

DAFTAR GAMBAR

Gambar 2.1 Top 10 kerentanan menurut OWASP.	18
Gambar 3.1 Diagram alir penelitian.	23
Gambar 4.1 Analisis <i>header</i> HTTP menggunakan WhatWeb.....	28
Gambar 4.2 Pemindaian menggunakan Nmap.	29
Gambar 4.3 Proses pemindaian direktori.....	31
Gambar 4.4 Percobaan intersepsi menggunakan Burpsuite.....	32
Gambar 4.5 Hasil <i>request proxy</i> menggunakan Burpsuite.	33
Gambar 4.6 Hasil percobaan <i>cryptographic failures</i> dengan Burpsuite.....	34
Gambar 4.7 Hasil serangan Blind SQL.	36
Gambar 4.8 Deteksi konfigurasi <i>header</i> tidak aman menggunakan Nuclei. 37	
Gambar 4.9 Hasil pengujian <i>vulnerable</i> menggunakan OWASP ZAP.	38
Gambar 4.10 Daftar <i>library</i> PHP.....	39
Gambar 4.11 Percobaan <i>login</i> menggunakan <i>browser</i> melalui Intercept.	40
Gambar 4.12 Hasil respon yang dikirim server.	40
Gambar 4.13 Konfigurasi Nuclei menggunakan VSCode	42
Gambar 4.14 Hasil <i>request proxy</i> menggunakan Burpsuite.	33
Gambar 4.15 Hasil percobaan <i>cryptographic failures</i> dengan Burpsuite.....	34
Gambar 4.16 Hasil serangan Blind SQL.	36
Gambar 4.17 Deteksi konfigurasi <i>header</i> tidak aman menggunakan Nuclei.	37

Gambar 4.18 Hasil pengujian <i>vulnerable</i> menggunakan OWASP ZAP.	38
Gambar 4.20 Percobaan <i>login</i> menggunakan <i>browser</i> melalui Intercept.	40
Gambar 4.21 Hasil respon yang dikirim server.	40
Gambar 4.23 Konfigurasi Nuclei menggunakan VSCode	42