DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PENGESAHAN ii
PERNYATAAN BEBAS PLAGIASI iii
KATA PENGANTAR iv
DAFTAR ISI vi
DAFTAR GAMBAR ix
INTISARI xiii
ABSTRACT xiv
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Batasan Masalah 3
1.5 Manfaat Penelitian 4
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 6
2.1. Tinjauan Pustaka 6
2.2. Dasar Teori 12
2.2.1 Keamanan Informasi 12
2.2.2 *Proof of Concept* 12
2.2.3 *Open Web Application Security Project* 13
2.2.4 *Testing Environment* 13
2.2.5 *Information Gathering Tools* 14
2.2.6 *Vulnerability Scanning Tools* 15

2.2.7 *Exploitation Tools* 16
2.2.8 Jenis Serangan 17
2.3. Hipotesis 18
BAB III BAHAN DAN METODE PENELITIAN 20
3.1. Alat Penelitian 20
3.2. Bahan Penelitian 20
3.3. Tahapan Penelitian 22
3.4. Instalasi dan Konfigurasi 24
3.4.1 Instalasi *Software* Virtual Oracle VM VirtualBox 24
3.4.2 Instalasi Sistem Operasi Kali Linux 27
3.4.3 Instalasi Laragon 34
3.4.4 Instalasi *Open Web Application Security Project Zed Attack Proxy* 36
3.4.5 Instalasi ParamSpider 39
3.4.6 Instalasi XSpear 40
3.4.7 Instalasi Dalfox 40
3.4.8 Instalasi Burp Suite 41
3.5. Pengujian Penelitian 43
3.5.1 Tahap *Information Gathering* 44
3.5.2 Tahap *Vulnerability Scanning* 45
3.5.3 Penyerangan *Cross-Site Scripting* 46
3.5.4 Penyerangan SQL *Injection* 49
3.5.5 Penyerangan *Cross-Site Request Forgery* 50
BAB IV HASIL PENELITIAN DAN PEMBAHASAN 56
4.1. Hasil Tahap *Information Gathering* 56
4.1.1 *Scanning Port* Terbuka 56
4.1.2 Identifikasi Konfigurasi Sistem 57

4.2. Hasil Tahap *Vulnerability Scanning* 58
4.3. *Vulnerability Analysis* 60
4.4. Hasil Tahap *Exploitation* 70
4.4.1 Serangan *Cross-Site Scripting* 71
4.4.2 Serangan SQL *Injection* 78
4.4.3 Serangan *Cross-Site Request Forgery* 80
4.5. Rekomendasi Solusi 82
BAB V PENUTUP 88
5.1. Kesimpulan 88
5.2. Saran 88
DAFTAR PUSTAKA 90
Lampiran 1 *Professional Penetration Testing Report* 94

DAFTAR GAMBAR

Gambar 3. 1 Diagram Alur Penelitian 22
Gambar 3. 2 Tampilan Pengunduhan VirtualBox 25
Gambar 3. 3 Mulai kostumisasi instalasi VirtualBox 25
Gambar 3. 4 Memilih fitur-fitur yang ingin diinstal 25
Gambar 3. 5 Meminta konfirmasi untuk melanjutkan instalasi 26
Gambar 3. 6 Memulai proses instalasi VirtualBox 26
Gambar 3. 7 Proses instalasi berhasil 27
Gambar 3. 8 File Installer Kali Linux 27
Gambar 3. 9 Penentuan nama dan sistem operasi 28
Gambar 3. 10 Spesifikasi virtual machine 28
Gambar 3. 11 Tampilan awal instalasi *Kali Linux* 29
Gambar 3. 12 Membuat nama host pada sistem 29
Gambar 3. 13 Membuat nama domain 30
Gambar 3. 14 Membuat nama user baru 30
Gambar 3. 15 Membuat nama domain 31
Gambar 3. 16 Membuat password untuk login 31
Gambar 3. 17 Membuat partisi disk untuk sistem 32
Gambar 3. 18 Membuat pastisi disk untuk sistem (lanjutan) 32
Gambar 3. 19 Membuat pastisi disk untuk sistem (lanjutan) 32
Gambar 3. 20 Membuat partisi disk untuk sistem (lanjutan) 33
Gambar 3. 21 Menginstall GRUB boot loader 33
Gambar 3. 22 Tampilan login Kali Linux 34
Gambar 3. 23 Tautan untuk mengunduh Laragon 34
Gambar 3. 24 Pemilihan bahasa untuk instalasi 34
Gambar 3. 25 Memilih lokasi tujuan instalasi 35
Gambar 3. 26 Mengatur opsi Auto start, Auto detect, dan create virtual hosts 35
Gambar 3. 27 Memulai proses instalasi 36
Gambar 3. 28 Proses instalasi selesai 36
Gambar 3. 29 Download file installer ZAP 36
Gambar 3. 30 Halaman pertama proses instalasi 37
Gambar 3. 31 Apache License Agreement 37

Gambar 3. 32 Pemilihan tipe instalasi 38
Gambar 3. 33 Jendela instalasi 38
Gambar 3. 34 Proses instalasi berhasil 39
Gambar 3. 35 Download file installer Burp Suite 41
Gambar 3.36 Halaman pertama proses instalasi 42
Gambar 3. 37 Memilih lokasi instalasi 42
Gambar 3. 38 Memilih nama folder di menu start 43
Gambar 3. 39 Proses instalasi berhasil 43
Gambar 3. 40 Diagram Alur Tahapam Pengujian 44
Gambar 3. 41 Scanning vulnerability menggunakan automated scan 45
Gambar 3. 42 Memasukkan URL target 45
Gambar 3. 43 Proses scanning berjalan 46
Gambar 3. 44 Diagram Alur Pengujian XSS 46
Gambar 3. 45 Input form pada website target 47
Gambar 3. 46 Input form website acunetix 48
Gambar 3. 47 Diagram Alur Pengujian SQL Injection 50
Gambar 3. 48 Diagram Alur Pengujian CSRF 51
Gambar 3. 49 Mengaktifkan intercept di tab Proxy 51
Gambar 3. 50 Tampilan “Intercept is on” 52
Gambar 3. 51 Form login dashboard perusahaan 52
Gambar 3. 52 Hasil request di tab HTTP History 53
Gambar 3. 53 Mengaktifkan Intercept di tab Proxy 53
Gambar 3. 54 Tampilan “Intercept is on” 54
Gambar 3. 55 Form login Simaster UGM 54
Gambar 3. 56 Hasil request di tab HTTP History 55
Gambar 4. 1 Captured HTTP Request 63
Gambar 4. 2 Pengecekan header CSP pada Response Headers 64
Gambar 4. 3 Pengecekan Request URL pada Response Headers 64
Gambar 4. 4 Pengecekan header X-Frame-Options pada Response Headers 65
Gambar 4. 5 Tampilan Retire.js pada aplikasi web 65
Gambar 4. 6 Pengecekan cookie di browser developer tools 66
Gambar 4. 7 Pengecekan header HSTS pada Response Headers 66

Gambar 4. 8 Pengecekan header X-Content-Type-Options pada Response Headers 67
Gambar 4. 9 Pengecekan suspisious comments pada source code 67
Gambar 4. 10 Pengecekan Request URL pada Response Headers 68
Gambar 4. 11 Pengecekan pengiriman infromasi menggunakan HTTPS 68
Gambar 4. 12 Pengecekan form data post dengan kredensial 68
Gambar 4. 13 Hasil eksekusi skrip XSS 69
Gambar 4. 14 Pengecekan header CSP pada Response Headers 69
Gambar 4. 15 Pengecekan Proxy HTTP History 70
Gambar 4. 16 Pengecekan Proxy HTTP History lanjutan 70
Gambar 4. 17 Hasil eksekusi payload sederhana 71
Gambar 4. 18 Hasil eksekusi payload karakter unik 72
Gambar 4. 19 Hasil eksekusi payload dengan DOM-based XSS 72
Gambar 4. 20 Hasil eksekusi payload sederhana 73
Gambar 4. 21 Hasil eksekusi payload karakter unik 73
Gambar 4. 22 Hasil eksekusi payload dengan DOM-based XSS 73
Gambar 4. 23 Hasil scraping parameter URL menggunakan ParamSpider 74
Gambar 4. 24 Hasil pemindaian kerentanan XSS menggunakan Dalfox 74
Gambar 4. 25 Hasil pemindaian kerentanan XSS menggunakan XSpear 75
Gambar 4. 26 Hasil scraping parameter URL menggunakan ParamSpider 76
Gambar 4. 27 Hasil pemindaian kerentanan XSS menggunakan Dalfox 76
Gambar 4. 28 Hasil eksekusi payload XSS 77
Gambar 4. 29 Hasil pemindaian kerentanan XSS menggunakan XSpear 77
Gambar 4. 30 Hasil eksekusi payload XSS 78
Gambar 4. 31 Hasil serangan SQL Injection website sistem informasi 78
Gambar 4. 32 Hasil serangan SQL Injection website sistem informasi (lanjutan) 78
Gambar 4. 33 Hasil serangan SQL Injection website Acunetix 79
Gambar 4. 34 Hasil serangan SQL Injection website Acunetix (lanjutan) 80
Gambar 4. 35 Button dari skrip HTML yang mereplikasi request 80
Gambar 4. 36 Berhasil mengakses dashboard sistem informasi perusahaan 81
Gambar 4. 37 Button dari skrip HTML yang mereplikasi request 81
Gambar 4. 38 Form login SSO UGM untuk masuk ke Simaster UGM 82
Gambar 4. 39 Burp Suite intercept Simaster UGM request 82

DAFTAR TABEL

Tabel 2. 1 Ringkasan Sumber Penelitian 10
Tabel 3. 1 Spesifikasi Laptop 20
Tabel 3. 2 Spesifikasi VirtualBox 20
Tabel 3. 3 Spesifikasi Kali Linux 21
Tabel 3. 4 Spesifikasi OWASP ZAP 21
Tabel 3. 5 Spesifikaspui Laragon 21
Tabel 4. 1 Hasil Scanning Port Terbuka 56
Tabel 4. 2 Hasil Identifikasi Konfigurasi Sistem 57
Tabel 4. 3 Hasil Vulnerability Scanning 59
Tabel 4. 4 Hasil Vulnerability Analysis 60
Tabel 4. 5 Rekomendasi Solusi 83