

DAFTAR GAMBAR

Gambar II.1 Perubahan OWASP Top 10 2021	18
Gambar II.2 Logo OWASP ZAP	20
Gambar II.3 Tampilan Burp Site.....	21
Gambar II.4 Logo Dirsearch	21
Gambar II.5 Logo Curl.....	22
Gambar II.6 Logo ParamSpider	22
Gambar II.7 Logo SQLMap.....	23
Gambar II.8 Tampilan Burp Clickbandit	23
Gambar III.1 Alur Penelitian	24
Gambar IV.1 Website <i>PT XYZ</i>	36
Gambar IV.2 Website Untuk Editor.....	37
Gambar IV.3 Website Untuk Jurnalis	37
Gambar IV.4 Hasil NMap	40
Gambar IV.5 Hasil Whois Lookup	42
Gambar IV.6 Hasil OWASP ZAP	44
Gambar V.1 PII Disclosure	46
Gambar V.2 Hasil Dirsearch	47
Gambar V.3 Secure Pages Include Mixed Content	48
Gambar V.4 STS Header Not Set.....	49
Gambar V.5 Hasil SSL Scan 1	50
Gambar V.6 Hasil SSL Scan 2	51
Gambar V.7 Hasil Curl.....	51
Gambar V.8 User Controllable HTML Element Attribute.....	52
Gambar V.9 Injeksi XSS Menggunakan Burp Suite Intruder pada Website Situs XYZ	53
Gambar V.10 Injeksi XSS Menggunakan Burp Suite Intruder pada Website XYZ Editor.....	53
Gambar V.11 Render response dari XYZ Editor	54
Gambar V.12 Injeksi XSS Menggunakan Burp Suite Intruder pada Website XYZ Jurnalis	54
Gambar V.13 Hasil Paramspider	55

Gambar V.14 Txt Url Hasil Paramspider	56
Gambar V.15 Hasil Paramspider Pada Subdomain XYZ Jurnal, Editor	57
Gambar V.16 Hasil SQLMap 1	58
Gambar V.17 Hasil SQLMap 2	59
Gambar V.18 Hasil 1 SQLMap pada XYZ Jurnal	59
Gambar V.19 Hasil 2 SQLMap pada XYZ Jurnal	60
Gambar V.20 Hasil 1 SQLMap pada XYZ Editor	60
Gambar V.21 Hasil 2 SQLMap pada XYZ Editor	60
Gambar V.22 Hasil <i>SQL Injection</i> pada <i>Situs XYZ</i>	61
Gambar V.23 Hasil <i>SQL Injection</i> pada XYZ Editor	62
Gambar V.24 Hasil <i>SQL Injection</i> pada XYZ Jurnal	62
Gambar V.25 Login Manual.....	63
Gambar V.26 CSP: Failure to Define Directive with No Fallback	63
Gambar V.27 CSP: <i>Wildcard Directive</i>	64
Gambar V.28 CSP: Header Not Set	65
Gambar V.29 Missing Anti-clickjacking Header	66
Gambar V.30 X-Content-Type-Options Header Missing.....	67
Gambar V.31 Clickjacking pada website Situs XYZ	68
Gambar V.32 Clickjacking pada website XYZ Editor	68
Gambar V.33 Clickjacking pada website XYZ Jurnal.....	68
Gambar V.34 Hasil Nuclei	69
Gambar V.35 Vulnerable JS Library	70
Gambar V.36 Hasil Wappalyzer.....	71
Gambar V.37 Hasil Wappalyzer XYZ Jurnal	71
Gambar V.38 Hasil Wappalyzer XYZ Editor	72
Gambar V.39 Uji Coba Manual Pada Website XYZ Editor.....	72
Gambar V.40 Hasil Bruteforce Menggunakan Burp Suite.....	73
Gambar V.41 Cross-Domain JavaScript Source File Inclusion	74
Gambar V.42 Hasil Curl pada adsbygoogle.js	74
Gambar V.43 Penerimaan Respon saat Bruteforcing.....	75
Gambar V.44 Format Raw Http Request Situs XYZ	75
Gambar V.45 Format Raw Http Request XYZ Editor	76