

ABSTRAK

Azarya Kairossutan Sacri Pusaka Dami

Skripsi

Analisa Keamanan *Website* dengan Automasi *Penetration Testing* Menggunakan Metode *Penetration Testing Execution Standard* (PTES) Secara Terstruktur

Keamanan website adalah prioritas penting bagi perusahaan dan pengguna internet. Ancaman seperti *hacker* dan kerentanan sistem dapat menyebabkan kerugian besar. Penelitian ini menganalisis keamanan *website* menggunakan metode *Penetration Testing Execution Standard* (PTES) dengan *automation script* dibandingkan dengan metode *Open Web Application Security Project* (OWASP) dengan *manual tools*. Objek penelitian ini adalah *Damn Vulnerable Web Application* (DVWA).

Hasil penelitian menunjukkan bahwa *automation script* dalam metode PTES mengurangi waktu eksekusi secara *manual* dari 1,5-2 jam menjadi 30 menit-1 jam secara otomatis. Meskipun lebih efisien, beberapa kerentanan memerlukan analisis *manual*. *Automation script* mendeteksi 30-40% kerentanan di DVWA dan berhasil mengeksploitasi 42,85% kerentanan utama. Tiga *automation script* yang dibuat mencakup tahapan *information gathering*, *vulnerability analysis*, dan *exploitation*. Penelitian ini diharapkan memberikan pemahaman mendalam tentang keamanan *website* dan metode otomatisasi *penetration testing* menggunakan PTES, sehingga membantu perusahaan dan pengembang *website* meningkatkan keamanan sistem informasi.

Kata Kunci:

keamanan *website*, *penetration testing*, *penetration testing execution standard*, automasi, *website vulnerable*, *automation script*, *ptes*, *owasp*, *dvwa*

ABSTRACT

Azarya Kairossutan Sacri Pusaka Dami

Undergraduate thesis

Website Security Analysis Using Automated Penetration Testing with the Comprehensive Penetration Testing Execution Standard (PTES) Method

Website security is an important priority for companies and internet users. Threats such as hackers and system vulnerabilities can cause huge losses. This research analyzes website security using the Penetration Testing Execution Standard (PTES) method with automated scripts compared to the Open Web Application Security Project (OWASP) method with manual tools. The object of this research is the Damn Vulnerable Web Application (DVWA).

The research results show that script automation in the PTES method reduces manual execution time from 1.5-2 hours to 30 minutes-1 hour automatically. Although more efficient, some vulnerabilities require manual analysis. Automation script detected 30-40% of vulnerabilities in DVWA and successfully exploited 42.85% of major vulnerabilities. The three automation scripts created include the stages of information gathering, vulnerability analysis, and exploitation. This research is expected to provide an in-depth understanding of website security and penetration testing automation methods using PTES, thereby helping companies and website developers improve information system security.

Keywords:

website security, penetration testing, penetration testing execution standard, automation, website vulnerable, automation script, ptes, owasp, dvwa

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH	iii
KATA PENGANTAR	iv
ABSTRAK	vi
DAFTAR ISI	viii
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xx
DAFTAR SEGMENT PROGRAM	xxi
1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	7
1.3 Tujuan Penelitian.....	8
1.4 Manfaat Penelitian	8
1.5 Ruang Lingkup	8
1.6 Metodologi Penelitian	11
1.7 Sistematika Penulisan	13
2. LANDASAN TEORI.....	14
2.1 Tinjauan Pustaka	14
2.1.1 Kejahatan Siber (<i>Cyber Crime</i>) dan Peretas (<i>Hacker</i>)	14
2.1.2 <i>Penetration Testing / Vulnerability Testing</i>	16
2.1.3 <i>Penetration Testing Execution Standard (PTES)</i>	17
2.1.4 Kali Linux	21
2.1.5 <i>Open Web/Worldwide Application Security Project (OWASP)</i>	22
2.1.6 <i>Damn Vulnerable Web App (DVWA)</i>	24
2.1.7 Burp Suite Community Edition	26
2.1.8 OWASP Zed Attack Proxy (ZAP)	27
2.1.9 SQLMap.....	27
2.1.10 Whois	27

2.1.11 Nmap.....	27
2.1.12 theHarvester	28
2.1.13 Wireshark.....	28
2.1.14 Metasploit.....	28
2.1.15 Nslookup	28
2.1.16 Wget.....	29
2.1.17 Netcat.....	29
2.1.18 WhatWeb	29
2.1.19 Sublist3r	29
2.1.20 Metagoofil.....	30
2.1.21 Wfuzz	30
2.1.22 Hydra.....	30
2.1.23 Nikto.....	30
2.2 Tinjauan Studi	31
2.2.1 Analisis Metode <i>Open Web Application Security Project</i> (OWASP) pada Pengujian Keamanan Website: <i>Literature Review</i>	31
2.2.2 Analisis Keamanan <i>Webserver</i> Menggunakan <i>Penetration Test</i>	32
2.2.3 Improved Deep Recurrent Q-Network of POMDPs for Automated Penetration Testing	33
2.2.4 Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning)..	33
3. ANALISA MASALAH DAN DESAIN SISTEM.....	35
3.1 Analisa Permasalahan	35
3.2 Desain Sistem	38
3.2.1 <i>Planning</i> dan <i>Preparation</i>	38
3.2.2 Pembuatan <i>Automation Script</i>	40
3.2.3 Implementasi <i>Penetration Testing</i>	44
3.2.4 Analisa Hasil	45
3.2.5 Kesimpulan dan Saran.....	45
4. IMPLEMENTASI SISTEM	46
4.1 <i>Planning</i> dan <i>Preparation</i>	46
4.1.1 Unduh dan <i>install</i> Kali Linux VMWare 2023.4 AMD64.....	46

4.1.2	Unduh dan Menjalankan Damn Vulnerable Web App (DVWA) pada Kali Linux.....	53
4.1.3	Unduh dan <i>install</i> Burp Suite Community Edition 2024.3.1.4 for Linux (x64)	68
4.1.4	Unduh dan <i>install</i> OWASP Zed Attack Proxy (ZAP)	72
4.1.5	Unduh dan <i>install</i> SQLMap	76
4.1.6	Unduh dan <i>install</i> Whois.....	77
4.1.7	Unduh dan <i>install</i> Nmap	78
4.1.8	Unduh dan <i>install</i> theHarvester.....	78
4.1.9	Unduh dan <i>install</i> Wireshark	79
4.1.10	Unduh dan <i>install</i> Wget	81
4.1.11	Persiapan Metasploit	82
4.1.12	Unduh dan <i>install</i> Netcat	83
4.1.13	Unduh dan <i>install</i> WhatWeb	83
4.1.14	Unduh dan <i>install</i> Hydra	84
4.1.15	Unduh dan <i>install</i> Wfuzz	85
4.1.16	Unduh dan <i>install</i> Nikto	85
4.2	Pembuatan <i>Automation Script</i>	86
4.2.1	Pembuatan <i>Script Fase Information Gathering</i>	91
4.2.2	Pembuatan <i>Script Fase Vulnerability Analysis</i>	113
4.2.3	Pembuatan <i>Script Fase Exploitation</i>	124
5.	PENGUJIAN SISTEM.....	135
5.1	Implementasi <i>Penetration Testing</i> berdasarkan Metode OWASP	135
5.1.1	Pelaksanaan Fase <i>Information Gathering</i>	135
5.1.2	Pelaksanaan Fase <i>Scanning and Enumeration</i>	152
5.1.3	Pelaksanaan Fase <i>Exploitation</i>	158
5.2	Implementasi <i>Penetration Testing</i> berdasarkan Metode PTES.....	171
5.2.1	Pelaksanaan Fase <i>Information Gathering</i>	171
5.2.2	Pelaksanaan Fase <i>Vulnerability Analysis</i>	178
5.2.3	Pelaksanaan Fase <i>Exploitation</i>	189
5.3	Analisa Waktu <i>Penetration Testing</i> antara Metode OWASP dan PTES.....	215
5.4	Analisa Keefektifan <i>Testing</i> antara Metode OWASP dan PTES.....	216
6.	KESIMPULAN DAN SARAN	221
6.1	Kesimpulan	221

6.2	Saran.....	222
DAFTAR REFERENSI		223
LAMPIRAN.....		227

DAFTAR TABEL

1.1	Perbandingan <i>Manual</i> dan <i>Automation Penetration Testing</i>	06
1.2	Kerentanan <i>Website</i> dan Penggunaan <i>Tools</i>	09
1.3	Segmentasi <i>Tools</i> pada Tahapan <i>Penetration Testing Execution Standard (PTES)</i>	10
2.1	Contoh Klasifikasi <i>Threat Agent/Community</i>	19
2.2	Tahapan dan <i>Tools</i> Pengujian Menggunakan Metode OWASP Versi 4	24
4.1	Fungsi Pada <i>Automation Script File “F2_InformationGathering”</i>	112
4.2	Fungsi Pada <i>Automation Script File “F4_VulnerabilityAnalysis”</i>	123
4.3	Fungsi Pada <i>Automation Script File “F5_Exploitation”</i>	133
5.1	Perbandingan Waktu <i>Penetration Testing</i> Antara OWASP dan PTES.....	215
5.2	Perbandingan Keefektifan Eksploitasi <i>SQL Injection</i>	218
5.3	Hasil <i>Brute Force DVWA</i> Menggunakan Wfuzz Pada <i>Script “F5_Exploitation”</i>	220

DAFTAR GAMBAR

1.1	<i>Number of Common IT Security Vulnerabilities and Exposures(CVEs) Worldwide from 2009 to 2024.....</i>	3
2.1	<i>Different Motivation When Breaking Into Systems of White, Black and Grey Hat Hacker.....</i>	16
2.2	Tampilan Menu Utama <i>Damn Vulnerable Web Application (DVWA).....</i>	26
3.1	Tahapan Desain Sistem.....	38
3.2	Ilustrasi <i>Environment Virtual Machine</i>	39
4.1	Tampilan Pencarian Kali Linux VMWare 64 pada Google.....	46
4.2	Tampilan Utama dari <i>Virtual Machine</i> VMware Workstation Pro 17.....	47
4.3	Membuka Menu <i>File</i> untuk Membuka Kali Linux VMWare.....	47
4.4	Tampilan Jendela Pencarian <i>Local File Explorer</i>	48
4.5	Kali Linux 2023.4 VMware AMD-64 pada VMware Workstation Pro 17.....	48
4.6	<i>Virtual Machine “Target-DVWA-kali-linux-2023.4-vmware-amd64”</i>	49
4.7	<i>Virtual Machine “Automation-Script-kali-linux-2023.4-vmware-amd64”</i>	49
4.8	Tampilan Proses <i>Booting</i> Awal Kali Linux.....	50
4.9	<i>Form Login</i> Kali Linux.....	50
4.10	Tampilan Halaman Utama Kali Linux.....	51
4.11	Tampilan <i>Icon</i> PowerShell pada Kali Linux.....	51
4.12	Tampilan PowerShell 7.2.6 © Microsoft Corporation pada Kali Linux.....	52
4.13	Pembaharuan Paket Sistem Perangkat Lunak Kali Linux.....	52
4.14	<i>Ping IP Address 192.168.81.130 (Virtual Machine Automation Script)</i>	53
4.15	<i>Ping IP Address 192.168.81.133 (Virtual Machine Target DVWA)</i>	53
4.16	Tampilan Pencarian DVWA pada Mesin Pencari.....	54
4.17	Tampilan <i>Download</i> DVWA melalui <i>Clone Packages</i>	54
4.18	<i>Cloning Packages</i> DVWA.....	54
4.19	Pesan <i>Error Cloning</i> DVWA.....	55
4.20	Tampilan Hasil <i>Cloning</i> DVWA Berhasil.....	55
4.21	Memberikan Izin Akses Penuh (<i>Read, Write dan Execute</i>) pada <i>Directory</i> DVWA.....	55
4.22	Tampilan Izin Akses Penuh (<i>Read, Write dan Execute</i>) pada <i>Directory</i> DVWA.....	56
4.23	Akses Subdirektori Config pada Direktori DVWA.....	56

4.24	Salin <i>File</i> Konfigurasi <i>Template</i>	56
4.25	Mengecek Alamat IP dari Lingkungan <i>Virtual Machine</i> yang Digunakan.....	57
4.26	Tampilan Isi <i>File</i> Konfigurasi DVWA Sebelum Mengalami Perubahan.....	58
4.27	Tampilan Isi <i>File</i> Konfigurasi DVWA Setelah Mengalami Perubahan.....	58
4.28	Pengaktifan dan Pengecekan Status MySQL.....	59
4.29	Menjalankan Shell Sebagai Pengguna <i>Root</i>	59
4.30	Masuk ke MySQL atau MariaDB <i>Command Line Interface</i>	60
4.31	Membuat <i>Database</i>	60
4.32	Membuat Pengguna Baru.....	60
4.33	Memberikan Semua Hak Akses (<i>Full Privileges</i>) Kepada Pengguna Baru.....	60
4.34	Pengaktifan dan Pengecekan Status <i>Web Server</i> Apache2.....	61
4.35	Dua Konfigurasi PHP pada <i>File</i> <i>php.ini</i> Sebelum Diubah.....	61
4.36	Dua Konfigurasi PHP pada <i>File</i> <i>php.ini</i> Setelah Diubah.....	62
4.37	Melakukan Akses <i>File</i> <i>50-server.cnf</i>	62
4.38	Pengaturan Konfigurasi <i>bind-address</i> pada <i>File</i> <i>50-server.cnf</i> Sebelum Diubah.....	62
4.39	Pengaturan Konfigurasi <i>bind-address</i> pada <i>File</i> <i>50-server.cnf</i> Setelah Diubah.....	63
4.40	Melakukan Akses <i>File</i> <i>ports.conf</i>	63
4.41	Pengaturan Konfigurasi <i>Listen</i> pada <i>File</i> <i>ports.conf</i> Sebelum Diubah.....	64
4.42	Pengaturan Konfigurasi <i>Listen</i> pada <i>File</i> <i>ports.conf</i> Setelah Diubah.....	64
4.43	Memulai Kembali Apache2.....	64
4.44	Memulai Kembali MySQL.....	64
4.45	Tampilan Halaman <i>Login Web Application</i> DVWA.....	65
4.46	<i>Input Username</i> dan <i>Password</i> pada <i>Form Login</i> DVWA.....	65
4.47	Tampilan Halaman Pengaturan (<i>Setup</i>) Awal DVWA.....	66
4.48	Melakukan <i>Create / Reset Database</i> DVWA.....	66
4.49	Tampilan Utama <i>Menu</i> Kerentanan DVWA.....	67
4.50	Tampilan Pencarian Burp Suite pada Mesin Pencari Google.....	68
4.51	<i>Form Input Email</i> pada <i>Menu Download</i> Burp Suite pada PortSwigger.....	68
4.52	Memilih Jenis Edisi Burp Suite dan Sistem Operasi yang Akan Digunakan.....	69
4.53	Proses Pengunduhan Burp Suite.....	69
4.54	Menjalankan <i>File</i> Unduhan Burp Suite Melalui <i>Terminal PowerShell</i>	69
4.55	Tampilan Awal Jendela <i>Setup</i> Pemasangan Burp Suite.....	70
4.56	Tampilan Proses Instalasi Burp Suite.....	70

4.57	Burp Suite <i>Icon</i> Setelah Proses Instalasi.....	71
4.58	Tampilan Utama Burp Suite.....	71
4.59	Tampilan Hasil Pencarian OWASP ZAP pada Mesin Pencari Google.....	72
4.60	<i>Linux Installer</i> OWASP ZAP.....	73
4.61	Proses Pengunduhan OWASP.....	73
4.62	Memberikan Hak Akses <i>Execute</i> pada <i>File</i> ZAP_2_15_0_unix.sh.....	73
4.63	Menjalankan <i>File Installer</i> ZAP.....	73
4.64	Tampilan Awal Jendela Instalasi OWASP ZAP.....	74
4.65	Proses Instalasi OWASP ZAP.....	74
4.66	Tampilan Akhir Jendela Instalasi OWASP ZAP.....	75
4.67	Tampilan Pencarian OWASP ZAP pada Kali Linux.....	75
4.68	Tampilan Fitur pada OWASP ZAP.....	76
4.69	Pengecekan SQLMap <i>version</i>	76
4.70	Proses Pembaharuan Versi SQLMap pada Kali Linux.....	77
4.71	Pengecekan Kembali Versi SQLMap pada Kali Linux.....	77
4.72	Pemasangan Whois pada Kali Linux.....	77
4.73	Pengecekan Versi Whois.....	78
4.74	Pengecekan Versi Nmap.....	78
4.75	Pemasangan theHarvester pada Kali Linux.....	78
4.76	Menjalankan dan Mengecek Versi theHarvester yang Terpasang.....	79
4.77	Pemasangan Wireshark pada Kali Linux.....	79
4.78	Pengecekan Versi Wireshark.....	80
4.79	Menjalankan Wireshark pada Kali Linux.....	80
4.80	Tampilan Awal Menu Utama Wireshark.....	81
4.81	Pemasangan Wget pada Kali Linux.....	81
4.82	Pengecekan Versi Wget.....	82
4.83	Pengecekan Versi Metasploit yang Terpasang pada Kali Linux	82
4.84	Menjalankan Metasploit pada Kali Linux.....	83
4.85	Pemasangan Netcat pada Kali Linux.....	83
4.86	Pemasangan WhatWeb pada Kali Linux.....	84
4.87	Pengecekan Versi WhatWeb.....	84
4.88	Pemasangan Hydra pada Kali Linux	84
4.89	Pengecekan Versi Hydra	84

4.90	Pemasangan Wfuzz pada Kali Linux	85
4.91	Pengecekan Versi Wfuzz	85
4.92	Pemasangan Nikto pada Kali Linux	85
4.93	Pengcekan Versi Nikto	85
4.94	Membuat dan Mengakses <i>Directory Khusus Automation Script</i>	86
4.95	Membuat dan Memberi Akses <i>Execute</i> pada File “install_tools”	86
4.96	Membuat File “Log_File.txt”	87
4.97	Shebang dan <i>Function</i> “command_exists”	89
4.98	<i>Function</i> “instal_tool”	90
4.99	<i>Function</i> “instal_tools”	90
4.100	Memanggil <i>Function</i> Utama “install_tools”	90
4.101	Membuat dan Mengecek File “F2_InformationGathering” telah Tersedia.....	91
4.102	Memberikan <i>Privilege Execute</i> pada <i>User</i>	91
4.103	Shellbang dan <i>Function</i> “resolve_ip”	99
4.104	<i>Input Target</i> dan Pengecekan Format IP.....	99
4.105	<i>Ping Target</i>	99
4.106	<i>Function</i> “run_whois”	100
4.107	<i>Function</i> “run_curl_headers”	101
4.108	<i>Function</i> “run_nmap”	102
4.109	<i>Function</i> “run_snmp_sweep”	102
4.110	<i>Function</i> “run_theharvester”	103
4.111	<i>Function</i> “run_dig”	104
4.112	<i>Function</i> “run_host”	104
4.113	<i>Function</i> “run_nslookup”	105
4.114	<i>Function</i> “run_wget”	106
4.115	<i>Function</i> “run_netcat”	106
4.116	<i>Function</i> “run_whatweb”	107
4.117	<i>Function</i> “run_sublist3r”	107
4.118	<i>Function</i> “run_metagoofil”	108
4.119	<i>Function</i> “run_all_tools”	109
4.120	<i>Function</i> “display_menu”	110
4.121	<i>Function</i> “run_tool”	111
4.122	<i>Do While Loop</i> untuk <i>Display Menu</i>	111

4.123 Membuat dan Memberikan Hak Akses <i>Execute File</i> “F4_VulnerabilityAnalysis”	113
4.124 Mengecek dan Memastikan Hak Akses <i>Exectue File</i> “F4_VulnerabilityAnalysis”	113
4.125 <i>Function</i> “run_sqlmap”	119
4.126 <i>Function</i> “run_nmap_vuln”	120
4.127 <i>Function</i> “run_nikto”	120
4.128 <i>Function</i> “run_all_vuln_analysis”	121
4.129 <i>Function</i> “display_menu”	121
4.130 <i>Function</i> “run_tool”	122
4.131 <i>Function</i> “resolve_ip”	122
4.132 <i>Loop Main Menu Execution</i>	123
4.133 Membuat <i>File</i> “F5_Exploitation” dan Memberi Hak Akses <i>Execute</i>	124
4.134 Memastikan Hak Akses <i>Execute</i> pada <i>File</i> “F5_Exploitation”	124
5.1 Hasil Pemindaian <i>Manual Whois</i> pada Fase <i>Information Gathering</i>	138
5.2 <i>Ping Host</i> dalam Rentang Alamat IP “192.168.81.0/24” oleh Nmap	139
5.3 Pemindaian <i>Port</i> pada Alamat IP “192.168.81.2” oleh Nmap	140
5.4 Pemindaian <i>Port</i> pada Alamat IP “192.168.81.130” oleh Nmap	140
5.5 Pemindaian Jaringan pada Alamat IP “192.168.81.130” oleh Nmap	141
5.6 Pendeteksian Layanan dan Sistem Operasi pada Alamat IP “192.168.81.130”	141
5.7 Pendeteksian Layanan dan Sistem Operasi Lebih Komprehensif oleh Nmap	142
5.8 Hasil Pemindaian <i>Domain</i> “dvwa.local” oleh theHarvester	143
5.9 Hasil Pemindaian Komprehensif Pada Seluruh <i>Source Data</i> oleh theHarvester	144
5.10 Membuka Menu Proxy pada Burp Suite	145
5.11 Tampilan <i>Default Proxy Setting</i>	145
5.12 Tampilan <i>Detail Proxy Setting</i>	146
5.13 Tampilan Awal Hasil <i>Intercept Website</i> DVWA	146
5.14 Informasi Awal yang Diperoleh saat <i>Login</i>	146
5.15 Struktur HTML DVWA pada Hasil <i>Response</i> Burp Suite	147
5.16 HTTP <i>History</i> saat Akses Setiap Halaman pada <i>Website</i> DVWA	147
5.17 Akses <i>Directory</i> dari <i>Local Image</i>	148
5.18 Akses <i>Directory</i> dari <i>Users Profile Image</i>	148
5.19 Menu Site Map dengan Hasil Proyeksi <i>Directory</i> yang telah Dikunjungi	149
5.20 Tampilan Wireshark Pertama Dibuka	151
5.21 Memilih <i>Interface</i> “Eth0” yang Melayani Target DVWA	151

5.22	Melakukan <i>Start Capture</i>	152
5.23	Menganalisa Protocol TCP dari Source IP "192.168.81.130"	152
5.24	<i>Port Scanning</i> Menggunakan Nmap.....	153
5.25	<i>Port Scanning</i> Menggunakan Nmap <i>NSE Script Banner</i>	154
5.26	Koneksi ke <i>Port</i> 80 dan 3306 IP 192.168.81.130 Menggunakan Netcat	155
5.27	<i>Scanning Server Web</i> DVWA pada IP 192.168.81.130 Menggunakan Netcat	156
5.28	Memasukan <i>Url</i> "http://192.168.81.130/DVWA"	157
5.29	Proses <i>Active Scan</i> OWASP ZAP.....	157
5.30	<i>Alerts Scan</i> OWASP ZAP.....	158
5.31	Hasil <i>Spider</i> OWASP ZAP.....	158
5.32	Memastikan Pada <i>Menu Proxy Intercept</i> Telah Aktif.....	162
5.33	<i>Login</i> Menggunakan <i>Username</i> dan <i>Password</i>	162
5.34	Hasil <i>Intercept</i> saat <i>Login</i> pada Kerentanan <i>Brute Force Level Low</i>	163
5.35	Mengirimkan Hasil <i>Intercept</i> ke Intruder.....	163
5.36	Memilih Jenis <i>Attack Cluster Bomb</i>	164
5.37	Tampilan dari Intruder Sebelum Diatur <i>Payload Positions</i>	164
5.38	Tampilan dari Intruder Setelah Diatur <i>Payload Positions</i>	164
5.39	Menambahkan Isi <i>List Username</i> pada <i>Payload</i> Pertama.....	165
5.40	Membuat dan Menambahkan Isi <i>List Password</i> pada <i>Payload</i> Kedua.....	165
5.41	Tampilan <i>Grep – Extract</i>	166
5.42	Tampilan Jendela Untuk Mendefinisikan <i>Grep item</i>	167
5.43	<i>Fetch Response</i> untuk <i>Grep</i> Pesan Kesalahan <i>Login</i>	167
5.44	Menambahkan Kolom Tambahan pada Hasil <i>Cluster Bomb Brute Froce</i>	168
5.45	Melakukan <i>Start Attack Brute Force</i>	168
5.46	Hasil <i>Intruder Attack Cluster Bomb Brute Force</i> terhadap http:192.168.81.130.....	169
5.47	Hasil <i>Query</i> pada Kerentanan <i>SQL Injection</i>	170
5.48	Menjalankan <i>Script File</i> "install_tools" dan Hasil Instalasi.....	171
5.49	Menjalankan <i>Script File</i> "F4_VulnerabilityAnalysis" dan Meminta Inputan <i>User</i>	178
5.50	Menampilkan Opsi atau Pilihan Menu untuk Memilih Alat Pindai.....	178
5.51	Hasil Pemindaian Nmap pada IP "192.168.81.130"	181
5.52	Waktu <i>Execution</i> Nmap pada IP "192.168.81.130"	181
5.53	Hasil Pemindaian Nikto pada IP "192.168.81.130"	184
5.54	Waktu <i>Execution</i> Nikto pada IP "192.168.81.130"	184

5.55 Hasil Pemindaian SQLMap pada IP “192.168.81.130.....	187
5.56 Proses Eksploitasi <i>Script</i> “F5_Exploitation”	189
5.57 Hasil Eksploitasi SQL <i>Injection</i> Menggunakan SQLMap.....	195
5.58 Hasil <i>Brute Force</i> Menggunakan Wfuzz	212

DAFTAR LAMPIRAN

1. *Screen Capture Manual Exploitation Kerentanan CSRF*..... 227
2. *Screen Capture Manual Exploitation Kerentanan File Inclusion* 230

DAFTAR SEGMENT PROGRAM

4.1	Isi <i>function</i> “command_exists”	87
4.2	Isi <i>function</i> “install_tool”	87
4.3	Isi <i>function</i> “install_tools”	88
4.4	Isi Lengkap dari <i>File</i> “F2_InformationGathering”	92
4.5	Isi Lengkap dari <i>File</i> “F4_VulnerabilityAnalysis”	114
4.6	Isi Lengkap dari <i>File</i> “F5_Exploitation”	124
5.1	Hasil <i>Information Gathering</i> Secara <i>Manual</i> Menggunakan <i>Whois</i>	137
5.2	Isi <i>File</i> <i>Javascript</i> DVWA Berhasil Diperoleh Menggunakan <i>Burp Suite</i>	149
5.3	Hasil <i>Information Gathering Script</i> “F2_InformationGathering”	171
5.4	Hasil <i>Vulnerability Analysis Nmap Script</i> “F4_VulnerabilityAnalysis”	179
5.5	Hasil <i>Vulnerability Analysis Nikto Script</i> “F4_VulnerabilityAnalysis”	182
5.6	Hasil <i>Vulnerability Analysis SQLMap Script</i> “F4_VulnerabilityAnalysis”	185
5.7	Hasil <i>Exploitation SQL Injection Script</i> “F5_Exploitation”	189
5.8	Hasil <i>Exploitation Brute Force</i> “F5_Exploitation” dengan <i>Hydra</i>	198
5.9	Hasil <i>Exploitation Brute Force</i> “F5_Exploitation” dengan <i>Wfuzz</i>	211
5.10	Hasil <i>Exploitation File Inclusion</i> “F5_Exploitation” dengan <i>Wfuzz</i>	214