

DAFTAR GAMBAR

Gambar 2. 1. Alur Kerja Vulnerability Assessment	8
Gambar 2. 2. Diagram Arsitektur OWASP ZAP.....	14
Gambar 2. 3. Diagram Arsitektur Nikto	18
Gambar 3. 1. Alur Kerja Vulnerability Assessment.....	19
Gambar 4. 1. Passive Scanning OWASP ZAP.....	25
Gambar 4. 2. Active Scanning OWASP ZAP	26
Gambar 4. 3. Spider OWASP ZAP	27
Gambar 4. 4. Eksekusi Pemindaian Keamanan Server dengan Nikto CLI.....	28
Gambar 4. 5. Halaman Asli	31
Gambar 4. 6. Bukti Simulasi Eksploitasi Berhasil	32
Gambar 4. 7. Tampilan Halaman Palsu	32
Gambar 4. 8. Kredensial Bocor Pada tab HTTP History	33
Gambar 4. 9. Hasil Eksekusi PoC Prototype Pollution pada Lodash $\leq 4.17.20$	33
Gambar 4. 10. Penyisipan Payload Inline JavaScript pada Halaman utama XYZ ..	34
Gambar 4. 11. Tampilan Panel Query Strings pada Webhook.site yang Menunjukkan Nilai Kosong	35
Gambar 4. 12. Tampilan Respons Menunjukkan header Set-Cookie	35
Gambar 4. 13. Penyisipan payload JavaScript.....	36
Gambar 4. 14. Bukti Penerimaan Cookie XSRF-TOKEN pada webhook.site melalui Query String.....	36
Gambar 4. 15. Modifikasi Request HTTP di Burp Suite.....	37
Gambar 4. 16. Clickjacking Tester	38
Gambar 4. 17. Permintaan Pre-flight OPTIONS dengan Origin Domain Asing dan Respon Server.....	38
Gambar 4. 18. Tidak Terdapat X-Content-Type-Options Pada Respons.....	39
Gambar 4. 19. Penyisipan Elemen Gambar Pada Bagian Respons HTTP	40
Gambar 4. 20. Tampilan Halaman Yang Sudah Disisipkan Gambar	41
Gambar 4. 21. Bukti Tidak Terdapat Timestamp	42
Gambar 4. 22. Tab Intruder Burp Suite.....	42
Gambar 4. 23. Mengisi Payload	44
Gambar 4. 24. Hasil Pengujian Intruder Burp Suite pada Apache 2.4.41	44
Gambar 4. 25. Respons Server Domain Utama XYZ.....	45
Gambar 4. 26. Perintah Curl Untuk Simulasi Kerentanan X-Powered-By: Next.js.	45

Gambar 4. 27. Pengujian Header X-Nextjs-Cache pada Berbagai Endpoint Menggunakan Perintah Curl	46
Gambar 4. 28. Penyisipan Skrip pada Respons.....	47
Gambar 4. 29. Muncul Permintaan Geolokasi pada Halaman Utama	47
Gambar 4. 30. Tampilan Query String pada Webhook.site	48
Gambar 4. 31. Mengedit Request	48
Gambar 4. 32. Tampilan Respons	49