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	HAC KORE
Contact Name	Gabriel Aditya
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	13/7/2024	Gabriel	

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.

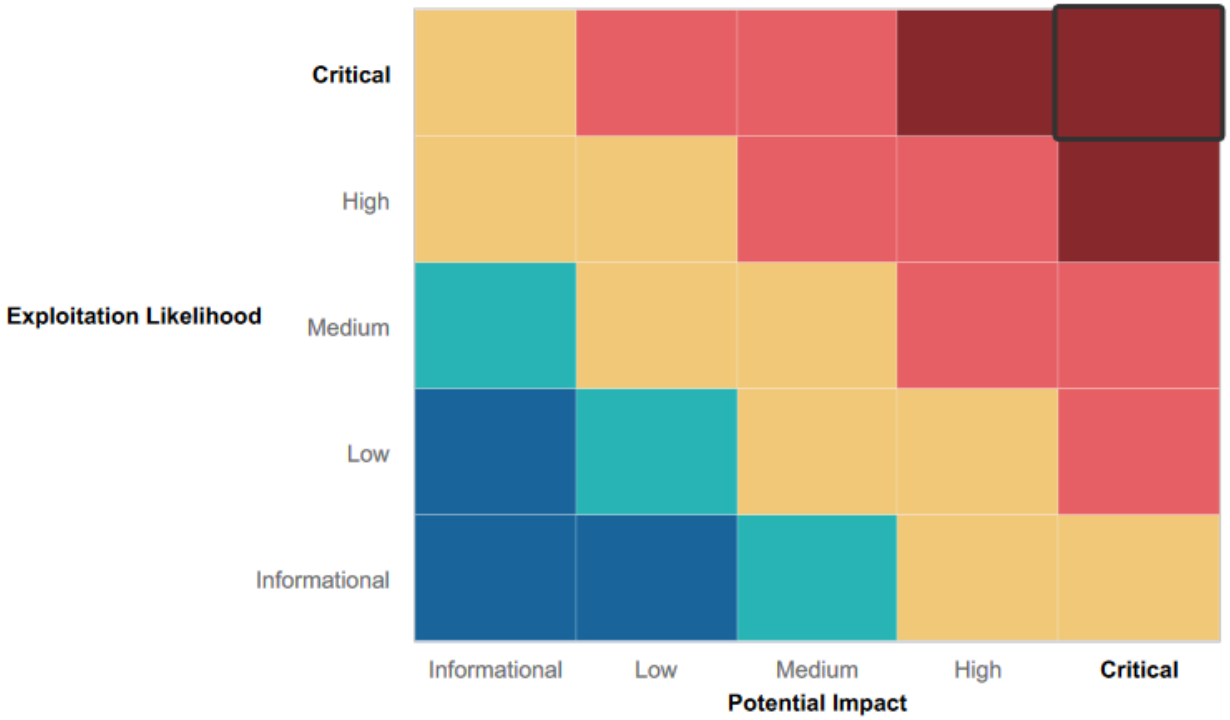
Executive Summary of Findings

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.

- Some input validation is present on the website. (Scripts can't be typed for one of the inputs)
- Website also filters out some command injections

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.

Critical Issues:

- Remote access gained on multiple devices due to RCE exploits.
- Weaknesses in internal network security allowed unauthorized access to resources.
- Escalated privileges and potential compromise of administrative accounts.
- Sensitive information leakage through various channels (WHOIS, HTTP headers, Robots.txt).
- SQL injection vulnerability allowing manipulation of database queries.
- Cross-site scripting (XSS) vulnerabilities enabling malicious script injection.
- Local File Inclusion (LFI) vulnerabilities allowing unauthorized file access.
- Brute force attack vulnerability.

High Issues:

- Potential for sensitive information disclosure through public code repositories.
- Web application vulnerabilities like XSS on multiple web pages.
- Techniques to enumerate usernames and locate data within compromised systems.

Low Issues:

- Information leakage through WHOIS lookup, but the impact is minimal.
- Techniques to secure a compromised Windows machine.

Executive Summary

Day 1
- Web App Exploitations (See Vulnerability Findings for more info)

Day 2
- Linux OS Exploitations (See Vulnerability Findings for more info)

Day 3
- Windows OS Exploitations (See Vulnerability Findings for more info)

Summary Vulnerability Overview

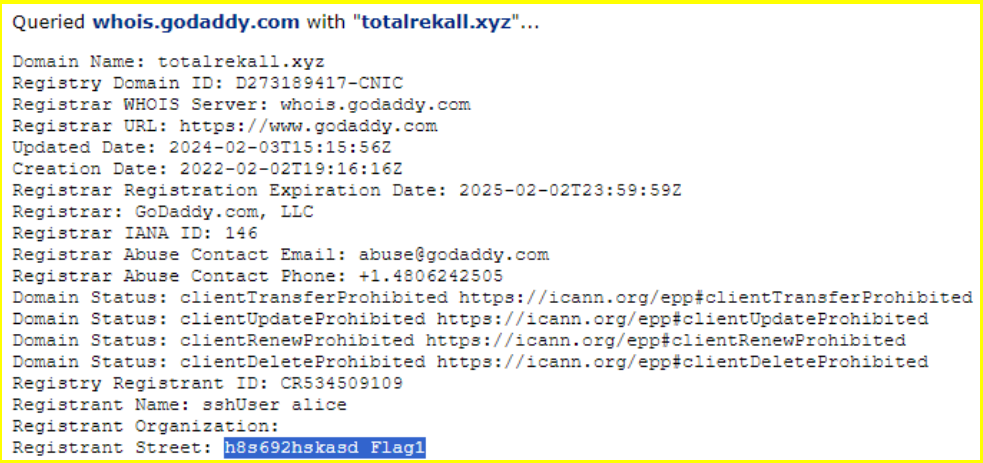
Vulnerability	Severity
Information Disclosure via WHOIS Lookup (Multiple)	Low
Host Count from Network Scan	Critical
Host Running Drupal via Aggressive Scan	High
Nessus Scan	Critical
Exploiting the Host via RCE (Multiple)	Critical
OSINT	High
HTTP Enumeration	Critical
FTP Enumeration	High
Metasploit	Critical
Common Tasks	Low
User Enumeration (Multiple)	Critical
File Enumeration (Multiple)	High
Lateral Movement	Critical
Escalating Access	Critical
Compromising Admin	Critical
Reflected XSS on Welcome.php	High
XSS on Memory-Planner.php (Multiple)	High
Hidden Details on Login.php	Critical
Sensitive Data Exposure via HTTP Headers	Critical
Local File Inclusion on Memory-Planner.php (Multiple)	Critical
SQL Injection on Login.php	Critical
Sensitive Data Exposure via Robots.txt	High
Command Injection via DNS Check	Critical
Advanced Command Injection via MX Record Checker	Critical
Brute Force Attack Vulnerability	Critical

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

Scan Type	Total
Hosts	192.168.14.3580, 192.168.13., 172.22.117.0/24, 172.22.117.20
Ports	21 (FTP), 80 (HTTP), 135 (Locfilestare), 443 (SSL)

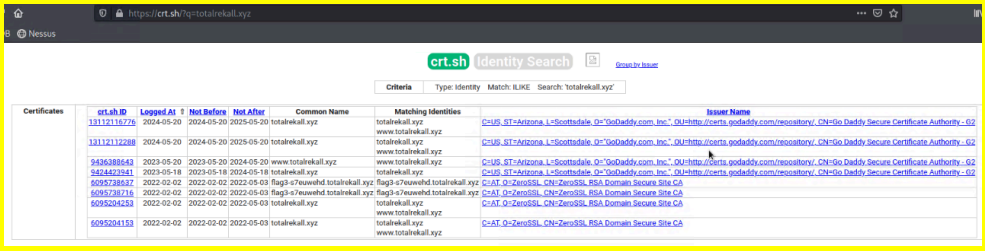
Exploitation Risk	Total
Critical	16
High	7
Medium	0
Low	2

Vulnerability Findings

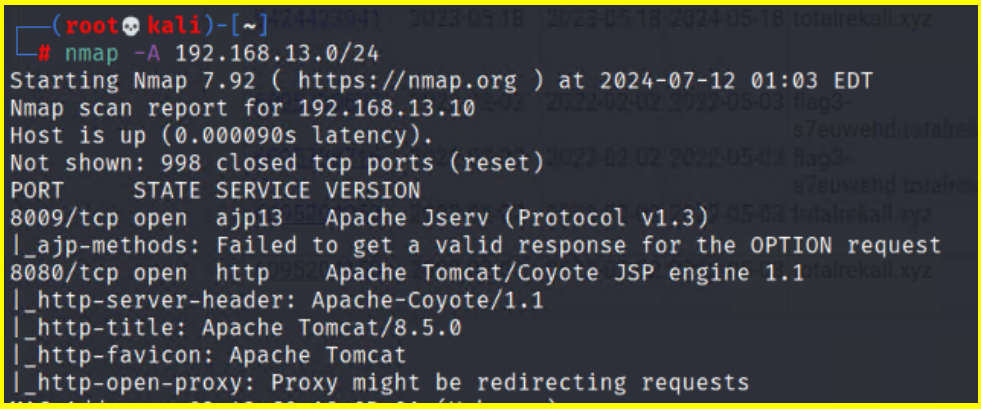
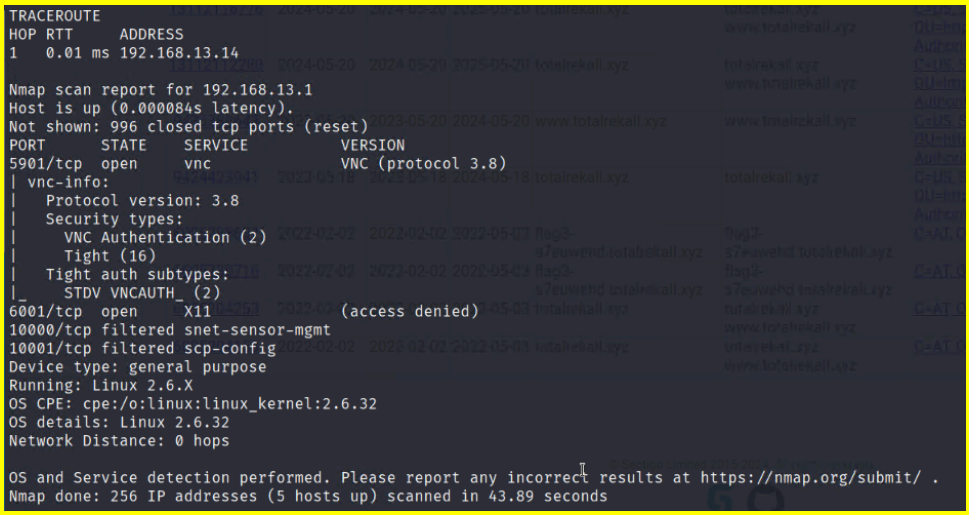
Vulnerability 1	Findings
Title	Information Disclosure via WHOIS Lookup
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	Using the Dossier tool from the OSINT Framework, an open-source intelligence (OSINT) tool, a WHOIS lookup on the domain `totalrekall.xyz` was performed. This lookup revealed public information about the domain's registration, including details that could be used for further OSINT activities. The information obtained could potentially be used by an attacker to gather more intelligence about the website, its owner, and possibly identify further attack vectors.
Images	 
Affected Hosts	192.168.14.35
Remediation	Consider using a domain privacy protection service to mask the WHOIS information. Regularly audit and update your WHOIS records to ensure no sensitive information is publicly available. Monitor and review OSINT data for potential exposure of sensitive information.

Vulnerability 2	Findings
Title	Information Disclosure via WHOIS Lookup
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	By using the Dossier tool from the OSINT Framework, a WHOIS lookup was performed on the domain `totalrekall.xyz`. This lookup revealed the IP address associated with the domain, which is crucial information for further reconnaissance activities. Knowing the IP address can help attackers in mapping the network and planning targeted attacks.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement domain privacy protection to hide sensitive information, including the IP address, in WHOIS records. Use web application firewalls (WAF) to monitor and block malicious traffic. Regularly update and patch all systems and services associated with the domain to reduce the attack surface. Monitor and review OSINT data regularly to ensure no sensitive information is publicly accessible.

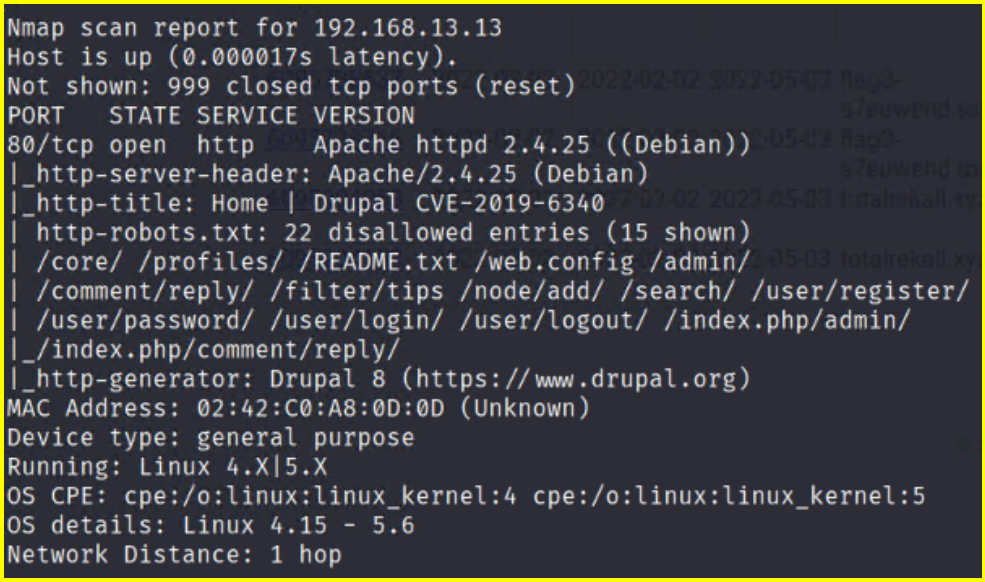
Vulnerability 3	Findings

Title	Information Disclosure via SSL Certificate Research
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	By conducting research on the SSL certificate for the domain `totalrekall.xyz`, additional details about the domain and its configuration were uncovered. SSL certificates often contain valuable information such as the issuer, validity period, and the certificate's public key. These details can be used for further OSINT activities and can help an attacker in profiling the target.
Images	
Affected Hosts	192.168.14.35
Remediation	Regularly renew and update SSL certificates to ensure they are up-to-date and secure. Consider using Extended Validation (EV) SSL certificates for additional trust and security. Monitor and manage your SSL certificates to avoid expired or misconfigured certificates. Implement certificate transparency logging to detect and respond to unauthorized certificate issuance.

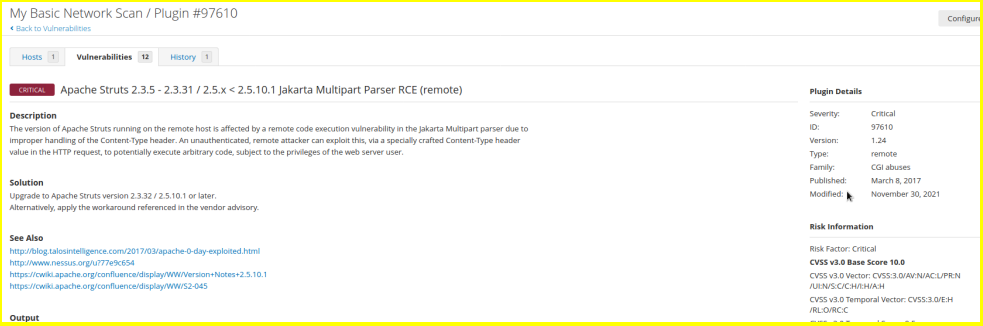
Vulnerability 4	**Findings**

Title	Host Count from Network Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Running an Nmap scan on the network starting with `192.168.13.` will help determine the number of active hosts. This type of scan can be used to map the network and identify available devices, which is a crucial step in network reconnaissance. The flag for this challenge is the total count of active hosts found on the network, excluding the host from which the scan is initiated.
Images	 
Affected Hosts	Any devices with IP addresses in the `192.168.13.*` range.
Remediation	Regularly monitor and audit your network for unauthorized devices. Implement network segmentation to limit the visibility of devices. Use firewalls and access control lists (ACLs) to restrict access to critical resources. Keep your network devices and security systems updated to protect against vulnerabilities.

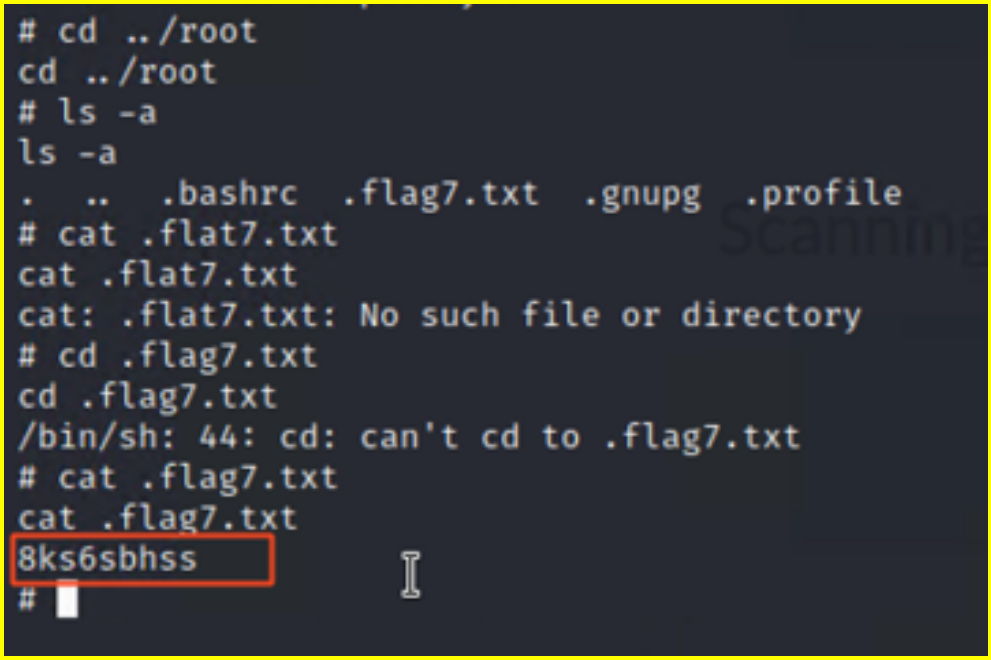
Vulnerability 5	Findings

Title	Host Running Drupal via Aggressive Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	An aggressive scan using Nmap against the discovered hosts in the network can help identify specific services and applications running on those hosts. The goal is to find the IP address of the host running Drupal, a popular content management system. Aggressive scans provide detailed information about open ports, services, and version information, which can be useful for identifying the presence of Drupal.
Images	
Affected Hosts	192.168.13.13
Remediation	Ensure all web applications, including Drupal, are up-to-date with the latest security patches. Regularly audit web servers and applications for vulnerabilities. Implement web application firewalls (WAF) to protect against common web attacks. Limit the exposure of administrative interfaces to trusted IP addresses only.

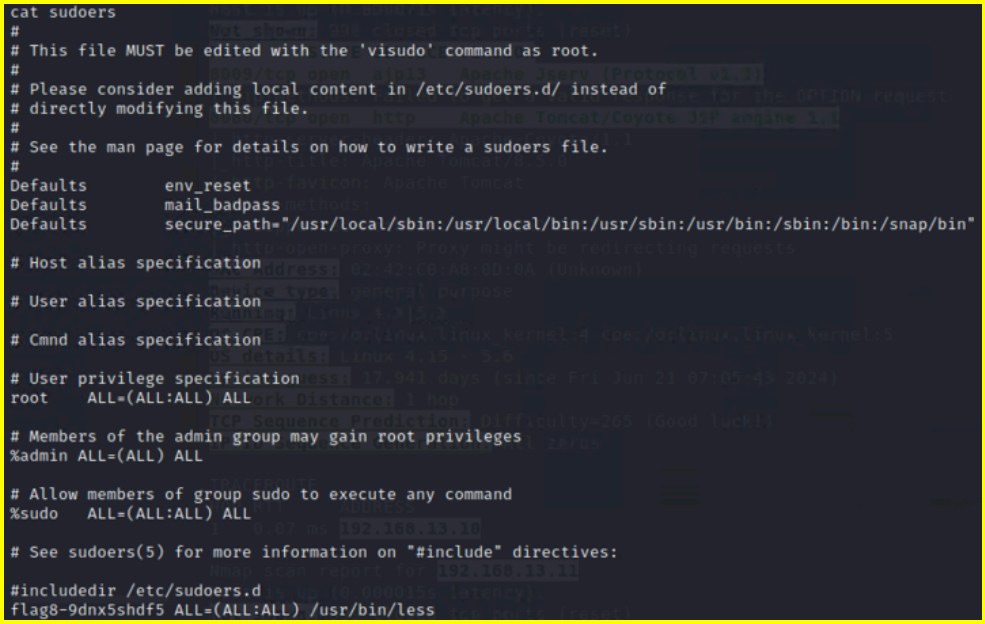
Vulnerability 6	Findings

Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Running a Nessus scan against the host with the IP address 192.168.13.12 helps identify vulnerabilities and potential security issues. Nessus is a comprehensive vulnerability scanner that provides detailed information about discovered vulnerabilities. The goal is to find the ID number of the critical vulnerability detected on the host.
Images	
Affected Hosts	192.168.13.12
Remediation	Address the critical vulnerability by applying necessary patches or updates. Follow the detailed remediation steps provided in the Nessus report. Regularly scan your network and systems for vulnerabilities. Implement security best practices to mitigate potential risks.

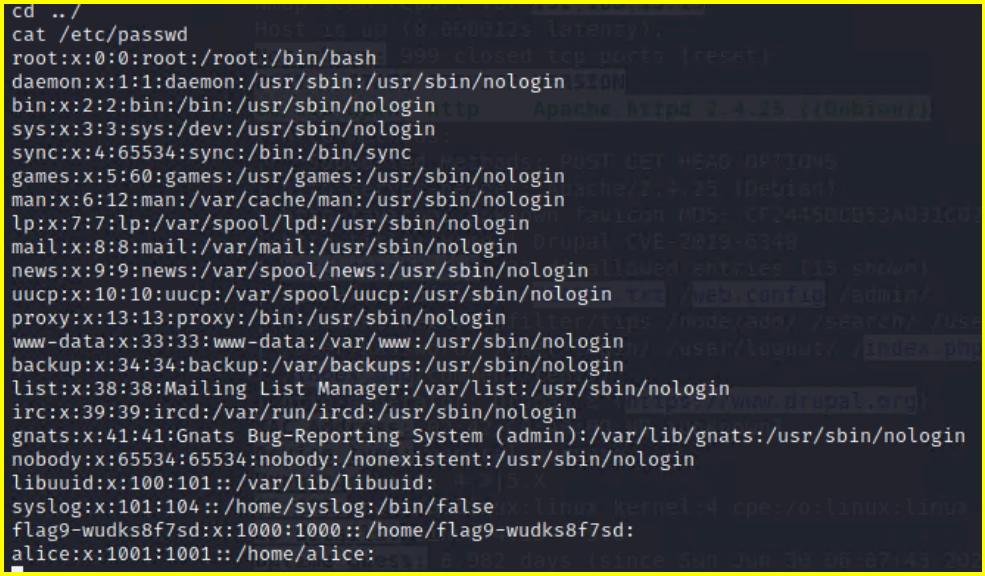
Vulnerability 7	Findings

Title	Exploiting the Host via RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using Metasploit, an RCE (Remote Code Execution) exploit was attempted against the host with the IP address 192.168.13.10. By leveraging information from the aggressive Nmap scan, the appropriate exploit was identified and successfully executed, granting access to the host. After gaining access, a search was conducted on the server to locate Flag 7.
Images	
Affected Hosts	192.168.13.10
Remediation	Patch the vulnerability that allowed the RCE exploit. Regularly update and secure all software and services running on the host. Implement strict access controls and monitoring to detect and respond to unauthorized access. Conduct regular vulnerability assessments and penetration tests to identify and mitigate security risks.

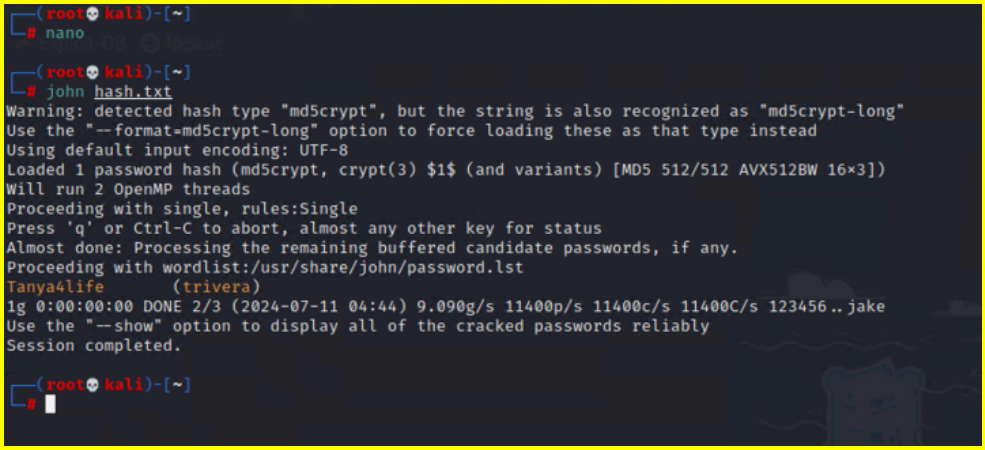
Vulnerability 8	Findings

Title	Exploiting the Host via the "Shocking" Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Using Metasploit, an RCE (Remote Code Execution) exploit, specifically known as the "Shocking" exploit, was attempted against the host with the IP address `192.168.13.11`. By setting the `TARGETURI` option to `/cgi-bin/shockme.cgi`, the exploit was successfully executed, granting access to the host. After gaining access, a search was conducted on the server to locate Flag 8.
Images	
Affected Hosts	192.168.13.11
Remediation	Patch the vulnerability that allowed the RCE exploit. Regularly update and secure all software and services running on the host. Implement strict access controls and monitoring to detect and respond to unauthorized access. Conduct regular vulnerability assessments and penetration tests to identify and mitigate security risks.

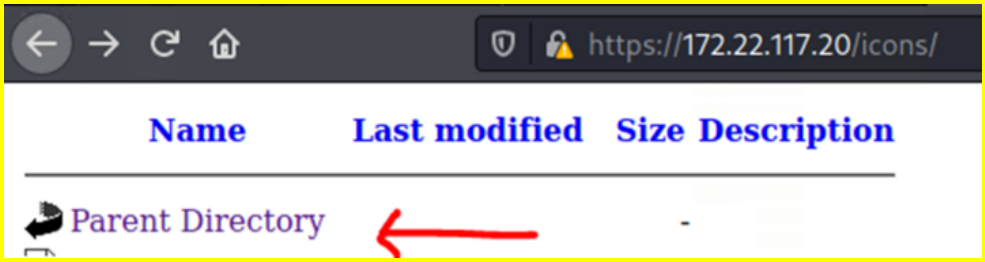
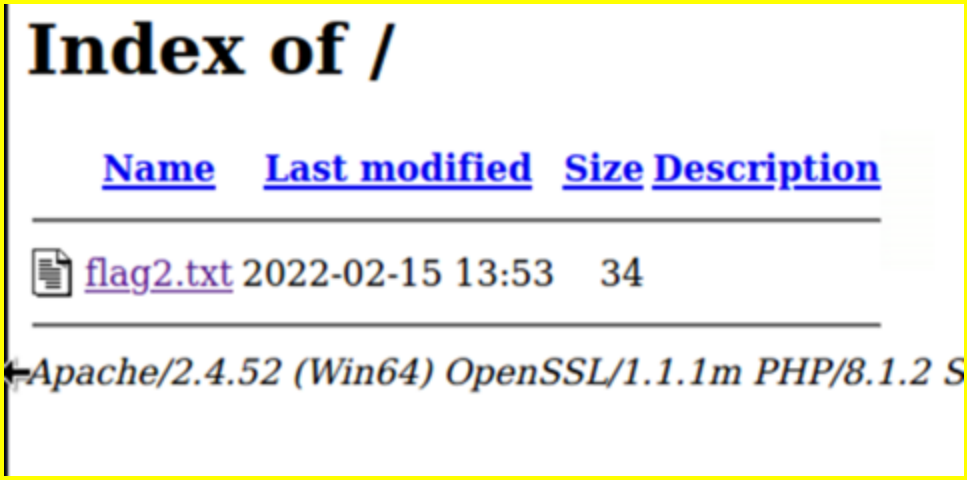
Vulnerability 9	Findings

Title	Continuing the Search on the Exploited Server
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	After successfully exploiting the host at 192.168.13.11 using the "Shocking" exploit and locating Flag 8, the next step is to continue the search on the same server to find Flag 9. Leveraging the access gained, further exploration and enumeration will be conducted to locate Flag 9.
Images	
Affected Hosts	192.168.13.11
Remediation	Ensure all discovered vulnerabilities are patched. Regularly update and secure all software and services running on the host. Implement strict access controls and monitoring to detect and respond to unauthorized access. Conduct regular vulnerability assessments and penetration tests to identify and mitigate security risks.

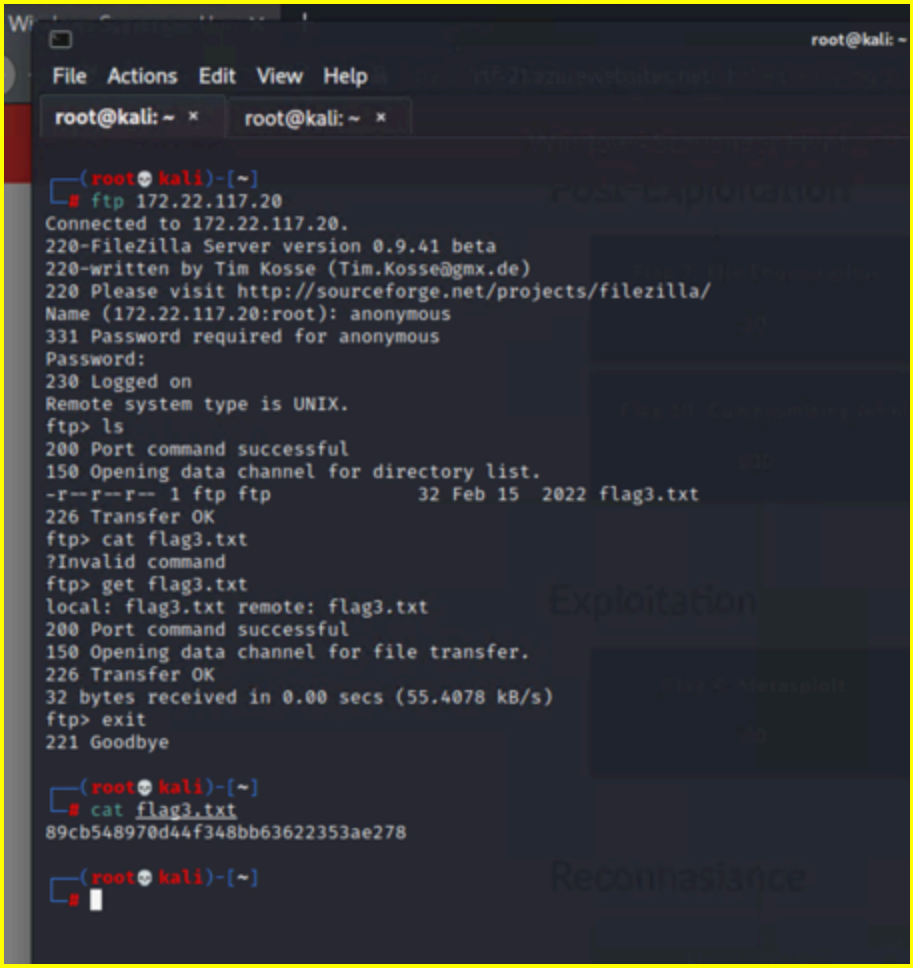
Vulnerability 10	Findings

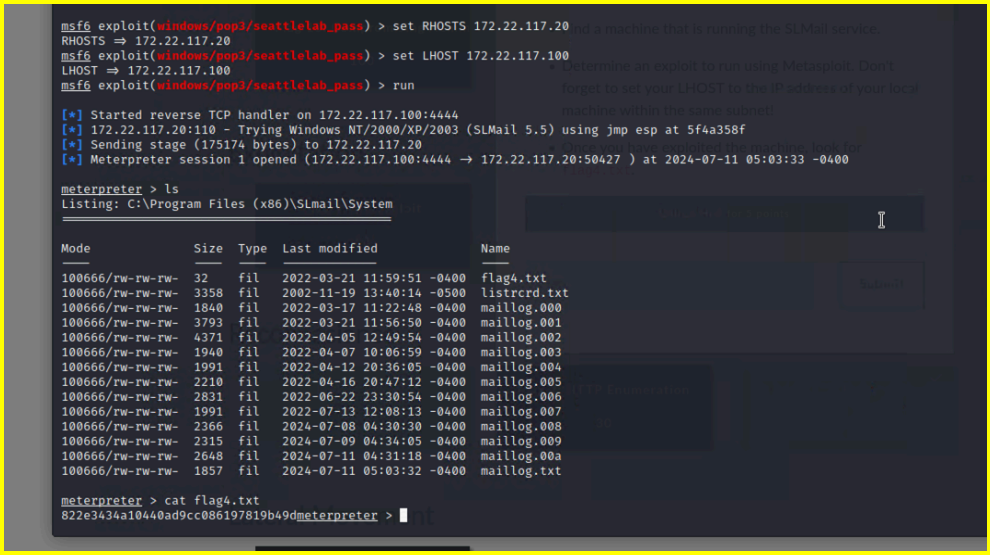
Title	OSINT
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using OSINT techniques, a search was conducted for GitHub repositories associated with the user or organization `totalrekall`. The goal was to find repositories containing user credentials. Once found, any hashed or encoded passwords were cracked to reveal plaintext passwords. The flag is the cracked password of one of the users.
Images	
Affected Hosts	
Remediation	Ensure no sensitive information, such as user credentials, is stored in public repositories. Use environment variables or secret management services to handle sensitive data securely. Regularly audit your code repositories for exposed credentials and other sensitive information. Enforce strong password policies and use multi-factor authentication (MFA).

Vulnerability 11	Findings

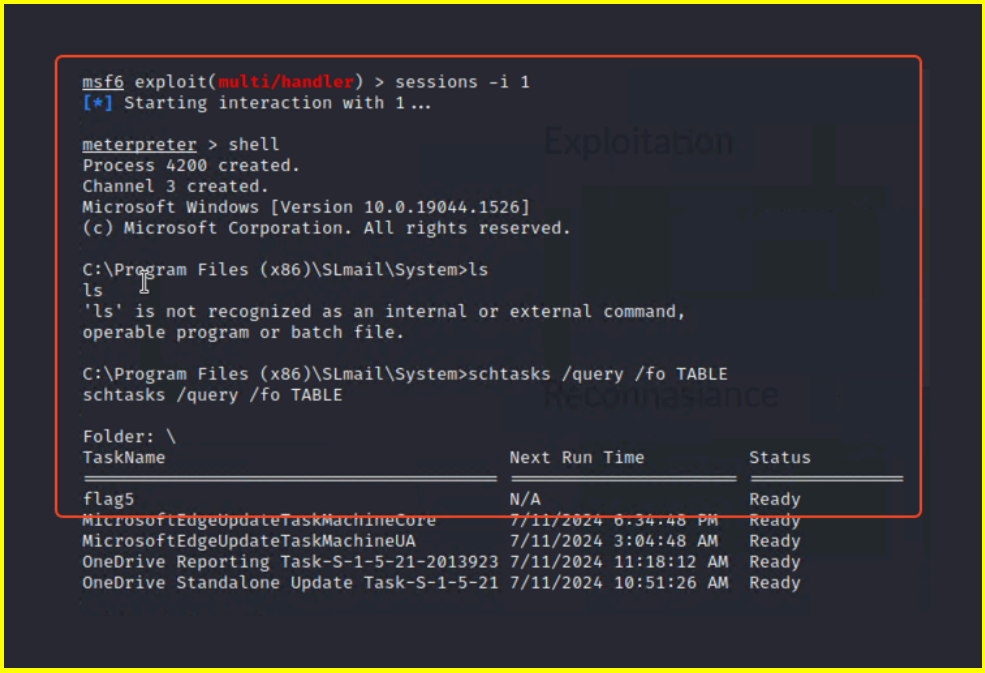
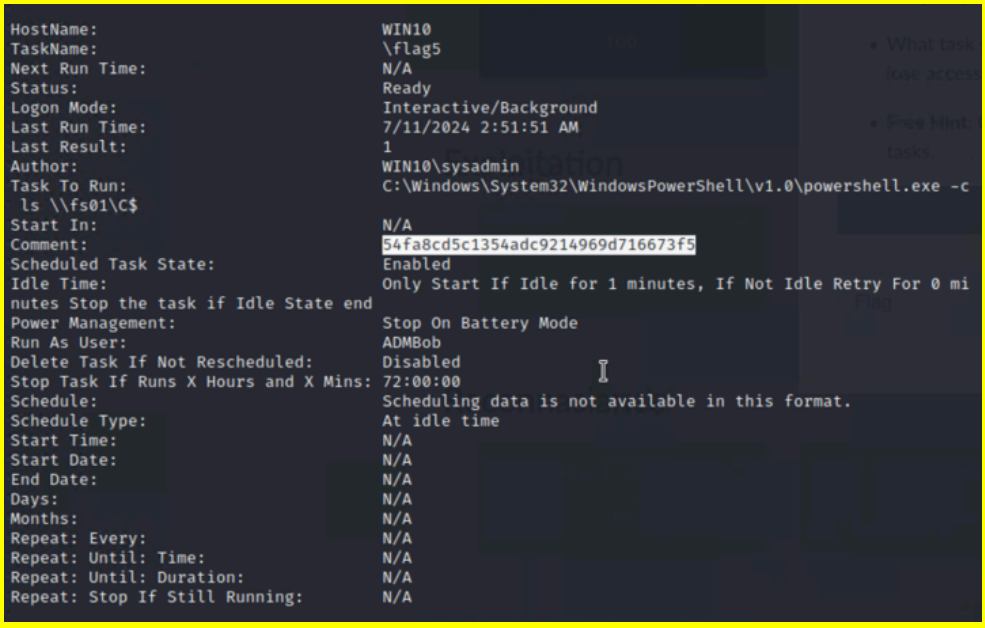
Title	HTTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Using the cracked credentials obtained from Flag 1, an HTTP enumeration was conducted on the internal Windows network with the subnet `172.22.117.0/24`. The goal was to find a website hosted on the internal network and locate a specific file containing the flag.
Images	 
Affected Hosts	Any web servers within the subnet `172.22.117.0/24`.
Remediation	Ensure all internal websites are properly secured and accessible only to authorized users. Regularly update and patch all web servers and applications to mitigate vulnerabilities. Implement network segmentation and firewall rules to restrict access to sensitive internal resources. Conduct regular security audits and penetration tests on internal networks and applications.

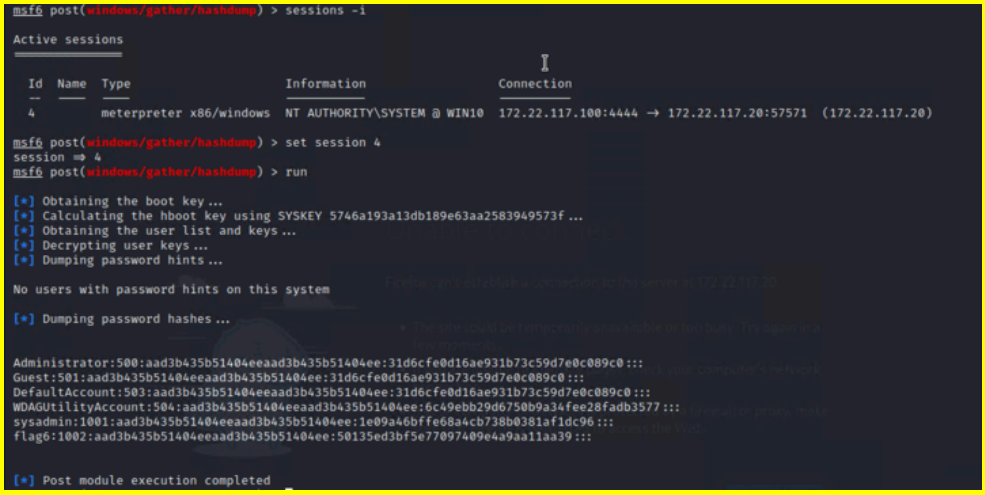
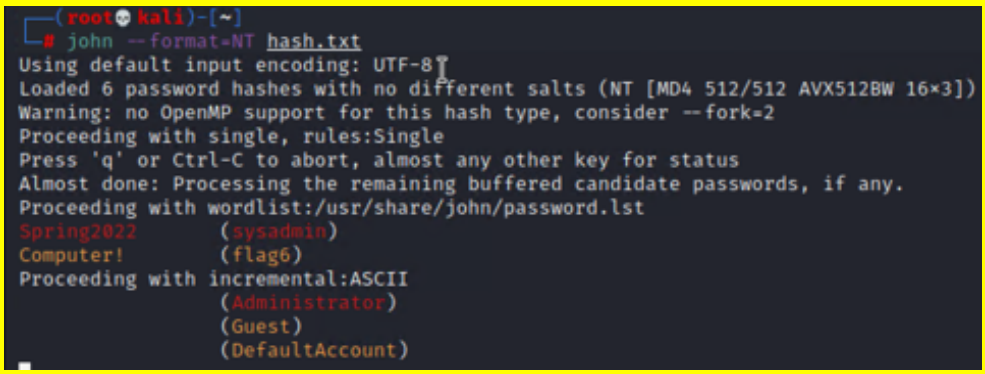
Vulnerability 12	Findings

Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using FTP enumeration, the goal is to access a file containing Flag 3. An aggressive Nmap scan will help determine the FTP service and its configuration on the target network. Once identified, the credentials from Flag 1 will be used to log into the FTP service and locate the file with the flag.
Images	
Affected Hosts	172.22.117.20
Remediation	Ensure all FTP servers are properly secured with strong credentials and regular updates. Disable anonymous FTP access if not needed. Implement secure alternatives such as SFTP or FTPS. Conduct regular security audits and penetration tests to identify and mitigate vulnerabilities.

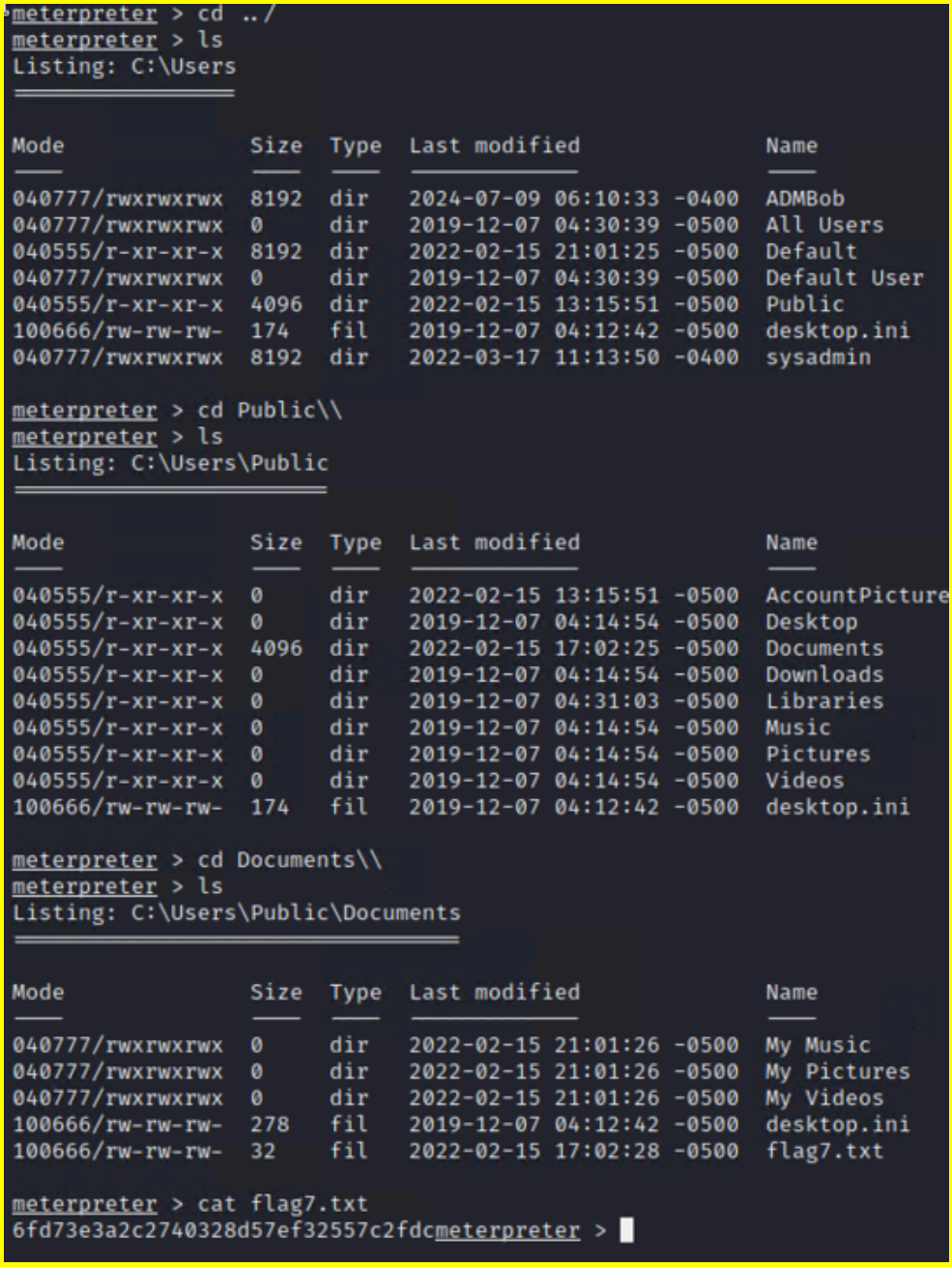
Vulnerability 13	Findings
Title	Metasploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	The objective is to find a machine running the SLMail service and exploit it using Metasploit. After successfully exploiting the machine, the goal is to locate and retrieve the file `flag4.txt`.
Images	
Affected Hosts	172.22.117.20
Remediation	Patch or update vulnerable SLMail servers to the latest versions. Implement network segmentation and firewall rules to restrict access to critical services. Monitor network traffic and system logs for suspicious activities.

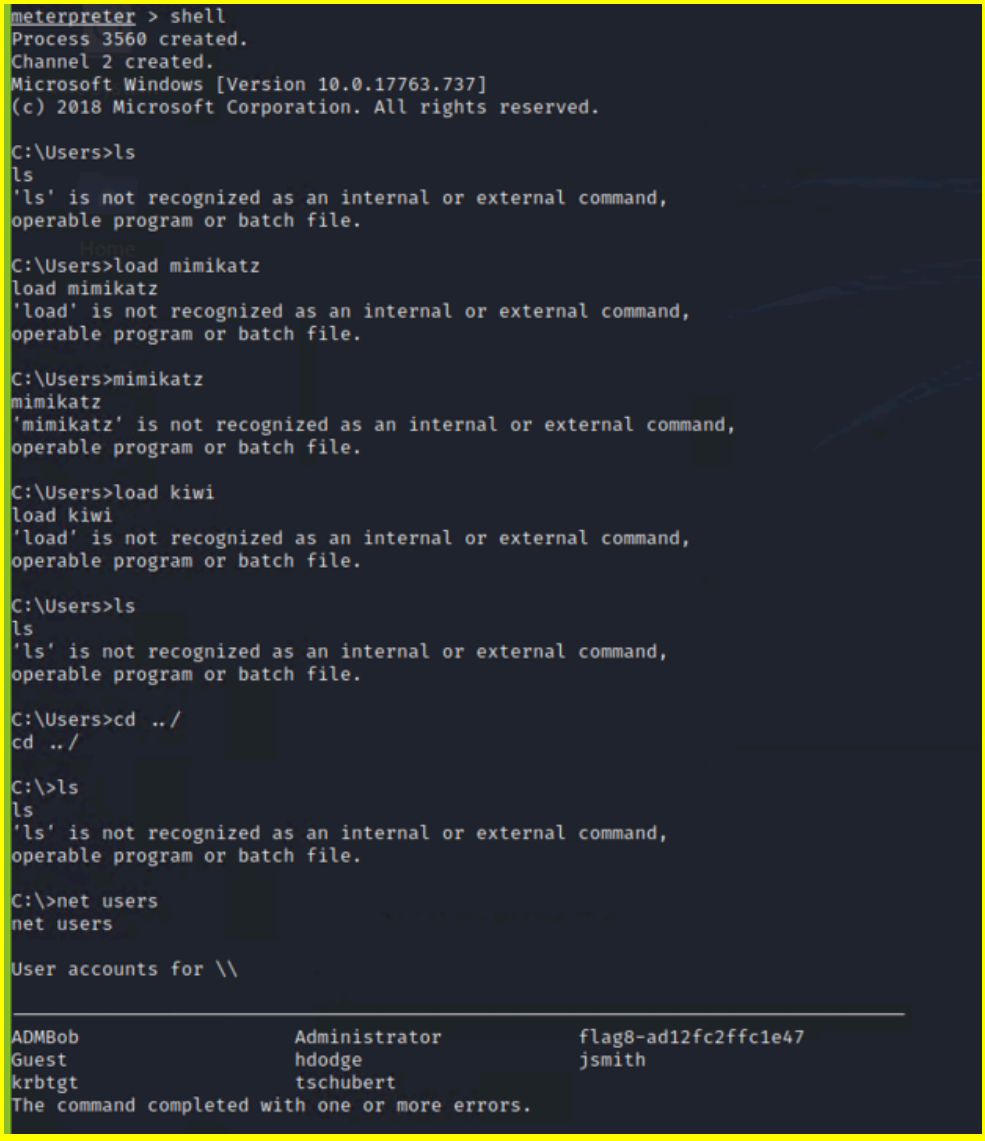
Vulnerability 14	Findings

Title	Common Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Low**
Description	The task involves determining the critical actions to take upon gaining initial access to a Windows 10 machine, preparing for potential loss of access.
Images	 
Affected Hosts	172.22.117.20
Remediation	Evaluate and disable unnecessary scheduled tasks to mitigate potential access loss risks.

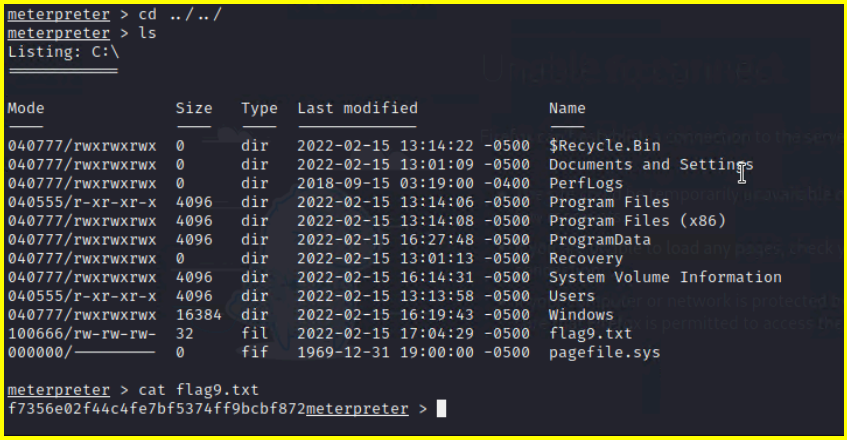
Vulnerability 15	Findings
Title	User Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Obtain plaintext password of a specific user on the exploited
Images	 
Affected Hosts	172.22.117.20
Remediation	Change compromised user's password, review access controls, and strengthen user authentication mechanisms.

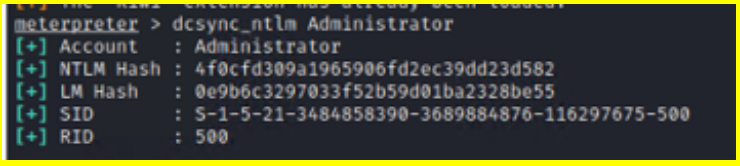
Vulnerability 16	Findings

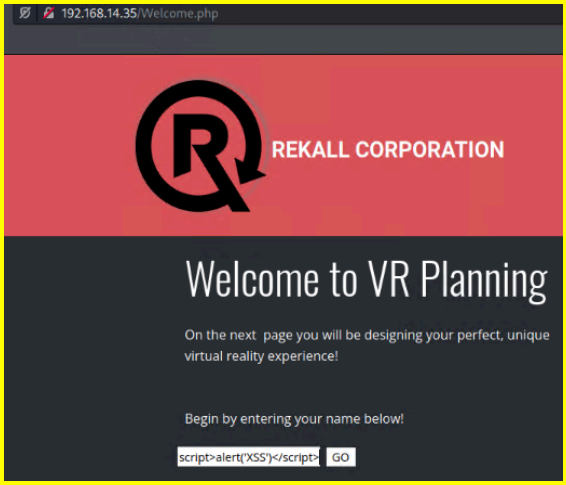
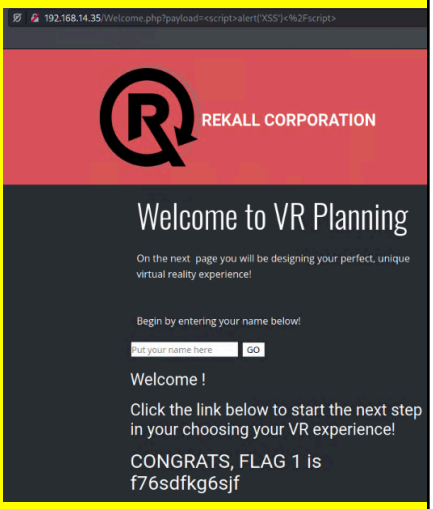
Title	File Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Locate the flag within publicly accessible files on the exploited
Images	
Affected Hosts	172.22.117.20
Remediation	Review and restrict access permissions to sensitive files, conduct regular audits of file permissions and contents.

Vulnerability 17	Findings
Title	User Enumeration pt.2
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Lateral movement from Windows 10 to Windows Domain Controller (WinDC) using compromised credentials. Search for accounts on the WinDC machine.
Images	
Affected Hosts	172.22.117.20
Remediation	Implement network segmentation, strong password policies, and monitor lateral movement to prevent unauthorized access between systems.

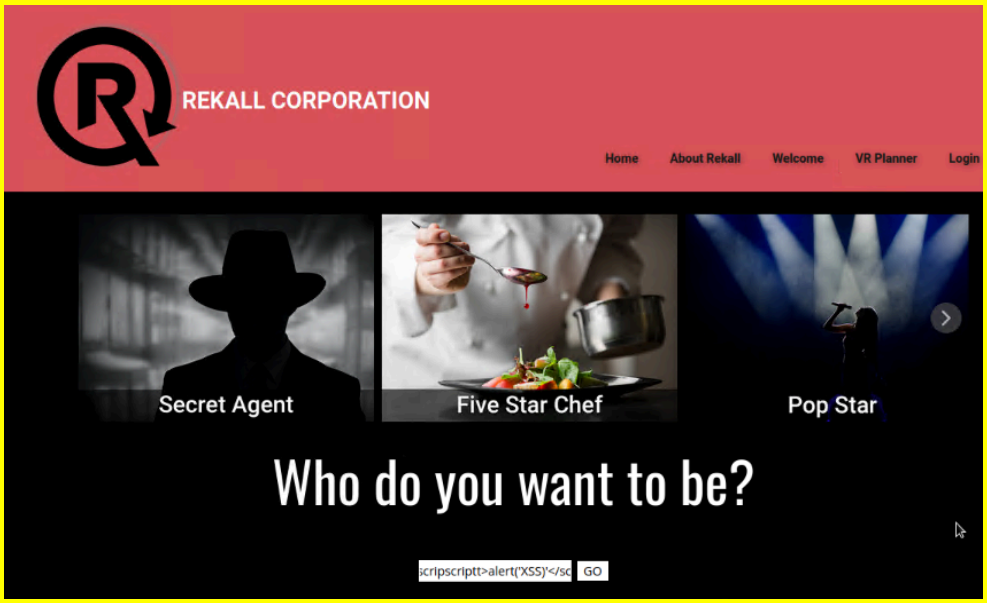
Vulnerability 18	Findings

Title	Escalating Access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Perform privilege escalation on the Windows Domain Controller (WinDC) machine by accessing a flag located deep within its file system.
Images	
Affected Hosts	172.22.117.20
Remediation	Implement least privilege principles, regularly update and patch systems, and conduct thorough security assessments to prevent privilege escalation attacks.

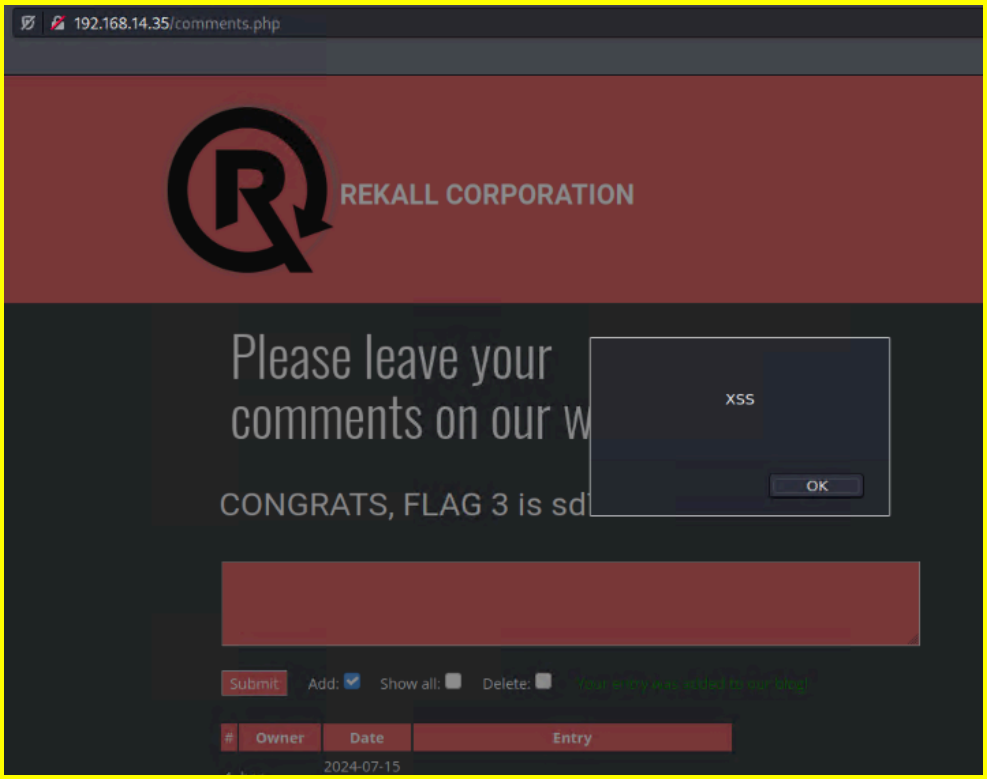
Vulnerability 19	Findings
Title	Compromising Admin
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Obtain the password hash of the Administrator user on the compromised Windows Domain Controller (WinDC).
Images	
Affected Hosts	172.22.117.20
Remediation	Reset Administrator password, enforce strong password policies, and implement multi-factor authentication to protect against credential theft and hash extraction techniques.

Vulnerability 20	Findings
Title	Reflected XSS on Welcome.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Exploit a reflected XSS vulnerability on the Welcome.php page by entering a payload in the "Put Your Name Here" input field, causing a pop-up to appear. Closing the pop-up reveals Flag 1.
Images	 
Affected Hosts	192.168.14.35
Remediation	Implement input validation and output encoding to prevent injection of malicious scripts. Conduct regular security testing to identify and fix XSS vulnerabilities.

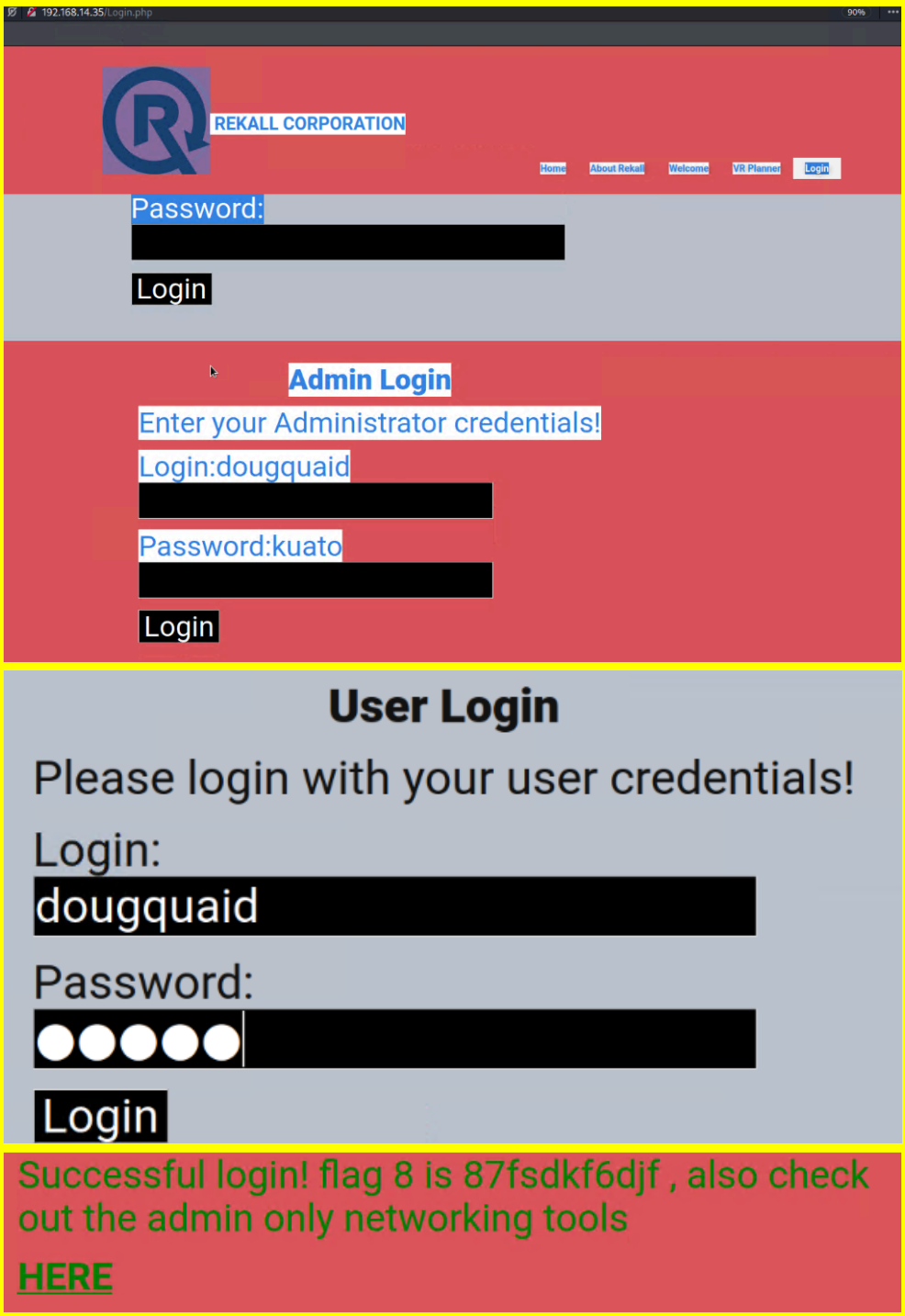
Vulnerability 21	Findings
Title	XSS on Memory-Planner.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Exploit an XSS vulnerability on the Memory-Planner.php page by entering a payload in the "Choose Your Character" field. The successful payload will bypass input validation that removes the word 'script' and causes a pop-up to appear, revealing Flag 2.

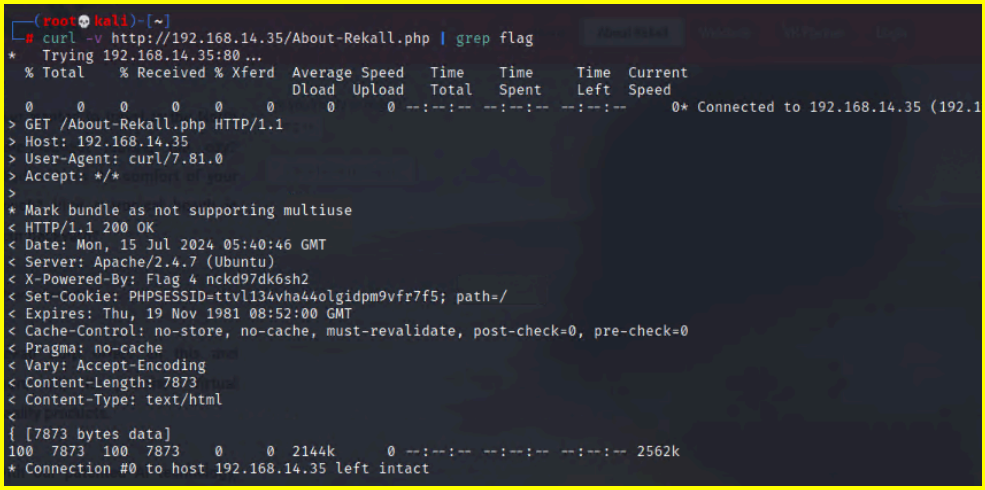
Images	 
Affected Hosts	192.168.14.35
Remediation	Enhance input validation mechanisms to prevent bypass techniques, use output encoding, and perform regular security testing to identify and mitigate XSS vulnerabilities.

Vulnerability 22	Findings
Title	XSS on Comments.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Exploit an XSS vulnerability on the Comments.php page by entering a payload that triggers a pop-up to appear. The successful execution of the payload will reveal Flag 3.

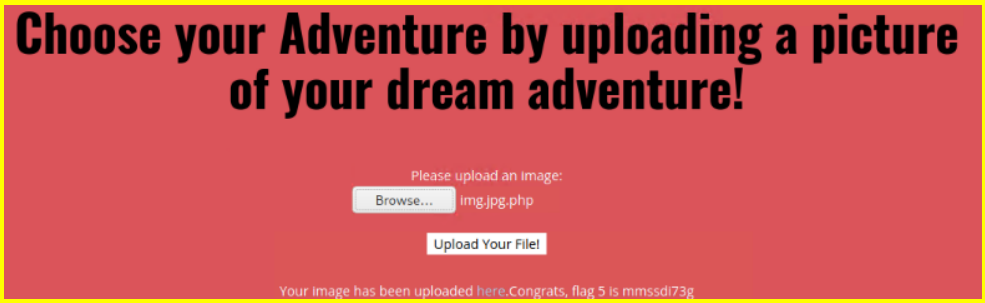
Images	
Affected Hosts	192.168.14.35
Remediation	Implement strict input validation and output encoding to prevent XSS attacks. Regularly conduct security testing to identify and fix such vulnerabilities.

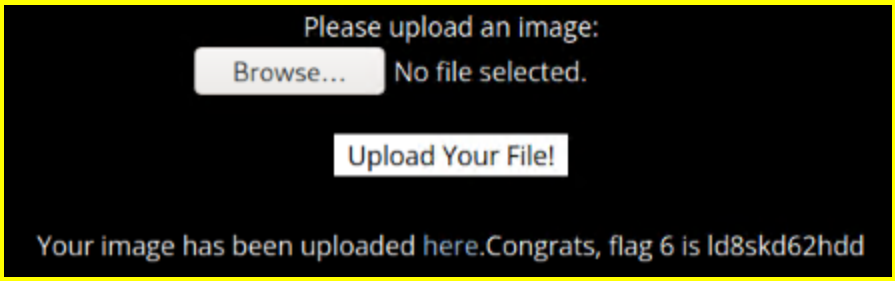
Vulnerability 23	Findings
Title	Hidden Details on Login.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	On the Login.php page, hidden details are present in the same color as the background, making them invisible to the naked eye. Revealing these hidden details will provide the flag.

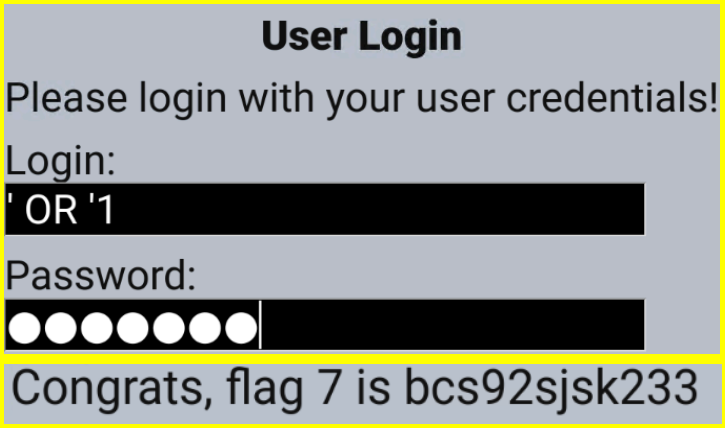
Images	
Affected Hosts	192.168.14.35
Remediation	Ensure that sensitive information is not hidden in the HTML or displayed in a manner that can be easily discovered. Implement security measures to protect hidden elements and conduct regular security reviews of web page.

Vulnerability 24	Findings
Title	Sensitive Data Exposure via HTTP Headers
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Sensitive data is exposed through the HTTP headers of the web server at 192.168.14.35. By using the curl command to inspect the headers, the flag can be discovered.
Images	
Affected Hosts	192.168.14.35
Remediation	Review and sanitize HTTP headers to ensure that sensitive data is not inadvertently exposed. Implement security best practices for handling HTTP headers and conduct regular security audits.

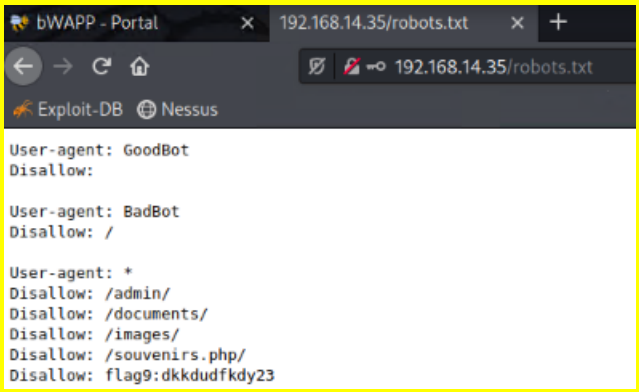
Vulnerability 25	Findings
Title	Local File Inclusion on Memory-Planner.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploit a Local File Inclusion (LFI) vulnerability on the Memory-Planner.php page by inputting a file such as img.jpg.php, which contains a command. Successfully exploiting this vulnerability will reveal Flag 5.

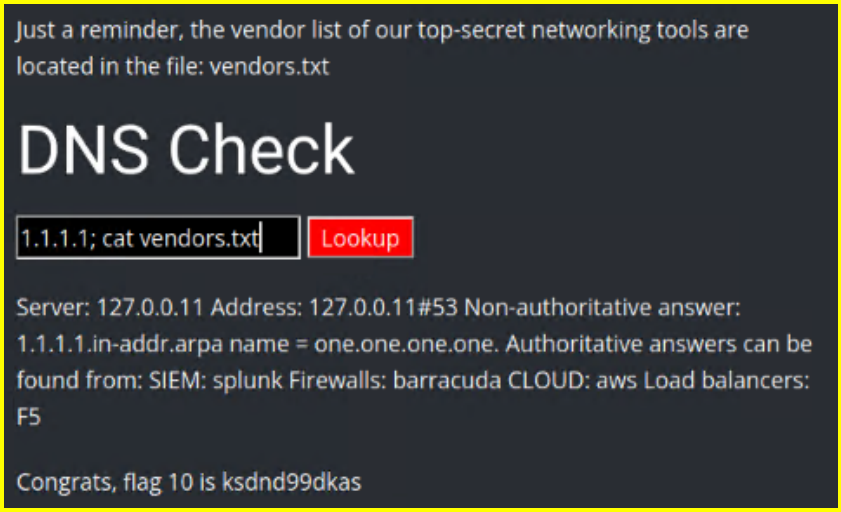
Images	
Affected Hosts	192.168.14.35
Remediation	Web server hosting the Memory-Planner.php page Remediation: Implement input validation to prevent inclusion of unauthorized files, use secure coding practices to avoid LFI vulnerabilities, and conduct regular security audits to identify and mitigate such risks.

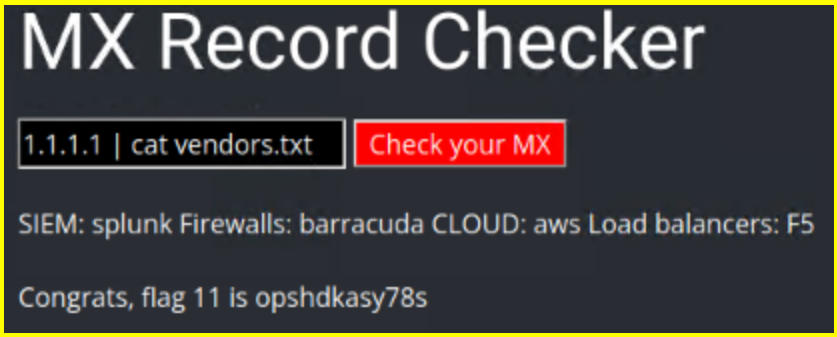
Vulnerability 26	Findings
Title	Advanced Local File Inclusion on Memory-Planner.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploit an advanced Local File Inclusion (LFI) vulnerability on the Memory-Planner.php page by inputting a file with ".jpg" in its name, such as exploit.jpg.php, to bypass input validation and load the file. Successfully exploiting this vulnerability will reveal Flag 6.
Images	
Affected Hosts	192.168.14.35
Remediation	Strengthen input validation to prevent bypass techniques, ensure proper file handling, and sanitize user inputs. Conduct regular security testing to identify and mitigate LFI vulnerabilities.

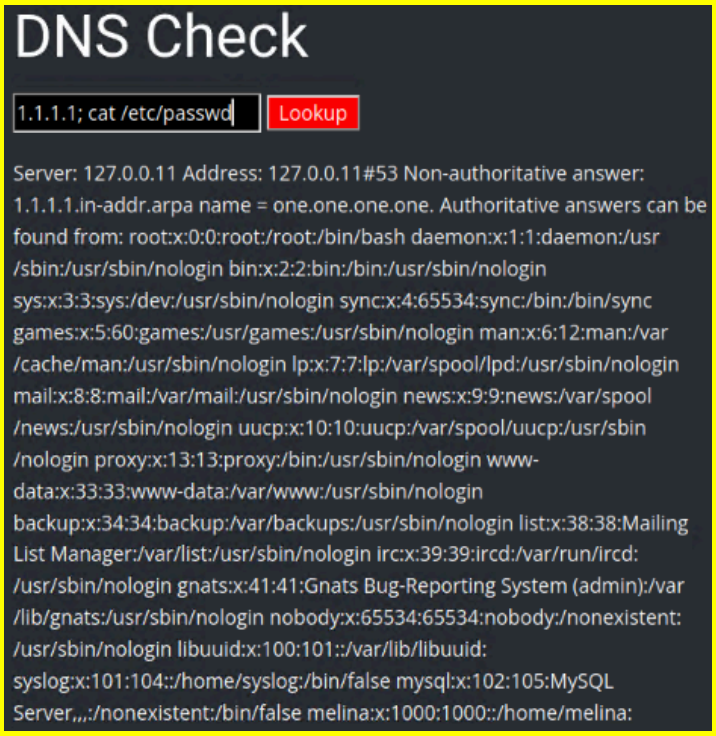
Vulnerability 27	Findings
Title	SQL Injection on Login.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploit an SQL injection vulnerability on the Login.php page to manipulate the SQL queries executed by the server. Successfully exploiting this vulnerability will allow access to sensitive information, including Flag 7.
Images	
Affected Hosts	192.168.14.35
Remediation	Use parameterized queries or prepared statements to prevent SQL injection, sanitize user inputs, and perform regular security assessments to identify and fix SQL injection vulnerabilities.

Vulnerability 28	Findings
Title	Sensitive Data Exposure via Robots.txt
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**High**
Description	Exploit a sensitive data exposure vulnerability involving the Robots.txt file on the web server. The flag can be found by accessing sensitive information intended for web crawlers and other automated agents.

Images	
Affected Hosts	192.168.14.35
Remediation	Review and restrict access to sensitive directories and files in the Robots.txt file. Ensure that sensitive information is not inadvertently exposed to unauthorized entities. Regularly update and review Robots.txt configurations for security best practices.

Vulnerability 29	**Findings**
Title	Command Injection via DNS Check
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploit a command injection vulnerability using the DNS Check feature to retrieve vendor.txt. Successful exploitation will reveal Flag 10.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input validation and command sanitization to prevent command injection attacks. Ensure that user inputs are properly validated and sanitized before being processed by the server. Regularly update and patch the application to mitigate command injection vulnerabilities.

Vulnerability 30	Findings
Title	Advanced Command Injection via MX Record Checker
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploit an advanced command injection vulnerability on the MX Record Checker feature, bypassing sanitization that removes '&' or ';'. Successfully exploiting this vulnerability will reveal Flag 11.
Images	
Affected Hosts	192.168.14.35
Remediation	Enhance command input validation to prevent bypass techniques, implement strict input sanitization, and apply least privilege principles to restrict commands executed by the application. Regularly update and patch the application to mitigate command injection vulnerabilities.

Vulnerability 31	Findings
Title	Brute Force Attack Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploit a brute force attack vulnerability on the web application to gain unauthorized access and retrieve Flag 12.This is done by finding through the DNS Check the users of this system. From here, guessing Melina's password which was just 'melina'
Images	
Affected Hosts	192.168.14.35
Remediation	Implement account lockout mechanisms, use strong and complex passwords, implement multi-factor authentication, and monitor for suspicious login attempts. Conduct regular security assessments and penetration testing to identify and mitigate brute force attack vectors.