DAFTAR TABEL

Tabel II.1 Penelitian Terdahulu..... 5
Tabel II.2 Penelitian Terdahulu..... 6
Tabel II.3 Penelitian Terdahulu..... 6
Tabel II.4 Penelitian Terdahulu..... 7
Tabel II.5 Penelitian Terdahulu..... 8
Tabel II.6 Penelitian Terdahulu..... 8
Tabel II.7 Penelitian Terdahulu..... 9
Tabel II.8 Penelitian Terdahulu..... 10
Tabel II.9 Penelitian Terdahulu..... 10
Tabel II.10 Penelitian Terdahulu..... 11
Tabel II.11 Perbandingan *Framework* 16
Tabel III.1 *Software* yang digunakan. 28
Tabel III.2 *Hardware* yang digunakan. 28
Tabel III.3 Skenario Pengujian *Broken Access Control*..... 32
Tabel III.4 Skenario Pengujian *Cryptographic Failures* 32
Tabel III.5 Skenario Pengujian *Injection* 33
Tabel III.6 Skenario Pengujian *Insecure design* 34
Tabel III.7 Skenario Pengujian *Security misconfiguration*..... 34
Tabel III.8 Skenario Pengujian *Vulnerable and Outdated Components*..... 35
Tabel III.9 Skenario Pengujian Identification and Authentication Failures 35
Tabel III.10 Skenario Pengujian *Software and Data Integrity Failures*..... 35
Tabel III.11 Skenario Pengujian *Security Logging and Monitoring Failures* 36
Tabel III.12 Skenario Pengujian *Server-Side Request Forgery*..... 36
Tabel IV.1 Hasil Wawancara..... 39
Tabel IV.2 Hasil Whois..... 41
Tabel IV.3 Hasil Nslookup 43
Tabel IV.4 Hasil Nmap 46
Tabel IV.5 Hasil Wappalyzer..... 47
Tabel IV.6 Hasil OWASP ZAP 49
Tabel V.1 Temuan WPScan..... 88
Tabel V.2 Tabel kerentanan hasil Wappalyzer 90

Tabel V.3 Analisis Hasil A01 101
Tabel V.4 Analisis Hasil A02 102
Tabel V.5 Analisis Hasil A03 103
Tabel V.6 Analisis Hasil A04 104
Tabel V.7 Analisis Hasil A05 105
Tabel V.8 Analisis Hasil A06 106
Tabel V.9 Analisis Hasil A07 108
Tabel V.10 Analisis Hasil A08 108
Tabel V.11 Analisis Hasil A09 109
Tabel V.12 Analisis Hasil A10 110
Tabel V.13 *Reporting* 112