

DAFTAR ISI

| | |
|--|------------|
| LEMBAR PENGESAHAN | i |
| LEMBAR PERNYATAAN ORISINALITAS | iii |
| ABSTRAK | iv |
| ABSTRACT | v |
| KATA PENGANTAR | vi |
| DAFTAR ISI | vii |
| DAFTAR TABEL | xi |
| DAFTAR GAMBAR | xii |
| DAFTAR LAMPIRAN | xiv |
| BAB I | 1 |
| PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Tujuan Penelitian..... | 3 |
| 1.4 Batasan dan Asumsi Penelitian | 3 |
| 1.5 Manfaat Penelitian..... | 4 |
| 1.6 Sistematika Penulisan..... | 4 |
| BAB II | 5 |
| LANDASAN TEORI | 5 |
| 2.1 Penelitian Terdahulu..... | 5 |
| 2.2 Dasar Teori | 12 |
| 2.2.1 Sistem Informasi | 12 |
| 2.2.2 Keamanan Sistem Informasi | 12 |
| 2.2.3 <i>Penetration Testing</i> | 13 |
| 2.2.4 OWASP (<i>Open Web Application Security Project</i>)..... | 13 |
| 2.2.5 Perbandingan <i>Framework</i> | 13 |
| 2.2.6 OWASP Top 10 2021 | 14 |
| 2.2.7 Analisis Tingkat Kerentanan Menggunakan CVSS 3.1 | 18 |
| 2.2.8 VirtualBox..... | 19 |
| 2.2.9 Kali Linux | 19 |

| | | |
|------------------------------------|---|-----------|
| 2.2.10 | Burp Suite | 20 |
| 2.2.11 | OWASP ZAP | 21 |
| 2.2.12 | Nmap | 22 |
| 2.2.13 | Sqlmap | 23 |
| 2.2.14 | <i>Secure Socket Layer</i> | 24 |
| 2.2.15 | Nuclei | 24 |
| 2.2.16 | <i>Waplyzer</i> | 25 |
| 2.2.17 | <i>Domain Information Groper</i> | 25 |
| 2.2.18 | Nslookup | 26 |
| 2.3 | Alasan Pemilihan Teori / Model / Kerangka Kerja | 26 |
| BAB III..... | | 27 |
| METODOLOGI PENELITIAN | | 27 |
| 3.1 | Sistematika Penyelesaian Masalah | 27 |
| 3.1.1. | Studi Literatur | 27 |
| 3.1.2. | Planning | 28 |
| 3.1.3. | Information Gathering | 28 |
| 3.1.4. | Vulnerability Scanning | 28 |
| 3.1.5. | Attacking..... | 28 |
| 3.1.6. | OWASP Top 10 2021 | 29 |
| 3.1.7. | Analisis Hasil | 29 |
| 3.1.7.1. | Jika Tidak Ditemukan | 29 |
| 3.1.7.2. | Jika Ditemukan..... | 29 |
| 3.1.8. | Validasi | 29 |
| 3.1.9. | Skenario Pengujian | 30 |
| 3.1.9.1. | Broken Access Control | 30 |
| 3.1.9.2. | <i>Cryptographic Failures</i> | 30 |
| 3.1.9.3. | <i>Injection</i> | 31 |
| 3.1.9.4. | <i>Insecure Design</i> | 31 |
| 3.1.9.5. | <i>Security Misconfiguration</i> | 31 |
| 3.1.9.6. | <i>Vulnerable and Outdated Components</i> | 32 |
| 3.1.9.7. | <i>Identification and Authentication Failures</i> | 32 |
| 3.1.9.8. | <i>Software and Data Integrity Failures</i> | 33 |

| | | |
|-----------------------------------|--|------------|
| 3.1.9.9. | <i>Security Logging and Monitoring Failures</i> | 33 |
| 3.1.9.10. | <i>Server Side Request Forgery (SSRF)</i> | 34 |
| 3.1.10. | <i>Reporting</i> | 34 |
| 3.1.11. | Sistematika Penyelesaian Masalah | 34 |
| BAB IV | | 36 |
| ANALISIS DAN PERANCANGAN | | 36 |
| 4.1 | Planning..... | 36 |
| 4.2 | Wawancara | 36 |
| 4.3 | <i>Information Gathering</i> | 38 |
| 4.3.1 | Wappalyzer | 38 |
| 4.3.2 | Network Mapping | 39 |
| 4.3.3 | Nslookup | 40 |
| 4.3.4 | Domain Information Groper | 41 |
| 4.4 | Vulnerability Scanning..... | 42 |
| BAB V | | 45 |
| IMPLEMENTASI DAN PENGUJIAN | | 45 |
| 5.1 | <i>Penetration Testing</i> | 45 |
| 5.1.1 | A01 : Broken Acces Control | 45 |
| 5.1.2 | A02 : Cryptographic Failures..... | 51 |
| 5.1.3 | A03 : Injection..... | 57 |
| 5.1.4 | A04 : Insecure Design..... | 60 |
| 5.1.5 | A05 : Security Misconfiguration..... | 62 |
| 5.1.6 | A06 : Vulnerable and Outdated Components | 69 |
| 5.1.7 | A07 : Identification and Authentecation Failures | 73 |
| 5.1.8 | A08 : Software and Data Integrity Failures | 77 |
| 5.1.9 | A09 : Security Logging and Monitoring Failures | 78 |
| 5.1.10 | A10 : Server-Side Request Forgery (SSRF) | 79 |
| 5.1.11 | Analisis Hasil | 82 |
| 5.2 | Validasi..... | 93 |
| 5.3 | <i>Reporting</i> | 94 |
| BAB VI | | 103 |
| KESIMPULAN DAN SARAN | | 103 |
| 6.1 | Kesimpulan..... | 103 |

| | | |
|-----|-----------------------------|------------|
| 6.2 | Saran..... | 103 |
| | DAFTAR PUSTAKA | 104 |
| | LAMPIRAN..... | 108 |