Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Access-Pointe PLC
Contact Name	Marian Baah
Contact Title	Chief Coordination Officer

Document History

Version	Date	Author(s)	Comments
001	04/25/2023	Marian Baah	

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.

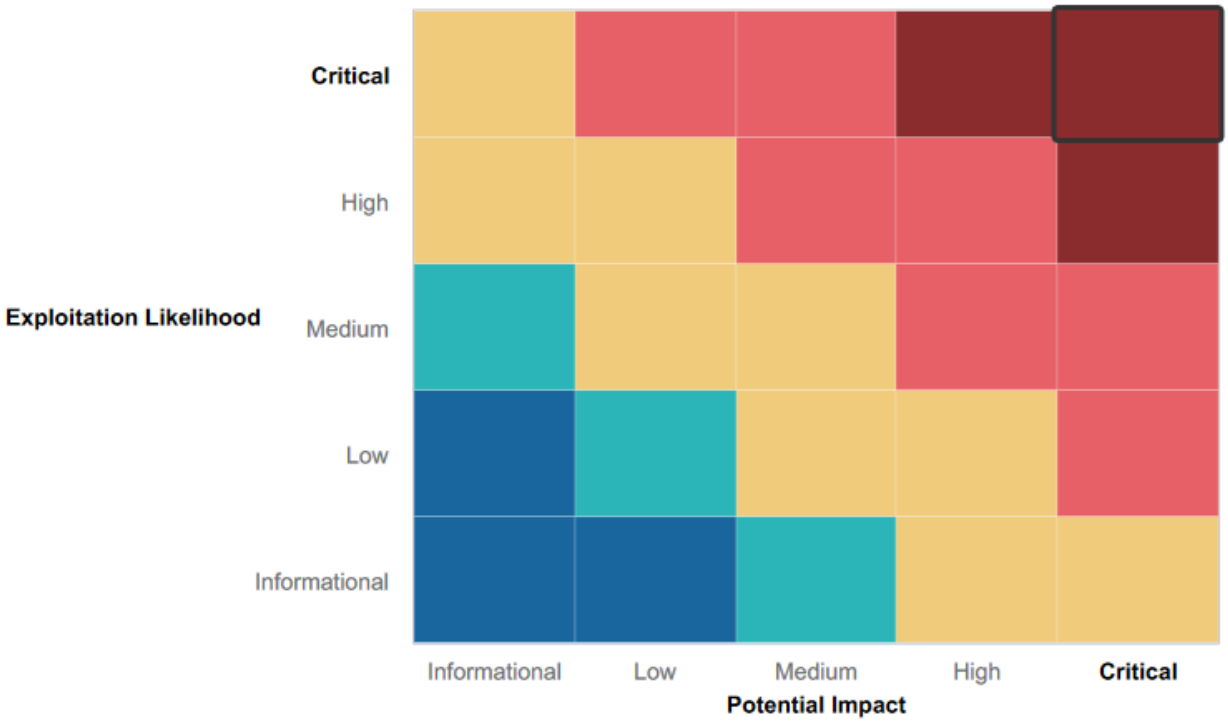
Executive Summary of Findings

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.

- Forward-thinking defensive and offensive strategy in place
- Current and continuing penetration testing to identify vulnerabilities for mitigation
- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability
- There was input validation checks for jpg files where the upload only accepts php files
- TCP and UDP ports 998,999 and 996 were closed and not open when Nmap scan was done.

Summary of Weaknesses

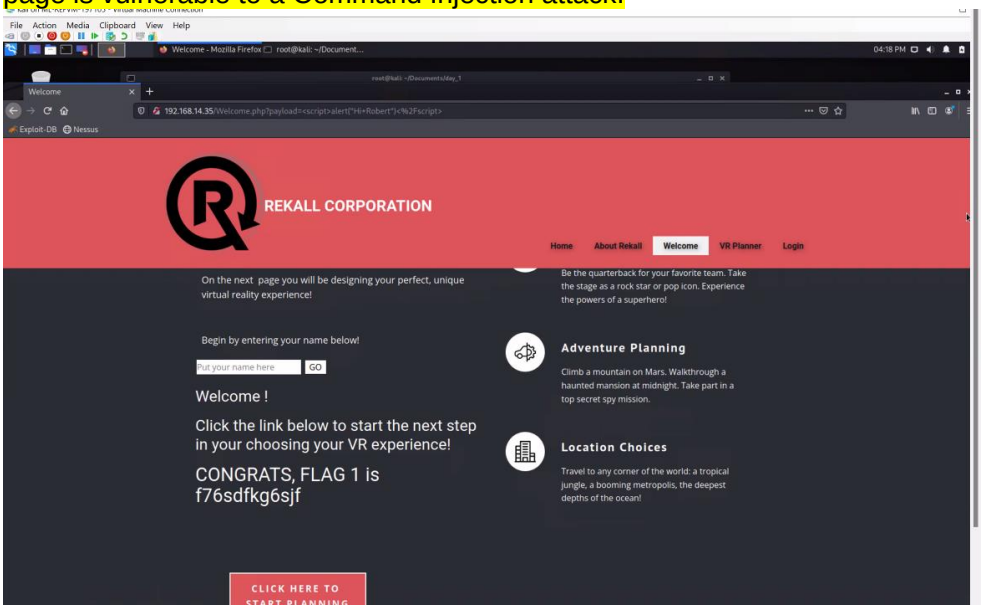
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

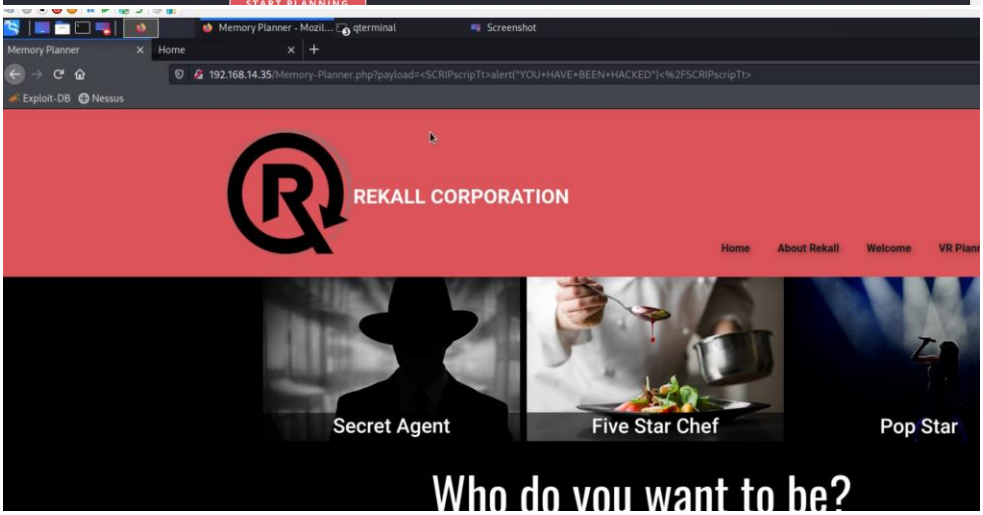
- Rekall's server's physical address is publicly available
- IP lookup displayed credentials exposed.
- Open ports found allow for file enumeration and unauthorized access
- Port scans showed IP addresses within Rekall's IP range displayed potential vulnerabilities like open ports,IP addresses etc
- Web Application is vulnerable to XSS (stored and reflected)and SQL payload injections.
- Credentials are being stored in HTML source code
- Apache web server in use is outdated and vulnerable to multiple exploits
- SLMail server is vulnerable to exploits which allow access to shell.
- Unauthorized access to password hashes allow for password cracking and privilege escalation

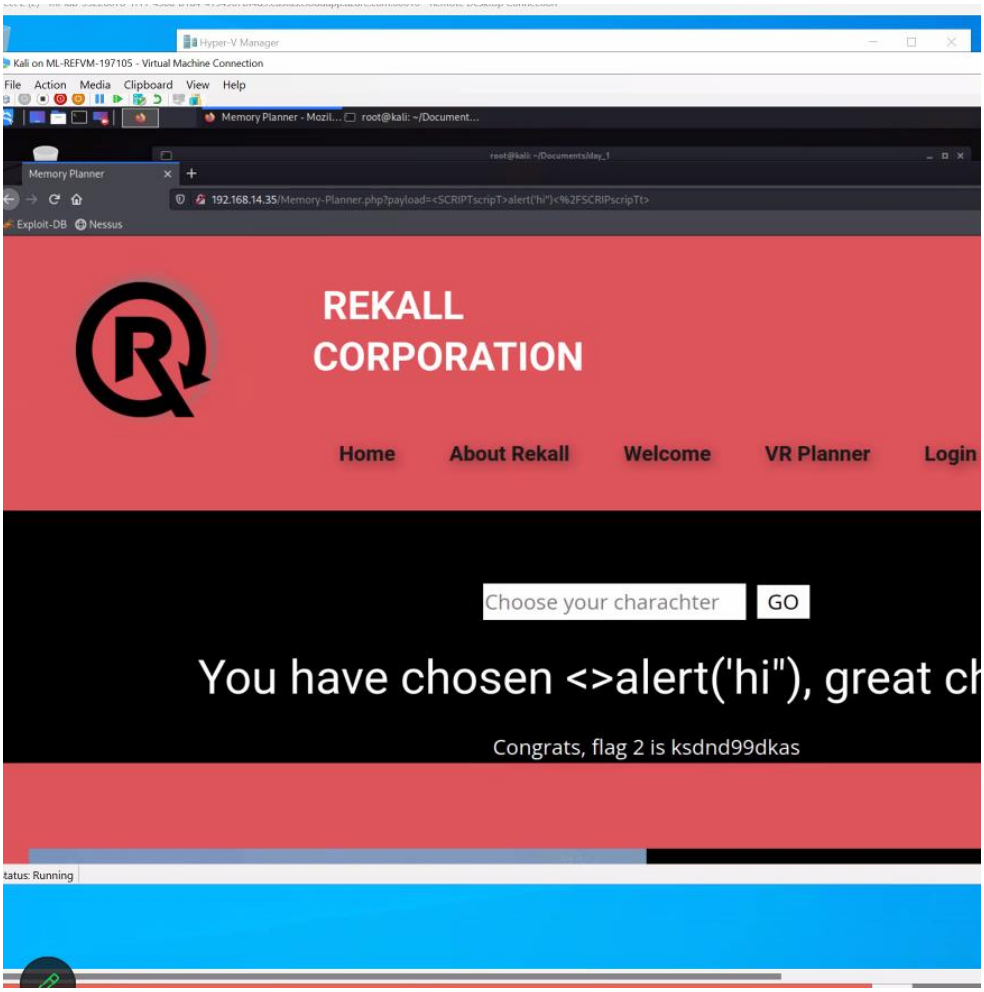
Executive Summary

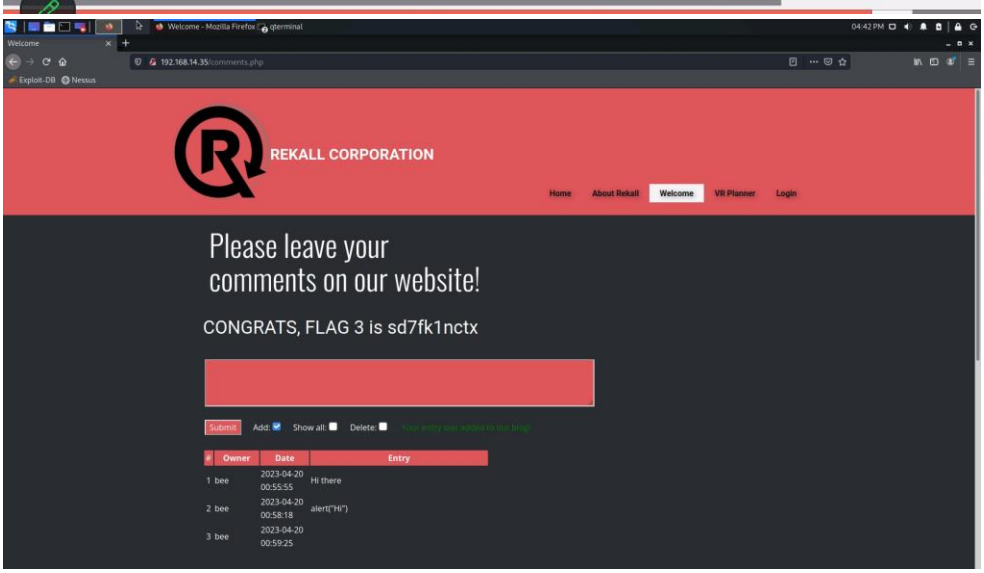
During the Penetration Testing of Rekall's IT assets, Access-Pointe LLC was able to identify multiple vulnerabilities, including a number of Critical vulnerabilities that could have a potentially harmful impact on the profits or reputation of Rekall. Access-Pointe LLC was able to access Rekall's assets, access sensitive data, and escalate privileges within systems as discussed below.

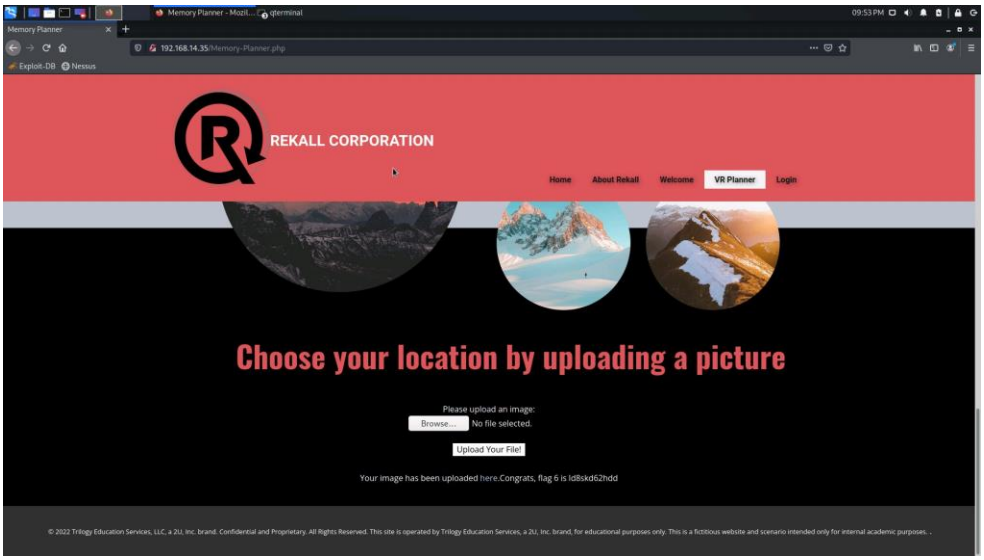
Access-Pointe LLC tested Rekall's Web Application first. We found it to be vulnerable to an XSS Reflected attack as malicious scripts can be run on the home page and several input fields. The Web App is also vulnerable to Local File Inclusion as files can be uploaded from the VR Planner web page. An XSS Stored vulnerability was identified on the Comments page as it allows scripting code to be run. SQL Injection attacks can also be run on the Login.php toolbar, and the Networking.php page is vulnerable to a Command Injection attack.



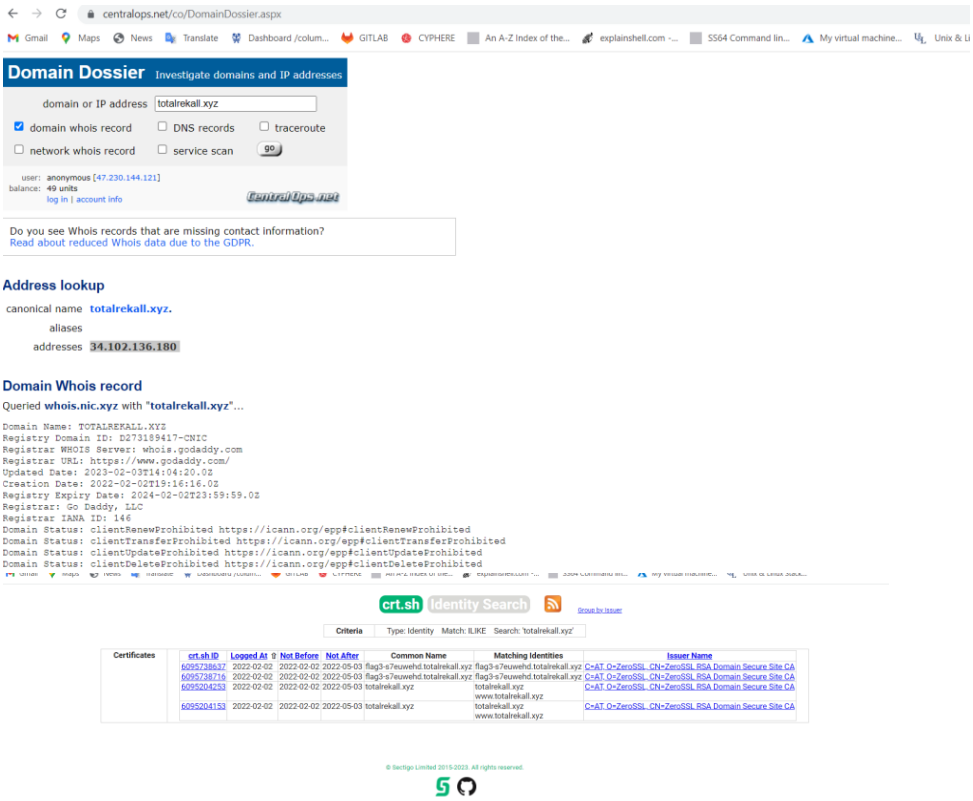


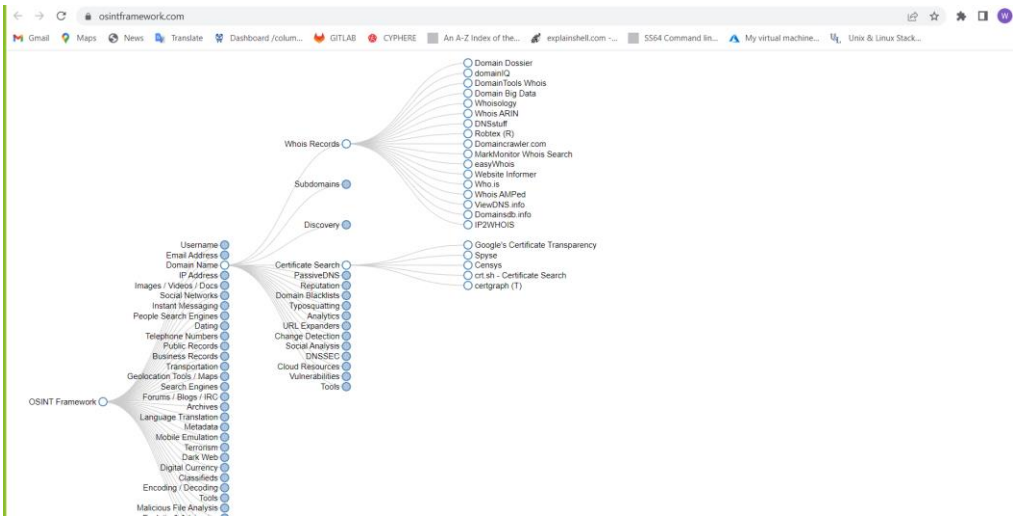


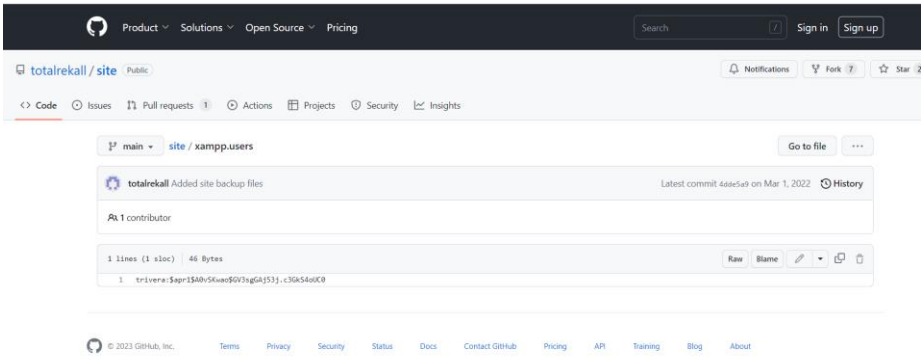


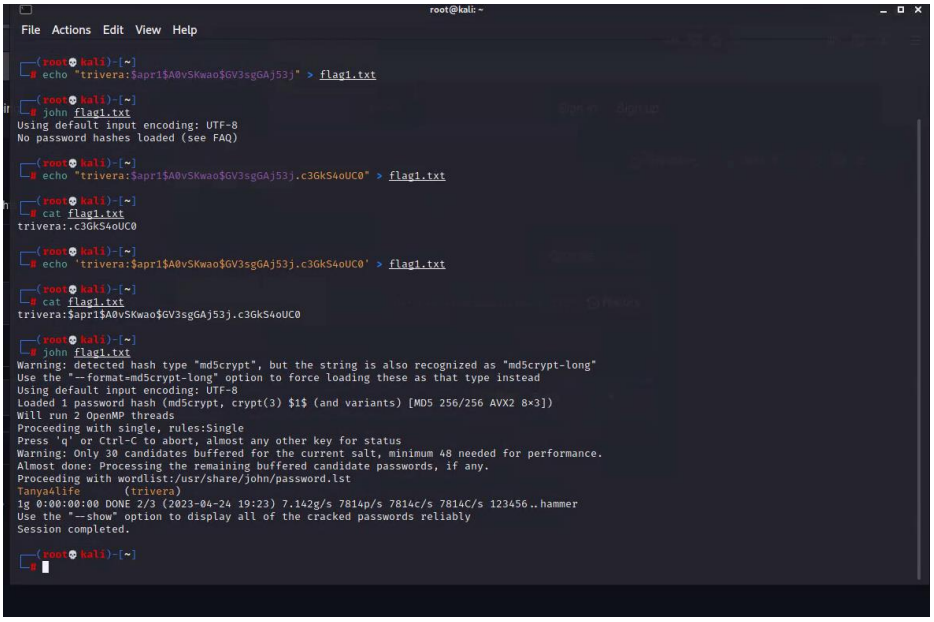


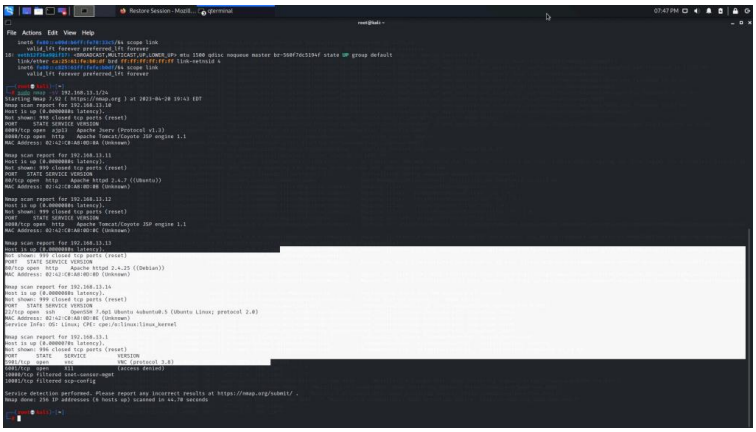
Open source data was determined to be exposed and viewable using OSINT, and searching crt.sh showed a stored certificate. User login credentials were actually stored in plain view within the HTML source code of the Login.php page and could even be seen while simply highlighting the page in a web browser. The file robots.txt was also determined to be exposed and readily accessible. Research uncovered user credentials in a Github repository that resulted in unauthorized access to the web hosts files and directories. The Apache server was found to be out-of-date with a Struts vulnerability.

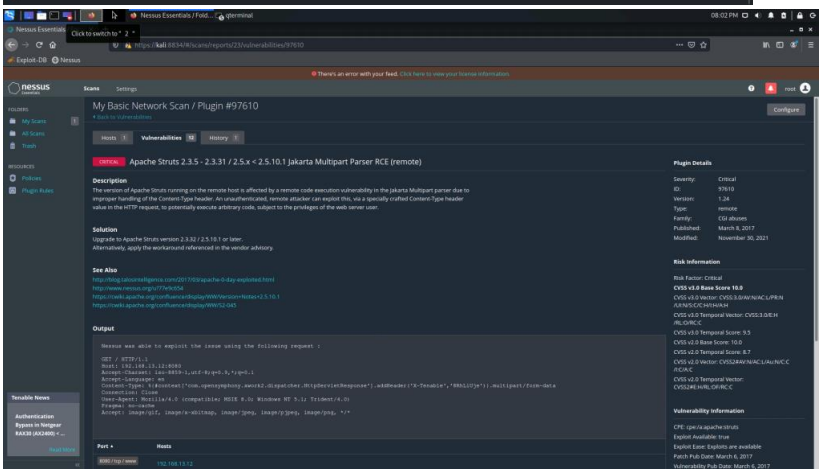




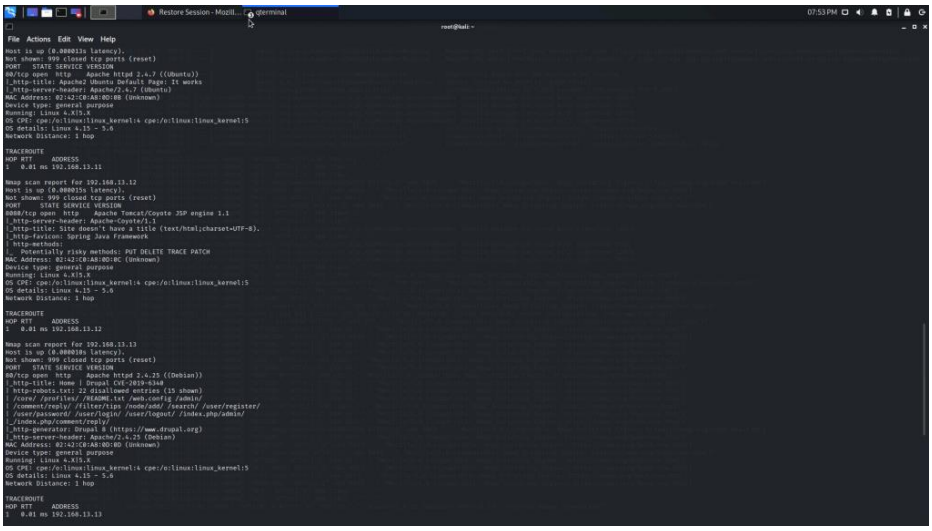


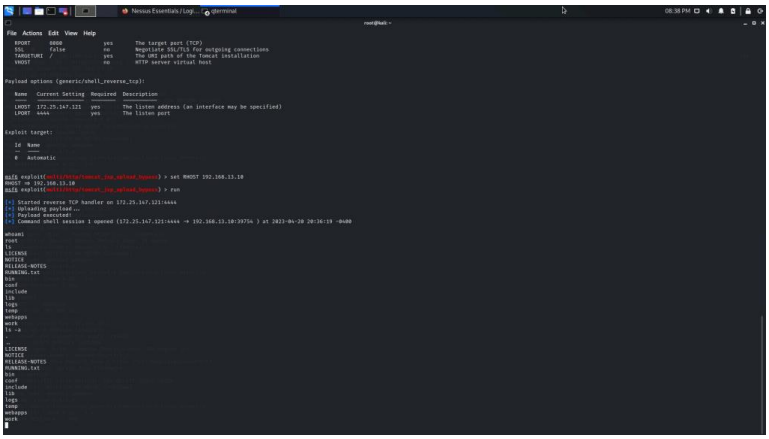


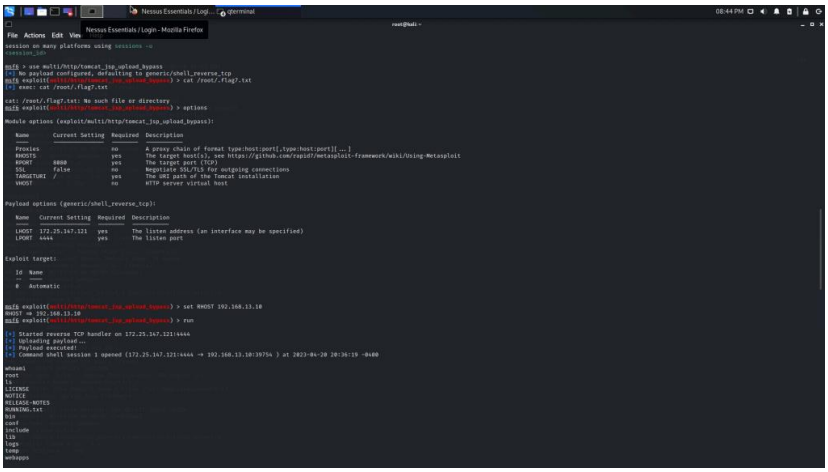


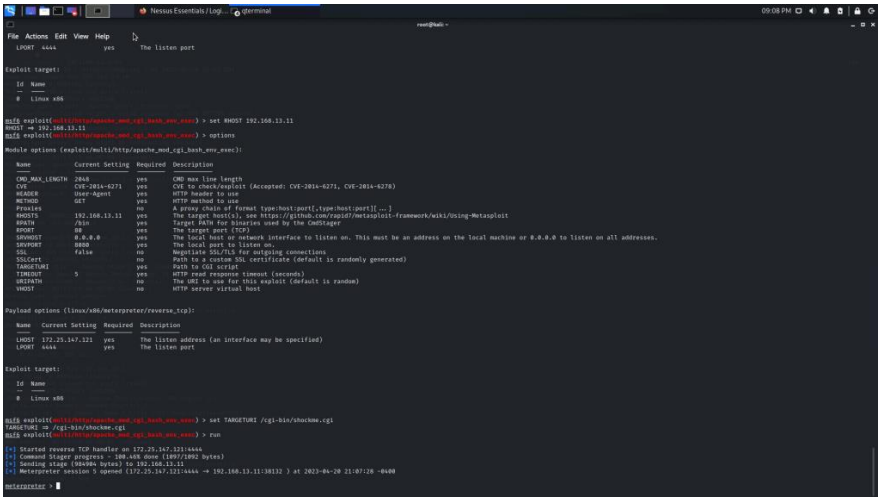


The Windows OS environment was also and Access-Pointe LLC discovered that FTP Port 21 was open and vulnerable, as was Port 110, which is used for SLMail service. Metasploit was used to discover this vulnerability, as well as to gain access to a password hash file which was subsequently cracked and enabled the creation of a reverse shell. Additionally, scheduled tasks were readily visible within the Windows 10 Machine Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

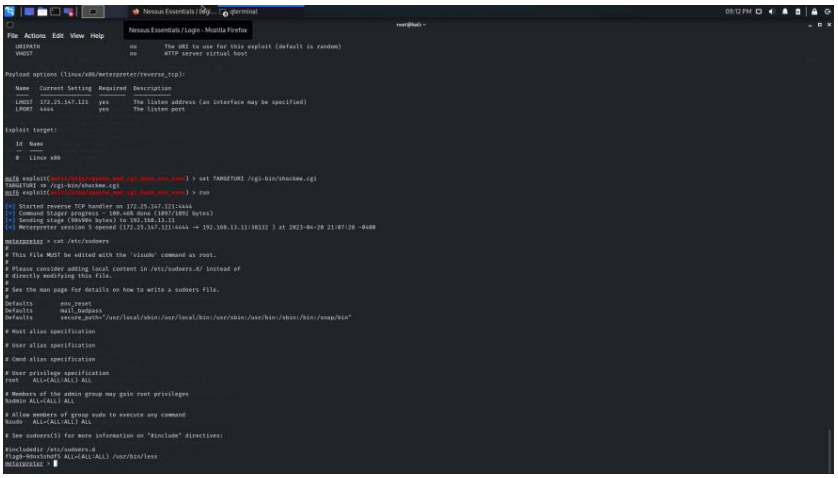


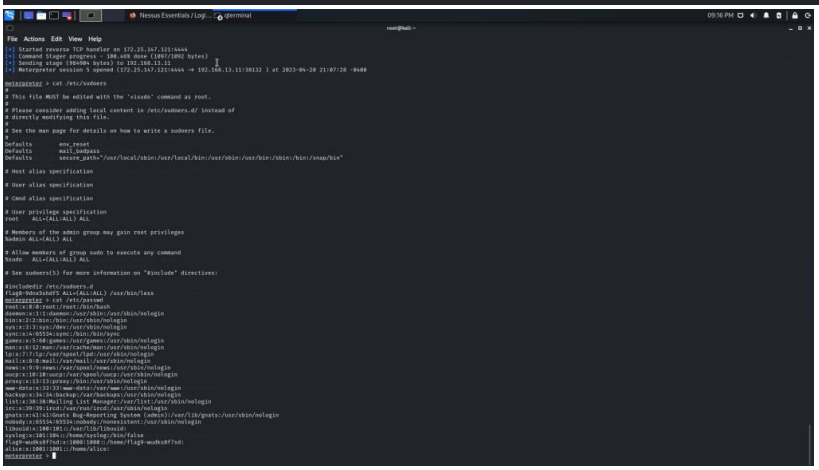


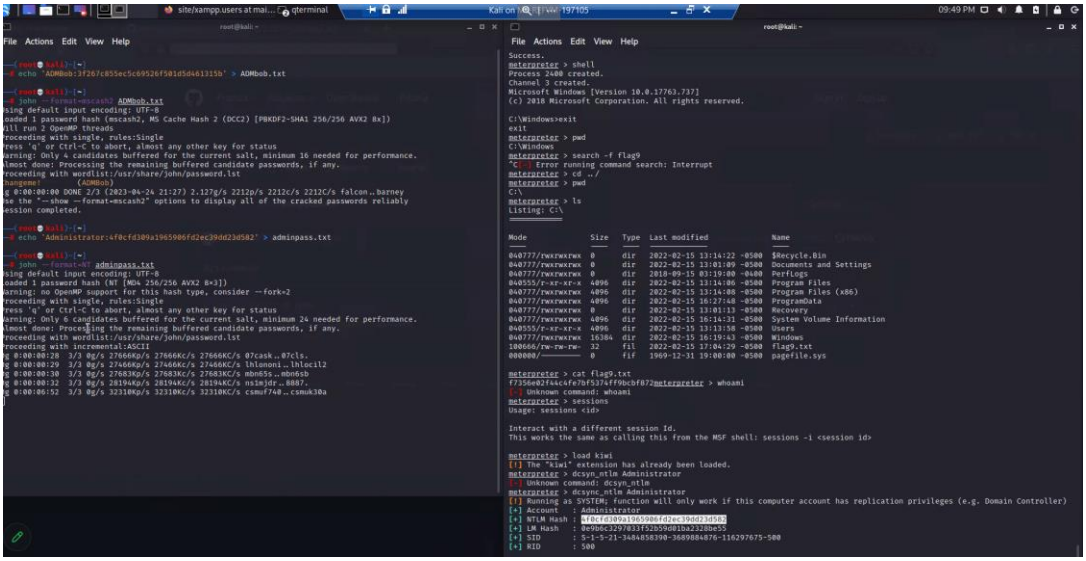




Within the Linux environment, Access-Pointe LLC was able to reveal 5 IP addresses that were publicly exposed and vulnerable, and one of the hosts was found to be running Drupal. Stolen credentials were used to access one host and escalate privileges to root. An additional common known shell RCE execution vulnerability was discovered using Meterpreter. The sudoers file was accessible using a Shellshock exploit in Metasploit as well.







In summary, these vulnerabilities could be exploited maliciously to cause massive damage within the assets and the functionality of the business in general.Access-Pointe LLC has provided detailed recommendations for mitigating each of these vulnerabilities to prevent harm and loss that could result.

Summary Vulnerability Overview

Vulnerability	Severity
Local File Inclusion	Critical
SQL Injection	Critical
Sensitive data exposure	Critical
User Credentials Exposure	Critical
Command Injection	Critical
Apache Struts (CVE-2017-5638)	Critical
Shellshock on Web Server (Port 80)	Critical
Linux Privilege Escalation	Critical
SLMail Port 110 Exploited via Metasploit (SeattleMail)	Critical
Drupal (CVE-2019-6340)	Critical
IPs visible with Nmap	Critical
System Shell Executed with Dumped Admin Server Credentials	Critical
Admin Server Credentials Dumped via Kiwi	Critical
Access System and Run lsa_dump_sam via Kiwi Shows Password Hashes	Critical
Cross Site Scripting XXS (Reflected and Stored)	High
Open Source Exposed Data	High
Run as ALL Sudoer (CVE-2019-14287)	High
Open FTP Port 21	High
Sensitive Information Stored in Public/Documents Folder	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Certificate Search via crt.sh	Medium

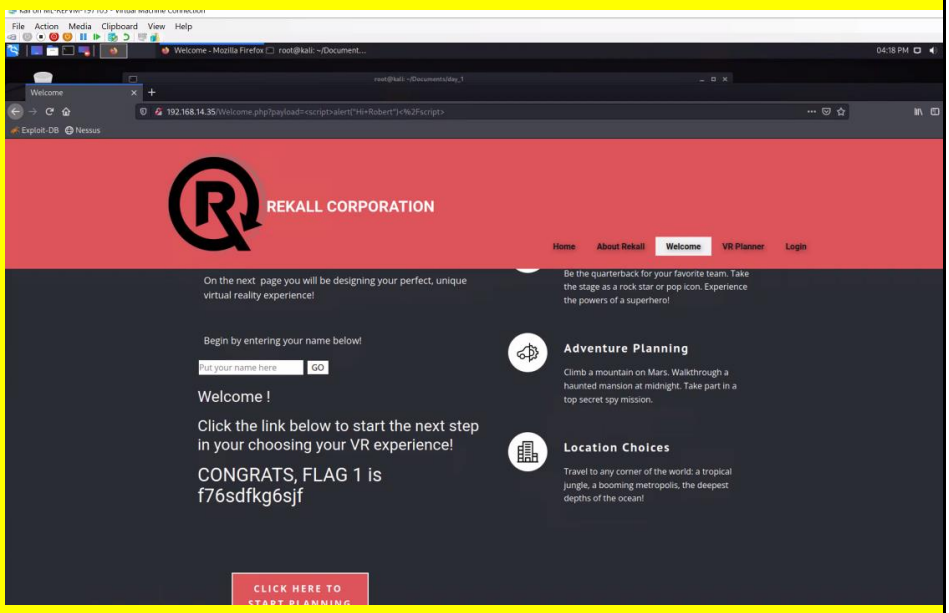
The following summary tables represent an overview of the assessment findings for this penetration test:

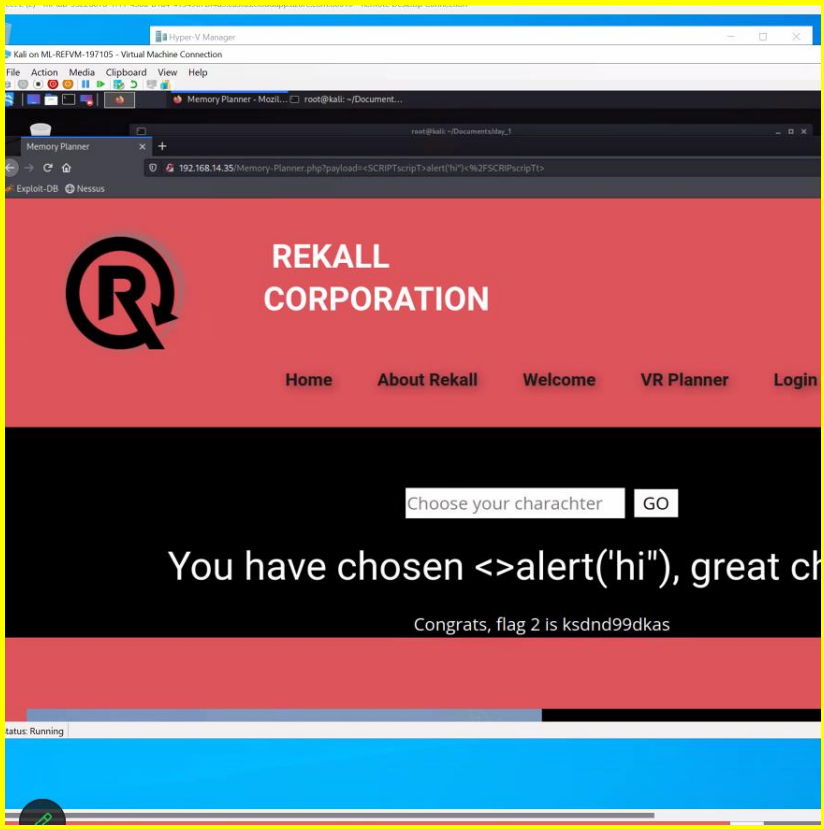
Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 106 110

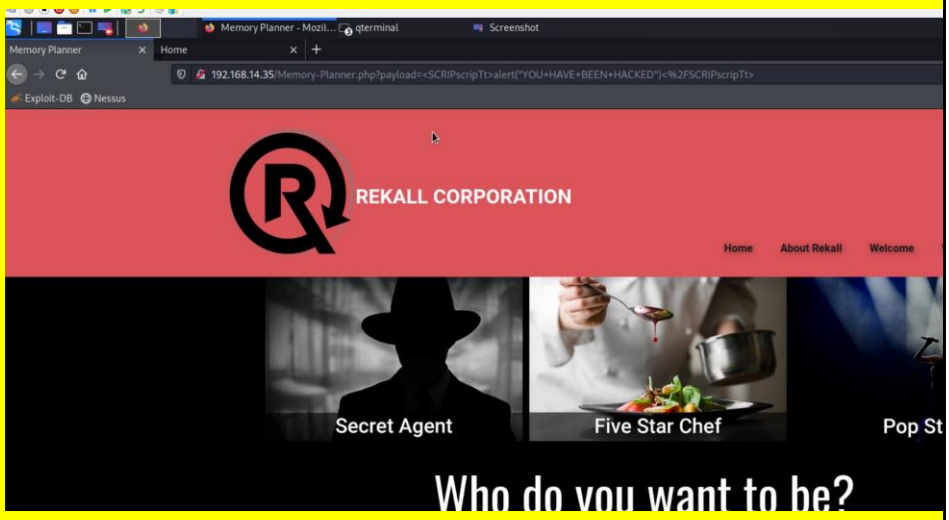
Exploitation Risk	Total

Critical	14
High	7
Medium	1
Low	0

Vulnerability Findings

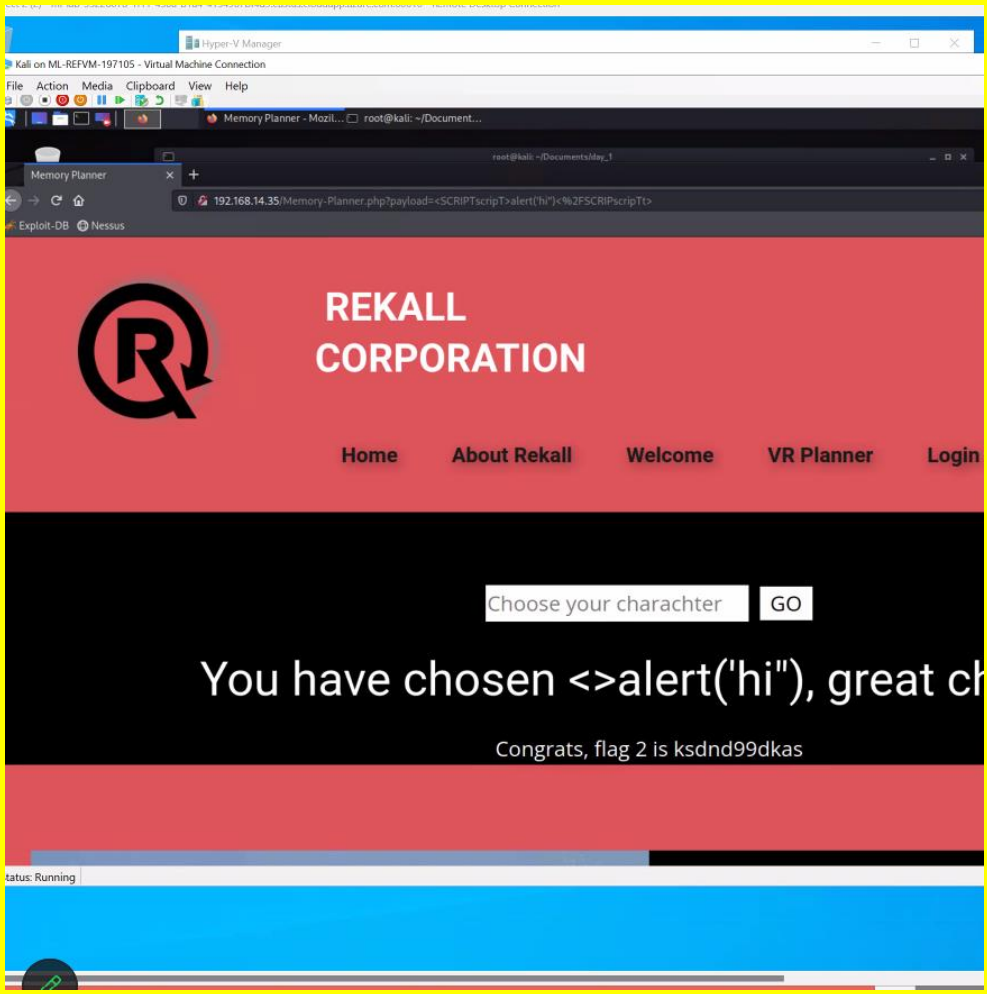
Vulnerability 1	Findings
Title	Cross-Site Scripting (XSS) Reflected
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Malicious script was injected into the input form which was accepted.
Images	

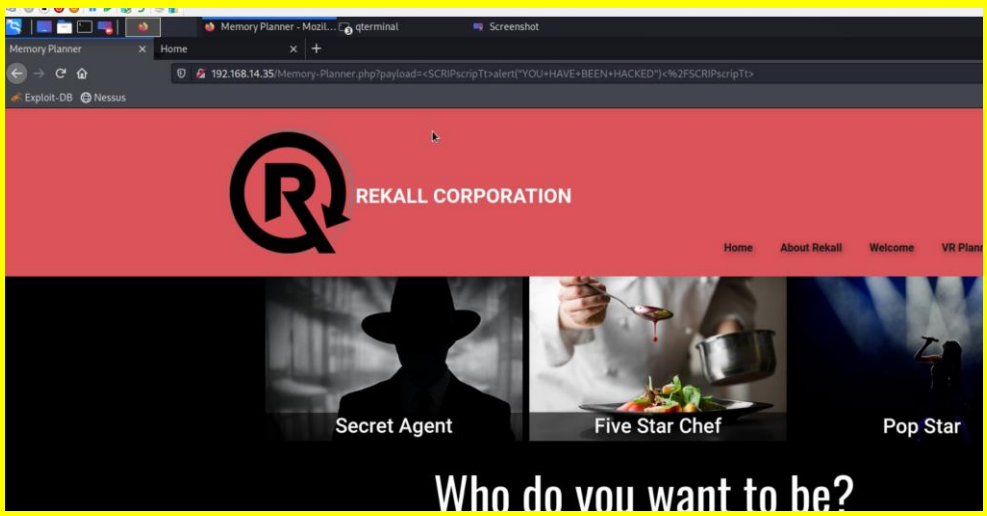


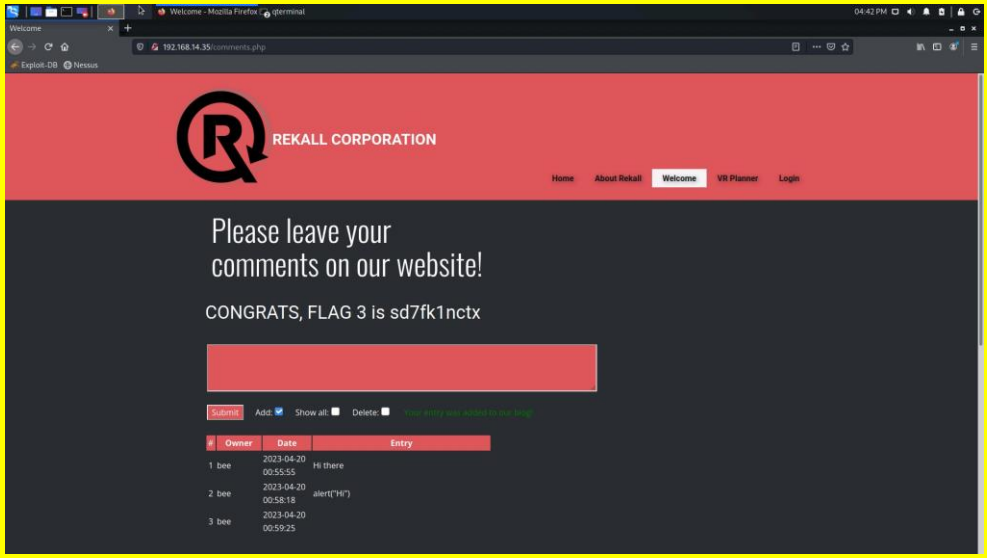


Affected Hosts	192.168.14.35
Remediation	Input Validation to catch potentially malicious user-provided input. The use of a web application firewall (WAF) can protect against XSS attacks.

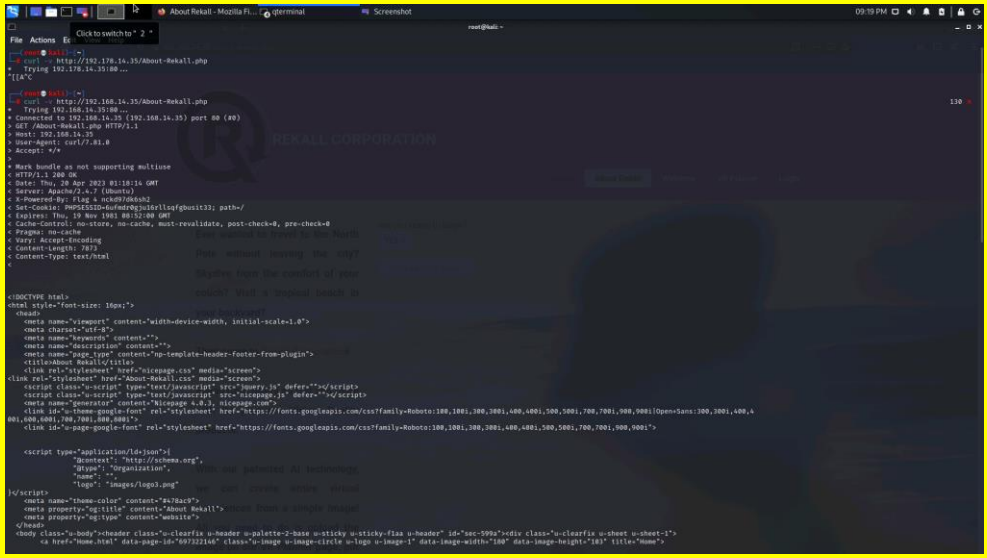
Vulnerability 2	Findings

Title	Cross Site Scripting (XSS Reflected)
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	Malicious script was injected into the input form which was accepted.
Images	

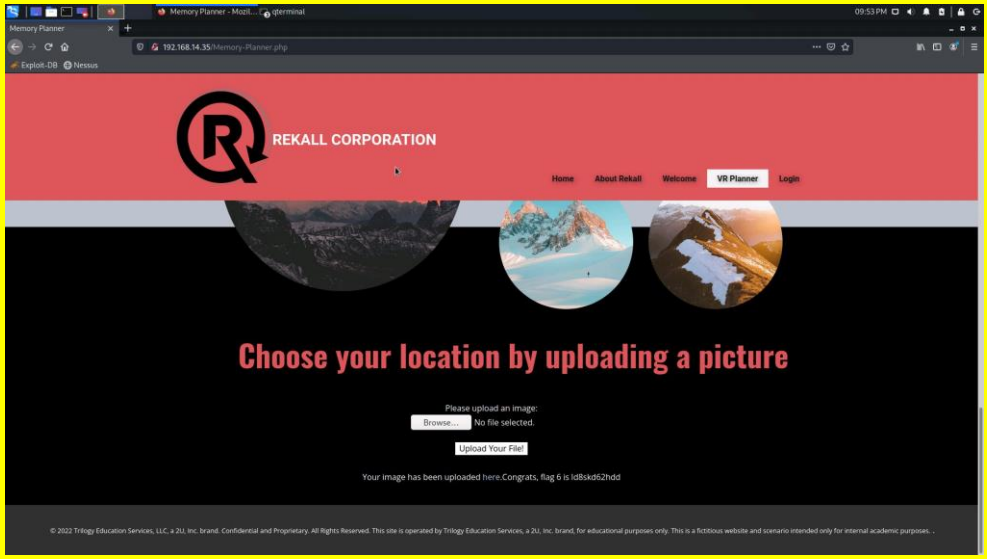
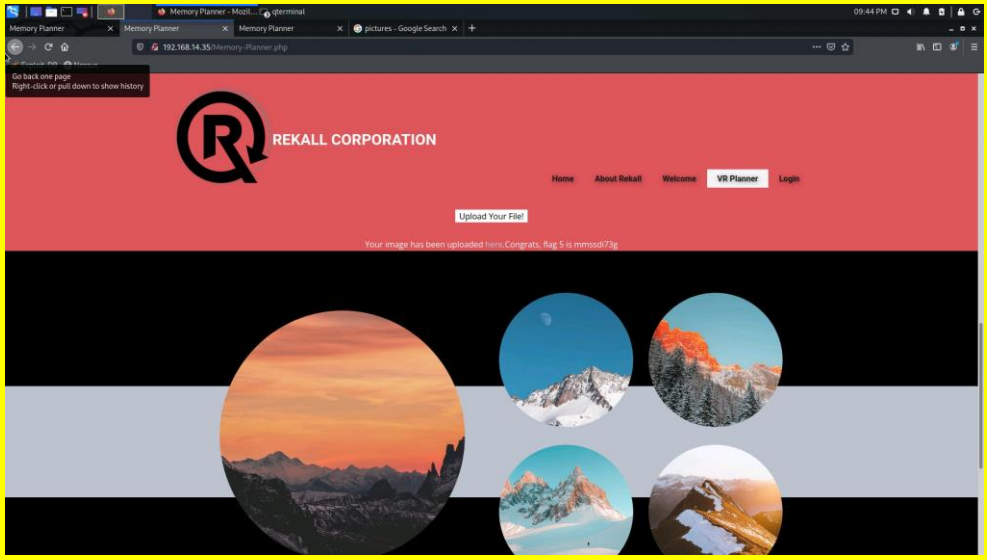
	
Affected Hosts	192.168.14.35
Remediation	Input Validation to catch potentially malicious user-provided input. The use of a web application firewall (WAF) can protect against XSS attacks.

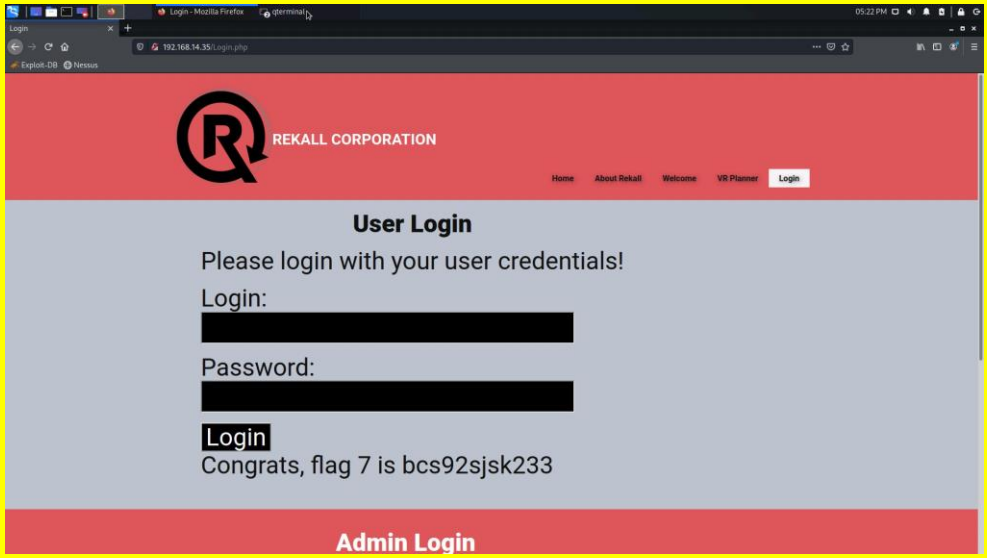
Vulnerability 3	**Findings**
Title	Cross Site Scripting (XSS Stored)
Type (Web app / Linux OS / WIndows OS)	Web application
Risk Rating	High
Description	While accessing the Comments.php page, the script <script>alert("Hi")</script> was used to reveal Flag 3.
Images	
Affected Hosts	192.168.14.35

Remediation	Secure handling of user input—Inspect all user-submitted input to ensure it doesn't include risky characters that may affect how a user's browser interprets the data on your website. You can use a WAF to detect and prevent XSS attacks in real time.

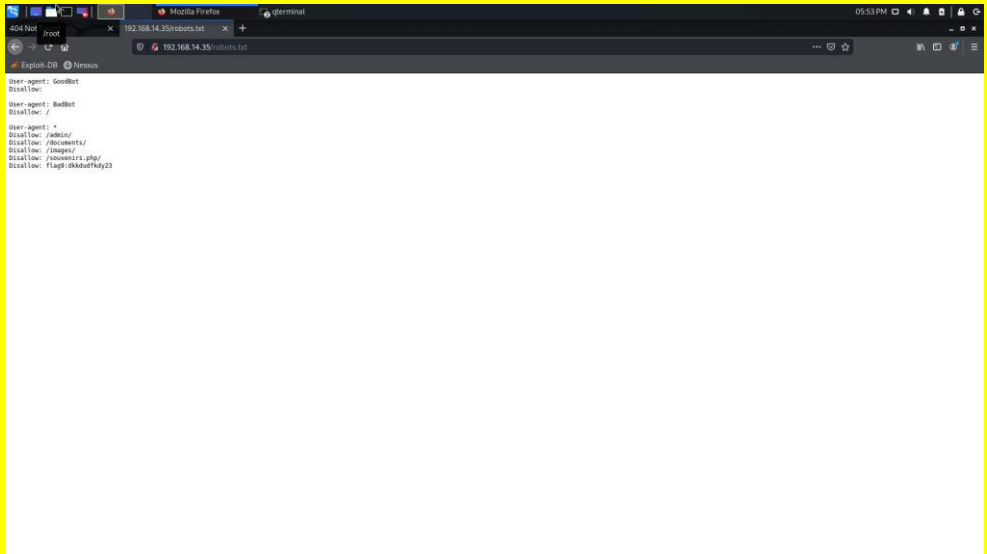
Vulnerability 4	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Curl Command was used by running curl -v http://192.168.14.35/About-Rekall.php and this showed sensitive data
Images	
Affected Hosts	192.168.14.35
Remediation	Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS). Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt or PBKDF2. Verify independently the effectiveness of configuration and settings.

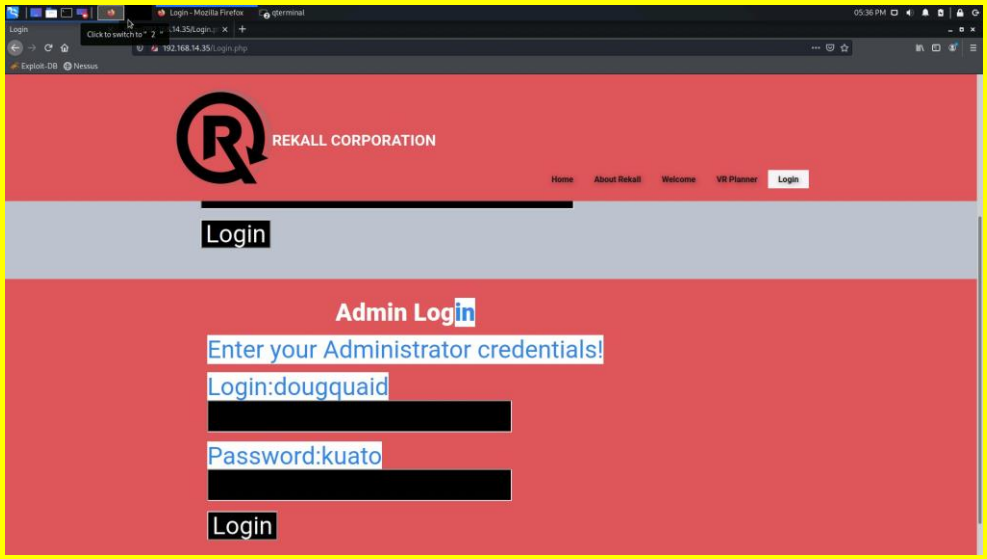
Vulnerability 5	**Findings**
Title	Local File Inclusion

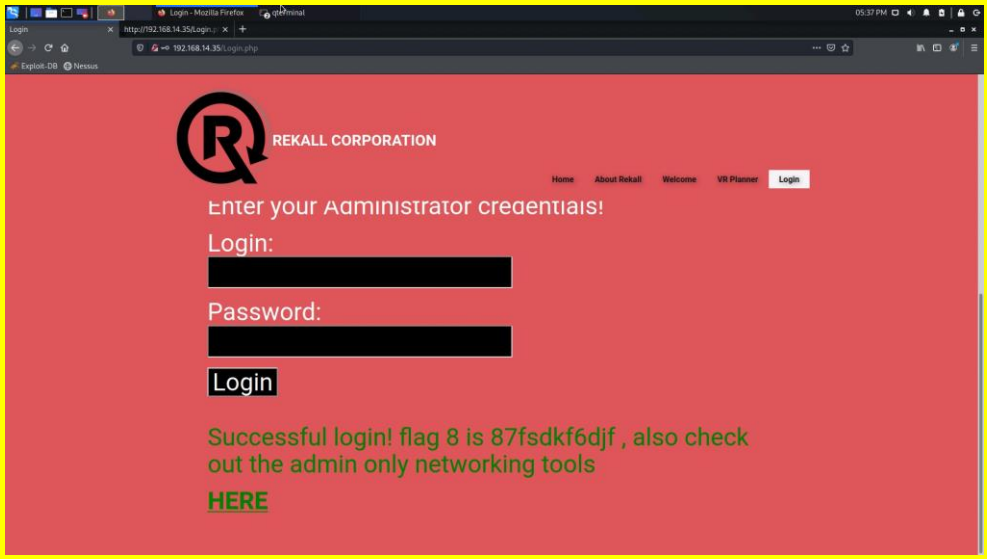
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	LFI successfully executed, as a .php file was uploaded from the toolbar located on the VR Planner page Images.
Images	 
Affected Hosts	192.168.14.35
Remediation	Avoid passing user-submitted input to any filesystem/framework API.If this is not possible the application can maintain a white list of files, that may be included by the page, and then use an identifier (for example the index number) to access to the selected file. Any request containing an invalid identifier has to be rejected, in this way there is no attack surface for malicious users to manipulate the path.

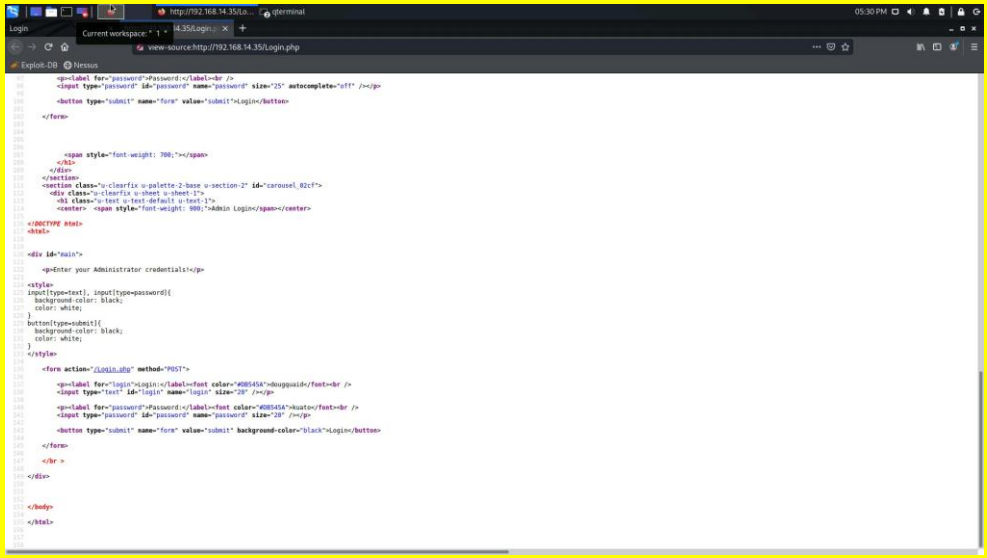
Vulnerability 6	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	While accessing /Login.php page, payload (' or 1=1 --) was entered in the toolbar intended for password and login successfully resulting in an exploit.
Images	
Affected Hosts	192.168.14.35
Remediation	The use of prepared statements with variable binding (also known as parameterized queries) should be the first line of defense for mitigating SQL injections. Putting in place an allowlist input validation Disallow web app to accept direct input and/or implement character escaping.

Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Unrestricted access to robots.txt page Highlighting the /Login.php page also shows user credentials. User credentials are also visible within HTML of the Login.php
Images	

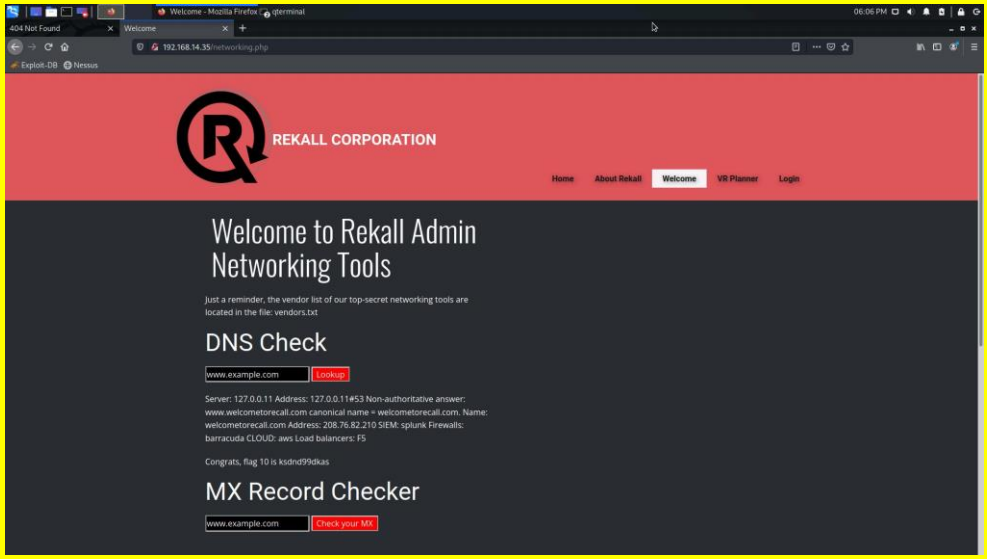
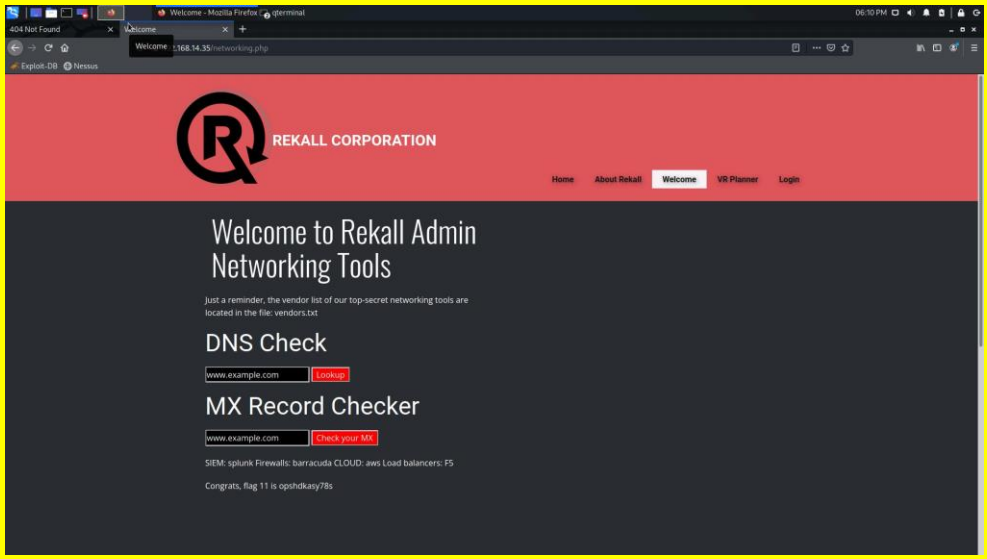




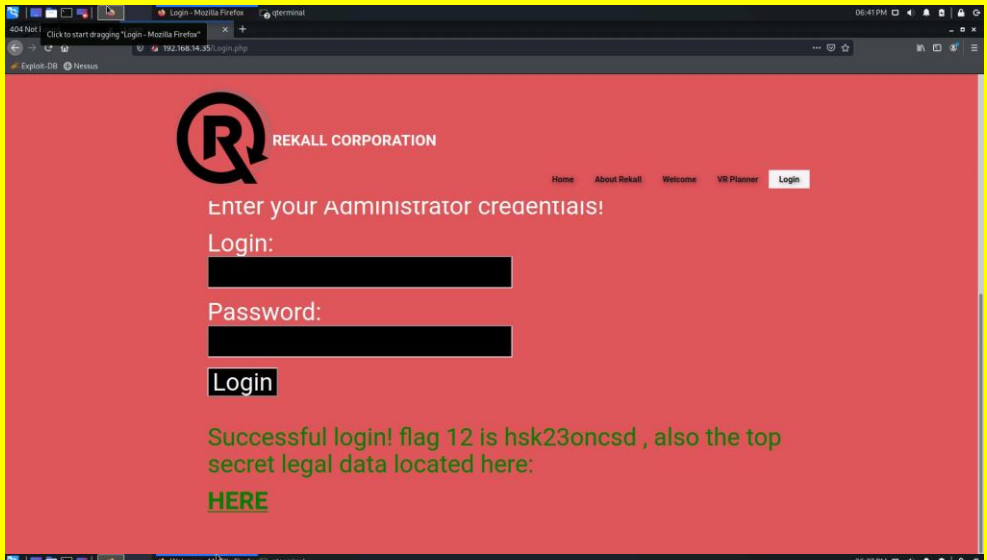
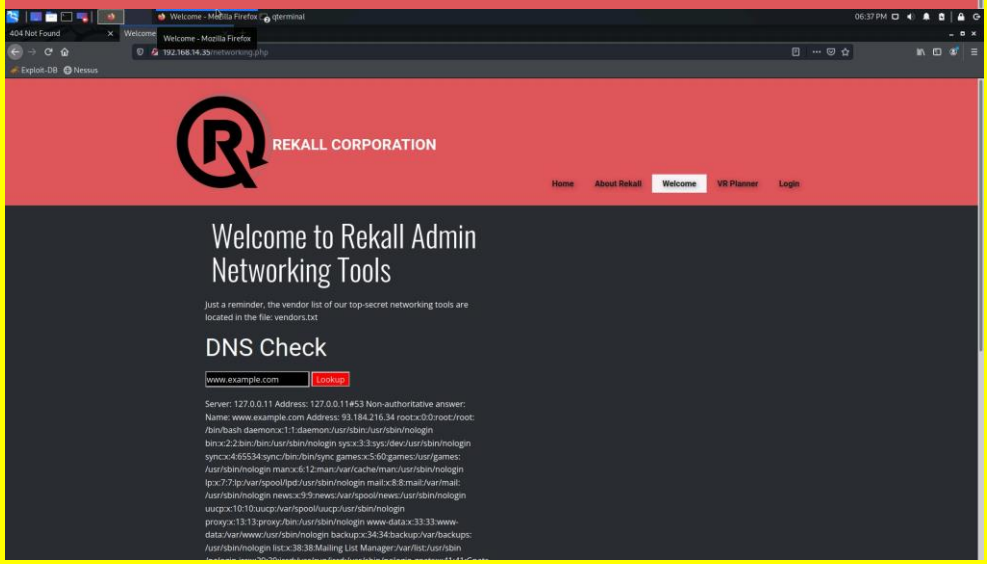


	
Affected Hosts	192.168.14.35
Remediation	Deleting user credential information from the HTML. Restrict access to robots.txt to authorized users.

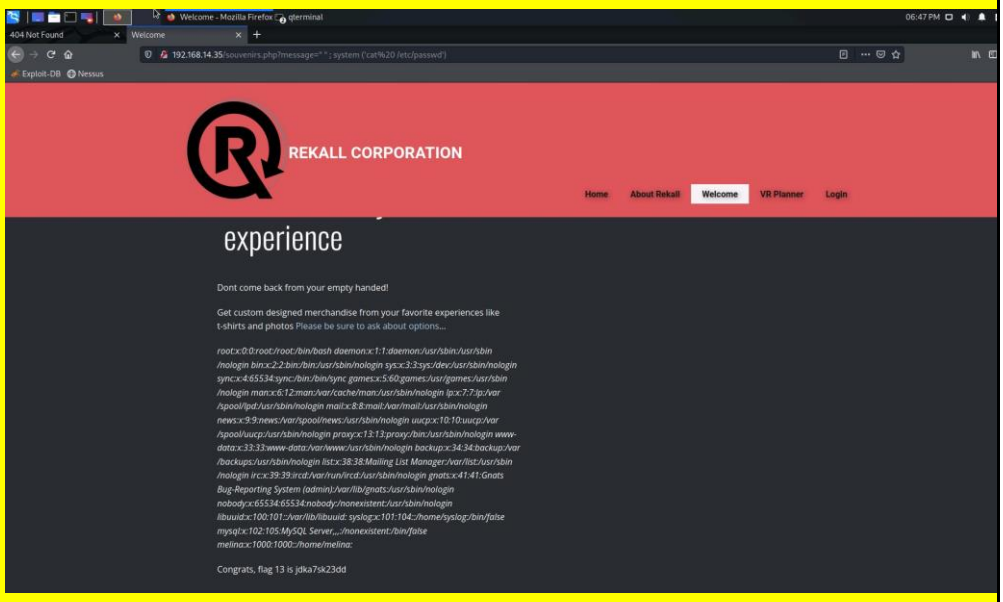
Vulnerability 8	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Used command www.welcometorecall.com && cat vendors.txt to show vendor information which was available.

Images	 
Affected Hosts	192.168.14.35
Remediation	Don't Run System Commands with User-Supplied Input. Use Strong Input Validation for Input Passed into Commands

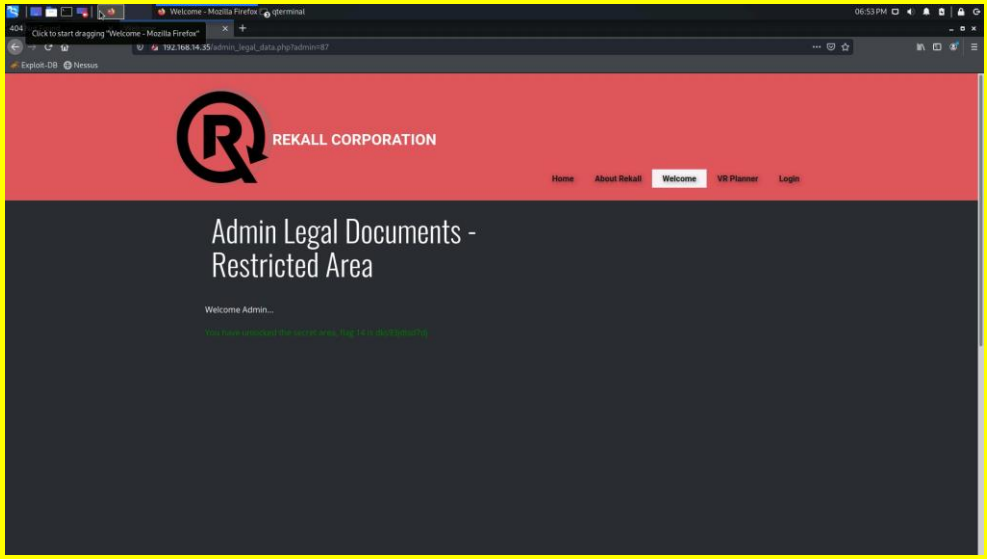
Vulnerability 9	Findings
Title	Brute Force attack
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical

Description	Used the cat command to access the etc/passwd file and user credential exposed was used to logged into the system
Images	 
Affected Hosts	192.168.14.35
Remediation	Use strong and inimitable passwords. ... Lock out accounts after a defined number of incorrect password attempts. Use two-factor authentication.

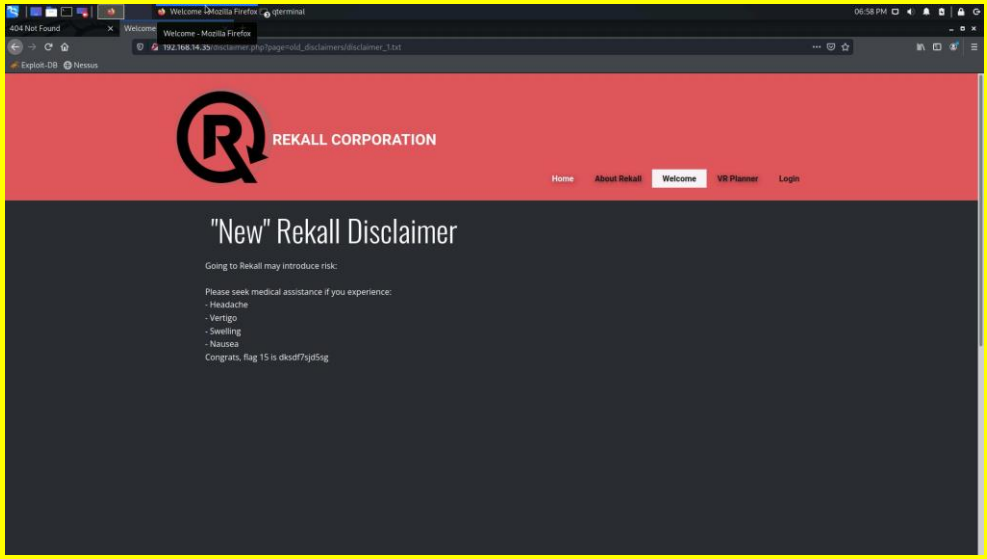
Vulnerability 10	Findings
Title	PHP Injection

Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Used the PHP code injection command http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd') which also displayed the content of the /etc/passwd
Images	
Affected Hosts	192.168.14.35
Remediation	Using the basename() and realpath() functions. Leverage Parameterized Queries and Criteria-Based APIs to interpret user data strings – This is done to ensure that APIs do not accept any string values other than those specified.

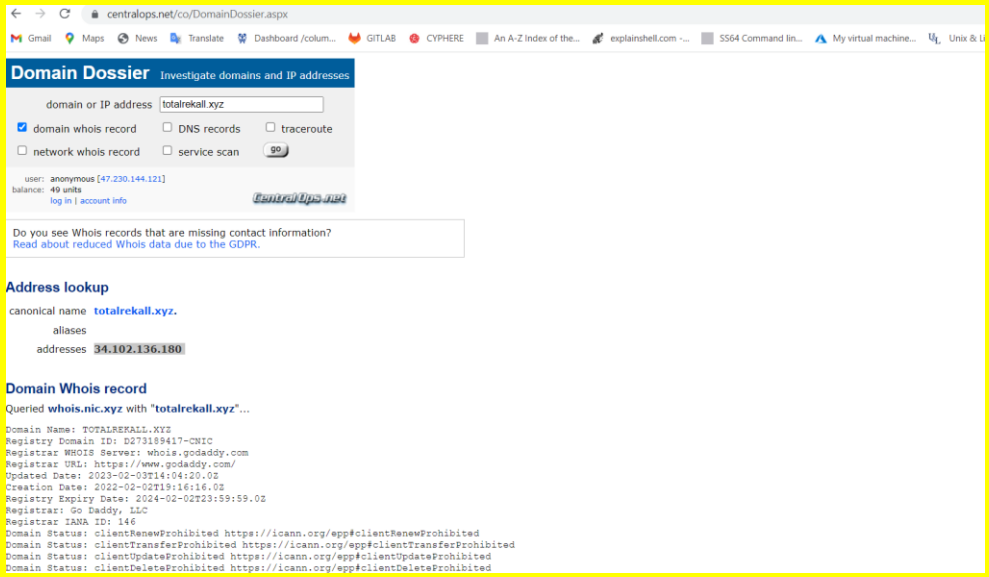
Vulnerability 11	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Used Burp Suite to test out different session IDs in the URL.

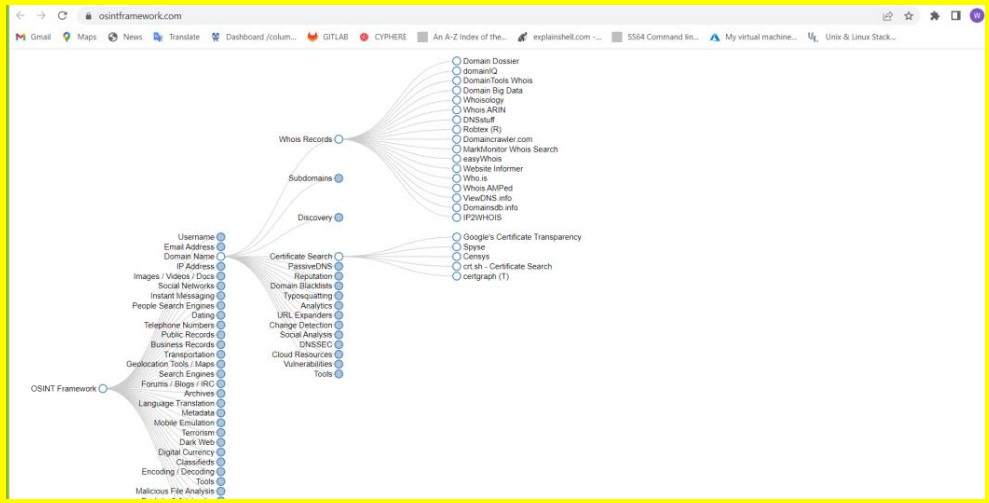
Images	
Affected Hosts	192.168.14.35
Remediation	Use an up-to-date web-server framework to generate and manage the session identifier token, as this will guarantee values that defy prediction. Take precaution to ensure that the session identifier remains confidential to the application .Never expose the session identifier in a URL, in the contents of a page, or any other insecure location or communication.

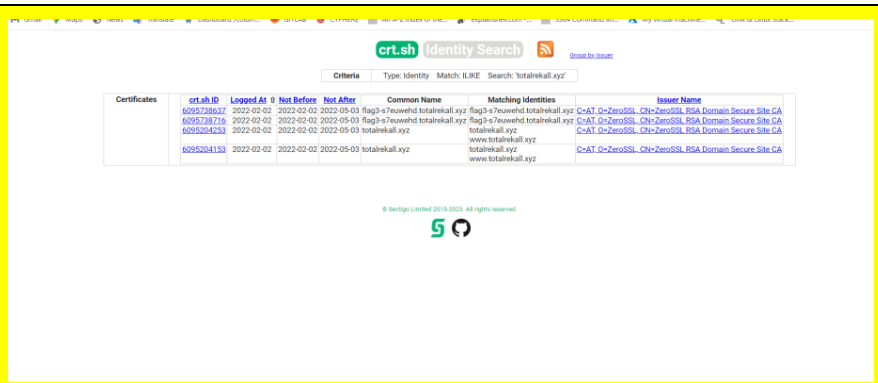
Vulnerability 12	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	Used command injection to access the directory http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt.

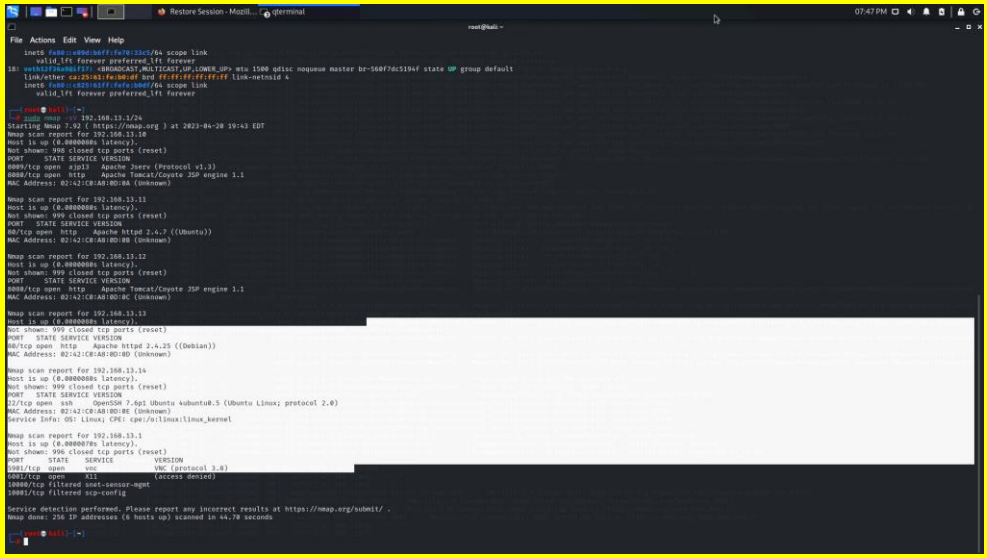
Images	
Affected Hosts	192.168.14.35
Remediation	Ensure the user cannot supply all parts of the path – surround it with your path code. Validate the user's input by only accepting known good – do not sanitize the data.

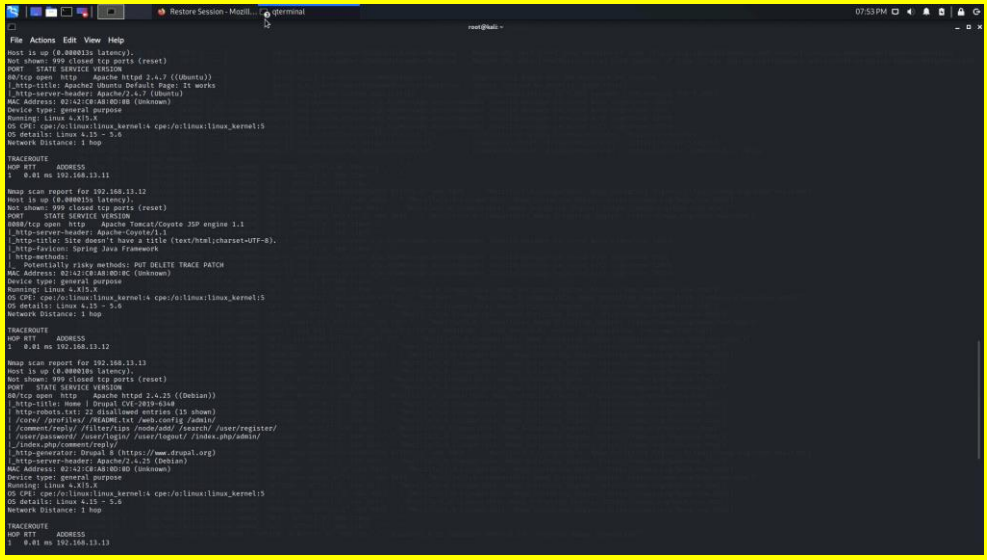
Vulnerability 13	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	On the Domain Dossier webpage, viewed the WHOIS data with OSINT for Total rekall.xyz to access sensitive information
Images	

	
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Ensure no sensitive data is being shared publicly, clean up WHOIS records.

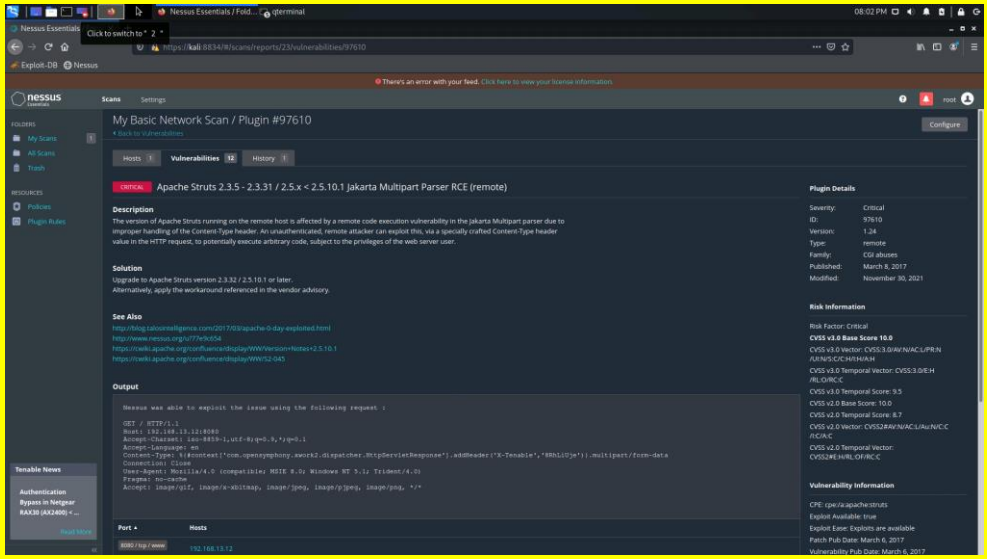
Vulnerability 14	Findings
Title	Certificate Search via crt.sh
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Searched for totalrekall.xyz on crt.sh
Images	

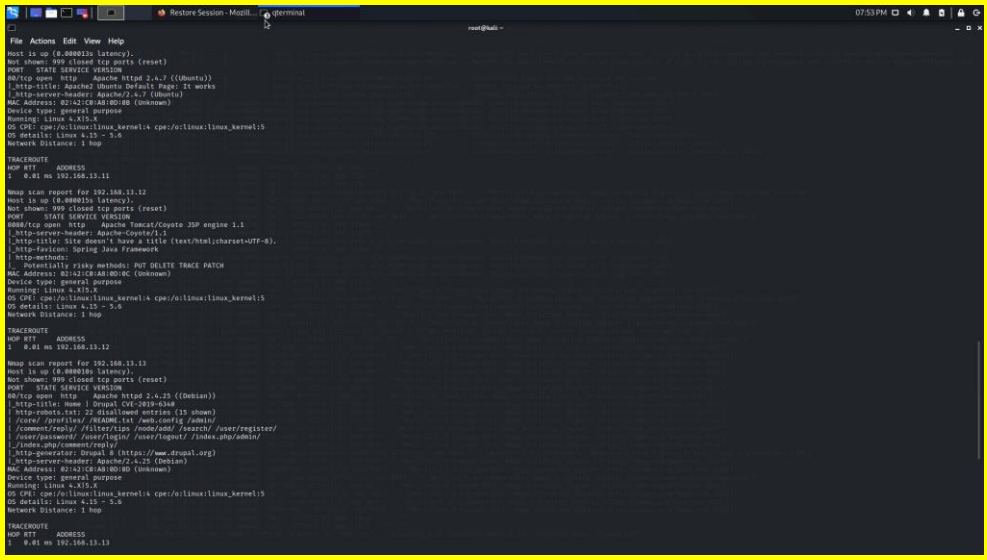
	
Affected Hosts	34.102.136.180
Remediation	Protect information from being exposed by the crt.sh site

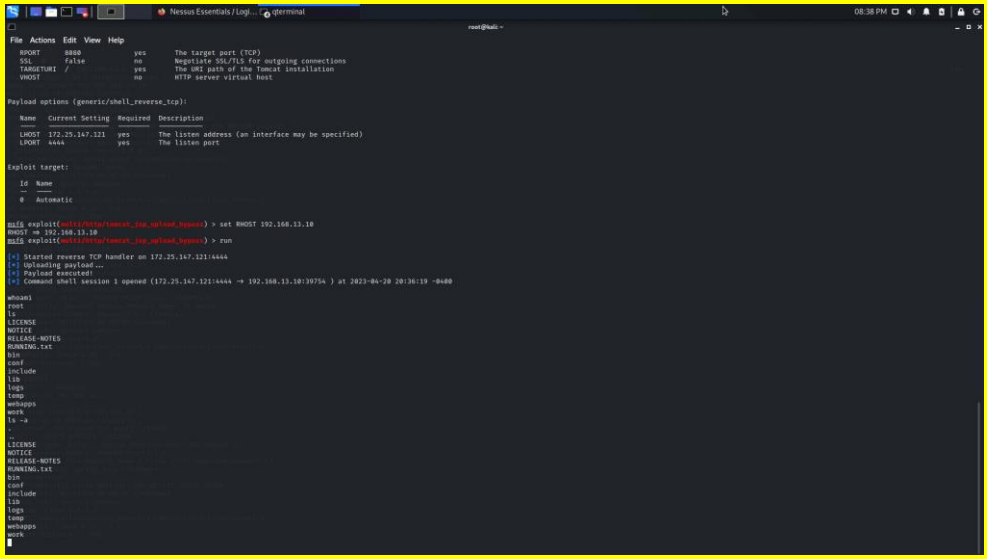
Vulnerability 15	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's
Images	
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Hide the IP addresses or Servers from unauthorized Users

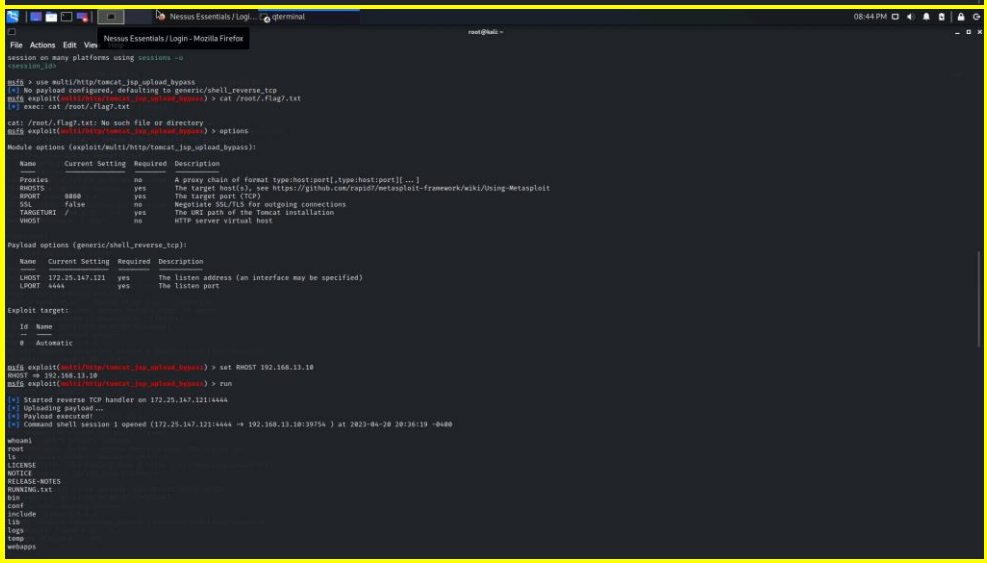
Vulnerability 16	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal
Images	
Affected Hosts	192.178.13.13
Remediation	Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information.

Vulnerability 17	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	

Images	
Affected Hosts	192.178.13.12
Remediation	Run the updated version of Apache or do continues updates of Apache

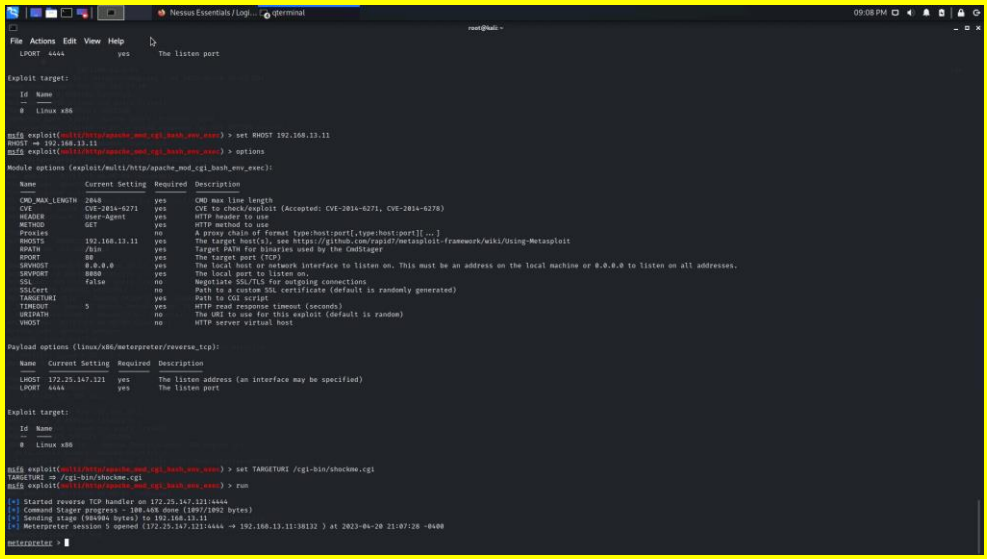
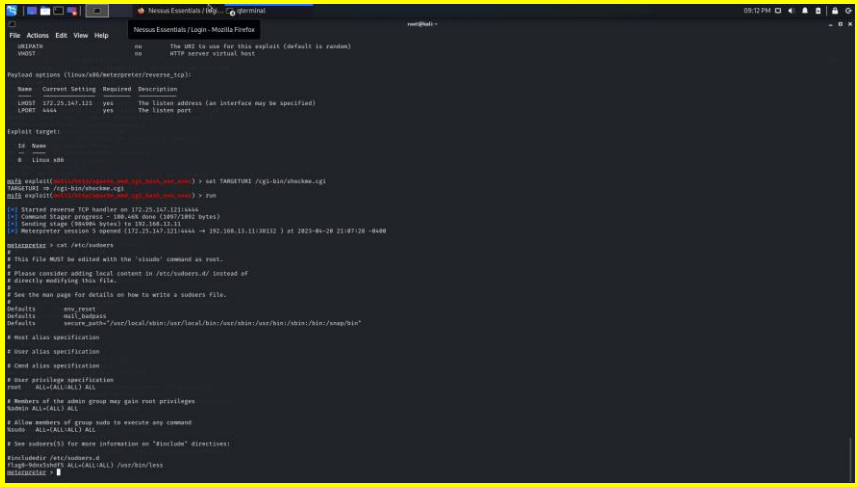
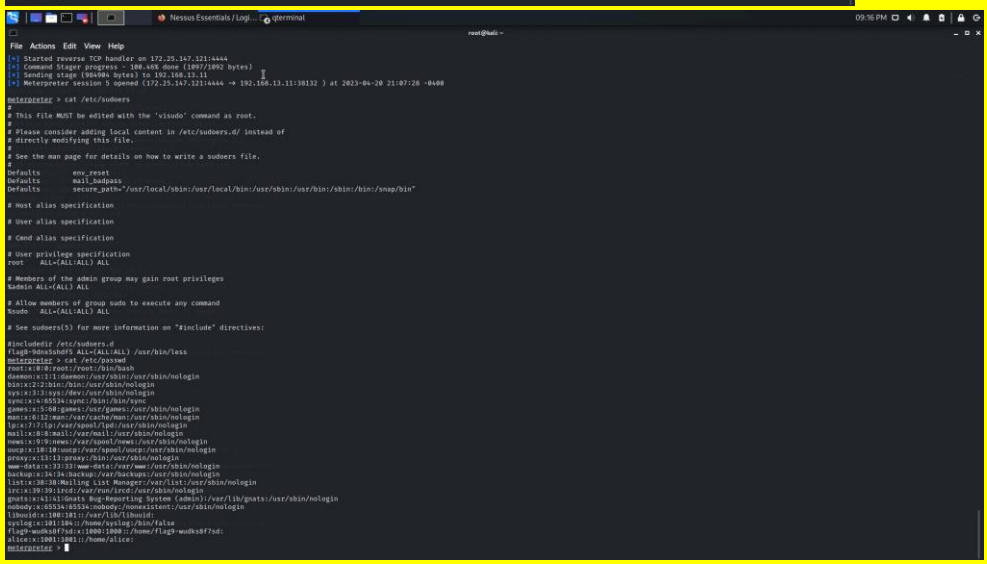
Vulnerability 18	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Run MSFconsole and search for exploits that have Tomcat and JSP. The exploit multi/http/tomcat_jsp_upload_bypass was used and set the option for the RHOST to 192.168.13.10. SHELL command was run once the Meterpreter shell was accessed to access the command line and cat/root/file.name was used.
Images	

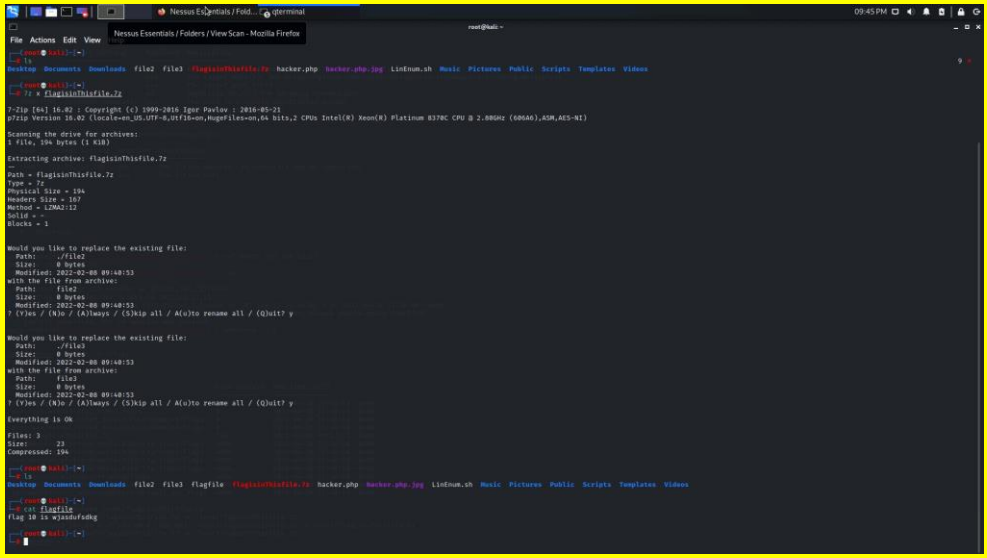


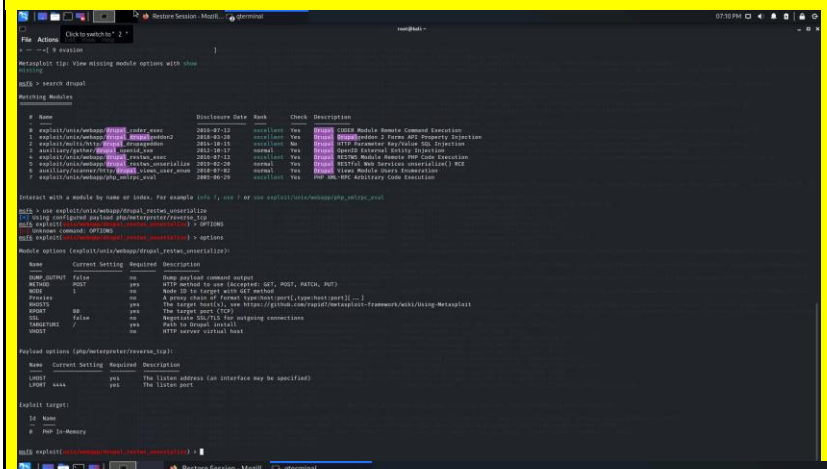
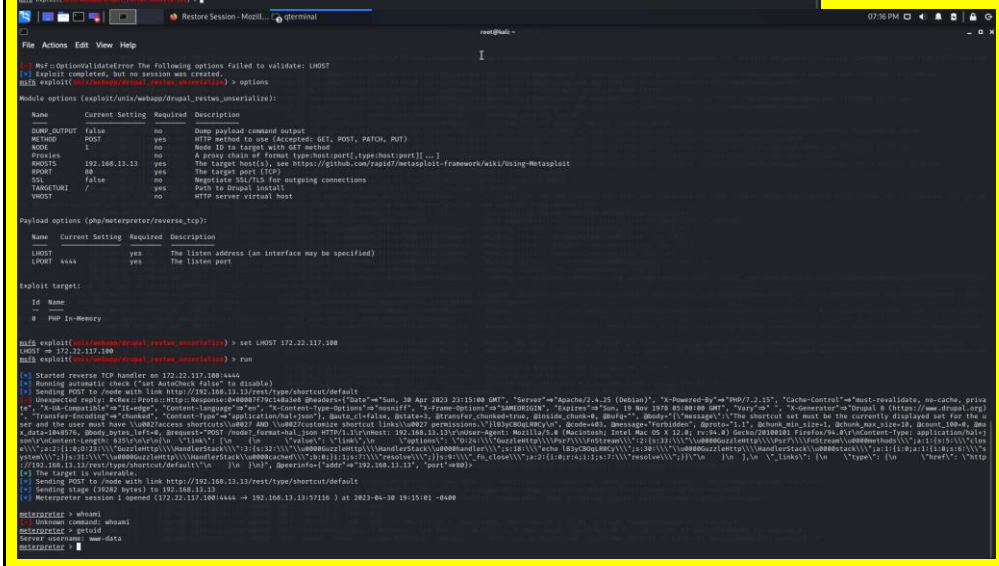


Affected Hosts	192.168.13.10
Remediation	Run Vendor recommended patches. Keep Apache up to date versions

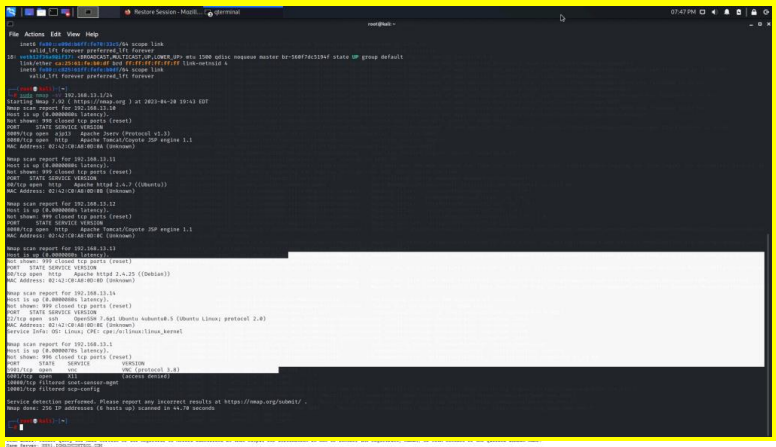
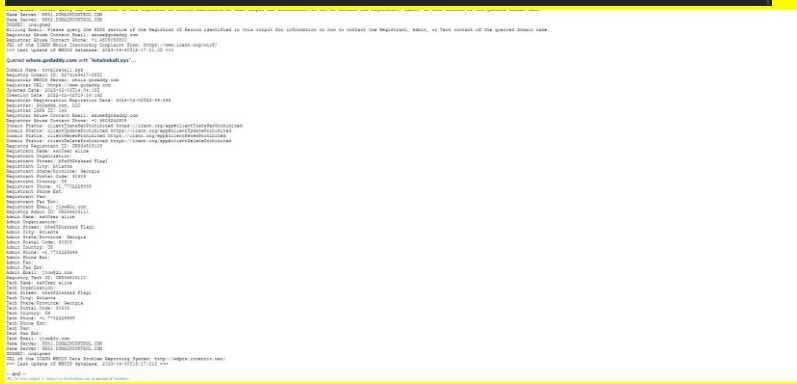
Vulnerability 19	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used exploit (multi/http/apache_mod_cgi_bash_env_exec) set TARGETURI /cgi-bin/shockme.cgi shell Navigate to /etc/sudoers for root privileges file

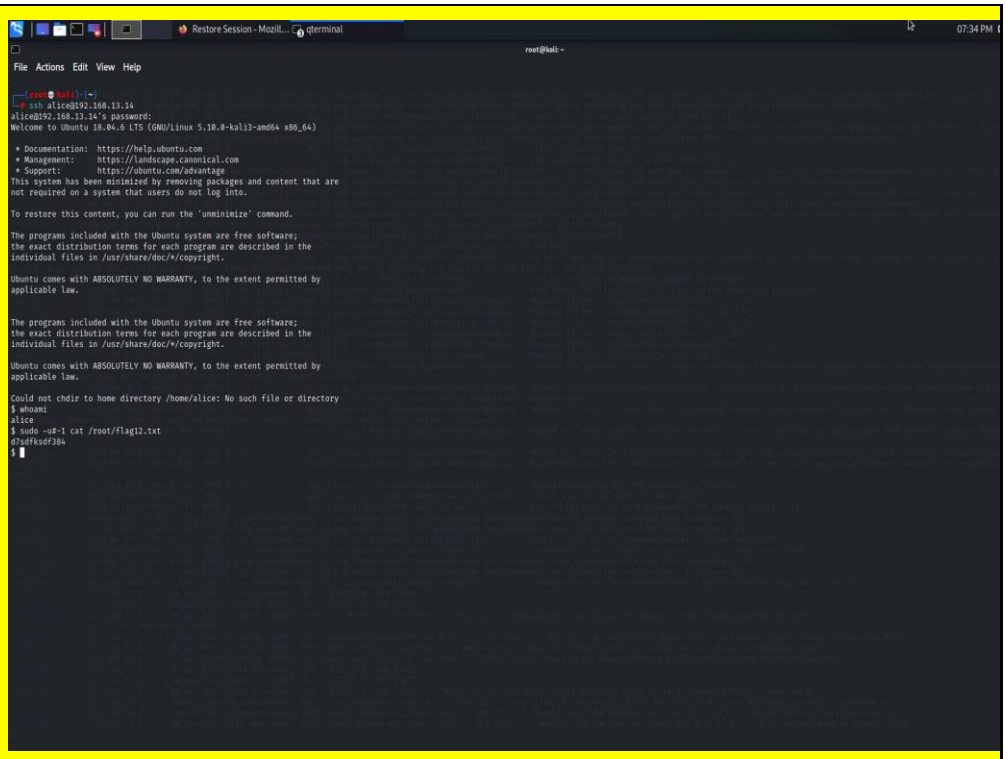
	Image Affected Hosts 192.168.13.11.
Images	  
Affected Hosts	192.168.13.11
Remediation	Edit the sudoers file to limit access for all sudo accounts.

Vulnerability 20	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Searched Apache Struts by connecting through MSFConsole . Used exploit to get a Meterpreter shell: multi/http/struts2_content_type_ognl. Set the RHOSTS to 192.168.13.12 Used Meterpreter to download file /root/flagisinThisfile.7z,unzip the file. Used cat with the file to view the file details.
Images	 
Affected Hosts	192.168.13.12
Remediation	Web application firewalls could mitigate this attack if the rules are set to approve valid content types. Apply updates per vendor instructions.

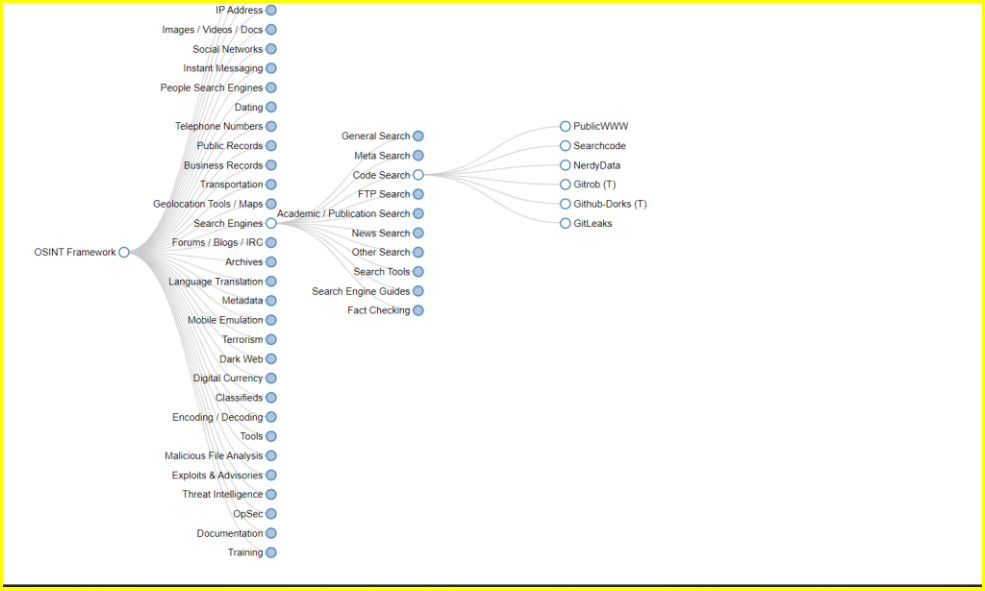
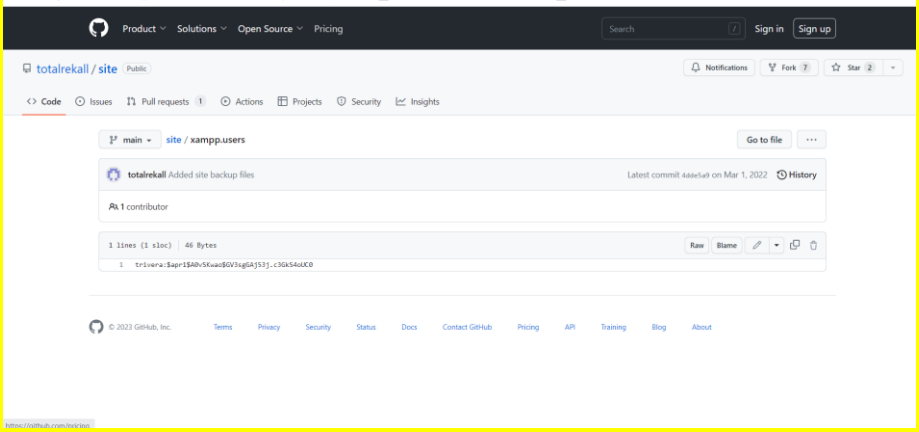
Vulnerability 21	Findings
Title	Drupal- CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Connected to MSFconsole and searched for Drupal expoilts. In the Meterpreter shell used unix/webapp/drupal_restws_unserialize. Set RHOSTS to 192.168.13.13. Runned getuid in the Meterpreter Shell to get the username.
Images	 
Affected Hosts	192.168.13.13

Remediation	Update and patch it to the correct Software version.

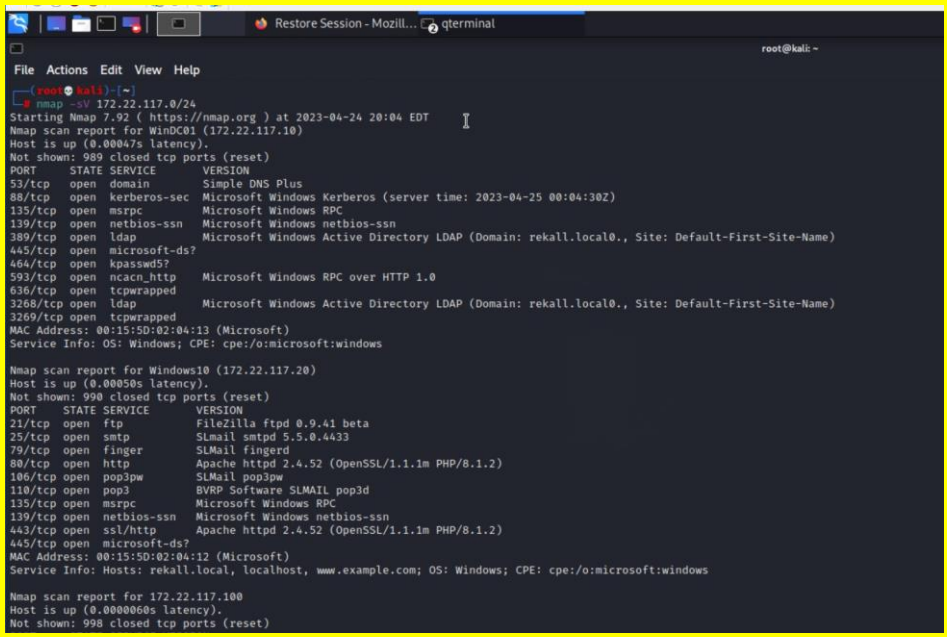
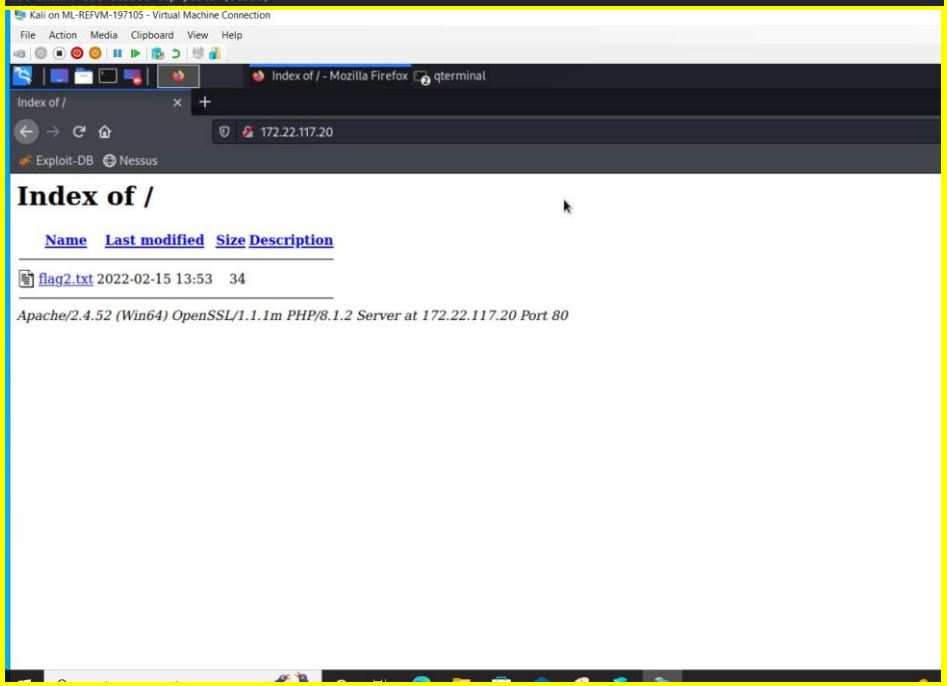
Vulnerability 22	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	This WHOIS data showed sshuser details for alice. SSH was used to access this user and password to escalate to root privileges.
Images	 

	
Affected Hosts	192.168.13.14
Remediation	Close open port 22. Delete user details from WHOIS or hide sensitive information . Enforce stronger credentials, and/or implement 2-factor authentication

Vulnerability 23	Findings
Title	Username and Password Hash in Repo
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Searched Github and found repository containing USER password hash, was able to crack password and gain access using John

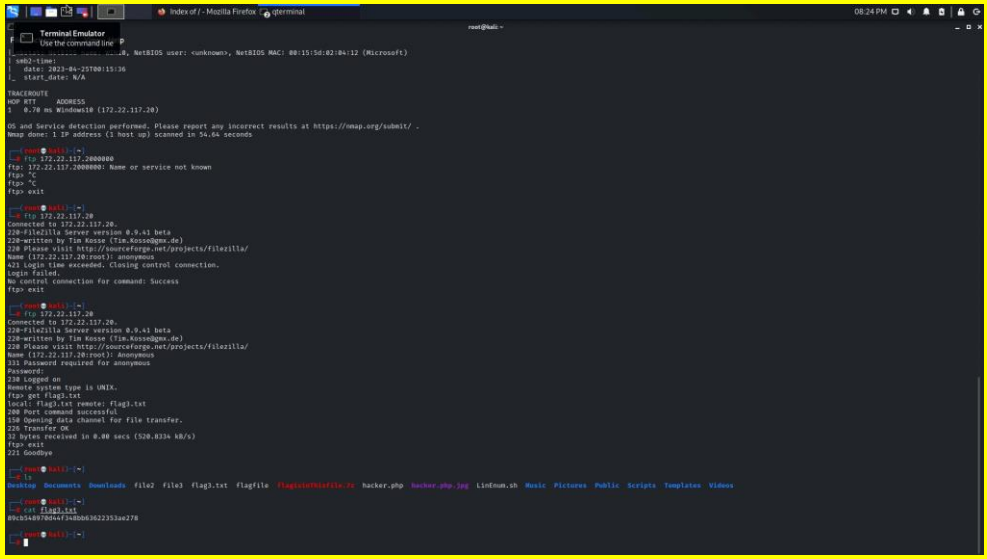
Images	 
Affected Hosts	Total Rekall
Remediation	Restrict access to Repository and remove credentials from Github.

Vulnerability 24	Findings
Title	Port Scan of Subnet
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Port Scan on 172.22.117.0/24 shows Win10 @172.22.117.20 open one of which is HTTP. Used Credentials from the cracked hash password (trivera / Tanya4life) to gain access Port scan using Nmap -A also shows that FTP anonymous access is possible as FTP port was also open.

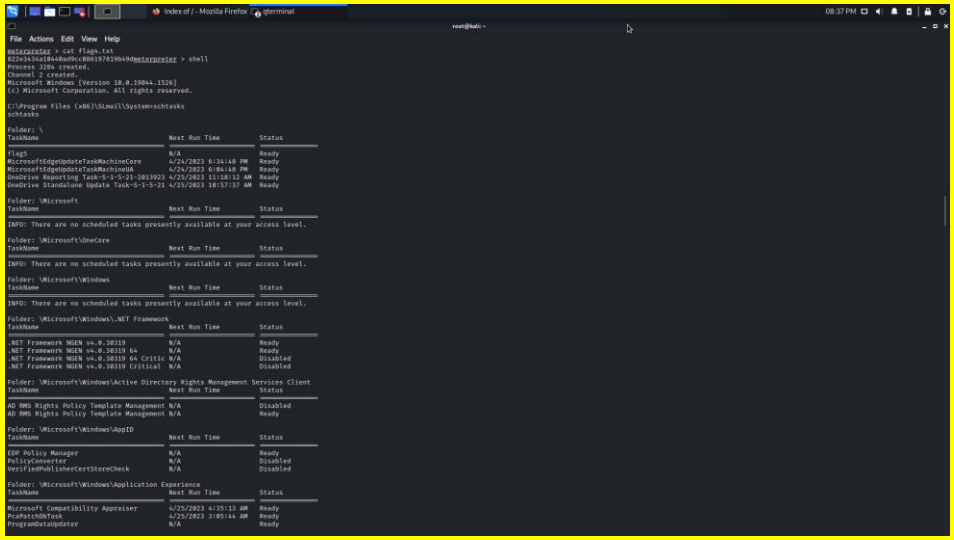
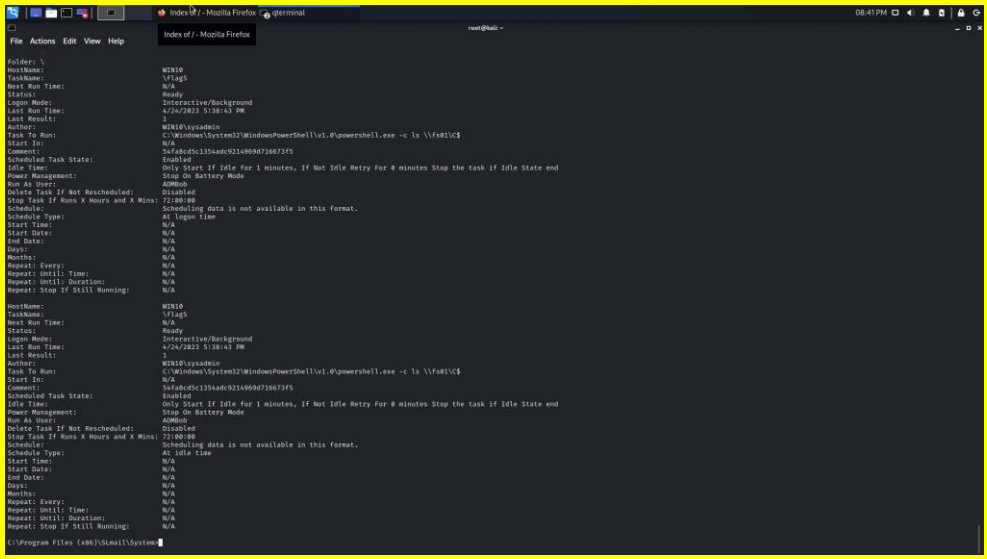
	SMTP port 25 and POP3 port 110 was also open as can be seen from the scans.Used searchsploit to find the version of SLMAIL that could be exploited. Metasplioit via MSFconsole was used to load the SLMail module and settings of the RHOSTS was changed tp 172.22.117.20.Exploit was done by listing the files in the directory. cat was used to view file content.
Images	 

```
Restore Session - Mozill...   qterminal
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-24 20:04 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00047s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-04-25 00:04:30Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:13 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00050s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
79/tcp   open  finger        SLMail fingerd
80/tcp   open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
106/tcp  open  pop3pw        SLMail pop3pw
110/tcp  open  pop3          BVRP Software SLMAIL pop3d
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
445/tcp  open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
```

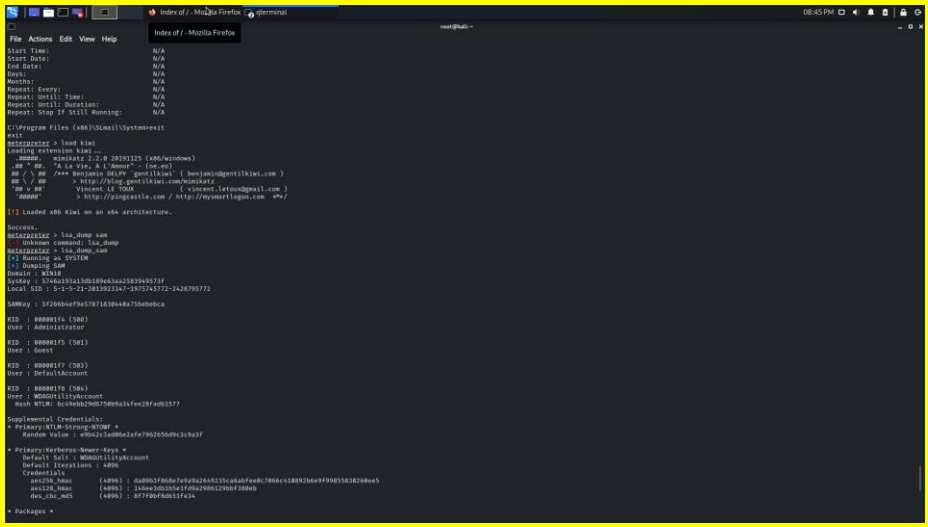
```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File  Action  Media  Clipboard  View  Help
Index of / - Mozilla Firefox   qterminal
Index of /
172.22.117.20
Exploit-DB  Nessus

Index of /

Name  Last modified  Size  Description

flag2.txt  2022-02-15 13:53  34

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80
```



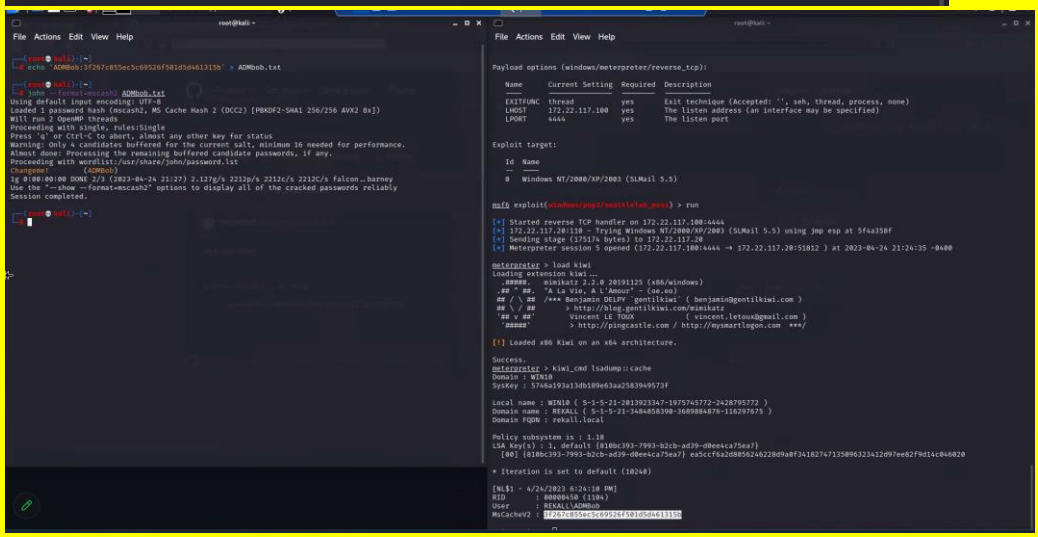
Affected Hosts	172.22.117.20
Remediation	Use stronger credentials or two factor authentication Ports can also be closed if not in use .

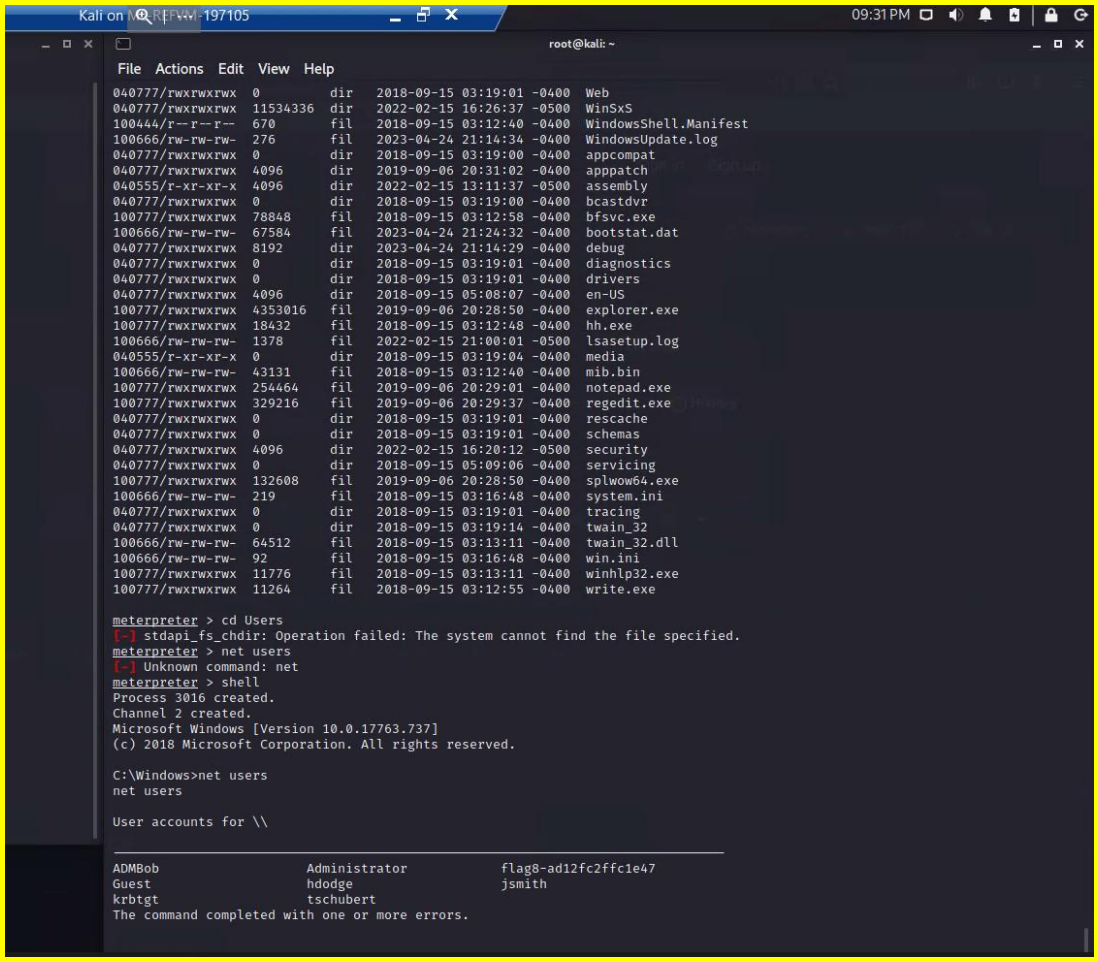
Vulnerability 25	Findings
Title	Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Within the Windows 10 machine, able to view details of scheduled tasks. This can be done by using the command shell within Meterpreter and using the schtasks command schtasks /query. task was viewed by using command schtasks /query /TN flag5 /FO list /v.
Images	 
Affected Hosts	172.22.117.20
Remediation	Change permissions on accounts to restrict unauthorized access.

Vulnerability 26	Findings

Title	Credential Dump (Kiwi)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Used Kiwi to dump credentials using command lsa_dump_sam.Cracked the password using John . Also used kiwi to dump the cached credentials on Win10 which revealed an administrator, ADMBob Used John to crack the password. By moving to root and listing the files, cat can be used to read the content
Images	

```
root@kali: ~
File  Actions  Edit  View  Help
    inet6 fe80::62ad:611a:932a:90e5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:02:04:20 brd ff:ff:ff:ff:ff:ff
    inet 172.31.31.68/20 brd 172.31.31.255 scope global dynamic noprefixroute eth2
       valid_lft 82807sec preferred_lft 82807sec
    inet6 fe80::ee0b:8c92:b931:9a69/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:02:04:16 brd ff:ff:ff:ff:ff:ff
    inet 172.22.117.100/16 brd 172.22.255.255 scope global noprefixroute eth3
       valid_lft forever preferred_lft forever
    inet6 fe80::5c1f:969a:2fcb:d99f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
6: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fb:39:db:39 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
7: br-17d0174e49db: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fb:6a:49:cf brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.1/24 brd 192.168.13.255 scope global br-17d0174e49db
       valid_lft forever preferred_lft forever
8: br-8ef4c456a6ce: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:b6:35:ba:83 brd ff:ff:ff:ff:ff:ff
    inet 192.168.14.1/24 brd 192.168.14.255 scope global br-8ef4c456a6ce
       valid_lft forever preferred_lft forever

┌──(root💀 kali)-[~]
└─# echo 'flag6:50135ed3bf5e77097409e4a9aa11aa39' > flag6.txt


┌──(root💀 kali)-[~]
└─# john --format=NT flag6.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
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
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (flag6)
1g 0:00:00:00 DONE 2/3 (2023-04-24 20:48) 9.090g/s 819590p/s 819590c/s 819590C/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀 kali)-[~]
└─#
```





Affected Hosts	172.22.117.20
Remediation	Considering multi-factor authentication (MFA). Another mitigation to restrict mimikatz/kiwi would be removing the debug privilege (SeDebugPrivilege), which is heavily used by it.

Add any additional vulnerabilities below.