

DAFTAR GAMBAR

Gambar 1. 1	<i>Flowchart</i> Alur Kerangka Berpikir	10
Gambar 2. 1	Halaman Utama <i>Website XYZ</i>	11
Gambar 2. 2	Halaman <i>login</i> akun dari <i>website XYZ</i>	12
Gambar 2. 3	Halaman utama dari <i>website XYZ</i>	12
Gambar 2. 4	Halaman Tambah Berita <i>website XYZ</i>	13
Gambar 2. 5	Halaman terakhir tambah berita <i>website XYZ</i>	14
Gambar 2. 6	Metode pada <i>Framework ISSAF</i>	15
Gambar 2. 7	Logo <i>Wappalyzer</i>	21
Gambar 2. 8	Logo <i>Nmap</i>	22
Gambar 2. 9	Tahapan <i>Penetration testing</i> secara umum.....	23
Gambar 2. 10	Logo Tools <i>Whois</i>	24
Gambar 2. 11	Proses <i>Vulnerability Assestment</i>	25
Gambar 2. 12	Logo Tools <i>Hydra</i>	25
Gambar 2. 13	Logo Tools <i>Burpsuite</i>	26
Gambar 2. 14	Logo Tools <i>SQLMap</i>	26
Gambar 2. 15	Logo Tools <i>Cookie Manager</i>	27
Gambar 3. 1	Metode <i>Black Box Testing</i>	39
Gambar 3. 2	Tahap 1 <i>Planning and Preparation</i>	40
Gambar 3. 3	Tahap 2 <i>Assestment</i>	41
Gambar 3. 4	Tahap 3 <i>Reporting, Clean-up and Destroy Artefacts</i>	43
Gambar 4. 1	Situs web <i>XYZ</i>	46
Gambar 4. 2	Halaman utama <i>website XYZ</i>	47
Gambar 4. 3	Hasil identifikasi menggunakan <i>tools wappalyzer</i>	47
Gambar 4. 4	Hasil <i>scan domain XYZ</i> menggunakan <i>ping</i>	48
Gambar 4. 5	Hasil <i>scan ip</i> menggunakan <i>tools whois</i>	48
Gambar 4. 6	Hasil identifikasi <i>Nslookup domain XYZ</i>	49
Gambar 4. 7	Hasil identifikasi <i>nmap website XYZ</i>	52
Gambar 4. 8	Hasil <i>scan</i> menggunakan <i>SSLabs</i>	53
Gambar 4. 9	Hasil <i>scan website XYZ</i> dengan <i>OWASP ZAP</i>	56
Gambar 4. 10	Bukti kategori <i>level Cloud Metadata Potentially Exposed</i>	58
Gambar 4. 11	Bukti kategori <i>level (CSP)Header Not Set</i>	58
Gambar 4. 12	Bukti kategori <i>level Cross-Domain Misconfiguration</i>	59

Gambar 4. 13 Bukti kategori <i>level Hidden File Found</i>	59
Gambar 4. 14 Bukti kategori <i>level Vulnerable JS Library</i>	60
Gambar 4. 15 Bukti kategori <i>level Big Redirect Detected</i>	60
Gambar 4. 16 Bukti kategori <i>level Cookie No HttpOnly Flag</i>	61
Gambar 4. 17 Bukti kategori <i>level Cookie Without Secure Flag</i>	61
Gambar 4. 18 Bukti kategori <i>level Cross-Domain JavaScript Source File Inclusion</i>	62
Gambar 4. 19 Bukti kategori <i>level Strict-Transport-Security Header Not Set</i>	62
Gambar 4. 20 Bukti kategori <i>level Timestamp Disclosure – Unix</i>	63
Gambar 4. 21 <i>X-Content-Type-Options Header Missing</i>	63
Gambar 4. 22 Hasil scan NIKTO website XYZ	64
Gambar 4. 23 Hasil scan Nuclei website XYZ	65
Gambar 5. 1 Hasil <i>Sql Injection</i> pada website XYZ	69
Gambar 5. 2 Hasil <i>Sql Injection</i> lanjutan pada website XYZ	69
Gambar 5. 3 Hasil <i>Sql Injection</i> pada fitur registrasi website XYZ	70
Gambar 5. 4 Hasil <i>Sql Injection</i> lanjutan pada fitur registrasi website XYZ	70
Gambar 5. 5 <i>Request payload XSS</i> pada Burpsuite	72
Gambar 5. 6 <i>Response payload XSS</i> pada Burpsuite	72
Gambar 5. 7 <i>Output error</i> pada Laravel	73
Gambar 5. 8 Hasil <i>request</i> pada burpsuite dalam fitur registrasi	74
Gambar 5. 9 Hasil <i>response</i> pada burpsuite dalam fitur registrasi	75
Gambar 5. 10 Hasil <i>inspect payload XSS</i>	76
Gambar 5. 11 Hasil Uji <i>Brute Force port 80 tools Metasploit</i>	78
Gambar 5. 12 Hasil Uji <i>Brute Force port 81 tools Metasploit</i>	79
Gambar 5. 13 Hasil Uji <i>Brute Force port 433 tools Metasploit</i>	79
Gambar 5. 14 Hasil Uji <i>Brute Force port 6789 tools Metasploit</i>	80
Gambar 5. 15 Hasil Uji <i>Brute Force port 8001 tools Metasploit</i>	81
Gambar 5. 16 Hasil Uji <i>Brute Force port 8080 tools Metasploit</i>	81
Gambar 5. 17 Hasil Uji <i>Brute Force port 8443 layanan tomcat tools Metasploit</i>	82
Gambar 5. 18 Hasil Uji <i>Brute Force port 8443 layanan webmin tools Metasploit</i>	82
Gambar 5. 19 Hasil Uji <i>Brute Force port 8443 layanan Jenkins tools Metasploit</i>	83
Gambar 5. 20 Hasil Uji <i>Brute Force port 10001 tools Metasploit</i>	84
Gambar 5. 21 Hasil <i>crunch gaining access</i>	84
Gambar 5. 22 Hasil penyerangan dengan <i>Hydra</i>	85
Gambar 5. 23 Hasil <i>request</i> dengan Burpsuite untuk cookie	87

Gambar 5. 24 Hasil mencari <i>Cookie</i>	87
Gambar 5. 25 Hasil <i>scan</i> data menggunakan <i>wireshark</i>	88