

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR ORISINALITAS	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
UCAPAN TERIMA KASIH	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
BAB 1 PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan dan Manfaat	3
1.4. Batasan Masalah	4
1.5. Jadwal Pelaksanaan	4
BAB 2 TINJAUAN PUSTAKA	6
2.1. OWASP	6
2.2. Urgensi Keamanan	7
2.3. SEEDS	10
2.4. <i>Literature Review</i>	10
BAB 3 METODE PENELITIAN	12
3.1. Analisis Kebutuhan	12
3.2. Perencanaan Pengujian	13
3.3. Pembuatan Skenario Uji	14
3.3.1. Pengujian Kerentanan A01: <i>Broken Access Control</i>	14
3.3.2. Pengujian Kerentanan A02: <i>Cryptographic Failure</i>	15
3.3.3. Pengujian Kerentanan A03: <i>Injection</i>	15
3.3.4. Pengujian Kerentanan A04: <i>Insecure Design</i>	15
3.3.5. Pengujian Kerentanan A05: <i>Security Misconfiguration</i>	16
3.3.6. Pengujian Kerentanan A06: <i>Vulnerable and Outdated Components</i>	16
3.3.7. Pengujian Kerentanan A07: <i>Identification and Authentication Failures</i>	17
3.3.8. Pengujian Kerentanan A08: <i>Software and Data Integrity Failures</i>	17
3.3.9. Pengujian Kerentanan A09: <i>Security Logging and Monitoring Failures</i>	18

3.3.10. Pengujian Kerentanan A10: <i>Server-Side Request Forgery</i>	18
3.4. Pengaturan Lingkungan Uji	18
3.5. Eksekusi Skenario Pengujian	18
3.6. Evaluasi Hasil Pengujian	19
BAB 4 HASIL PERCOBAAN DAN ANALISIS	21
4.1. Hasil Percobaan	21
4.1.1. Hasil Uji Kerentanan A01: <i>Broken Access Control</i>	21
4.1.2. Hasil Uji Kerentanan A02: <i>Cryptographic Failure</i>	25
4.1.3. Hasil Uji Kerentanan A03: <i>Injection</i>	27
4.1.4. Hasil Uji Kerentanan A04: <i>Insecure Design</i>	29
4.1.5. Hasil Uji Kerentanan A05: <i>Security Misconfiguration</i>	30
4.1.6. Hasil Uji Kerentanan A06: <i>Vulnerable and Outdated Components</i>	31
4.1.7. Hasil Uji Kerentanan A07: <i>Identification and Authentication Failures</i>	33
4.1.8. Hasil Uji Kerentanan A08: <i>Software and Data Integrity Failures</i>	35
4.1.9. Hasil Uji Kerentanan A09: <i>Security Logging and Monitoring Failures</i>	36
4.1.10. Hasil Uji Kerentanan A10: <i>Server-Side Request Forgery</i>	39
4.2. Analisis	40
4.2.1. Analisis Uji Kerentanan A01: <i>Broken Access Control</i>	40
4.2.2. Analisis Uji Kerentanan A02: <i>Cryptographic Failure</i>	41
4.2.3. Analisis Uji Kerentanan A03: <i>Injection</i>	41
4.2.4. Analisis Uji Kerentanan A04: <i>Insecure Design</i>	41
4.2.5. Analisis Uji Kerentanan A05: <i>Security Misconfiguration</i>	41
4.2.6. Analisis Uji Kerentanan A06: <i>Vulnerable and Outdated Components</i>	42
4.2.7. Analisis Uji Kerentanan A07: <i>Identification and Authentication Failures</i>	42
4.2.8. Analisis Uji Kerentanan A08: <i>Software and Data Integrity Failures</i>	42
4.2.9. Analisis Uji Kerentanan A09: <i>Security Logging and Monitoring Failures</i>	43
4.2.10. Analisis Uji Kerentanan A10: <i>Server-Side Request Forgery</i>	43
4.3. Rekomendasi Mitigasi Kerentanan Pada Aplikasi S.E.E.D.S	43
4.3.1. Rekomendasi Mitigasi Kerentanan A01: <i>Broken Access Control</i>	43
4.3.2. Rekomendasi Mitigasi Kerentanan A02: <i>Cryptographic Failures</i>	44
4.3.3. Rekomendasi Mitigasi Kerentanan A03: <i>Injection</i>	44
4.3.4. Rekomendasi Mitigasi Kerentanan A04: <i>Insecure Design</i>	44
4.3.5. Rekomendasi Mitigasi Kerentanan A05: <i>Security Misconfiguration</i>	44
4.3.6. Rekomendasi Mitigasi Kerentanan A06: <i>Vulnerable and Outdated Component</i>	45
4.3.7. Rekomendasi Mitigasi Kerentanan A07: <i>Identification and Authentication Failures</i>	45
4.3.8. Rekomendasi Mitigasi Kerentanan A08: <i>Software and Data Integrity Failures</i>	45
4.3.9. Rekomendasi Mitigasi Kerentanan A09: <i>Security Logging and Monitoring Failures</i>	46
4.3.10. Rekomendasi Mitigasi Kerentanan A10: <i>Server-Side Request Forgery(SSRF)</i>	46

4.4. Analisis Kerentanan OWASP Pada Aplikasi S.E.E.D.S	46
BAB 5 KESIMPULAN DAN SARAN	51
5.1. Kesimpulan	51
5.2. Saran	52
DAFTAR PUSTAKA	53
LAMPIRAN	56
Lampiran 1	56
Lampiran 2	56
Lampiran 3	59
Lampiran 4	60
Lampiran 5	61
Lampiran 6	61
Lampiran 7	64
Lampiran 8	64
Lampiran 9	66
Lampiran 10	66
Lampiran 11	67