

## DAFTAR ISI

LEMBAR PENGESAHAN .....	ii
PERNYATAAN BEBAS PLAGIASI .....	iii
KATA PENGANTAR .....	iv
DAFTAR ISI.....	vi
DAFTAR GAMBAR.....	ix
DAFTAR TABEL .....	xiii
DAFTAR LAMPIRAN.....	xiv
INTISARI .....	xv
<i>ABSTRACT</i> .....	xvi
BAB I.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah.....	3
1.3. Tujuan Penelitian .....	3
1.4. Batasan Masalah .....	4
1.5. Manfaat Penelitian .....	4
1.6. Sistematika Penulisan .....	5
BAB II .....	6
2.1. Lingkup Tinjauan Pustaka .....	6
2.2. Dasar Teori.....	12
2.2.1. Pengujian Penetrasi ( <i>Penetration testing</i> ) .....	12
2.2.2. <i>Black Box Testing</i> .....	14
2.2.3. <i>Vulnerability</i> (Kerentanan) .....	14
2.2.4. <i>Path traversal Exploitation</i> .....	14
2.2.5. <i>Remote Code Execution</i> .....	16
2.2.6. <i>Apache Webserver</i> .....	18
2.2.7. <i>Common Vulnerabilities and Exposures</i> (CVE) .....	19
2.2.8. CVE-2021-42013.....	20

2.2.9. <i>Framework</i> Flask .....	21
2.3. Hipotesis .....	21
BAB III .....	22
3.1. Waktu dan Tempat Penelitian .....	22
3.2. Peralatan Penelitian .....	22
3.3. Bahan Penelitian .....	23
3.4. Tahapan Penelitian .....	25
3.5.2. Skenario Penyerangan .....	29
3.5.3. Diagram Alir Program .....	31
3.6. Pengembangan Program .....	36
3.6.1. Pengembangan Program Eksploitasi .....	36
3.6.2. Pengembangan Backend <i>Website</i> .....	44
3.6.3. Pembuatan Pelaporan Otomatis .....	47
3.6.4. Pembuatan <i>Frontend Website</i> .....	51
3.7. Pembuatan Lab Virtual .....	56
3.7.1. Pembuatan Lab Virtual Apache <i>Vulnerable</i> CVE-2021-42013 .....	56
3.7.2. Pembuatan Lab Virtual Tidak Rentan .....	57
3.8. Pengujian <i>Website</i> .....	59
3.8.1. Pengujian Fungsionalitas <i>Website</i> .....	59
3.8.2. Pengujian Program Eksploitasi .....	60
3.8.3. Pengujian Program <i>Reporting</i> .....	61
3.9. Pengujian dengan Perbandingan Antara Metode Otomatis dengan Manual .....	61
3.9.1. Pengambilan Waktu dengan Metode Otomatis .....	61
3.9.2. Pengambilan Waktu dengan Metode Manual .....	62
3.9.3. Langkah <i>penetration testing</i> secara manual .....	62
3.9.4. <i>Payload</i> Pengujian Metode Otomatis dan Manual .....	64
3.9.5. Teknik Request Payload Pengujian Metode Otomatis dan Manual .....	65
BAB IV .....	67

4.1 Hasil Pengujian <i>Website</i> .....	67
4.1.1. Analisis Metode <i>Black Box</i> .....	67
4.1.2. Analisis Log Program untuk Evaluasi Kinerja .....	72
4.1.3. Analisis Hasil Pengujian Program Eksploitasi .....	73
4.1.4. Analisis Hasil Pengujian Program <i>Reporting</i> .....	78
4.2 Perbandingan Antara Metode Otomatis dengan Manual .....	81
4.2.1. Waktu Pengujian .....	81
4.2.2. Fleksibilitas.....	87
4.3 Perbandingan Akses Laporan .....	89
BAB V .....	92
5.1 Kesimpulan .....	92
5.2 Saran .....	92
DAFTAR PUSTAKA .....	93
LAMPIRAN .....	96

## DAFTAR GAMBAR

Gambar 2. 1 Visualisasi Tahapan Uji Penetrasi .....	12
Gambar 2. 2 Ilustrasi <i>Path traversal</i> .....	15
Gambar 2. 3 <i>Payload</i> Apache 2.4.49.....	16
Gambar 2. 4 <i>Payload</i> Apache 2.4.50.....	16
Gambar 2. 5 <i>Payload</i> RCE Apache 2.4.49 .....	17
Gambar 2. 6 <i>Payload</i> RCE Apache 2.4.50 .....	18
Gambar 2. 7 Laporan Shodan Terkait CVE-2021-42013 .....	21
Gambar 3. 1 Sistem Operasi Ubuntu .....	22
Gambar 3. 2 Spesifikasi Apache HTTP <i>Server</i> .....	23
Gambar 3. 3 Spesifikasi VS Code .....	23
Gambar 3. 4 Spesifikasi Python .....	24
Gambar 3. 5 Spesifikasi Flask.....	24
Gambar 3. 6 Spesifikasi Nmap .....	24
Gambar 3. 7 Diagram Alir Tahapan Penelitian.....	25
Gambar 3. 8 <i>Diagram Activity Web Uji Penetrasi Otomatis</i> .....	28
Gambar 3. 9 Skenario Penyerangan .....	29
Gambar 3. 10 Diagram Alir main.py .....	31
Gambar 3. 11 Diagram Alir scanner.py .....	34
Gambar 3. 12 Diagram Alir generate_report_apache.py .....	35
Gambar 3. 13 Melakukan Import Library .....	37
Gambar 3. 14 Melakukan Penetapan User-Agent dan Bypass SSL .....	37
Gambar 3. 15 Pendefinisian run_nmap_scan().....	38
Gambar 3. 16 Pendefinisian Fungsi find_apache_services().....	39
Gambar 3. 17 Pendefinisian filter_apache_services() .....	39
Gambar 3. 18 Pendefinisian urlCheck() .....	40
Gambar 3. 19 Pendefinisian <i>exploitPT()</i> .....	40
Gambar 3. 20 Pendefinisian <i>exploitRCE()</i> .....	41
Gambar 3. 21 Pendefinisian <i>exploitPT()</i> .....	42
Gambar 3. 22 Pendefinisian curlRCE().....	42
Gambar 3. 23 Pendefinisian RCE() .....	43

Gambar 3. 24 Pendefinisian <code>proccess_target()</code> .....	44
Gambar 3. 25 Import Library <code>main.py</code> .....	44
Gambar 3. 26 Inisialisasi app Variable .....	45
Gambar 3. 27 Mengatur <i>Logging</i> .....	45
Gambar 3. 28 <i>Rendering</i> <code>index.html</code> .....	45
Gambar 3. 29 <i>Routing</i> <code>/select_tool</code> .....	45
Gambar 3. 30 <i>Routing</i> Masing-Masing <i>Tools</i> .....	46
Gambar 3. 31 Pendefinisian <code>run_apache()</code> .....	46
Gambar 3. 32 Inisialisasi Flask dalam Mode Debug.....	46
Gambar 3. 33 Import Library <code>generate_report_apache.py()</code> .....	47
Gambar 3. 34 Pengaturan <i>Logging</i> .....	47
Gambar 3. 35 Pendefinisian <code>sanitize_text()</code> .....	47
Gambar 3. 36 Pendefinisian <code>add_header(document)</code> .....	48
Gambar 3. 37 Pendefinisian <code>generate_report()</code> .....	49
Gambar 3. 38 Pendefinisian Fungsi <code>generate_report()</code> .....	50
Gambar 3. 39 Deklarasi HTML5 dan Pembuatan Head HTML .....	51
Gambar 3. 40 Pendefinisian Body <code>index.html</code> .....	52
Gambar 3. 41 Divisi <i>Class Container</i> .....	52
Gambar 3. 42 <i>Heading Pentest Tool</i> .....	52
Gambar 3. 43 <i>Form</i> Pemilihan <i>Tools</i> .....	53
Gambar 3. 44 <i>Class Keterangan Tools</i> .....	53
Gambar 3. 45 Pembuatan <code>apache_form.html</code> .....	55
Gambar 3. 46 Pendefinisian Head <code>message.html</code> .....	55
Gambar 3. 47 Pembuatan Body <code>message.html</code> .....	56
Gambar 3. 48 <i>Git Clone Repository Lab</i> .....	56
Gambar 3. 49 Pembuatan Docker <i>Image</i> Lab Virtual.....	57
Gambar 3. 50 Menjalankan Docker <i>Image</i> .....	57
Gambar 3. 51 Pengujian Lab Apache <i>Webserver</i> CVE-2021-42013.....	57
Gambar 3. 52 Pembuatan <i>Dockerfile</i> Lab Apache Tidak Rentan .....	58
Gambar 3. 53 Membuat Docker Image Lab Apache Tidak Rentan.....	58
Gambar 3. 54 Menjalankan Docker Image Lab Apache Tidak Rentan .....	58
Gambar 3. 55 Pengecekan Lab Apache Tidak Rentan.....	58

Gambar 3. 56 Input Target Eksploitasi untuk Pengujian Uji Penetrasi .....	60
Gambar 3. 57 Report Otomatis.....	61
Gambar 3. 58 Penambahan Kode Pengukuran Waktu.....	62
Gambar 3. 59 Pengambilan Waktu Pengujian Manual.....	62
Gambar 3. 60 Langkah Uji Penetrasi Manual .....	63
Gambar 3. 61 Membentuk URL <i>Payload</i> .....	65
Gambar 3. 62 Pemeriksaan Respons .....	65
Gambar 3. 63 Membentuk URL dengan <i>Payload</i> .....	65
Gambar 3. 64 Mengirim Permintaan HTTP POST .....	66
Gambar 3. 65 Memeriksa Respons.....	66
Gambar 4. 1 Halaman Menu Utama.....	69
Gambar 4. 2 Halaman Menu Apache Tool .....	70
Gambar 4. 3 Eksploitasi <i>Path traversal</i> .....	70
Gambar 4. 4 Eksploitasi RCE.....	70
Gambar 4. 5 Eksploitasi <i>Path traversal</i> dan RCE.....	71
Gambar 4. 6 Pengujian Kesalahan Input .....	71
Gambar 4. 7 Pengunduhan Laporan Sekali Kli .....	72
Gambar 4. 8 Log Program Saat Dilakukan Pengujian Komponen.....	72
Gambar 4. 9 Log Pemindaian Nmap .....	74
Gambar 4. 10 Hasil Eksploitasi <i>Path traversal</i> .....	74
Gambar 4. 11 <i>Output Vulnerability Scanning</i> dan Eksploitasi RCE .....	75
Gambar 4. 12 Log Pemindaian Nmap .....	76
Gambar 4. 13 Eksekusi Pemindaian dan Eksploitasi <i>Path Transversal</i> dan RCE .....	76
Gambar 4. 14 HTTPError.....	76
Gambar 4. 15 Eksploitasi RCE.....	77
Gambar 4. 16 Halaman Sampul Generated Report .....	78
Gambar 4. 17 Menampilkan Pendahuluan .....	79
Gambar 4. 18 Hasil Pemindaian Nmap .....	79
Gambar 4. 19 Hasil Eksploitasi .....	80
Gambar 4. 20 Bagian Rekomendasi pada Laporan .....	81
Gambar 4. 21 Waktu Pengujian Otomatis .....	82
Gambar 4. 22 Waktu Pemindaian Nmap Uji Penetrasi Otomatis.....	82

Gambar 4. 23 Waktu Pemindaian Kerentanan dan Eksploitasi Uji Otomatis .....	83
Gambar 4. 24 Waktu Pembuatan Laporan Uji Penetrasi Otomatis .....	83
Gambar 4. 25 Perintah Eksploitasi Manual .....	83
Gambar 4. 26 Waktu Pemindaian Target Manual Menggunakan Nmap .....	83
Gambar 4. 27 Langkah Pemindaian Kerentanan dan Eksploitasi Pengujian Manual ....	84
Gambar 4. 28 Waktu Pemindaian Kerentanan dan Eksploitasi Manual .....	84
Gambar 4. 29 Waktu Pembuatan Report Manual .....	85
Gambar 4. 30 Perbandingan Waktu Uji Penetrasi Manual dan Otomatis.....	85
Gambar 4. 31 Perbandingan Durasi Setiap Proses Uji Penetrasi .....	86
Gambar 4. 32 Grafik Penyusutan Waktu Berdasarkan Proses Spesifik.....	87
Gambar 4. 33 Akses Laporan Uji Penetrasi Berbasis Web.....	90
Gambar 4. 34 Akses Laporan Uji Penetrasi Berbasis Manual.....	90
Gambar 4. 35 Akses Laporan Uji Penetrasi Berbasis Skrip .....	91

## DAFTAR TABEL

Tabel 2. 1 Ruang Lingkup Kajian Pustaka .....	8
Tabel 3. 1 Spesifikasi Laptop .....	22
Tabel 3. 2 Rincian Pengujian <i>Black Box</i> .....	59
Tabel 4. 1 Analisis Pengujian Metode <i>Black Box</i> .....	67
Tabel 4. 2 Perbandingan Taktik yang Dilakukan.....	88



## DAFTAR LAMPIRAN

Lampiran 1 Diagram Alir main.py .....	96
Lampiran 2 Diagram Alir scanner.py .....	97
Lampiran 3 Diagram Alir generate_report_apache.py .....	98
Lampiran 4 Kode main.py .....	99
Lampiran 5 Kode scanner.py .....	104
Lampiran 6 Kode generate_report_apache.py .....	109
Lampiran 7 Kode index.html .....	113
Lampiran 8 Kode apache_form.html .....	114
Lampiran 9 Kode message.html .....	115
Lampiran 10 Format dan Bentuk Report .....	116