

DAFTAR ISI

| | |
|---|------------|
| LEMBAR PENGESAHAN | ii |
| LEMBAR PERNYATAAN ORISINALITAS | iii |
| ABSTRAK | iv |
| ABSTRACT | v |
| KATA PENGANTAR..... | vi |
| DAFTAR ISI..... | vii |
| DAFTAR TABEL | x |
| DAFTAR GAMBAR..... | xii |
| DAFTAR LAMPIRAN | xiv |
| BAB I 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..... | 3 |
| 1.6. Sistematika Penelitian | 4 |
| BAB II LANDASAN TEORI | 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. Black Box Testing..... | 16 |
| 2.2.5. Confusion Matrix | 16 |
| 2.2.6. OWASP..... | 17 |
| BAB III METODOLOGI PENELITIAN | 24 |
| 3.1. Sistematika Penyelesaian Masalah..... | 24 |
| 3.2. Alur Penelitian..... | 24 |
| 3.3. Alat dan Bahan | 25 |

| | | |
|--|--|-----------|
| 2.2.7. | 3.3.1. Software | 25 |
| 2.2.8. | 3.3.2. Hardware..... | 25 |
| 3.4. | Prosedur Penelitian..... | 26 |
| 3.5. | Skenario Pengujian..... | 29 |
| BAB IV ANALISIS DAN PERANCANGAN | | 36 |
| 4.1. | Perencanaan..... | 36 |
| 2.2.9. | 4.1.1 Wawancara | 37 |
| 4.2. | Pengumpulan Informasi | 39 |
| 4.2.1. | Wappalyzerr | 39 |
| 4.2.2. | Nmap | 40 |
| 4.2.3. | Whois | 41 |
| 4.2.4. | OWASP ZAP | 44 |
| BAB V IMPLEMENTASI DAN PENGUJIAN..... | | 46 |
| 5.1. | <i>Penetration Testing</i> | 46 |
| 5.1.1. | A01:2021 – Broken Access Control..... | 46 |
| 5.1.2. | A02:2021 – Cryptographic Failures..... | 48 |
| 5.1.3. | A03:2021 – Injection..... | 52 |
| 5.1.4. | A04:2021 – Insecure Design | 62 |
| 5.1.5. | A05:2021 – Security Misconfiguration..... | 63 |
| 5.1.6. | A06:2021 – Vulnerable and Outdated Component..... | 70 |
| 5.1.7. | A07:2021 – Identification and Authentication Failures..... | 72 |
| 5.1.8. | A08:2021 – Software and Data Integrity Failures | 74 |
| 5.1.9. | A09:2021 – Security Logging and Monitoring..... | 75 |
| 5.1.10. | A10:2021 – Server-Side Request Forgery..... | 75 |
| 5.2. | Analisis Hasil | 77 |
| 5.2.1. | Hasil Temuan A01:2021 – Broken Access Control | 77 |
| 5.2.2. | Hasil Temuan A02:2021 – Cryptographic Failures | 78 |
| 5.2.3. | Hasil Temuan A03:2021 – Injection | 79 |
| 5.2.4. | Hasil Temuan A04:2021 – Insecure Design | 81 |
| 5.2.5. | Hasil Temuan A05:2021 – Security Misconfiguration..... | 81 |
| 5.2.6. | Hasil Temuan A06:2021 – Vulnerable and Outdated Component . | 83 |
| 5.2.7. | Hasil Temuan A07:2021 – Identification and Authentication Failures | 83 |

| | | |
|--|---|-----------|
| 5.2.8. | Hasil Temuan A08:2021 – Software and Data Integrity Failures... | 84 |
| 5.2.9. | Hasil Temuan A09:2021 – Security Logging and Monitoring | 85 |
| 5.2.10. | Hasil Temuan A10:2021 – Server-Side Request Forgery | 86 |
| 5.3. | Validasi..... | 86 |
| 5.4. | Pelaporan | 87 |
| BAB VI KESIMPULAN DAN SARAN | | 90 |
| 6.1. | Kesimpulan..... | 90 |
| 6.2. | Saran | 91 |
| DAFTAR PUSTAKA | | 92 |
| LAMPIRAN | | 94 |
| Lampiran Surat Pengantar dan Pengambilan Data..... | 94 | |
| Lampiran Telah Melakukan Wawancara..... | 95 | |
| Lampiran Kerahasiaan Pengujian Bertanda Tangan | 96 | |
| Lampiran Profil Validator | 97 | |
| Lampiran Sertifikat CEH Validator | 99 | |
| Lampiran Surat Pernyataan Rahasia Validator | 100 | |
| Lampiran Lembar Validator | 101 | |
| Lampiran Buku Reporting..... | 103 | |
| Lampiran Dokumentasi Penyerahan Buku | 104 | |
| Lampiran Konfirmasi Reporting | 105 | |