DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI v
DAFTAR GAMBAR ix
DAFTAR TABEL xi
DAFTAR SIMBOL xiv
DAFTAR LAMPIRAN xv
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Identifikasi Masalah 2
1.3 Maksud dan Tujuan 3
1.4 Batasan Masalah 3
1.5 Metodelogi Penelitian 4
1.6 Alur Penelitian 5
1.7 Sistematika Penulisan 7
BAB II LANDASAN TEORI 9
2.1 Profil dan tempat penelitian 9
2.1.1 Profil Diskominfo Kabupaten Bandung 9
2.1.2 Struktur Organisasi 9
2.2 Landasan Teori 14
2.2.1 Internet 14
2.2.2 Keamanan Informasi 15
2.2.3 Open Sistem Interconnection 16
2.2.4 Proof Of Concept Exploit(PoC) 19
2.2.5 NIST SP 800-115 19
2.2.6 OWASP Risk Ranting Methodology 21
2.2.7 Apache 28

2.2.8 *Common Weakness Enumeration* (*CWE*) 29
2.2.9 Eksploitasi terhadap Website 29
2.2.9.1 Deface 29
2.2.9.2 SQL Injection 29
2.2.9.3 XXS(Cross Site Scriting) 30
2.2.9.4 Denial of Service(DoS) 30
2.2.10 Unified Modeling Language (UML) 31
2.2.11 Black Box Testing 32
2.2.12 Whois 32
2.2.13 Nmap 33
2.2.14 Acunetix Vulnerabilities Scanner 33
2.2.15 Vega 34
2.2.16 C# 34
2.2.17 *Object Oriented Programming* (OOP) 35
2.2.18 Xampp 36
2.2.19 Kali Linux 36
BAB III ANALISIS DAN PERANCANGAN SISTEM 39
3.1 Analisis Sistem 39
3.1.2 Analisis Data Penelitian 40
3.1.3 Analisis Metode 41
3.1.3.1 NIST SP 800-115 42
3.1.3.1.1 Planning 43
3.1.3.1.2 Discovery 43
3.1.3.2 OWASP Risk Rating Methodology 53
3.1.3.2.1 Likelihood 53
3.1.3.2.2. Impact 68
3.1.3.2.2 Klasifikasi Kerentanan 82
3.1.4 Analisis Sistem yang dibangun 83
3.1.5 Analisis Software Pendukung 86
3.1.5.1 Nmap 86
3.1.5.2 SQLmap 87

3.1.6 Analisis Arsitektur Sistem 89
3.1.7 Analisis Kebutuhan Non-Fungsional 91
3.1.7.1 Analisis Perangkat Keras 92
3.1.7.2 Analisis Perangkat Lunak 92
3.1.7.3 Analisis Pengguna 93
3.1.8 Analisis Kebutuhan Fungsional 93
3.1.8.1 Use Case Diagram 95
3.1.8.2 Use Case Scenario 96
3.1.8.3 Activity Diagram 102
3.1.8.4 Class Diagram 108
3.1.8.5 Sequence Diagram 109
3.2 Perancangan Sistem 115
3.2.1 Skema Relasi 115
3.2.2 Struktur Tabel 116
3.2.3 Perancangan Menu 117
3.2.4 Perancangan Antarmuka 119
3.2.5 Perancangan Pesan 125
3.2.6 Perancangan Jaringan Semantik 128
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM 131
4.1. Implementasi Kerentanan 131
4.1.1. Attack 131
4.1.2. Reporting 133
4.1.2.1. Management Summary 133
4.1.2.2. Vulnerability Report 133
4.2. Implementasi Sistem 134
4.2.1. Implementasi Metode 134
4.2.2. Implementasi Perangkat Keras 139
4.2.3. Implementasi Perangkat Lunak 140
4.2.4. Implementasi Antarmuka 140
4.3. Pengujian Sistem 147
4.3.1. Pengujian Black Box 148

4.3.1.1. Skenario Pengujian 148
4.3.1.2. Hasil Pengujian 151
BAB V KESIMPULAN DAN SARAN 153
5.1. Kesimpulan 153
5.2. Saran 154
Daftar Pustaka 155