Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

<u>Student Note</u>: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	JM Security (JMS)
Contact Name	Janice Mitchell
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	01/20/2024	Janice Mitchell	
002	01/22/2024	Janice Mitchell	added additional screenshots
003	1/25/2024	Janice Mitchell	finalize summary and review vulnerability details for accuracy for final submission

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.

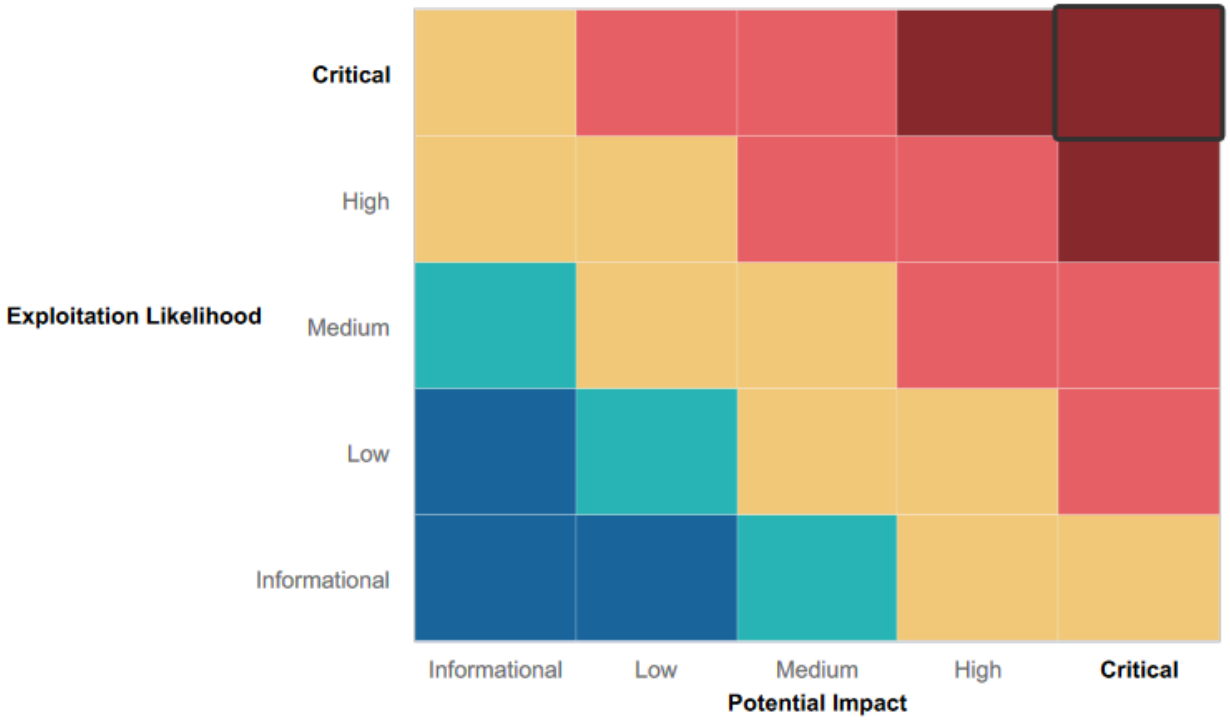
Executive Summary of Findings

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.

- Web Application includes validation criteria in several fields which delayed efforts to exploit possible vulnerabilities of this medium (specifics discussed in the vulnerability findings section).

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.

- Multiple areas of vulnerability on the web application.
- Linux machines with vulnerable ports/processes allowing access and subsequent directory traversal/enumeration/privilege escalation.
- Windows machines with vulnerable ports/processes allowing access and subsequent directory traversal/enumeration/privilege escalation ultimately culminating with domain control administrative access.

Executive Summary

(Includes screenshots for illustration of information encountered/used)

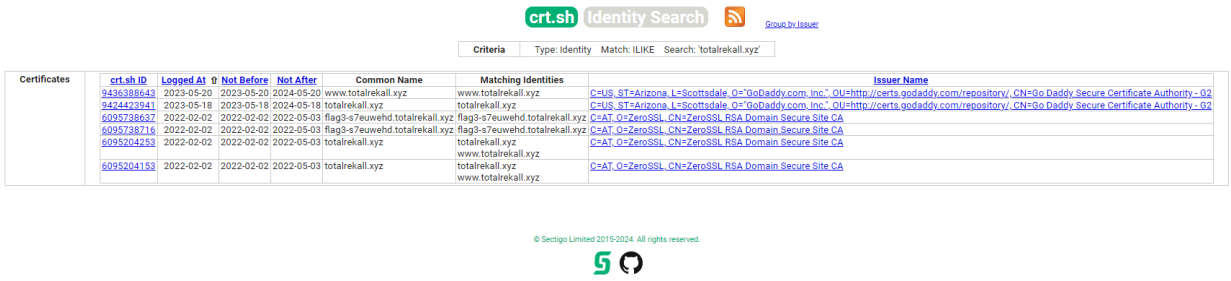
We began our investigation by looking for publicly available information via various sources including google searches, site registry details, certificate details, DNS records, and affiliated repositories for the domain.

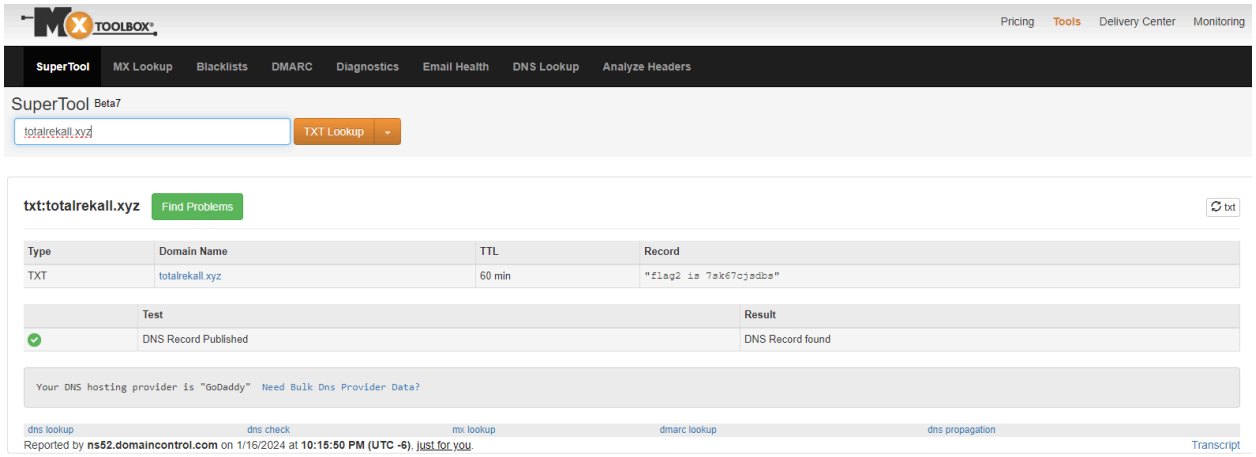
Queried **whois.nic.xyz** with "**totalrekall.xyz**"...

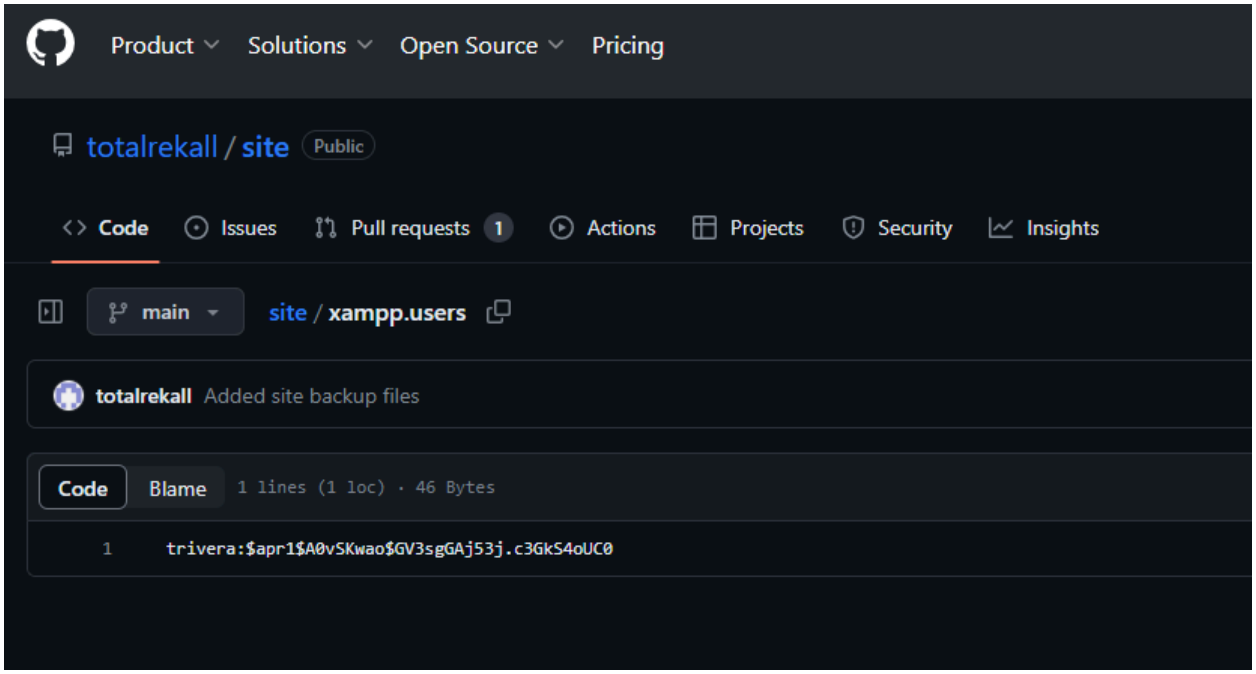
```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-08-31T16:55:47.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2024-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in
Admin Email: Please query the RDDS service of the Registrar of Record identified in this
Tech Email: Please query the RDDS service of the Registrar of Record identified in this
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in th
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-01-17T01:16:19.0Z <<<
```

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

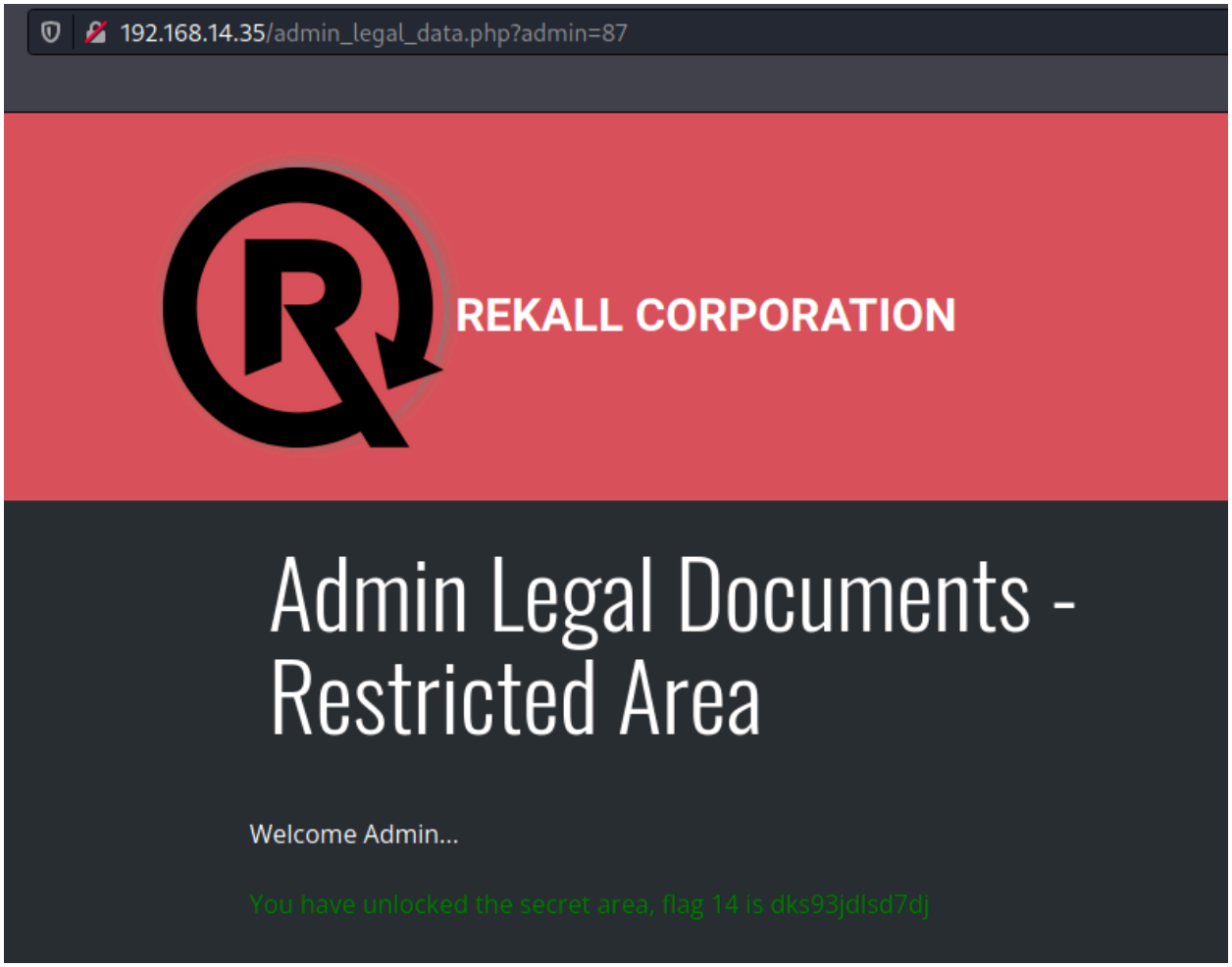
```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, 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:
```



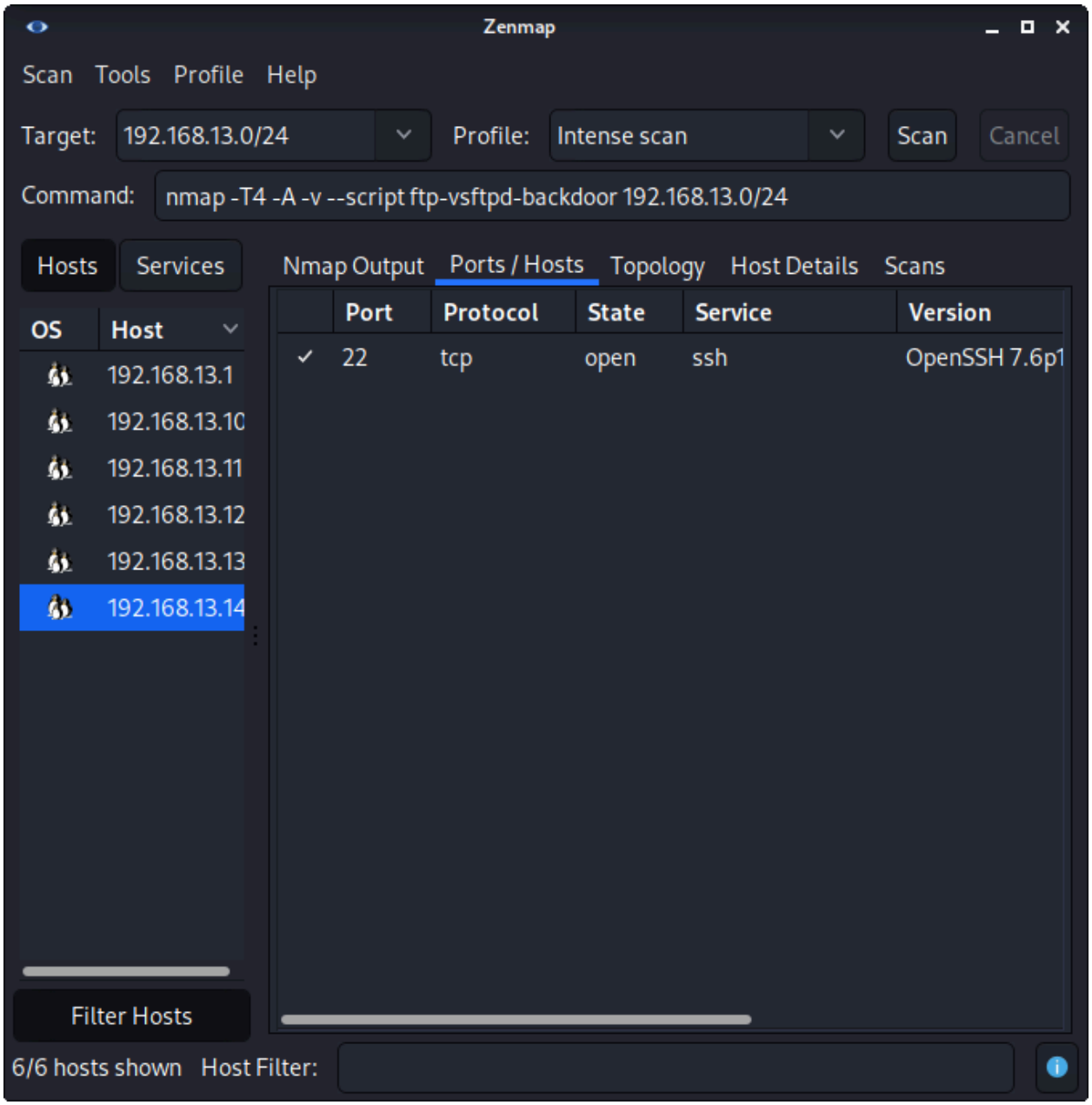




We visited the web application and attempted several common methods of attack to test the defenses of the publicly facing app As vulnerabilities were identified and exploited (see vulnerability details starting on page 20), we were able to move further within the site into areas limited to administrative access. While in the process of attempting to compromise the site, we identified fields that included input validation which prevented some basic exploits, but which were ultimately able to be worked around.



Next, we ran a scan on the network to determine the available hosts and which operating systems are running, along with what open ports and protocols could be possible methods of entry onto the network.

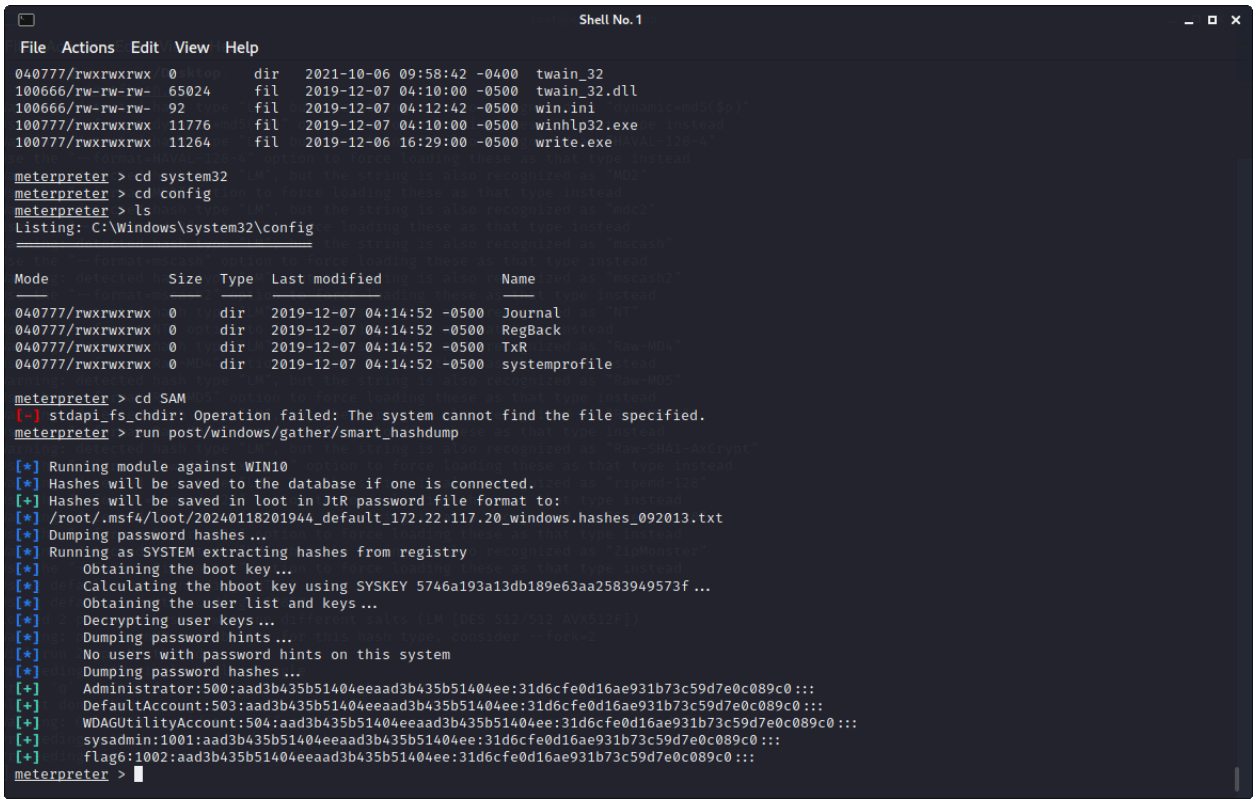


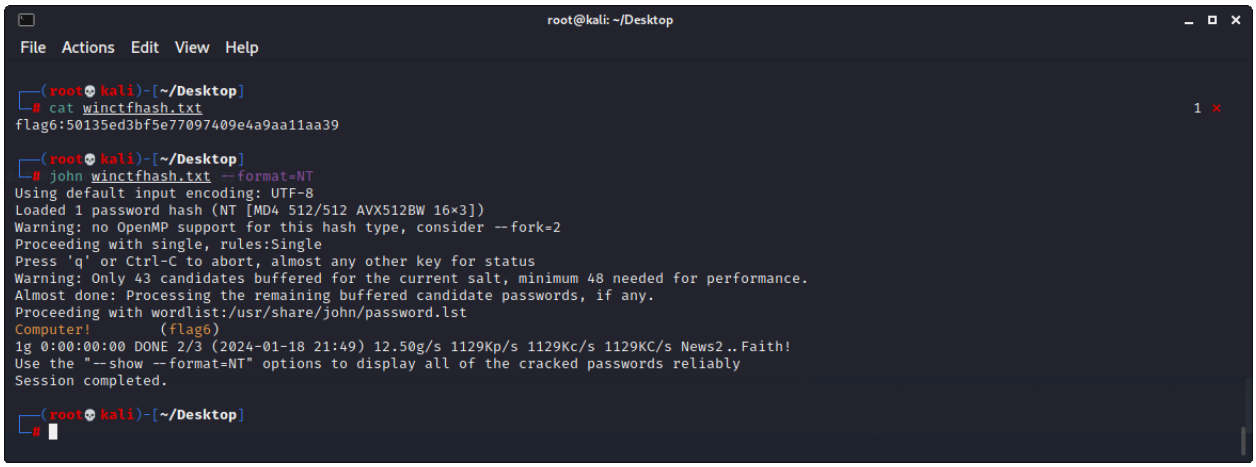
```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-17 19:49 EST
Nmap scan report for 192.168.13.13
Host is up (0.000094s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-title: Home | Drupal CVE-2019-6340
|_http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.09 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.77 seconds

┌──(root💀kali)-[~]
└─#
```

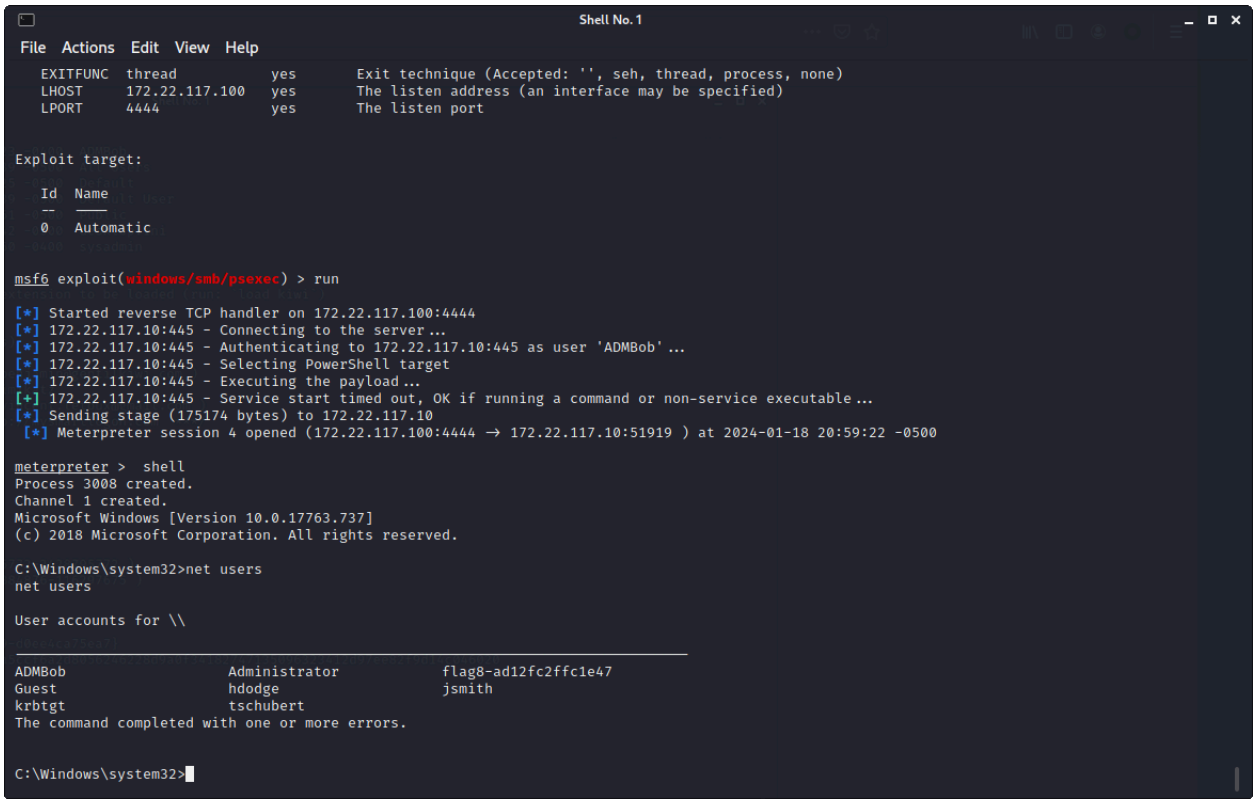
Using the IP addresses of the identified machines, we ran a scan using Nessus to determine what known exploits they could be vulnerable to, including the industry codes for those vulnerabilities as specified by community members who contribute to the CVE database. One example of a critical finding pictured here:

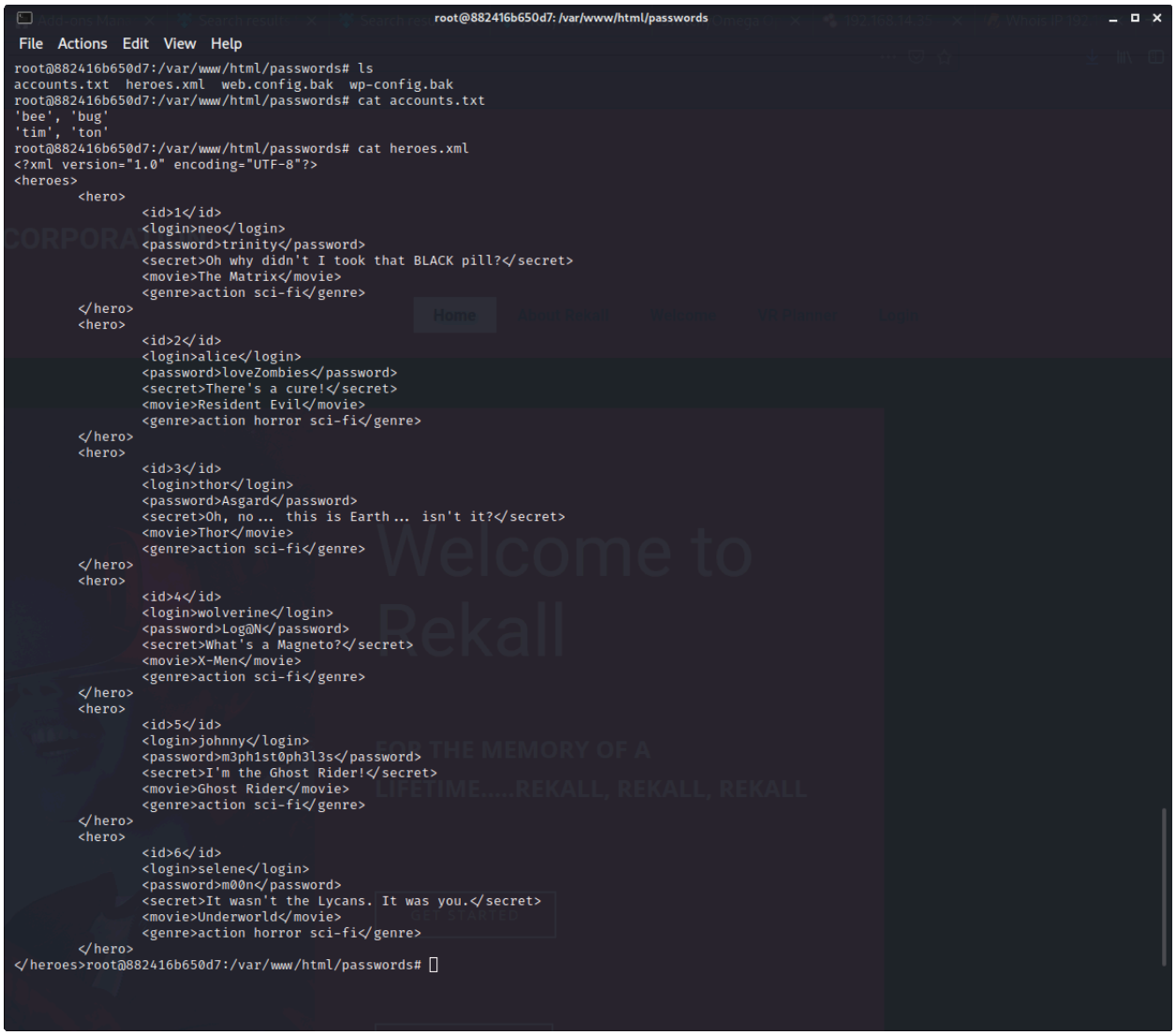
Using the information gathered, various attempts were made to access machines running either Linux or Windows operating systems. Vulnerabilities discovered are outlined in detail starting on page 20 of this report.

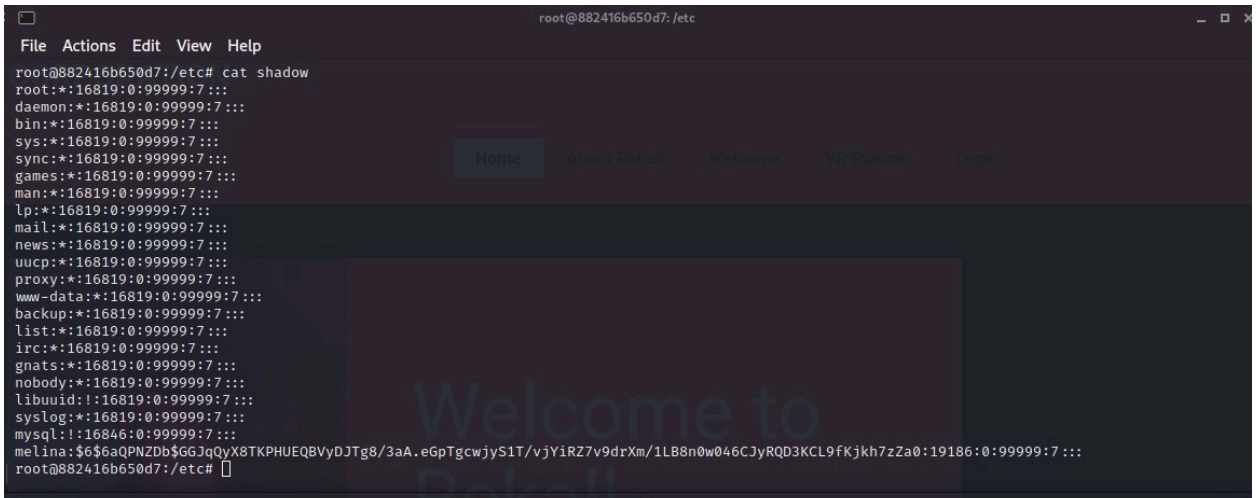
After initially gaining access, we were able to traverse directories to get information necessary to move between machines using logon credentials either stored insecurely, brute-forced, or deduced from decryption of password hashes obtained after escalating to root privilege. Ultimately, we were able to compromise 5 Linux machines, a Windows 10 machine, and the Windows based Domain Control.

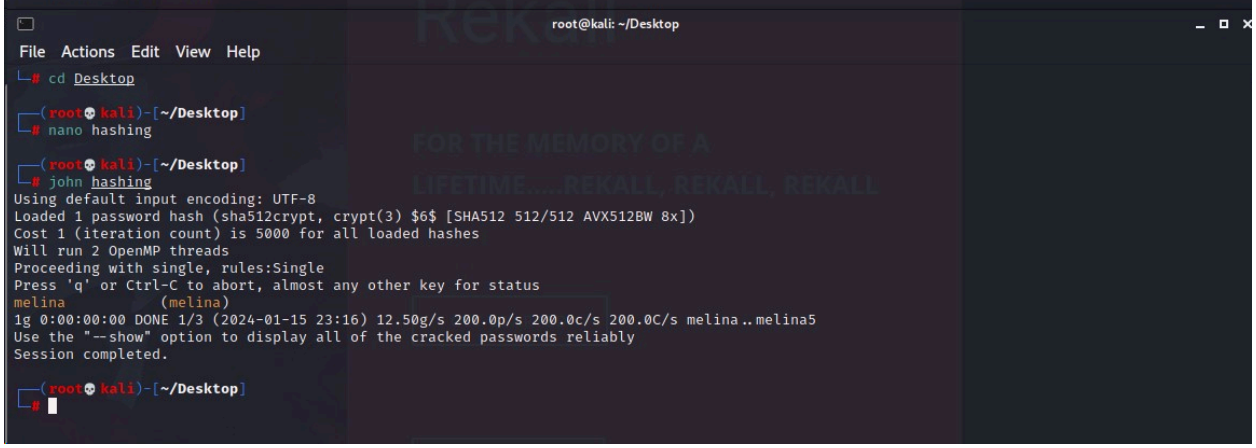


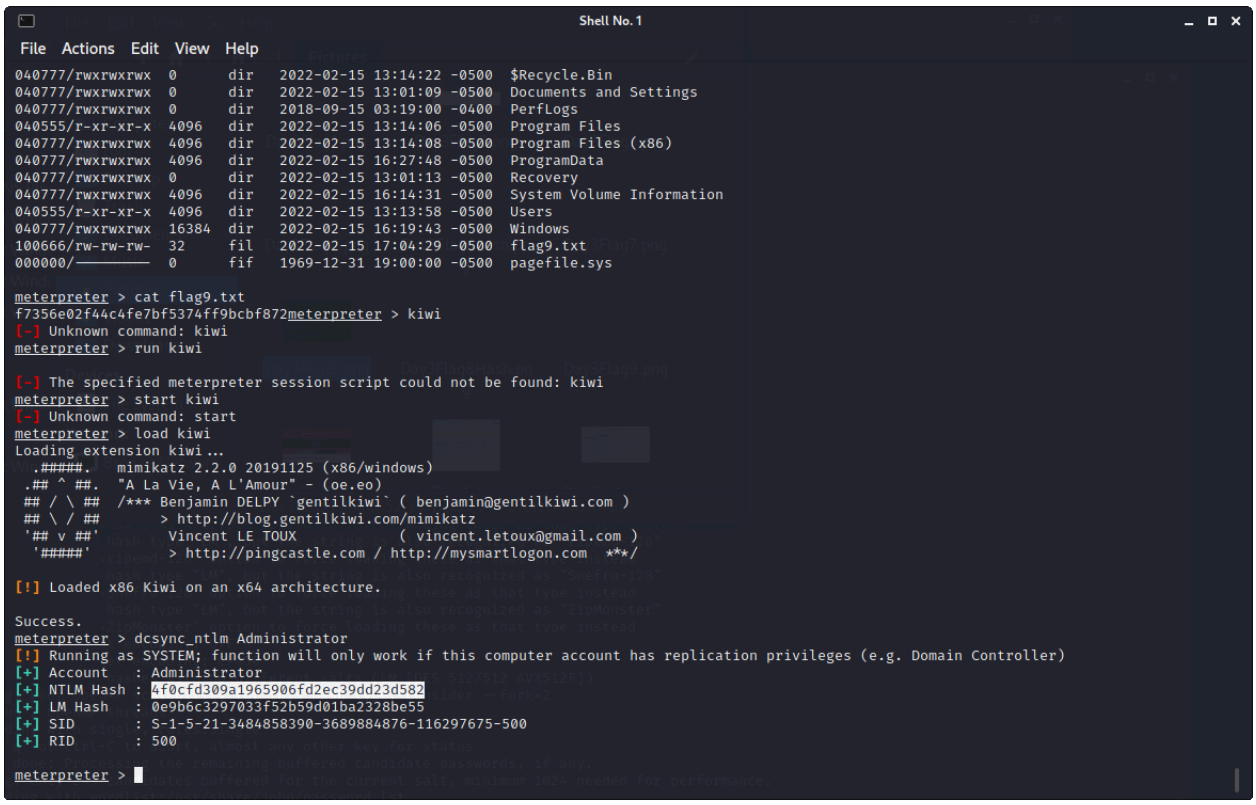












Summary Vulnerability Overview

Vulnerability	Severity
XSS Vulnerabilities	Critical
Sensitive Data Exposure	Critical
LFI Vulnerability	Critical
SQL Injection Vulnerability	Critical
Command Injection Vulnerability	Critical
PHP Injection Vulnerability	Critical
Apache Tomcat JSP Vulnerability (CVE-2017-12617)	High
Shocking Exploit Vulnerability (CVE-2014-6271)	High
Apache Struts Exploit Vulnerability (CVE-2017-2638)	High
Drupal Exploit Vulnerability (CVE-2019-6340)	High
FTP Vulnerability	Medium
SLMail Service Vulnerability (CVE-2003-0264)	Medium
Cached Credential Exposure (Kiwi Exploit)	Medium

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

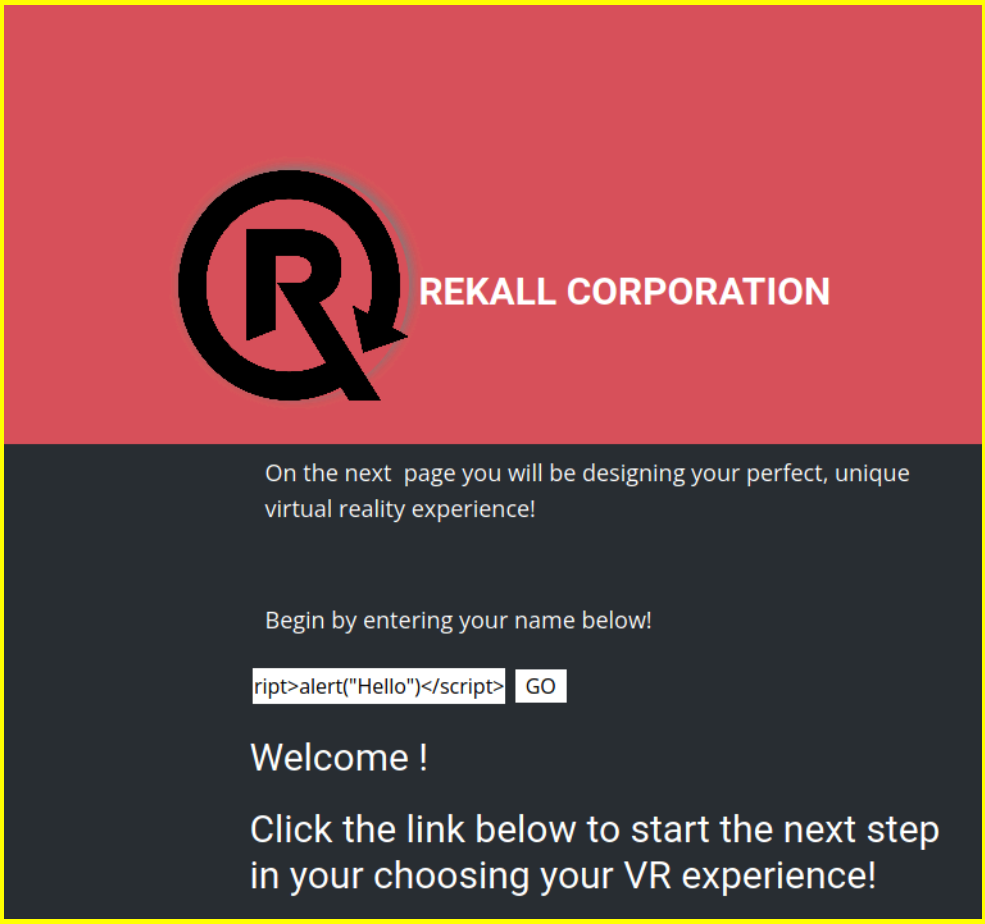
Scan Type	Total
Hosts	totalrekall.com 192.168.14.35 Linux 192.168.13.10; 192.168.13.11; 192.168.13.12; 192.168.13.13; 192.168.13.14 Windows10 172.22.117.20 WindowsDC 172.22.117.10
Ports	21(FTP), 25(SMTP), 80 (HTTP), 110 (POP3), 135 (RPC), 8009 (TCP), 8080 (HTTP)

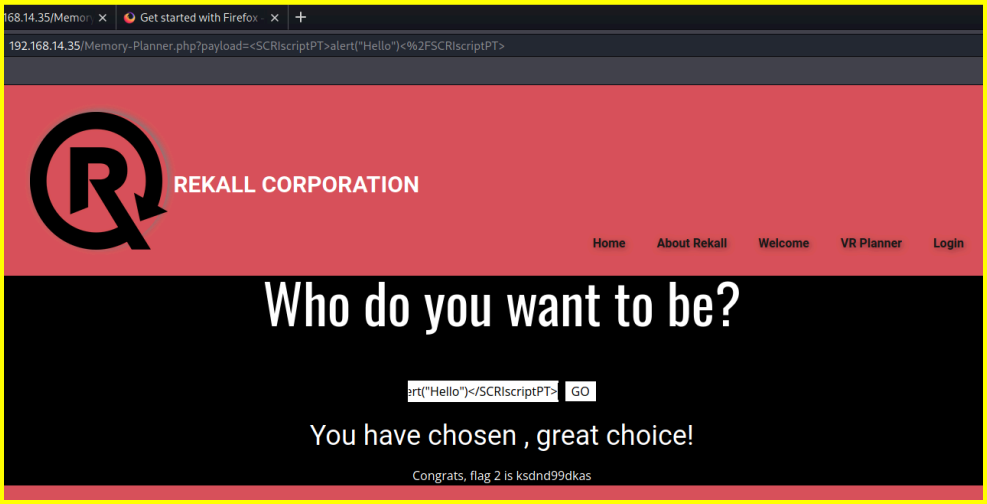
Exploitation Risk	Total
Critical	6
High	4
Medium	3
Low	0

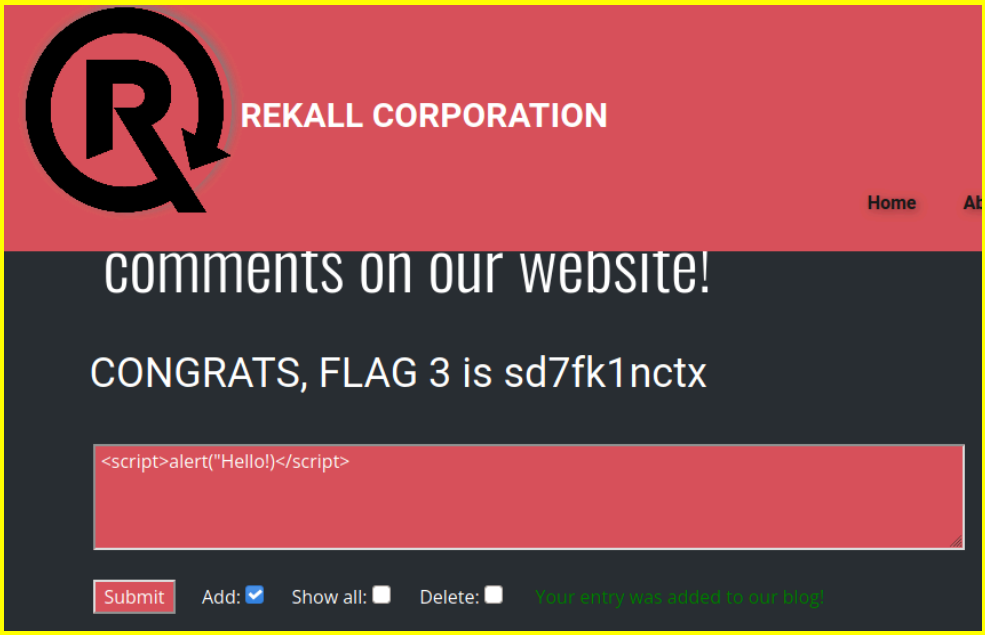
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	The welcome page, memory-planner page, and comments pages are vulnerable to cross site scripting attacks. While input validation appears to have been attempted to prevent this from being exploited on the memory-planner, and the comments pages, after trying various workarounds, both were able to be circumvented. This could potentially lead to user login sessions being hijacked and compromised.

Images



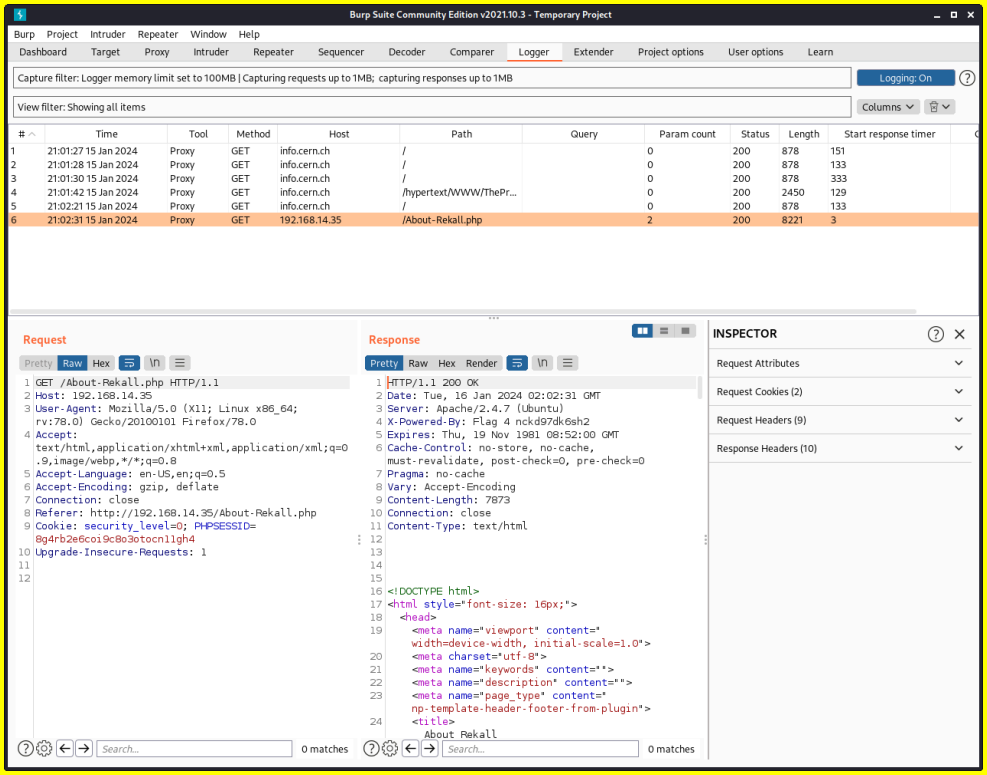


	
Affected Hosts	Total Rekall Web Application
Remediation	• Implement stricter input validation workarounds, including those that prohibit common scripting symbols such as greater than and less than.

Vulnerability 2	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application / Linux OS / Windows OS
Risk Rating	**Critical**
Description	On the web application, the HTTP response header of the About Rekall page includes sensitive information that can be viewed when using a proxy and intercepting the request/response details. Additionally, the HTML coding on the Login page includes the username and password for administrative access. Information stored in these places is easy for any party to access, so it is important that sensitive/confidential data be stored elsewhere. Additionally, the robots.txt file, used to communicate with web crawlers and other web robots, is easily accessible. A threat actor could use this information to identify the location of sensitive data. Information in the public registration data for the domain, include the registrant name "sshuser Alice." User Alice has a password that matches their username, something threat actors are likely to use as a guess when attempting brute force attacks. Because of this, we were able to SSH into the Linux machine using Alice's login credentials. This user has escalated privileges, including access to sensitive data such as password hashes which could be decrypted in order to sign in as other users on the network. Similarly, a password hash associated with a Windows login was located on

	the Github repository for Totalrekall.

Images




```
        <button type="submit" name="form" value="submit">Login</button>

    </form>

Congrats, flag 7 is bcs92sjsk233


          <span style="font-weight: 700;"></span>
        </h1>
      </div>
    </section>
    <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf">
      <div class="u-clearfix u-sheet u-sheet-1">
        <h1 class="u-text u-text-default u-text-1">
        <center>  <span style="font-weight: 900;">Admin Login</span></center>

<!DOCTYPE html>
<html>


<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">

        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

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

    </form>

    </br >
    <font color="red">Invalid credentials!</font>
</div>
```

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

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-08-31T16:55:47.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2024-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in
Admin Email: Please query the RDDS service of the Registrar of Record identified in this
Tech Email: Please query the RDDS service of the Registrar of Record identified in this
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in th
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-01-17T01:16:19.0Z <<<
```

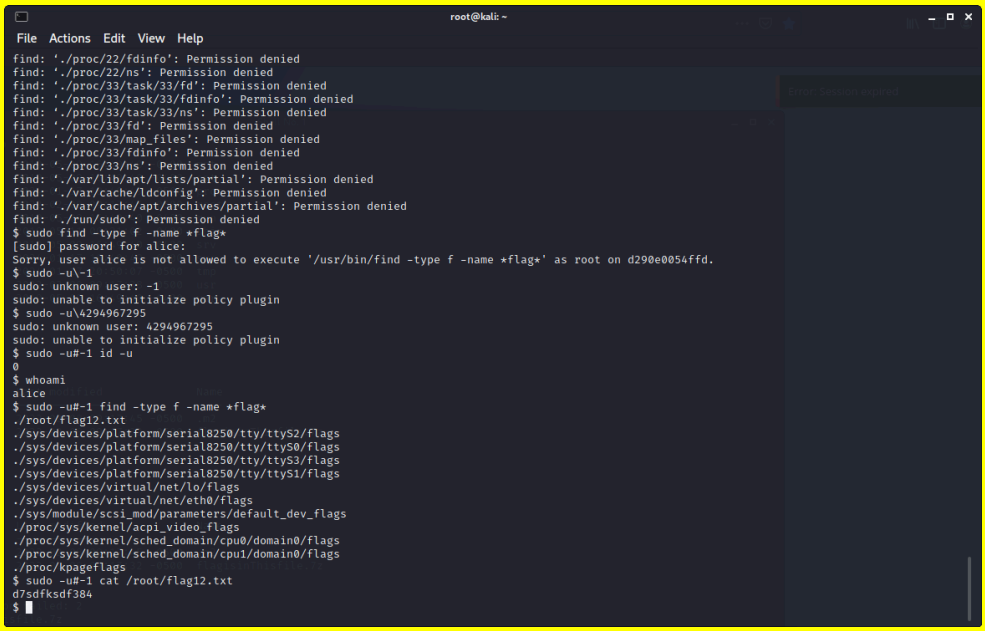
Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

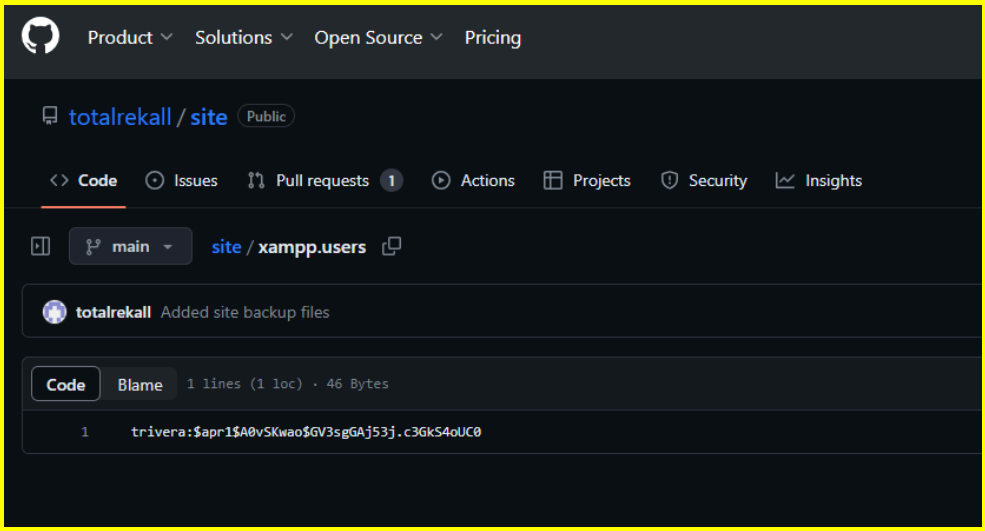
```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, 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:
```

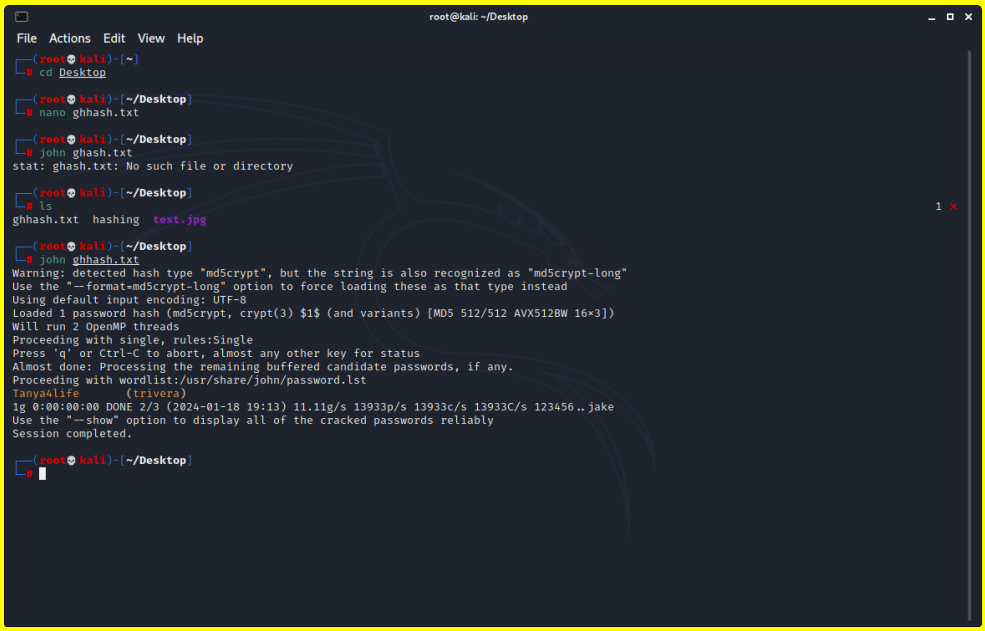
Shell No. 1

File Actions Edit View Help

```
100444/r--r--r--  800   fil   2022-02-28 10:40:30 -0500  sudoers
040755/rwxr-xr-x  4096  dir   2019-12-17 10:01:22 -0500  sudoers.d
100644/rw-r--r--  2084  fil   2013-03-31 22:25:31 -0400  sysctl.conf
040755/rwxr-xr-x  4096  dir   2019-12-17 10:01:11 -0500  sysctl.d
040755/rwxr-xr-x  4096  dir   2019-12-17 10:01:24 -0500  systemd
040755/rwxr-xr-x  4096  dir   2019-12-17 10:00:08 -0500  terminfo
100644/rw-r--r--  8     fil   2019-12-17 10:00:50 -0500  timezone
040755/rwxr-xr-x  4096  dir   2019-12-17 10:01:24 -0500  ubuntu-advantage
100644/rw-r--r--  1260  fil   2013-06-30 21:01:00 -0400  ucf.conf
040755/rwxr-xr-x  4096  dir   2019-12-17 10:01:12 -0500  udev
040755/rwxr-xr-x  4096  dir   2022-02-28 10:40:02 -0500  ufw
040755/rwxr-xr-x  4096  dir   2019-12-17 10:00:38 -0500  update-motd.d
100644/rw-r--r--  222   fil   2014-04-11 17:54:15 -0400  upstart-xsessions
040755/rwxr-xr-x  4096  dir   2019-12-17 10:01:22 -0500  vim
100644/rw-r--r--  158   fil   2014-01-29 08:39:45 -0500  vtrgb
100644/rw-r--r--  4812  fil   2019-04-08 18:55:26 -0400  wgetrc
040755/rwxr-xr-x  4096  dir   2022-02-28 10:40:03 -0500  xml

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

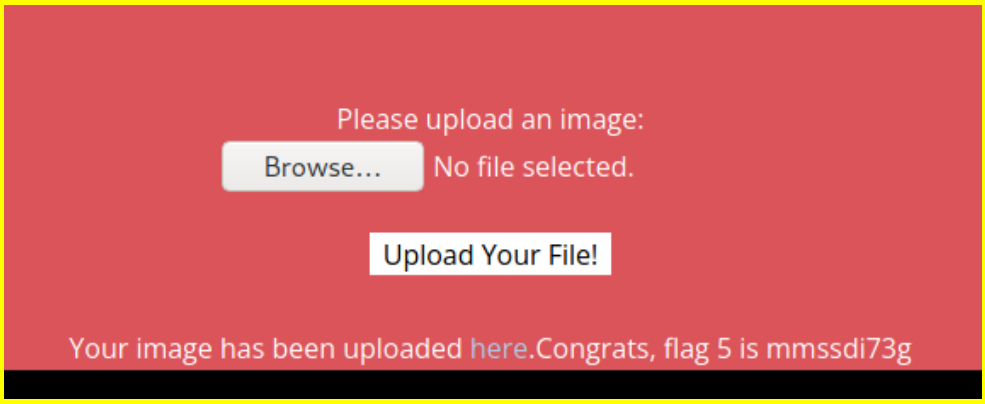


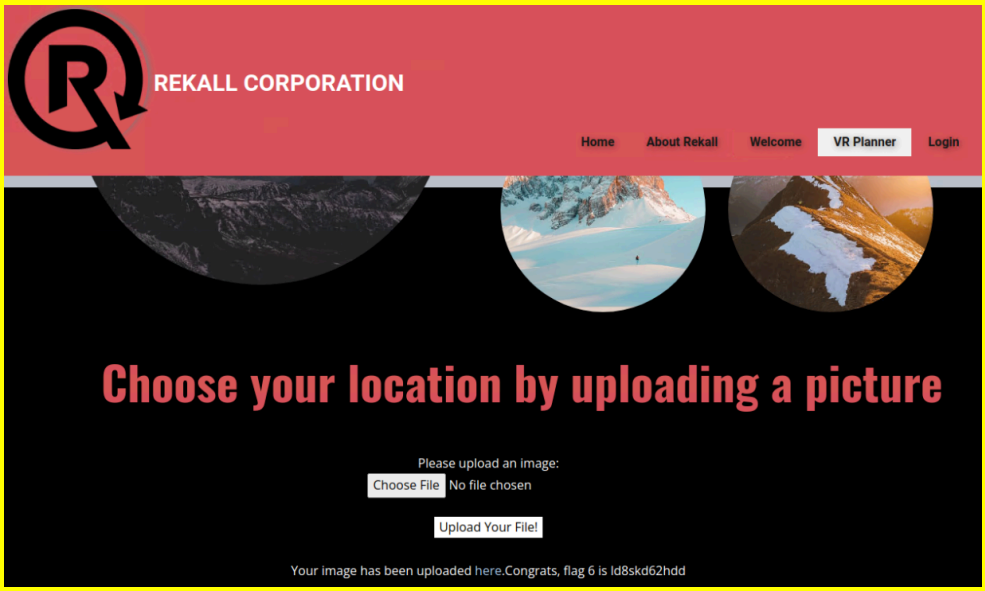




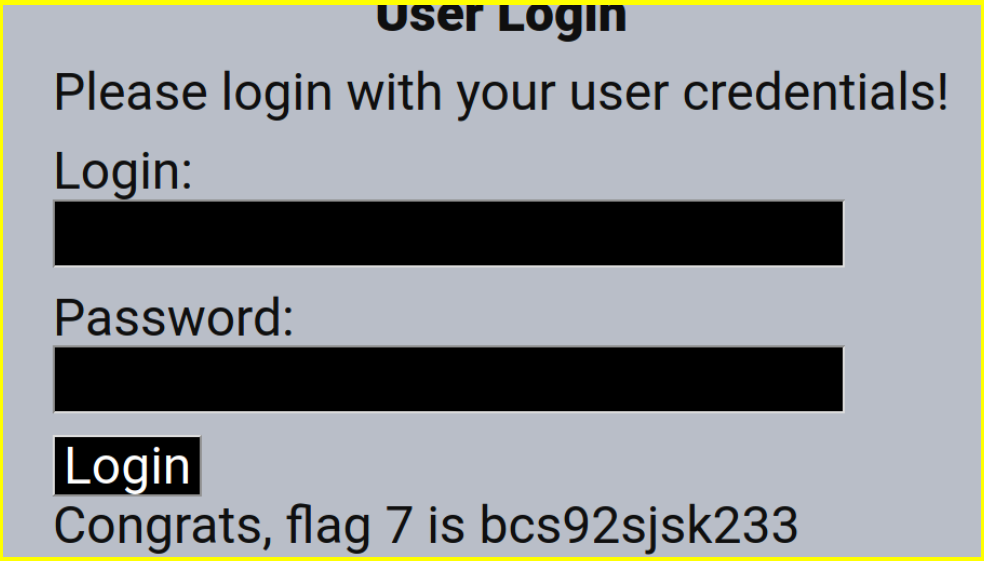
Remediation	• Audit information stored in HTML files and sent in response to HTTP

	requests to remove any unnecessary information which could be used to infiltrate other areas of the network and/or server. ● Store all login information in secure password managers that utilize encryption. ● Secure access to robots.txt file. ● Clear sensitive data from Github repository.

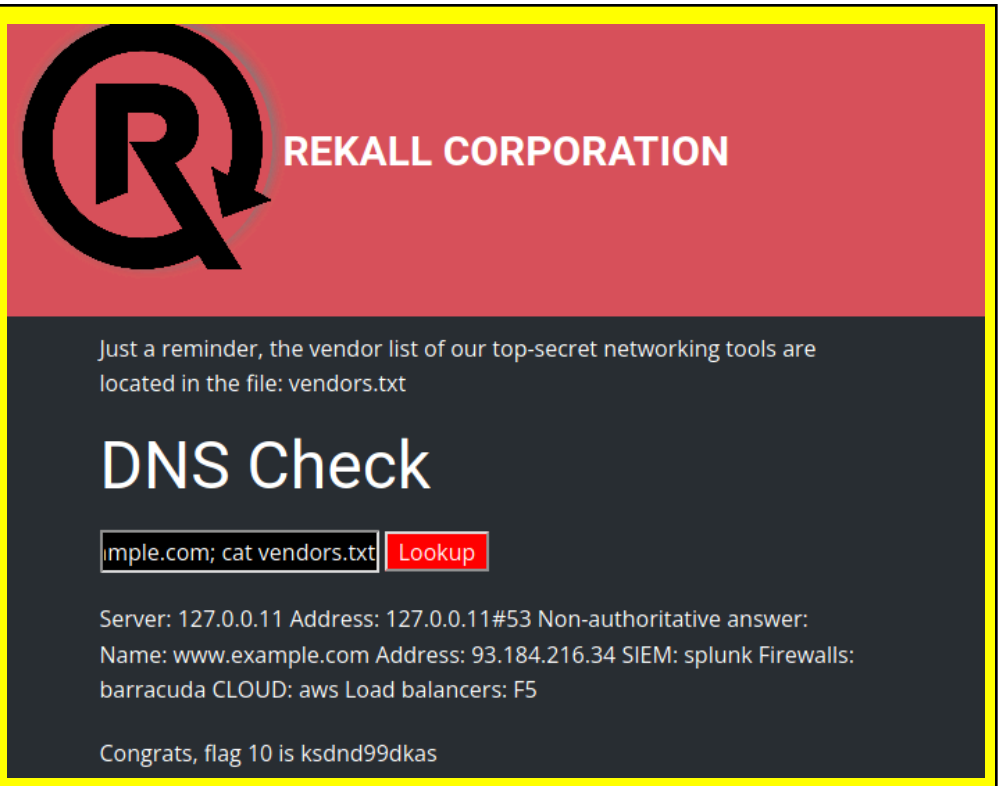
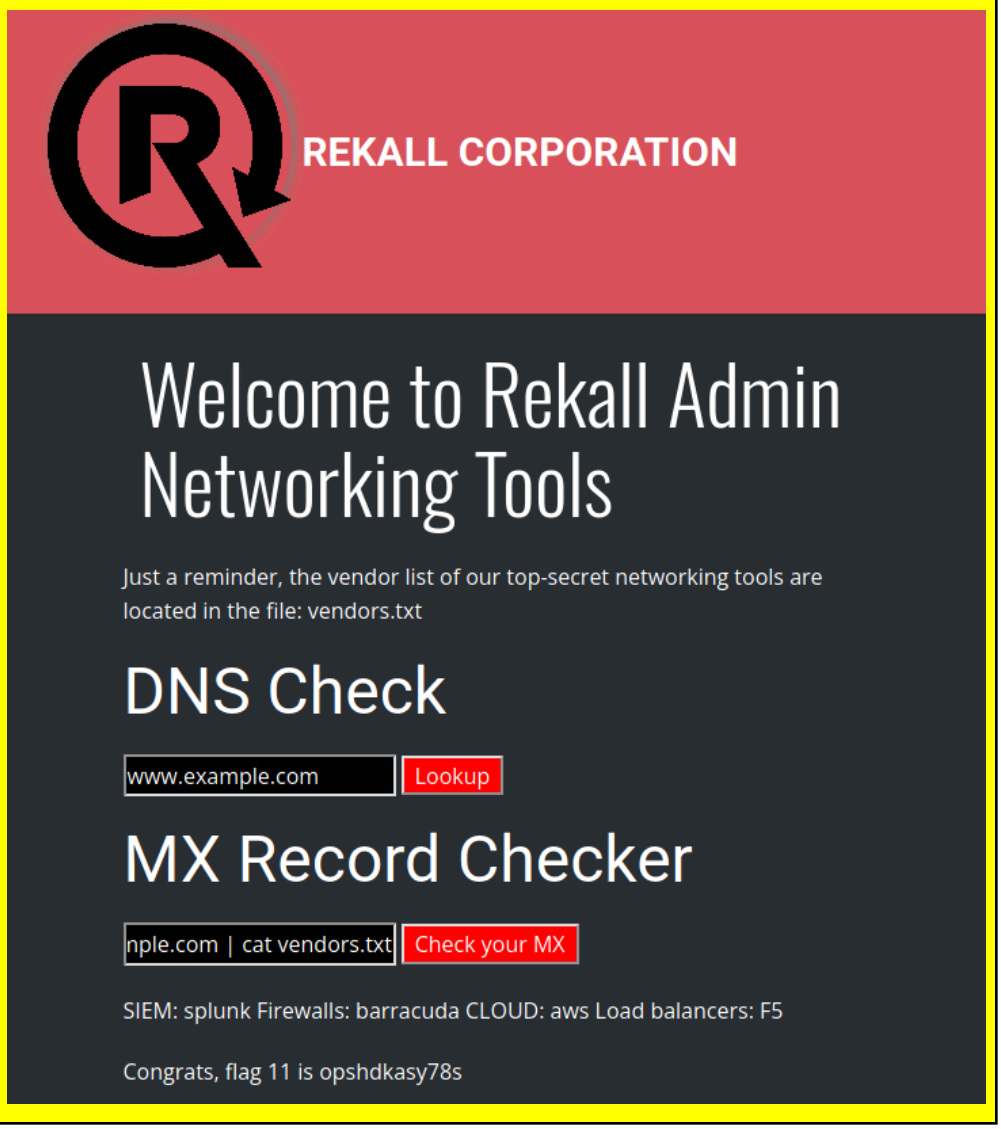
Vulnerability 3	Findings
Title	LFI (Local File Inclusion) Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	On the memory-planner page, where users are prompted to upload image files, it is possible to upload .php files which can be used to execute commands on the host machine. While there is a mitigation in place for the location photo upload, limiting file types uploaded to .jpg image files, it was possible to get around this limitation by changing the file name of the php file to script.php.jpg.
Images	

	
Affected Hosts	Total Rekall Web Application
Remediation	• Implement stronger input validation criteria including validation of the filetype separate from validation of the file extension.

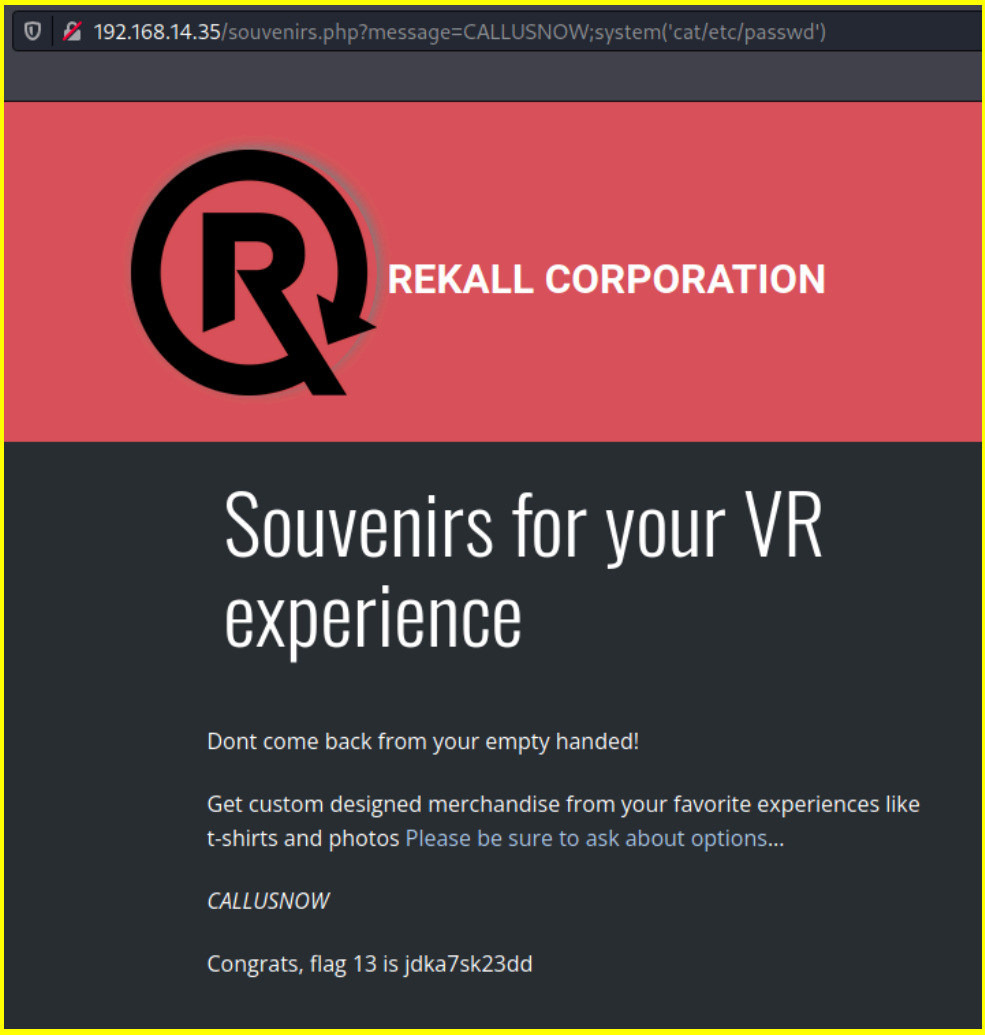
Vulnerability 4	Findings
Title	SQL Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	On the login page, the password field can be exploited to auto login using an entry that includes an always true statement, so if a threat actor knows a username, they can sign in regardless of whether or not they know the password. In the example below, user we were able to log in as 'admin' using the following in the password field: 1' OR '1' = '1

Images	
Affected Hosts	Total Rekall Web Application
Remediation	• Implement input validation limiting the types of characters allowed, specifically excluding those commonly used in SQL injection attacks such as the equals sign. • Implement server side input validation that checks for malicious code and removes it from the query.

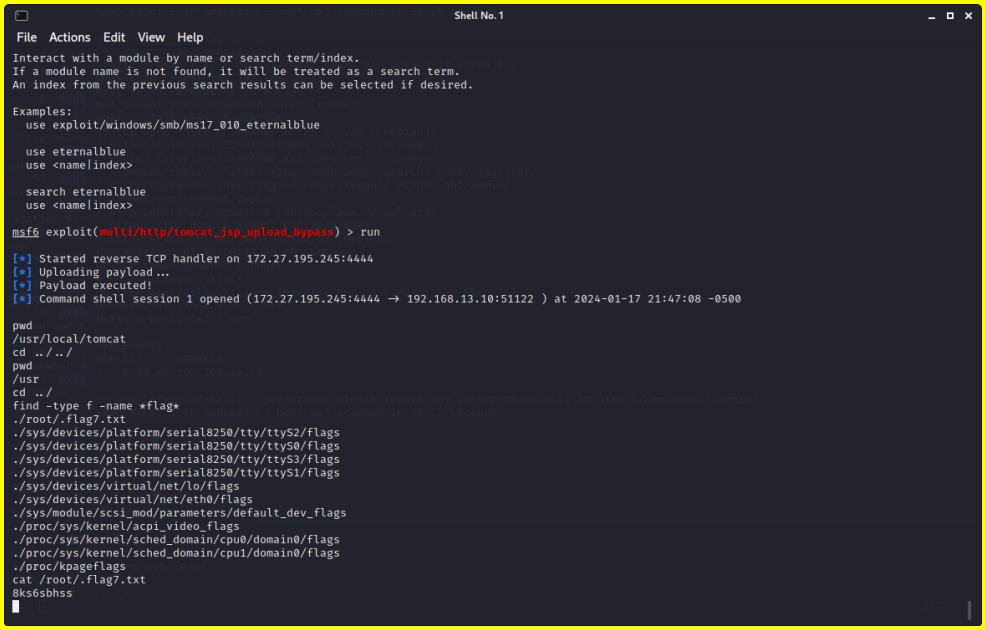
Vulnerability 5	**Findings**
Title	Command Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	After accessing the network page once administrative access was gained, code command was used in the DNS check and MX record check to return info on .txt files stored on the server.

Images	 

Affected Hosts	Total Rekall Web Application
Remediation	• Implement input validation limiting the types of characters allowed, specifically excluding those commonly used in command injection attacks such as the greater than and less than signs, semi-colon, and pipe. • Implement server side input validation that checks for malicious code and removes it from the query.

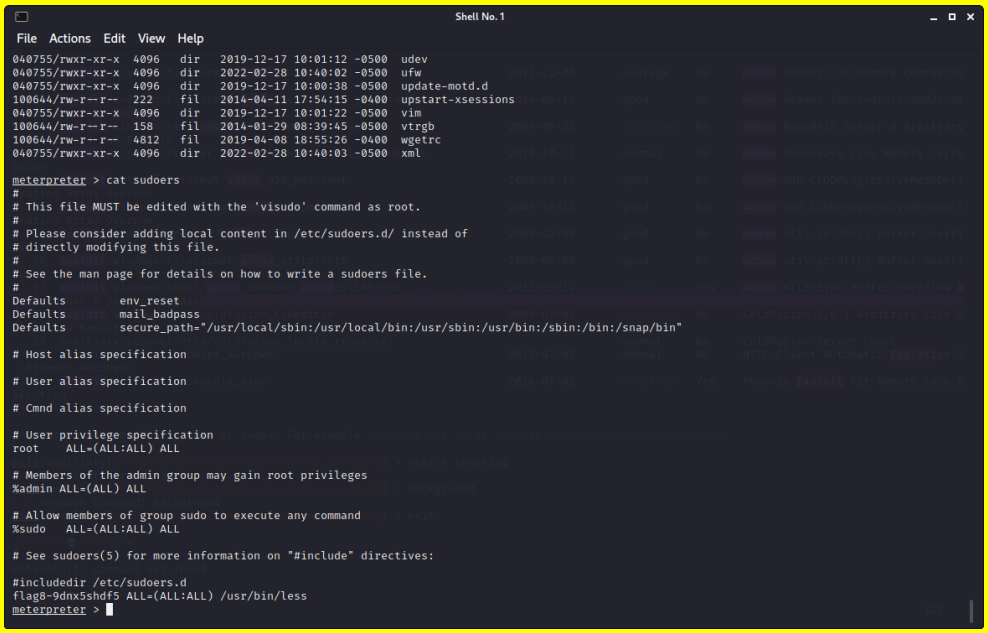
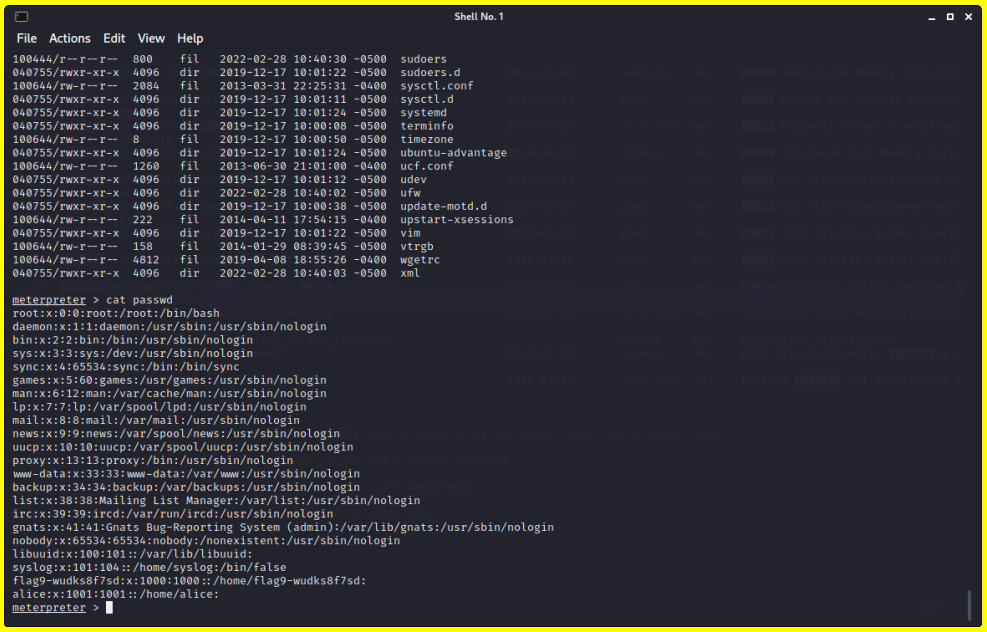
Vulnerability 6	**Findings**
Title	PHP Injection vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	**Critical**
Description	On the souvenirs page, we were able to exploit the URL with ".../souvenirs.php?message=CALLUSNOW" to include other commands including viewing other, sensitive files on the server.
Images	

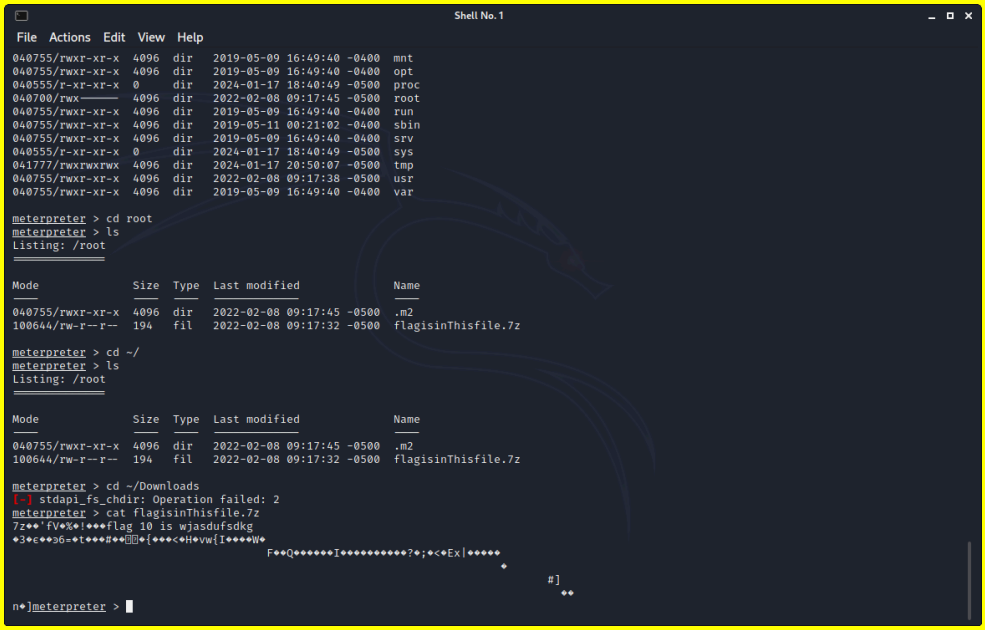
Affected Hosts	Total Rekall Web Application
Remediation	• Consider storing sensitive files on a separate server that cannot be easily accessed through manipulation of the URL. • Implement use of a PHP security linter

Vulnerability 7	**Findings**
Title	Apache Tomcat JSP Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	The machine running Apache Jserv and Apache Tomcat is vulnerable to a known exploit of TCP. Using the established exploit, we were able to sign in and open a shell on this machine which ultimately was used to access the root directory, where sensitive/privileged information is stored.
Images	
Affected Hosts	192.168.13.10
Remediation	• Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

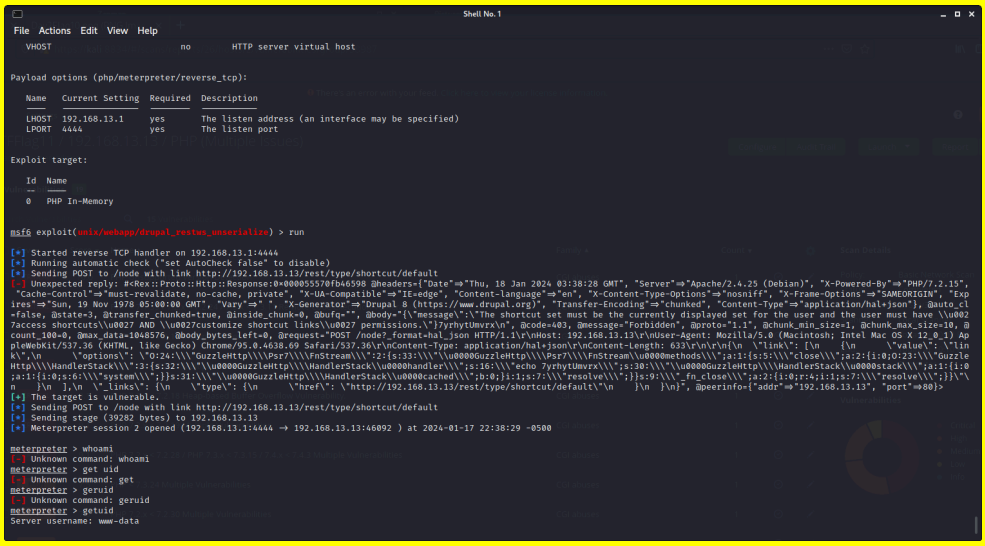
-

Vulnerability 8	**Findings**
Title	Shocking Exploit Vulnerability (CVE-2014-6271)
Type (Web app / Linux OS / WIndows OS)	Linux OS

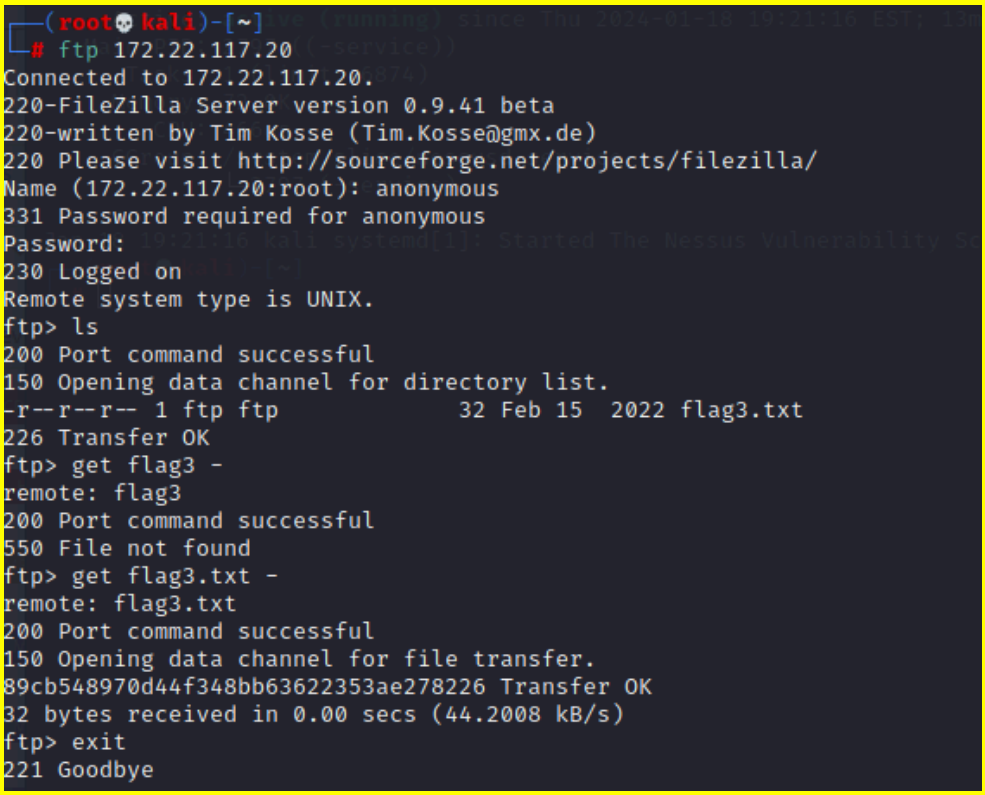
Risk Rating	High
Description	Bash can be exploited because of an improper parsing function in this version. This lets attackers execute commands on the machine with this vulnerability, ultimately allowing for root access to the sudo privileges file. This could be used to alter permissions of users, including potential malicious added users that could be used to later enact attacks on the system. Root access also allows for the threat actor to access sensitive files such as passwd and shadow which can be used to compromise existing users on the network.
Images	 
Affected Hosts	192.168.13.11
Remediation	• Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

Vulnerability 9	Findings
Title	Apache Struts Exploit Vulnerability (CVE-2017-2638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Using a known exploit of Apache struts, we were able to connect to this machine and establish a shell session to be able to navigate through files and download them to the attacking machine for use/viewing later.
Images	
Affected Hosts	192.168.13.12
Remediation	• Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

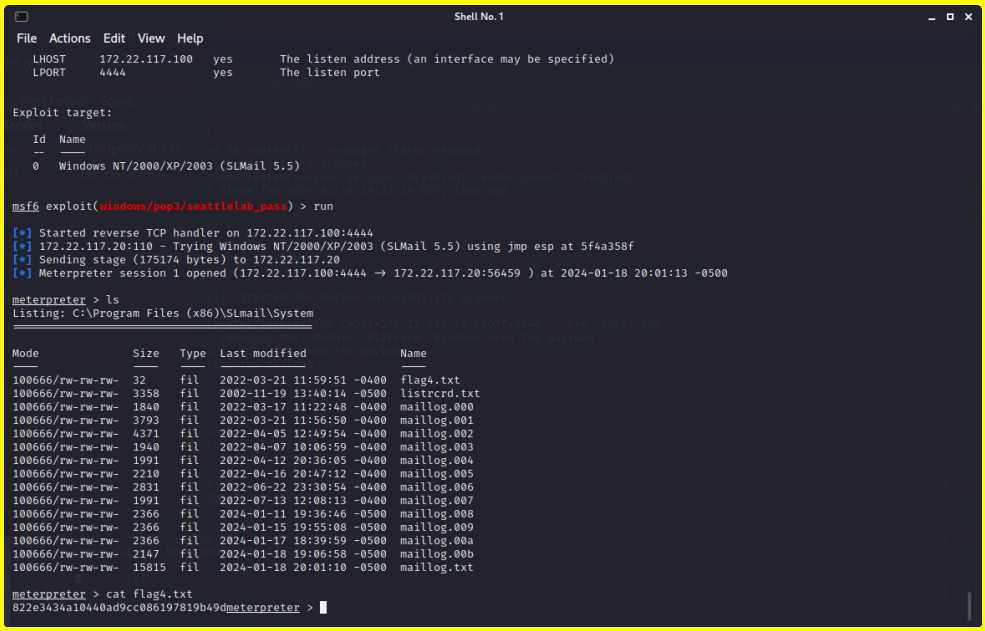
Vulnerability 10	Findings
Title	Drupal Exploit Vulnerability (CVE 2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Certain versions of Drupal do not sanitize data from outside forces, which can allow for PHP code usage to obtain information from the compromised system.

Images	
Affected Hosts	192.168.13.13
Remediation	• Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

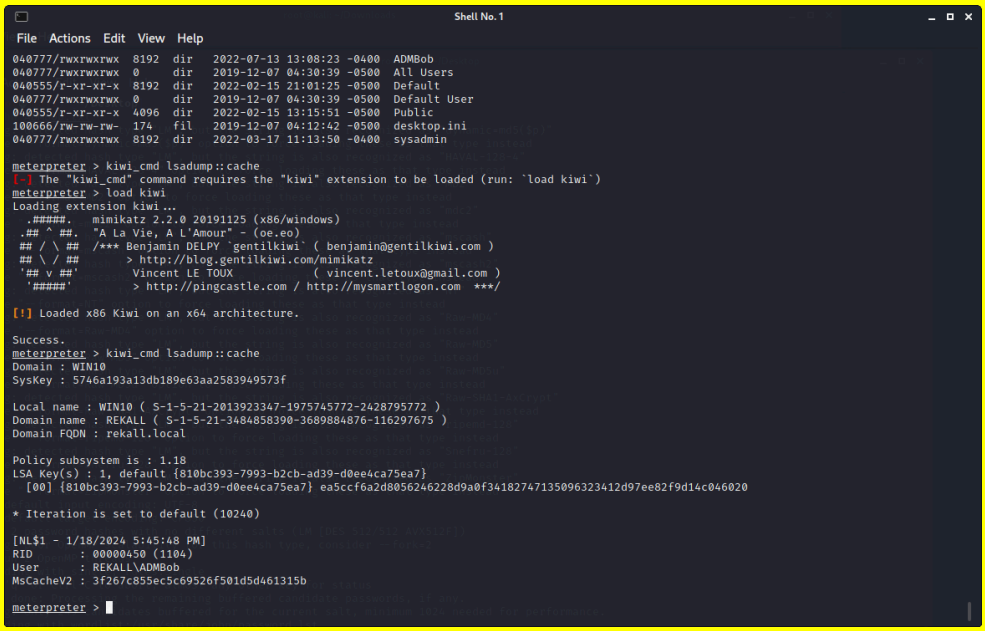
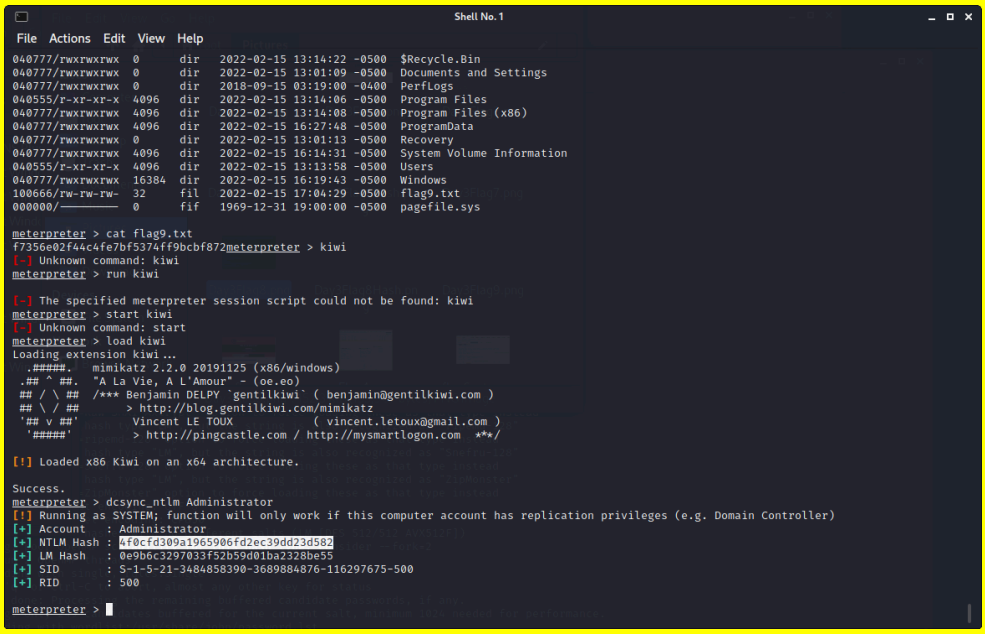
Vulnerability 11	Findings
Title	FTP Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	A Windows machine was identified that allowed for connection via FTP that ultimately resulted in us accessing and downloading files on that machine.

Images	
Affected Hosts	172.22.117.20
Remediation	• Close FTP ports to prevent outside/unauthorized IP addresses

Vulnerability 12	Findings
Title	SLMail Service Vulnerability (CVE 2003-0264)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Identified SLMail service running on a machine which was vulnerable to known exploit allowing for manipulation of the password argument by use of an unknown variable in order to obtain remote access via code without user authentication.

Images	
Affected Hosts	172.22.117.20
Remediation	• Keep up to date on any patches available from the vendor or upgrade to newer versions if available.

Vulnerability 13	Findings
Title	Cached Credential Exposure (Kiwi Exploit)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	On the Windows 10 Machine, credentials were found in the cache for an administrative user which could be used to access the Domain Control. Using a program called Kiwi, which can pull stored credentials for decryption, we were able to access this data for use in making our way to the WindowsDC host.

Images	 
Affected Hosts	172.22.117.10 and 172.22.117.20
Remediation	• Implement usage of LSAAS protected mode so non-protected processes are not able to call up LSAAS and obtain the info via credential dump. • Utilize the protected users security group within Windows for users with escalated privileges in order to apply additional protections for users within a specified group.

Additional Sources:
https://CVE.org
https://OSINTframework.com

https://www.beyondsecurity.com/resources/vulnerabilities/robots-txt-detection#:~:text=This%20file%20can%20be%20viewed,t%20contain%20any%20sensitive%20information.
https://cheatsheetseries.owasp.org/cheatsheets/File_Upload_Cheat_Sheet.html
https://snyk.io/blog/prevent-php-code-injection/
https://github.com/rapid7/metasploit-framework/
https://www.openwall.com/lists/oss-security/2019/10/14/1
https://www.reliaquest.com/blog/credential-dumping-part-2-how-to-mitigate-windows-credential-stealing/