DAFTAR ISI

ABSTRAK iv
ABSTRACT v
Kata Pengantar vi
Daftar Isi vii
Daftar Gambar xi
Daftar Tabel xiv
Bab I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Perumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Batasan Penelitian 3
1.5 Metodologi Penelitian 3
Bab II TINJAUAN PUSTAKA 5
2.1 Penelitian Terdahulu 5
2.2 Dasar Teori 15
2.2.1 Sistem Informasi 15
2.2.2 Keamanan Sistem Informasi 15
2.2.3 *Penetration Testing* 15
2.2.4 VAPT *(Vulnerability Assessment & Penetration Testing)* 16
2.3 OWASP 17
2.3.1 OWASP Top 10 2021 18
2.4 Tools 26
2.4.1 OWASP ZAP (Zed Attack Proxy) 26
2.4.2 Burp Suite 27
2.4.3 Nmap 27
2.4.4 Nuclei 28

2.4.5 Dirsearch 28
2.4.6 sqlmap 29
2.4.7 Dalfox 29
Bab III Metodologi Penelitian 30
3.1 Alur Penelitian 30
3.2 Alat dan Bahan Penelitian 31
3.2.1 *Software* 31
3.2.2 *Hardware* 32
3.3 Prosedur Penelitian 32
3.3.1 Studi Literatur 33
3.3.2 *Planning* 33
3.3.3 *Information Gathering* 33
3.3.4 *Vulnerability Scanning* 33
3.3.5 *Attacking* 33
3.3.6 Validasi 34
3.3.7 Analisa Hasil 34
3.3.8 *Reporting* 35
3.4 Jadwal 35
Bab IV PENGUMPULAN DAN PENGOLAHAN DATA 38
4.1 Planning 38
4.2 Information Gathering 38
4.2.1 Wappalyzer 38
4.2.2 *Nettwork Mapping* 40
4.3 Vulnerability Scanning 42
Bab V ANALISA DAN PEMBAHASAN 47
5.1 Attacking 47
5.1.1 A01:2021 - Broken Access Control 47

5.1.2 A02:2021 - Cryptographic Failures 56
5.1.3 A03:2021 – Injection..... 57
5.1.4 A04:2021 - *Insecure Design* 65
5.1.5 A05:2021 - *Security Misconfiguration*..... 67
5.1.6 A06:2021 - *Vulnerable and Outdated Components*..... 74
5.1.7 A07:2021 - *Identification and Authentication Failures*..... 75
5.1.8 A08:2021 - *Software and Data Integrity Failures*..... 76
5.1.9 A09:2021 - *Security Logging and Monitoring Failures* 76
5.1.10 A10:2021 - *Server-Side Request Forgery* 77
5.2 Validasi..... 78
5.3 Analisa Hasil 78
5.3.1 *Private IP Disclosure*..... 78
5.3.2 *Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)*..... 78
5.3.3 *Cookie without SameSite Attribute* 78
5.3.4 XSS *Injection* 79
5.3.5 *Generation of Error Message Containing Sensitive Information* . 79
5.3.6 *No Rate Limit on Reset Password*..... 79
5.3.7 *.htaccess Information Leak* 80
5.3.8 *Hidden File Found* 80
5.3.9 *Content Security Policy (CSP) Header Not Set* 80
5.3.10 *Missing Anti-clickjacking Header*..... 80
5.3.11 *Cookie No HttpOnly Flag* 81
5.3.12 *Cookie Without Secure Flag* 81
5.3.13 *Server Leaks Version Information via "Server" HTTP Response Header Field*..... 81

5.3.14 X-*Content-Type-Options Header Missing* 82
5.3.15 Script Served From Malicious Domain (polyfill) 82
5.3.16 Vulnerable JS Library 82
5.4 Reporting 83
Bab VI Kesimpulan dan Saran 93
6.1 Kesimpulan 93
6.2 Saran 94
Daftar Pustaka 95