>Information System Security Assesment Framework</i> .....	23
2.2.4 <i>Penetration Testing</i> .....	24
2.2.5 <i>Black Box Testing</i> .....	24
2.2.6 <i>Covert</i> .....	25
2.2.7 Kali Linux .....	25
2.2.8 <i>Wappalyzer</i> .....	25
2.2.9 <i>Nmap</i> .....	25
2.2.10 <i>Nessus</i> .....	26
2.2.11 <i>SSL Labs</i> .....	26
2.2.12 <i>Burp Suites</i> .....	26
2.2.13 <i>Hydra</i> .....	27
2.2.14 <i>Wireshark</i> .....	27
2.2.15 <i>Cookie Manager</i> .....	27
2.2.16 <i>Vulnerability Assessment</i> .....	27
2.2.17 Eksploitasi.....	28

2.2.18	<i>Brute Force Attack</i> .....	28
2.2.19	SQL Injection menggunakan <i>SQLMap</i> .....	28
2.2.20	<i>Cross-Site Scripting</i> .....	29
2.2.21	<i>Backdoor Access</i> .....	29
2.2.22	<i>Metasploit Framework</i> .....	29
2.2.23	SSL/TLS.....	29
2.2.24	<i>Domain Name Server</i> .....	30
2.2.25	<i>Cookies</i> .....	30
BAB 3	METODOLOGI.....	31
3.1	Metode Pengumpulan Data.....	31
3.2	Alat dan Bahan Penelitian.....	31
3.3	Metodologi Penelitian.....	32
3.3.1	Menentukan Topik.....	33
3.3.2	Studi Literatur.....	33
3.3.3	<i>Planning and Preparation</i> .....	33
3.3.3.1	Wawancara Persetujuan.....	33
3.3.3.2	Observasi.....	33
3.3.4	<i>Assessment</i> .....	33
3.3.4.1	Information Gathering.....	33
3.3.4.2	Network Mapping.....	34
3.3.4.3	Vulnerability Identification.....	34
3.3.4.4	Penetration Testing.....	34
3.3.4.5	Gaining Access and Previlage Escalation.....	34
3.3.4.6	Enumerating Further.....	35
3.3.4.7	Compromise Remote User/Sites.....	35
3.3.4.8	Maintaining Access.....	35
3.3.4.9	Corvering Tracks.....	35
3.3.5	<i>Reporting, Clean-up and Destroy Artefacts</i> .....	35
3.3.5.1	Analisis dan Pembahasan.....	35
3.3.5.2	Wawancara Konfirmasi.....	36
3.3.5.3	Clean-up and Destroy Artefacts.....	37
3.3.6	Kesimpulan.....	37
BAB 4	HASIL DAN PEMBAHASAN.....	38
4.1	<i>Planning and Preparation</i> .....	38

4.1.1	Wawancara Persetujuan .....	38
4.1.2	Observasi.....	38
4.2	<i>Assessment</i> .....	39
4.2.1	<i>Information Gathering</i> .....	39
4.2.1.1	Hasil Information Gathering .....	42
4.2.2	<i>Network Mapping</i> .....	42
4.2.2.1	Hasil Network Mapping.....	44
4.2.3	<i>Vulnerability identification</i> .....	45
4.2.3.1	Hasil Vulnerability Identification .....	46
4.2.4	<i>Penetration Testing</i> .....	47
4.2.4.1	Hasil Penetration Testing .....	50
4.2.5	<i>Gaining Access and Privillage Escalation</i> .....	51
4.2.5.1	Hasil Gaining Access and Privillage Escalation.....	54
4.2.6	<i>Enumerating Further</i> .....	56
4.2.6.1	Hasil Enumerating Further .....	58
4.2.7	<i>Compromise Remote User/Sites</i> .....	59
4.2.8	<i>Maintaining Access</i> .....	59
4.2.9	<i>Corvering Tracks</i> .....	59
4.3	<i>Reporting dan Clean-up and Destroy Artefacts</i> .....	59
4.3.1	Analisis dan Pembahasan.....	60
4.3.2	Wawancara Konfirmasi .....	69
4.3.3	<i>Clean-up and Destroy Artefacts</i> .....	70
4.4	<i>Kondisi Website</i> .....	71
BAB 5	KESIMPULAN DAN SARAN.....	73
5.1	Kesimpulan.....	73
5.2	Saran .....	74
	DAFTAR PUSTAKA .....	75
	LAMPIRAN.....	79
	Lampiran 1. Persetujuan dan Wawancara 1 .....	79
	Lampiran 2. Persetujuan dan Wawancara 2 .....	80
	Lampiran 3. Persetujuan dan Wawancara 3 .....	81
	Lampiran 4. Persetujuan dan Wawancara 4.....	82
	Lampiran 5. Dokumentasi Wawancara.....	83
	Lampiran 6. Pencarian <i>payload</i> XSS.....	84

Lampiran 7. Pencarian <i>shell</i> PHP .....	85
Lampiran 8. <i>Disable Function shell</i> PHP .....	86
Lampiran 9. Media Pembelajaran.....	87
Lampiran 10. Buku Laporan Rekomendasi .....	88
Lampiran 11. Dokumentasi Laporan .....	89
Lampiran 12. Lembar Pengesahan Laporan.....	90
BIODATA PENULIS .....	91

## DAFTAR GAMBAR

<b>Gambar 2.3</b> Tahapan pada framework ISSAF [11] .....	23
<b>Gambar 2.4</b> Tahapan penetration testing secara umum [1].....	24
<b>Gambar 2.5</b> Proses black box testing [6].....	24
<b>Gambar 3.1</b> Flowchart framework ISSAF .....	32
<b>Gambar 4.1</b> Situs utama pada website PPDB sekolah XYZ .....	39
<b>Gambar 4.2</b> Hasil dari wappalyzer.....	39
<b>Gambar 4.3</b> Hasil scan menggunakan ping .....	40
<b>Gambar 4.4</b> Hasil scan whois pertama.....	40
<b>Gambar 4.5</b> Hasil scan whois kedua .....	41
<b>Gambar 4.6</b> Hasil scan whois ketiga.....	41
<b>Gambar 4.7</b> Hasil scan menggunakan nmap .....	43
<b>Gambar 4.8</b> Hasil scan nmap menggunakan versi.....	43
<b>Gambar 4.9</b> Hasil scan menggunakan SSLabs.....	44
<b>Gambar 4.10</b> Hasil scan vulnerability menggunakan Basic Network Scan.....	45
<b>Gambar 4.11</b> Hasil scan vulnerability menggunakan web application test.....	45
<b>Gambar 4.12</b> Hasil percobaan sql injection pertama .....	47
<b>Gambar 4.13</b> Hasil percobaan sql injection kedua .....	48
<b>Gambar 4.14</b> Input stored XSS pada form pendaftaran .....	48
<b>Gambar 4.15</b> Hasil input stored XSS .....	49
<b>Gambar 4.16</b> Hasil upload menggunakan skrip PHP shell .....	50
<b>Gambar 4.17</b> Hasil scan brute force menggunakan metasploit .....	52
<b>Gambar 4.18</b> Hasil scan brute force menggunakan hydra .....	52
<b>Gambar 4.19</b> Hasil eskplorasi port 80.....	53
<b>Gambar 4.20</b> Halaman dashboard user .....	53
<b>Gambar 4.21</b> Hasil filterisasi oleh WAF.....	54
<b>Gambar 4.22</b> Menangkap hasil request dengan burpsuites .....	56
<b>Gambar 4.23</b> Hasil simpan cookie pada cookie manager .....	57
<b>Gambar 4.24</b> Halaman login website PPDB sekolah XYZ.....	57
<b>Gambar 4.25</b> Rekam data melalui wireshark .....	58
<b>Gambar 4.26</b> Sebelum dihapus pada folder sistem pengujian .....	70
<b>Gambar 4.27</b> Sesudah dihapus pada folder sistem pengujian.....	70

## DAFTAR TABEL

<b>Tabel 2.1</b> Penelitian terdahulu .....	18
<b>Tabel 3.1</b> Tabel alat dan bahan.....	31
<b>Tabel 3.2</b> Contoh struktur tabel analisa dan rekomendasi .....	36
<b>Tabel 4.1</b> Hasil pada tahap information gathering.....	42
<b>Tabel 4.2</b> Hasil pengujian network mapping dan SSL/TLS.....	44
<b>Tabel 4.3</b> Hasil kategori kerentanan .....	46
<b>Tabel 4.4</b> Hasil vulnerability identification.....	47
<b>Tabel 4.5</b> Hasil pengujian penetration testing .....	51
<b>Tabel 4.6</b> Hasil dari gaining access and privillage escalation.....	55
<b>Tabel 4.7</b> Hasil Enumerating further .....	58
<b>Tabel 4.8</b> Tabel Analisis dan Pembahasan.....	60
<b>Tabel 4.9</b> Rangkuman terkait kondisi website saat ini .....	71