DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI v
DAFTAR GAMBAR vi
DAFTAR TABEL ix
DAFTAR SIMBOL xi
DAFTAR LAMPIRAN xii
BAB 1 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 Metode Penelitian 3
1.6 Tahapan Penelitian 4
1.7 Sistematika Penulisan 6
BAB II TINJAUAN PUSTAKA 9
2.1 Profil Dan Tempat Penelitian 9
2.1.1 Profil Dinas Komunikasi Dan Informatika Kabupaten Tangerang 9
2.1.2 Visi dan Misi 9
2.1.3 Struktur Organisasi 10
2.2 Landasan Teori 12
2.2.1 Keamanan Informasi 12
2.2.2 Internet 13
2.2.3 Jaringan Komputer 15
2.2.4 Black Box Testing 18

2.2.5 Proof of Concept Exploit 19
2.2.6 Information Systems Security Assessment Framework (ISSAF) 19
2.2.7 Penilaian Keamanan Web Aplikasi (ISSAF) 21
2.2.8 Penilaian Keamanan Web Aplikasi Lanjutan(ISSAF) SQLi 22
2.2.9 Dnsdumpster 24
2.2.10 NSE (Nmap Scripting Engine) 24
2.2.11 Jenis Kerentanan 25
2.2.12 WAMP (Windows-Apache-MySQL-PHP) 26
2.2.13 Acunetix 27
2.2.14 Vega 27
2.2.15 Nikto 28
2.2.16 Burpsuite 28
2.2.17 Kali Linux 29
2.2.18 Payload 29
2.2.19 Common Weakness Enumeration (CWE) 30
2.2.20 Web crawler 32
BAB 3 ANALISIS DAN PERANCANGAN SISTEM 33
3.1 Analisis Sistem 33
3.2 Analisis Masalah 33
3.2.1 Planning & preparation 33
3.2.2 Assessment 34
BAB 4 IMPLEMENTASI DAN PEMBAHASAN 57
4.1 Implementasi Kerentanan 57
4.1.1 Penetration 57
4.1.2 Gaining Access & Privilege Escalation 60
4.1.3 Enumerating Further 64
4.1.4 Compromise Remote User/Sites 66
4.1.5 Maintaining Access 68

4.1.6 Covering Tracks 69
4.2 Pembahasan 69
4.2.1 Reporting 70
4.2.3 Clean-up And Destroy Artefacts 76
BAB 5 KESIMPULAN DAN SARAN 77
5.1 Kesimpulan 77
5.2 Saran 77
DAFTAR PUSTAKA 78