

DAFTAR ISI

| | Halaman |
|--|---------|
| HALAMAN PERNYATAAN KEASLIAN | ii |
| HALAMAN PENGESAHAN SEMINAR PROPOSAL | iii |
| HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH | iv |
| KATA PENGANTAR | vi |
| ABSTRAK | viii |
| DAFTAR ISI | x |
| DAFTAR TABEL | xiii |
| DAFTAR GAMBAR | xiv |
| DAFTAR SIMBOL | xv |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 4 |
| 1.3 Tujuan Tugas Akhir | 4 |
| 1.4 Manfaat Tugas Akhir | 4 |
| 1.5 Lingkup Tugas Akhir | 5 |
| 1.6 Kerangka Berpikir | 5 |
| 1.7 Sistematika Penulisan Tugas Akhir | 6 |
| BAB 2 TINJAUAN PUSTAKA | 8 |
| 2.1 Studi Literatur Jurnal | 8 |
| 2.2 Teori Umum | 10 |
| 2.2.1 Keamanan Informasi | 10 |
| 2.2.2 Pengertian Aplikasi | 11 |
| 2.2.3 Perpustakaan Digital | 11 |
| 2.2.4 <i>Penetration Testing</i> | 11 |
| 2.2.5 NIST 800-115 <i>Framework</i> | 12 |
| 2.2.5.1 <i>Planning</i> | 12 |
| 2.2.5.2 <i>Discovery</i> | 13 |
| 2.2.5.3 <i>Attack</i> | 13 |
| 2.2.5.4 <i>Reporting</i> | 13 |
| 2.2.6 OWASP Top 10 2021 | 13 |
| 2.2.6.1 A01:2021- <i>Broken Access Control</i> | 14 |

| | | |
|--------------|---|-----------|
| 2.2.6.2 | A02:2021- <i>Cryptographic Failures</i> | 14 |
| 2.2.6.3 | A03:2021- <i>Injection</i> | 15 |
| 2.2.6.4 | A04:2021- <i>Insecure Design</i> | 16 |
| 2.2.6.5 | A05:2021- <i>Security Misconfiguration</i> | 16 |
| 2.2.6.6 | A06:2021- <i>Vulnerable and Outdated Components</i> | 17 |
| 2.2.6.7 | A07:2021- <i>Identification and Authentication Failures</i> | 18 |
| 2.2.6.8 | A08:2021- <i>Software and Data Integrity Failures</i> | 18 |
| 2.2.6.9 | A09:2021- <i>Security Logging and Monitoring Failures</i> | 19 |
| 2.2.6.10 | A10:2021- <i>Server-Side Request Forgery</i> | 20 |
| 2.3 | Teori Pendukung | 21 |
| 2.3.1 | Kali Linux | 21 |
| 2.3.1.1 | OWASP ZAP | 21 |
| 2.3.1.2 | Burp Suite | 21 |
| 2.3.1.3 | Nmap..... | 21 |
| 2.3.1.4 | Zenmap | 22 |
| 2.3.2 | OWASP Risk Rating Methodology | 22 |
| 2.3.3 | VirusTotal.com..... | 23 |
| 2.3.4 | Pentest-Tools..... | 23 |
| 2.3.5 | Flowchart | 23 |
| BAB 3 | METODOLOGI PENELITIAN | 25 |
| 3.1 | Jadwal Penelitian | 25 |
| 3.2 | Waktu dan Tempat Penelitian | 25 |
| 3.2.1 | Waktu Penelitian | 25 |
| 3.2.2 | Tempat Penelitian..... | 25 |
| 3.3 | Objek Penelitian | 25 |
| 3.3.1 | Profil Perpustakaan Universitas Esa Unggul..... | 25 |
| 3.3.2 | Visi dan Misi Organisasi | 26 |
| 3.3.3 | Struktur Organisasi..... | 27 |
| 3.4 | Teknik Pengumpulan Data | 27 |
| 3.4.1 | Observasi..... | 27 |
| 3.4.2 | Wawancara | 28 |
| 3.4.3 | Survei | 28 |
| 3.5 | Tahapan Penelitian | 29 |
| 3.5.1 | Planning | 29 |
| 3.5.2 | Discovery..... | 29 |
| 3.5.3 | Attack..... | 29 |

| | | |
|--|--|-----------|
| 3.5.4 | <i>Reporting</i> | 29 |
| BAB 4 HASIL DAN PEMBAHASAN | | 30 |
| 4.1 | <i>Planning</i> | 30 |
| 4.2 | <i>Discovery</i> | 31 |
| 4.3 | Mendeteksi Serangan (<i>Attack</i>)..... | 39 |
| 4.3.1 | Hasil <i>Clickjacking</i> – High | 40 |
| 4.3.2 | Hasil Cross-Site Scripting (XSS) – High | 41 |
| 4.3.3 | Hasil Brute Force – Medium | 43 |
| 4.3.4 | Hasil Session Hijacking – High..... | 44 |
| 4.3.5 | Hasil Cross-Site Request Forgery (CSRF) – High | 46 |
| 4.4 | <i>Reporting</i> | 47 |
| 4.5 | Rekomendasi Perbaikan Kerentanan..... | 57 |
| 4.6 | Perbandingan Penelitian | 64 |
| BAB 5 KESIMPULAN DAN SARAN | | 65 |
| 5.1 | Kesimpulan..... | 65 |
| 5.2 | Saran..... | 66 |
| DAFTAR REFERENSI | | 68 |
| Lampiran 1 DAFTAR RIWAYAT HIDUP | | 72 |
| Lampiran 2 SURAT PERMOHONAN IZIN PENELITIAN | | 73 |
| Lampiran 3 SURAT PEMBERIAN IZIN PENELITIAN..... | | 74 |
| Lampiran 4 HASIL WAWANCARA | | 75 |
| Lampiran 5 HASIL AUTOMATED SCANNING OWASP ZAP..... | | 79 |