UNIVERSITAS
GADJAH MADA
PERANCANGAN PRAKTIK PEMBELAJARAN KEAMANAN SISTEM INFORMASI BERBASIS SISTEM PENILAIAN CAPTURE THE FLAG
MUHAMMAD FATHAN K, Dani Adhipta, S.Si., M.T.; Sujoko Sumaryono, Ir., M.T.
Universitas Gadjah Mada, 2016 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN PENGESAHAN ii
HALAMAN PERNYATAAN iii
HALAMAN PERSEMBAHAN iv
KATA PENGANTAR v
DAFTAR ISI vii
DAFTAR TABEL x
DAFTAR GAMBAR xi
DAFTAR SINGKATAN xiv
Intisari xvi
Abstract xvii
BAB I PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Perumusan Masalah 5
1.3. Tujuan Penelitian 5
1.4. Manfaat Penelitian 5
1.5. Batasan Masalah 5
1.6. Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI 7
2.1. Layanan Internet 7
2.2. Perkembangan Layanan *Website* 9
2.3. Apache Tomcat Server 15
2.4. Fundamental Keamanan Informasi 17
2.5. Peretas Sistem (*Hacker* dan *Cracker*) 19
2.6. *Top 10 OWASP vulnerabilities* 23
2.7. OWASP ZAP 38
2.8. Metode Pembelajaran Keamanan Sistem Informasi 40
2.8.1. Webgoat 40
2.8.2. *Capture the Flag* (CTF) 41

UNIVERSITAS GADJAH MADA
PERANCANGAN PRAKTIK PEMBELAJARAN KEAMANAN SISTEM INFORMASI BERBASIS SISTEM PENILAIAN CAPTURE THE FLAG
MUHAMMAD FATHAN K, Dani Adhipta, S.Si., M.T.; Sujoko Sumaryono, Ir., M.T.
Universitas Gadjah Mada, 2016 | Diunduh dari http://etd.repository.ugm.ac.id/

2.8.3. Sistem Penilaian *Capture the Flag* 46
2.9. Teknik Pengujian Sistem 47
BAB III METODE PENELITIAN 50
3.1. Alat yang Digunakan 50
3.1.1. Perangkat Keras 50
3.1.2. Perangkat Lunak 50
3.2. *Framework* 51
3.3. Diagram Alir Penelitian 52
3.3.1. Identifikasi Kebutuhan 53
3.3.2. Analisis Sistem *Framework* 53
3.3.3. Perancangan Soal OWASP *Top 10 Vulnerabilities* 54
3.3.4. Pembuatan *Scoring System* 56
3.3.5. Pengujian Sistem 59
3.3.6. Penulisan Laporan 59
BAB IV HASIL DAN PEMBAHASAN 60
4.1. Hasil Identifikasi Kebutuhan 60
4.2. Hasil Analisis Sistem *Framework* 60
4.2.1. Konfigurasi Awal Webgoat 61
4.2.2. Konfigurasi *Proxy* OWASP ZAP 63
4.3. Pembuatan Soal OWASP *Top 10 Vulnerabilities* 63
4.3.1. *Injection* 64
4.3.2. *Broken Authentication and Session Management* 65
4.3.3. *Cross-Site Scripting* (XSS) 67
4.3.4. *Insecure Direct Object References* 68
4.3.5. *Security Misconfiguration* 69
4.3.6. *Sensitive Data Exposure* 70
4.3.7. *Missing Function Level Access Control* 71
4.3.8. *Cross-Site Request Forgery* (CSRF) 72
4.3.9. *Using Components with Known Vulnerabilities* 73
4.3.10. *Unvalidated Redirects and Forwards* 74
4.4. Pembuatan *Scoring System* 76

UNIVERSITAS
GADJAH MADA
PERANCANGAN PRAKTIK PEMBELAJARAN KEAMANAN SISTEM INFORMASI BERBASIS SISTEM PENILAIAN CAPTURE THE FLAG
MUHAMMAD FATHAN K, Dani Adhipta, S.Si., M.T.; Sujoko Sumaryono, Ir., M.T.
Universitas Gadjah Mada, 2016 | Diunduh dari http://etd.repository.ugm.ac.id/

4.4.1. Skenario *Capture the Flag* 76
4.4.2. Pembuatan Halaman *Scoring System* 78
4.5. Pengujian Sistem 81
4.5.1. Pengujian Soal *OWASP Top 10 Vulnerabilities* 81
4.5.2. Pengujian *Scoring System* 94
4.6. Kelebihan dan Kekurangan 97
4.6.1. Kelebihan Aplikasi 97
4.6.2. Kekurangan Aplikasi 98
BAB V KESIMPULAN DAN SARAN 99
5.1. Kesimpulan 99
5.2. Saran 100
DAFTAR PUSTAKA 101
LAMPIRAN 106