

## DAFTAR GAMBAR

Gambar II.1 OWASP	17
Gambar II.2 Pembaruan OWASP Top 10 2021	18
Gambar II.3 OWASP ZAP	26
Gambar II.4 Burp Suite	27
Gambar II.5 Nmap	27
Gambar II.6 Nuclei	28
Gambar II.7 Dirsearch	28
Gambar II.8 sqlmap	29
Gambar II.9 Dalfox	29
Gambar III.1 Alur Penelitian	30
Gambar IV.1 <i>Alert ZAP</i> Situs A	42
Gambar V.1 Hasil <i>tool</i> dirsearch Situs A	47
Gambar V.2 Hasil <i>Tool</i> dirsearch Situs B	48
Gambar V.3 Firewall Memblokir Situs Web B	49
Gambar V.4 Hasil <i>Tool</i> Nuclei Situs A	49
Gambar V.6 Hasil <i>Tool</i> Nuclei Situs Web B	50
Gambar V.7 Firewall Memblokir Akses Situs B	50
Gambar V.8 Kerentanan Private IP Disclosure pada situs A	51
Gambar V.9 Informasi X-Powered-By	51
Gambar V.10 Kerentanan Timestamp Disclosure – Unix Pada Situs A	52
Gambar V.11 Tidak Ada Atribut SameSite Pada Situs B	52
Gambar V.12 Parameter ‘X-Xsrf-Token’	53
Gambar V.13 <i>Respon Payload</i>	53
Gambar V.14 Source Code Respons Kerentanan <i>Information Disclosure - Sensitive Information in URL</i> Pada Situs A	54
Gambar V.15 Source Code Respons Kerentanan <i>Information Disclosure - Sensitive Information in URL</i> Pada Situs B	55
Gambar V.16 <i>Source Code Respons</i> Kerentanan <i>Information Disclosure - Sensitive Information in URL</i>	55
Gambar V.17 Proses penyerangan IDOR menggunakan Burp Suite	56
Gambar V.18 Data Diri Korban Tidak Berubah	56

Gambar V.19 Pemindaian Dalfox pada situs A	57
Gambar V.20 Pemindaian Dalfox pada situs B	58
Gambar V.21 Hasil Serangan XSS Injection Dengan Burp Suite Pada Situs A	58
Gambar V.22 Hasil Serangan XSS Injection Dengan Burp Suite Pada Situs B	59
Gambar V.23 Mengubah Jenis File Pada Permintaan	60
Gambar V.24 Pesan <i>Error</i>	60
Gambar V.25 Mengisi Skrip	61
Gambar V.26 XSS Berhasil	62
Gambar V.27 Hasil Pencarian <i>error</i>	62
Gambar V.28 Serangan <i>SQL Injection</i> menggunakan SQLMap	63
Gambar V.29 Serangan SQLMap gagal	63
Gambar V.30 Hasil Serangan <i>SQL Injection Tool</i> Burp Suite	64
Gambar V.31 Hasil Serangan <i>Bypass</i> Login	64
Gambar V.32 Halaman Error	65
Gambar V.33 Mengatur <i>Payload</i>	66
Gambar V.34 Permintaan <i>Reset password</i> Masuk di Email	66
Gambar V.35 <i>Source Code Respons</i> Kerentanan <i>Big Redirect Detected (Potential Sensitive Information Leak)</i>	67
Gambar V.36 File <i>.htaccess</i>	68
Gambar V.37 File <i>composer.lock</i>	68
Gambar V.38 Akses Metadata Gagal	69
Gambar V.39 Curl Tidak Menampilkan <i>Header</i> CSP pada situs A dan B	69
Gambar V.40 Hasil <i>Response Code</i>	70
Gambar V.41 Curl Tidak Menampilkan <i>Header</i> X-Frame-Options Pada Situs A dan B	70
Gambar V.42 <i>Clickjacking</i> Berhasil	71
Gambar V.43 Cookie XSRF-Token Tidak Ada Atribut <i>HttpOnly</i> Pada Situs B	72
Gambar V.44 Serangan Terdeteksi WAF Pada Situs B	72
Gambar V.45 Informasi Server Terlihat Pada <i>Header</i>	73
Gambar V.46 Tidak Ditemukan <i>Header</i> X-Content-Type-Options	74
Gambar V.47 Parameter Login	75
Gambar V.48 <i>Attack Log</i> Fortiweb	77

