Penetration Test Report

Cybersecurity

Rekall Corporation

Penetration Test Report

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	Totalrekall.xyz
Contact Name	Joshua Dyke
Contact Title	Penetration tester

Document History

Version	Date	Author(s)	Comments
001	7/8/2024	Joshua Dyke	N/A

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.

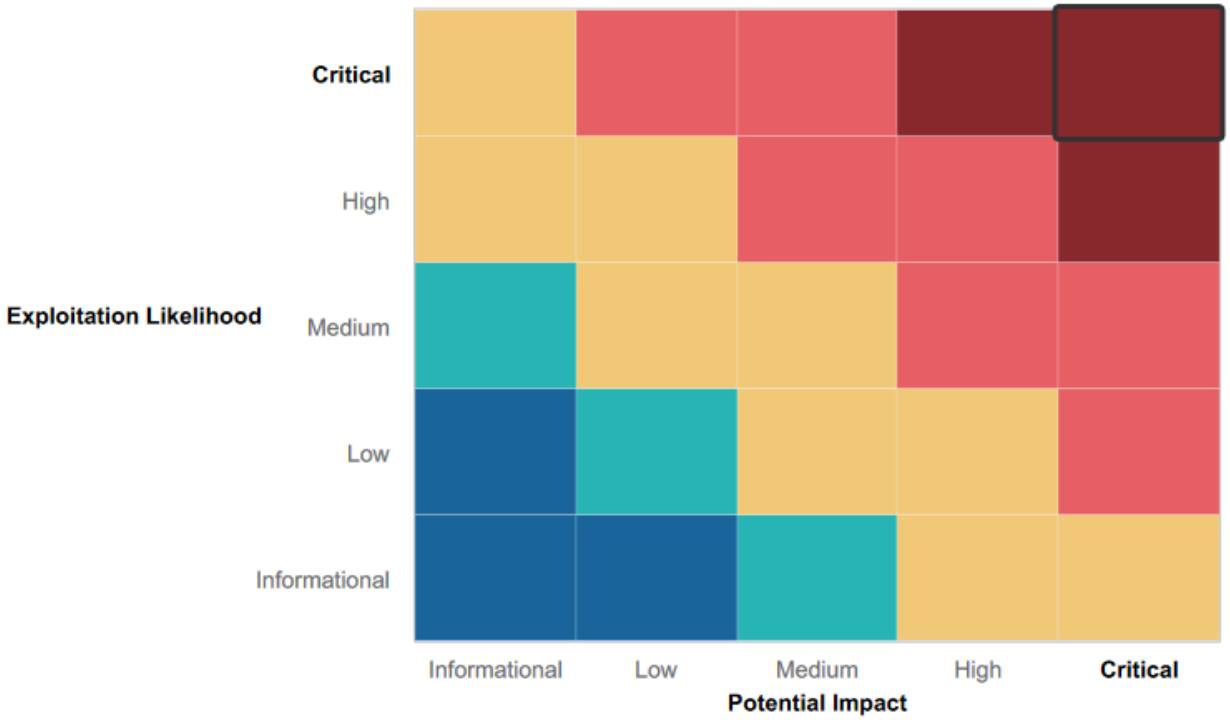
Executive Summary of Findings

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.

- **Input Validation:** Despite some successful XSS and PHP injection exploits, there were instances where input validation prevented or limited the impact of these attacks. This suggests that Rekall employs robust input validation mechanisms to sanitize user inputs and prevent malicious payloads from executing as intended.
- **Access Controls:** The presence of authentication and authorization mechanisms on sensitive pages (admin login) indicates that Rekall prioritizes access control. The use of specific credentials (admin username and password) required for accessing privileged information (legal data) demonstrates effective access management practices
- **File Upload Restrictions:** Despite successful PHP injection via disguised file uploads, the platform likely had restrictions in place that prevented direct execution of uploaded PHP scripts as demonstrated in the challenge. This indicates proactive measures to validate file types and prevent unauthorized script execution.
- **Comprehensive Security Testing:** The presence of diverse challenges across web application security, network enumeration, and system exploitation indicates that Rekall conducts comprehensive security testing. This approach ensures that the organization tests its defenses against a wide range of attack vectors, thereby strengthening overall resilience.

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.

Insufficient Input Validation:

- Across various challenges (XSS and PHP injection) it was evident that input validation measures were either insufficient or improperly implemented. This allowed attackers to inject malicious scripts and execute unauthorized commands. Implementing strict input validation routines can mitigate these risks by sanitizing user inputs effectively.

Weak Password Management:

- In cases where default or easily guessable credentials (e.g., username 'dougquaid' and password 'kuato' in Vulnerability 7) were exposed or used, it indicates weaknesses in password management practices. Implementing strong password policies, enforcing multi-factor authentication (MFA) where feasible, and regularly auditing and rotating credentials can strengthen defenses against unauthorized access attempts.

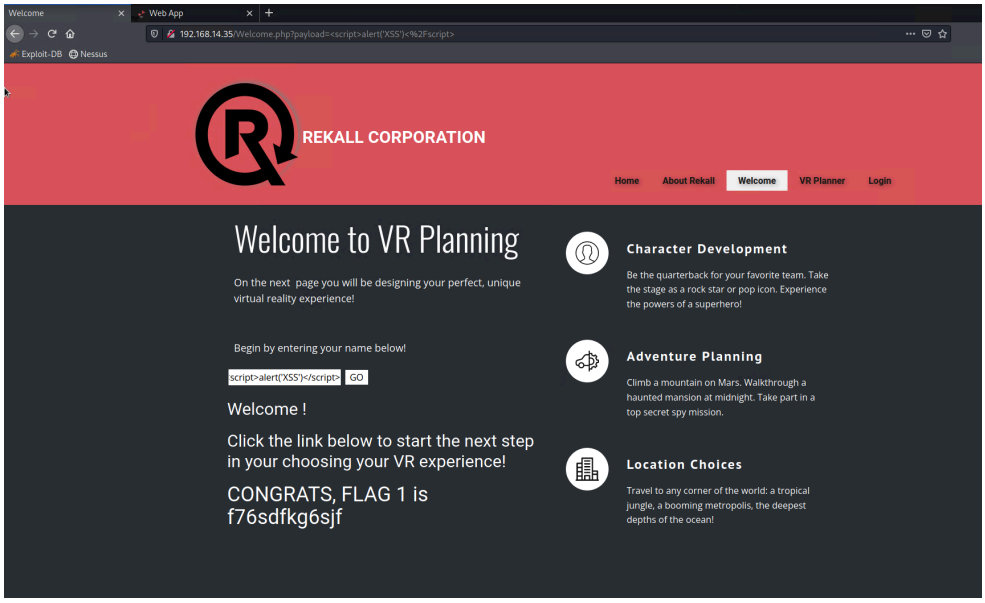
Executive Summary

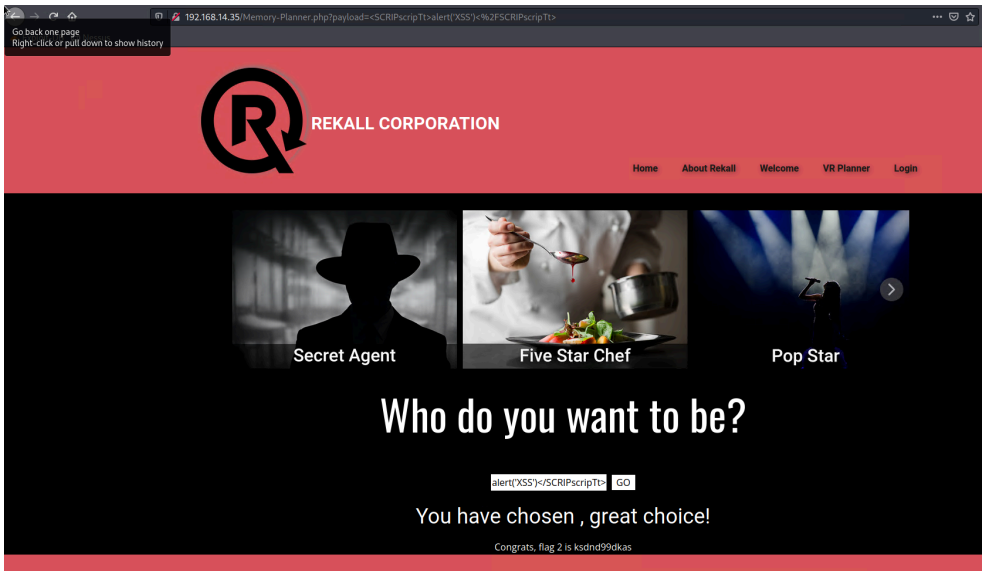
Executive Summary
This penetration testing exercise focused on evaluating the security posture of the Total Rekall network and web applications. The assessment was conducted over three days, uncovering multiple vulnerabilities across various systems and services. The findings and recommendations outlined in this report aim to assist Total Rekall in improving their overall security stance.

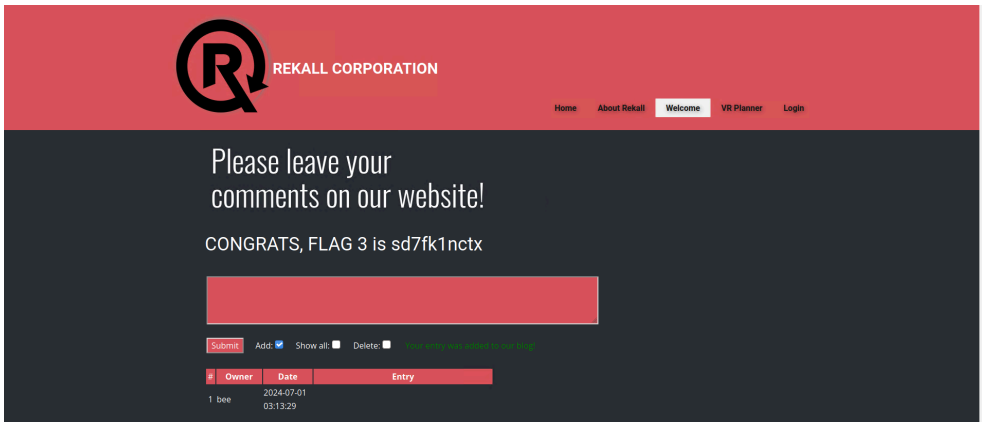
Key Findings:

Cross-Site Scripting (XSS) Vulnerabilities

Identified on welcome.php, Memory-Planner.php, Comments.php.
Risk: Medium
Impact: Allows execution of arbitrary scripts.
Recommendation: Implement input validation and output encoding.

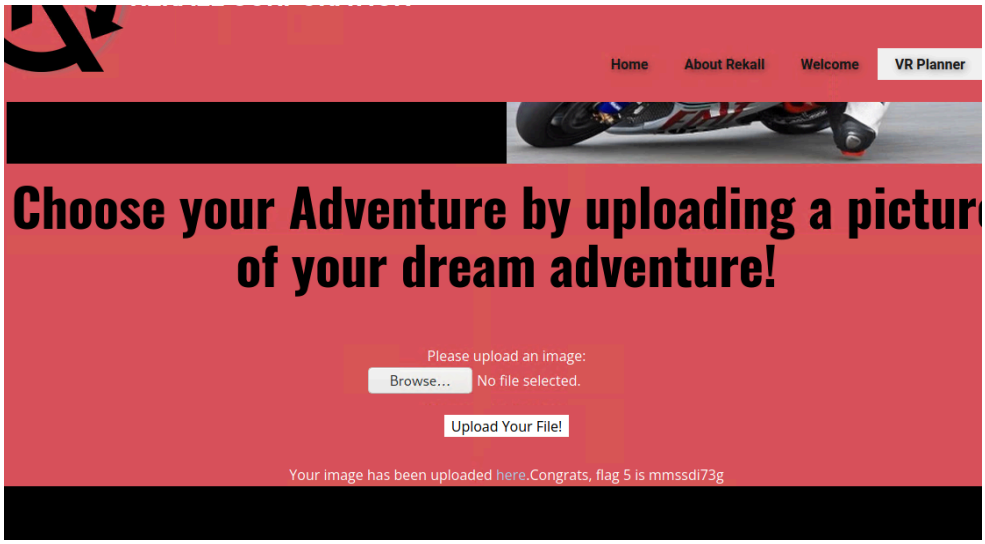






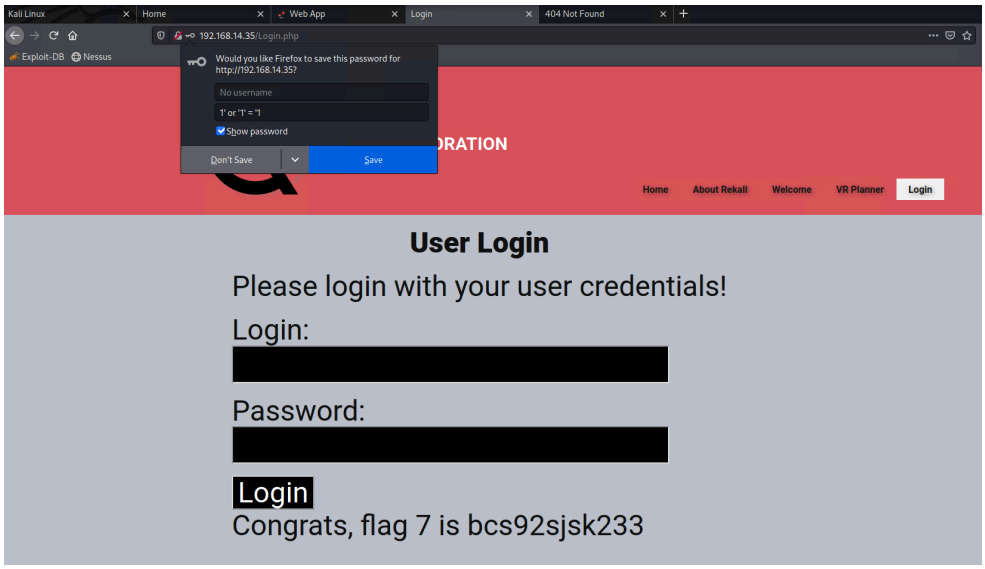
File Upload Vulnerabilities

PHP files uploaded disguised as JPEGs.
Risk: Critical
Impact: Allows execution of arbitrary PHP code.
Recommendation: Enhance file validation.



SQL Injection Vulnerabilities

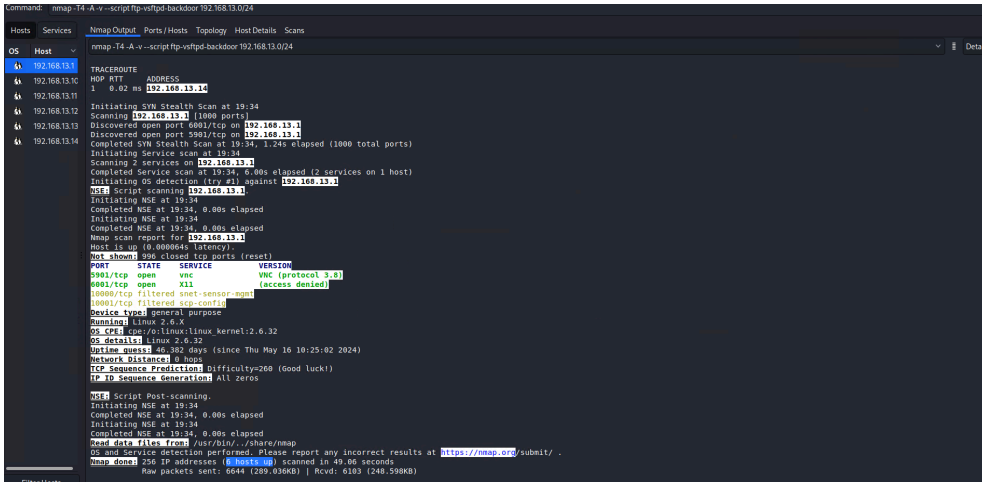
Exploited on Login.php.
Risk: High
Impact: Allows unauthorized access.
Recommendation: Implement parameterized queries.



Network and System Vulnerabilities:

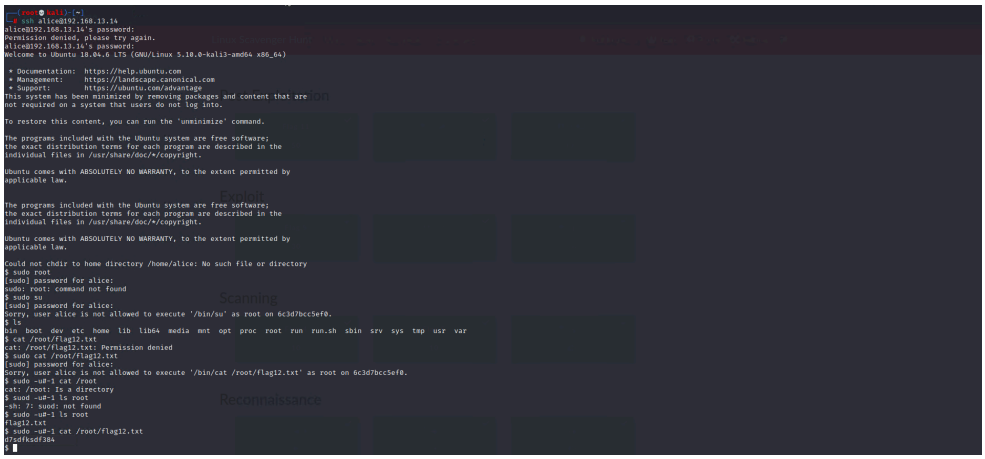
Network Scans and Exploitation

Identified using NMAP and exploited services.
Risk: High
Impact: Allows unauthorized access and command execution.
Recommendation: Patch and secure exposed services.



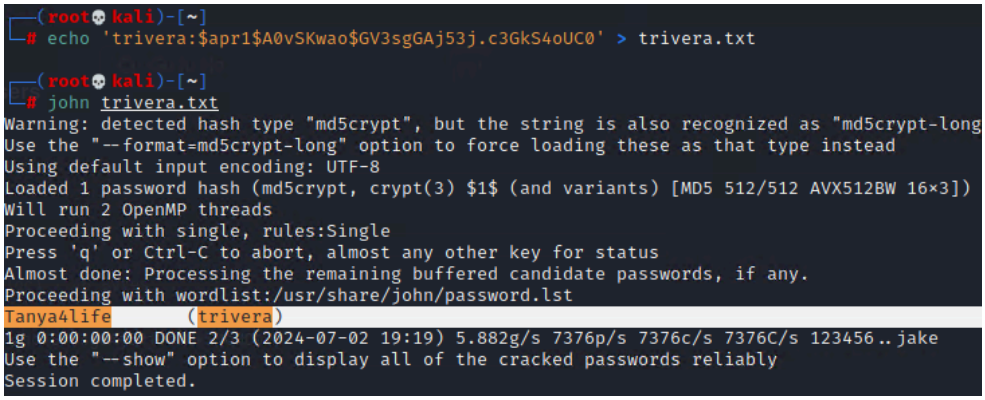
Privilege Escalation

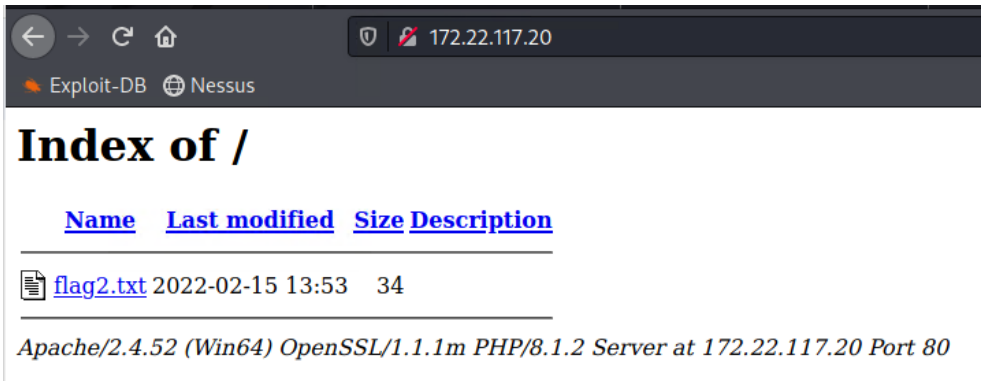
Exploited CVE-2019-14287.
Risk: High
Impact: Allows elevation of privileges.
Recommendation: Implement least privilege principles.



Credential and Information Exposure
Credential Management

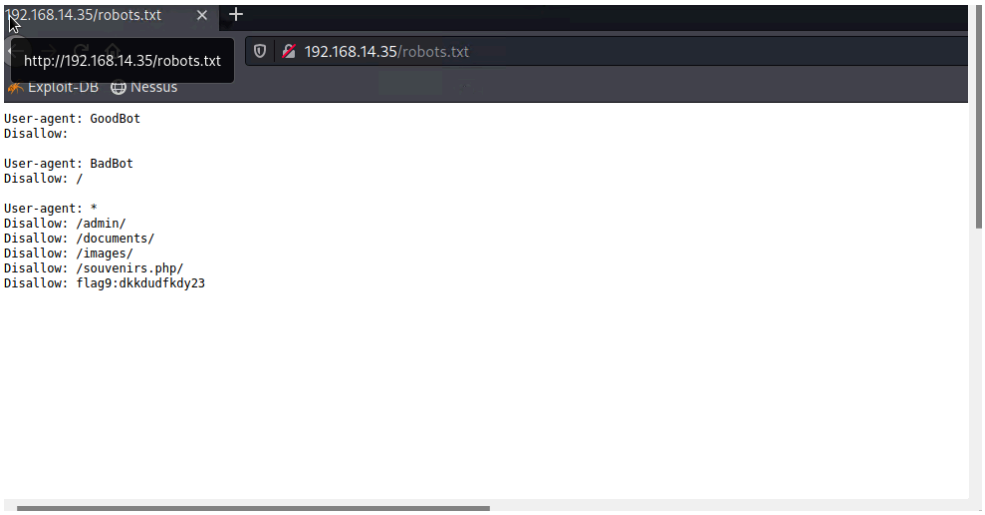
Plaintext credentials found in HTML source code.
Risk: High
Impact: Allows unauthorized access.
Recommendation: Use secure credential storage.





Information Leakage

Exposed directories and files via robots.txt.
Risk: Medium
Impact: Allows attackers to find hidden resources.
Recommendation: Review and secure directory listings.



Recommendations:
Web Application Security: Implement input validation and output encoding.
Enforce strict file upload restrictions.
Network and System Hardening: Regularly update and patch all software and services.
Implement strong access controls.
Credential Management: Avoid storing plaintext credentials.
Enforce multi-factor authentication.
Training and Awareness: Conduct regular security awareness training.
Implement a formal incident response plan.

Conclusion

The penetration testing engagement identified significant vulnerabilities across Total Rekall's network and web applications, emphasizing critical areas requiring immediate attention and remediation. By addressing these issues and implementing the recommended security measures, Total Rekall can enhance its overall security posture and better protect its assets from potential threats.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS Vulnerability on Welcome.php pages	High
Reflected XSS vulnerability Exploitation on Memory-Planner.php	Medium
Reflected XSS Vulnerability on Comments.php	Medium
HTTP Response Information Disclosure	Medium
File upload and execution (PHP Disguised as JPG)	Critical
SQL Injection In the Login.PHP	High
Credentials in the Login.php	High
Information Via Robots.txt	Medium
Command Injection in networking.php 192.168.14.35	High
Command injection VIA DNS 192.168.14.35	High
Authentication bypass via Command Injection in login.php	Critical
PHP injection VIA souvenirs.php 192.168.14.35	High
Brute Force Admin Legal Data	High
Path Traversal Via Disclaimer.php	High
Exploitable WHOIS Information Disclosure	High
DNS Information Leakage via CentralOps	Medium
SSL Information leak	Medium
Nmap Assessment	High
Drupal Via Intense Scan	High
Nessus Scan Vulnerability	Critical
Remote File Inclusion	Critical
Shellshock Vulnerability	Critical
File Permissions on /etc/passwd	High
Remote Code Execution	Critical
Drupal Vulnerability	Medium
Privilege Escalation	Critical
Credentials on Public GitHub Repository	Critical
Compromised Credentials	Critical
FTP Vulnerability	High
Remote Code Execution Exploit	Medium
Scheduled tasks in the Windows 10 Machine	Low

Unauthorized access using Kiwi and Password Cracking With John The Ripper	**High**
Sensitive Data In Public User Documents	**High**
Metasploit Exploit Unauthorized Access On The Windows 10 Machine	**High**
File Access on Windows DC10	**High**
Admin Password Hash	**Critical**

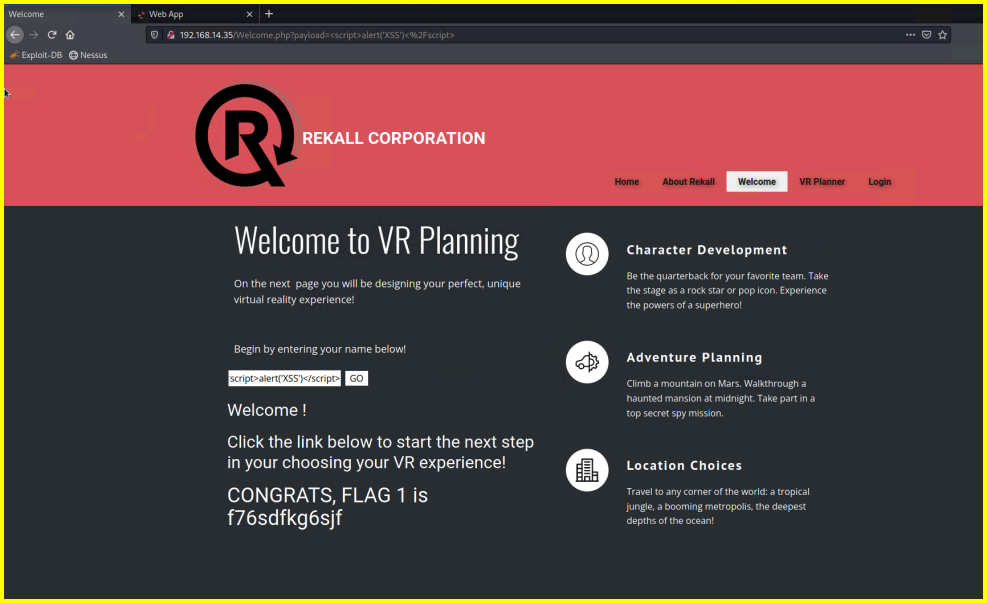
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35 192.168.13.0/24 15.197.148.33 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.20 172.22.117.10
Ports	80 443 21 22 110 445 8080

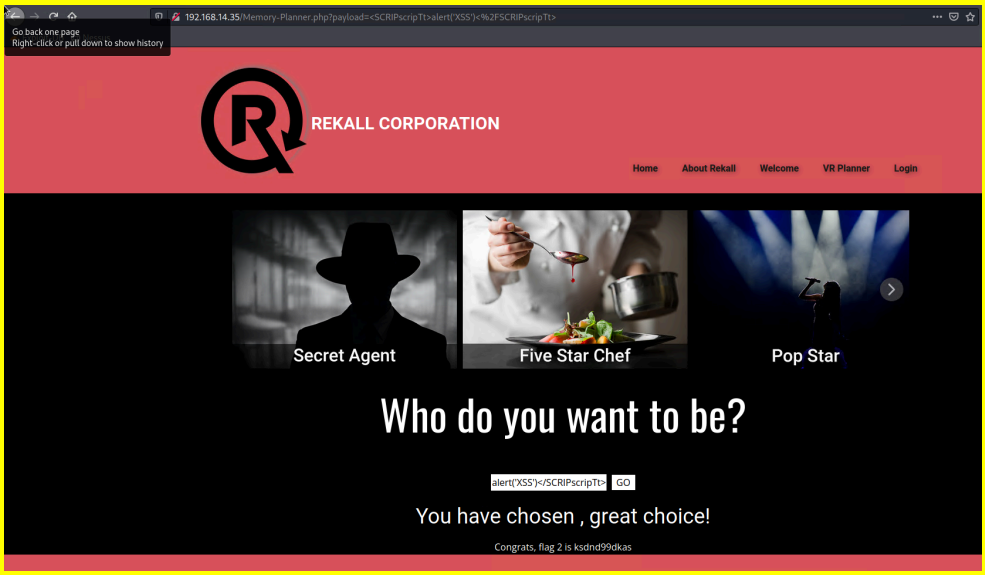
Exploitation Risk	Total
Critical	10
High	17
Medium	8
Low	1

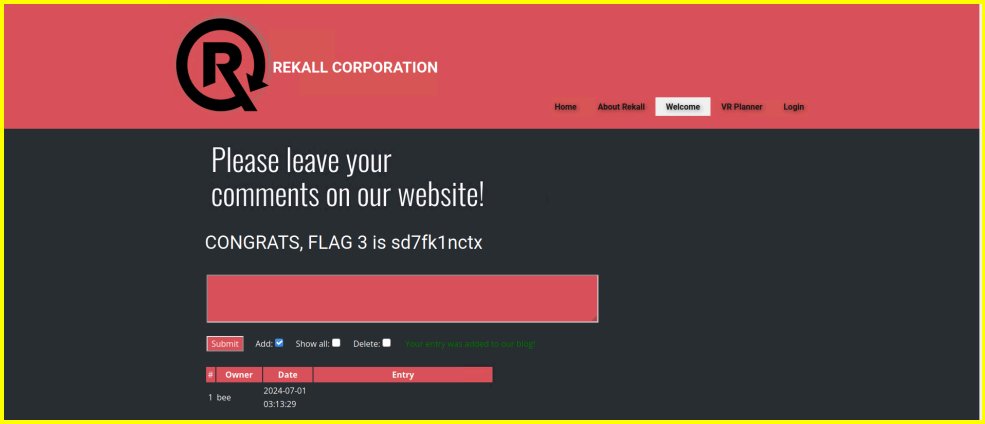
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS Vulnerability on Welcome.php pages

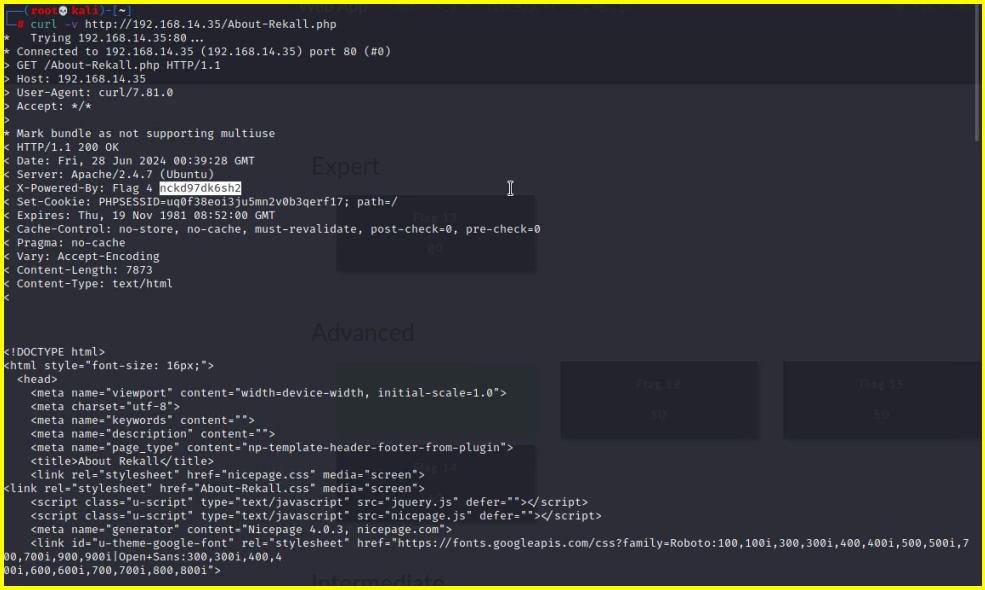
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Impact: Medium : Likelihood for exploitation High (Risk Rating High)
Description	Entering this successful payload will make a pop up appear on the website. Entering this script will generate a reflected XSS payload. <script>alert(‘any text goes here’)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	Modifying the application codes to use HTML entity coding which would prevent scripts and codes from being executed from their browser.

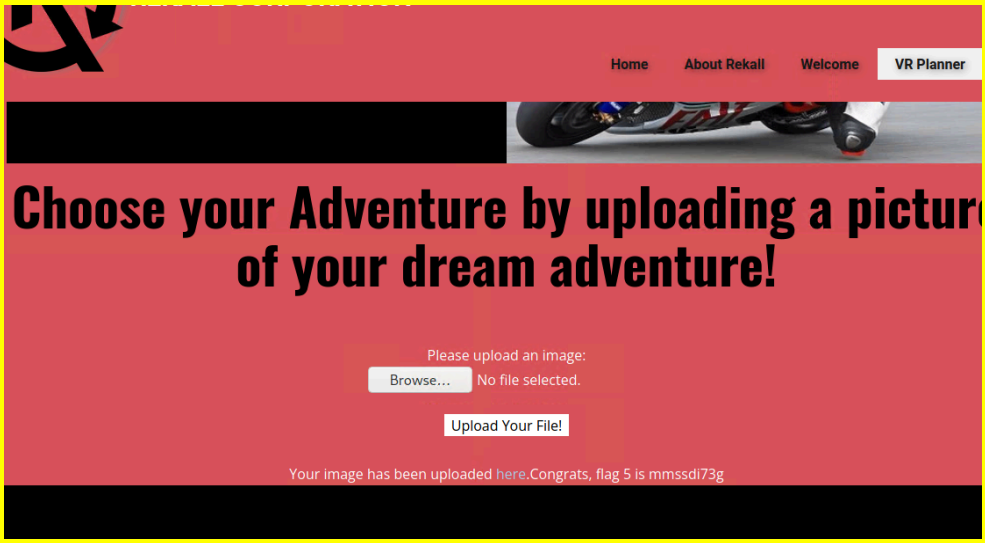
Vulnerability 2	Findings
Title	Reflected XSS vulnerability Exploitation on Memory-Planner.php
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Medium
Description	This Vulnerability exists in the Memory-planner.php part of the web page. After refining the scripts after initial attempts that were failed. After using this script <SCRIPscriptT>alert("hi")</SCRIPscripTt> we were successfully able to evade the filtering mechanisms for input validation and a flag was produced.

Images	
Affected Hosts	192.168.14.35
Remediation	Choose your character input field ensuring that no HTML tags or javascript code that could be executed from the browser. Using HTML encoding this will help to ensure scripts will show as harmless text and cannot be executed.

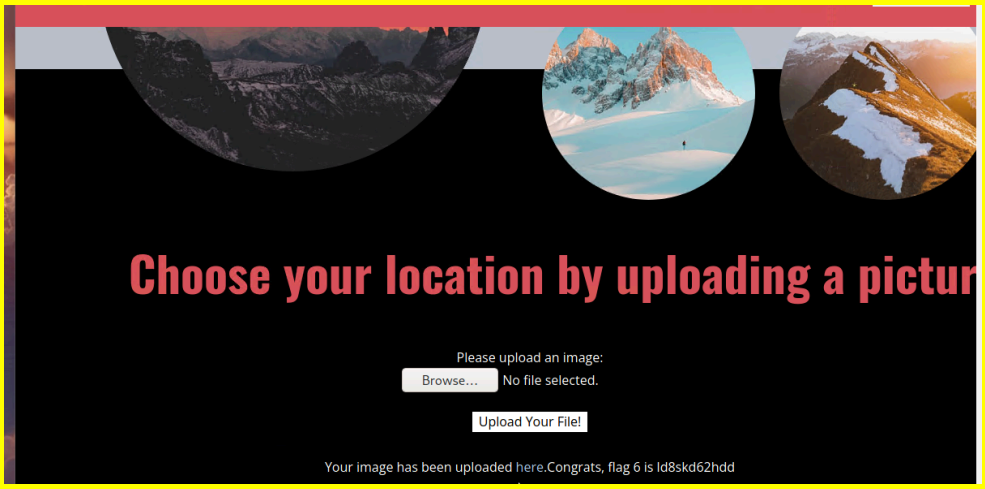
Vulnerability 3	Findings
Title	Reflected XSS Vulnerability on Comments.php
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Medium
Description	Injection of the script <script>alert('XSS')</script> can allow scripts to be executed from within their browsers. This vulnerability was found within the comments section within the webpage. This area of the comments has no encoding which can allow for the malicious script to be put in and executed.
Images	

Affected Hosts	192.168.14.35
Remediation	Remediation tips that could prevent this from happening in the future are. Implementation of input validation would be one way to prevent the injection of malicious scripts. Setting up a Content security policy would also prevent all unwanted scripts from being executed. This would only allow scripts from trusted sources to be exectuted.

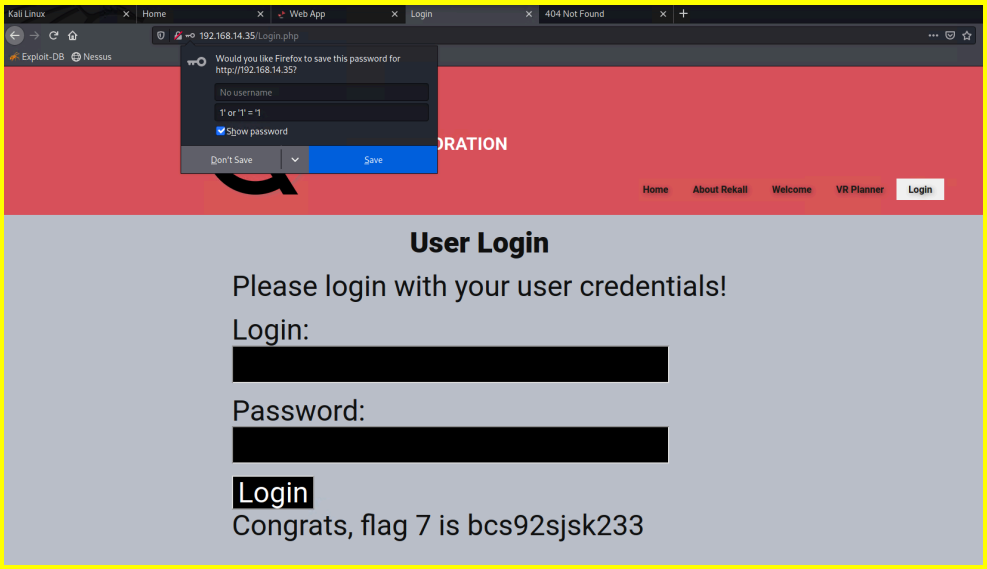
Vulnerability 4	Findings
Title	HTTP Response Information Disclosure
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Medium
Description	Entering the command curl -v http://192.168.14.35/About-Rekall.php will provide you with a request for HTTP fetch content for the about-rekall.php. This command itself is not a huge exploit but the data that can be read can be relevant for finding other exploits in the webpage. The verbose command will provide you with very detailed information about HTTP headers and how the server is responding. If there is any sensitive data in the headers it will be read and leaked.
Images	
Affected Hosts	192.168.14.35
Remediation	Ensuring that sensitive information is not put into the headers for html is one way that could prevent this information from being leaked. Also limiting the -V for verbose in production environments would help limit the data that can be pulled from a public webpage. Using Curl commands to test any vulnerabilities in the future will show if they have any more vulnerabilities in the html headers.

Vulnerability 5	Findings
Title	File upload and execution (PHP Disguised as JPG)
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Critical
Description	Creation of a fake PHP file that is disguised as a JPG. This then is uploaded into the adventure upload option on the webpage. Once the PHP script is uploaded you can then navigate to the script via the URL.http://192.168.14.35/uploads/script.jpg.php?cmd=ls The “ls” cmd will now show an output.
Images	
Affected Hosts	192.168.14.35
Remediation	File validation checks the file type based on content inspection and not just reading file extensions. This would help ensure that a php.file cannot be disguised as a jpg.

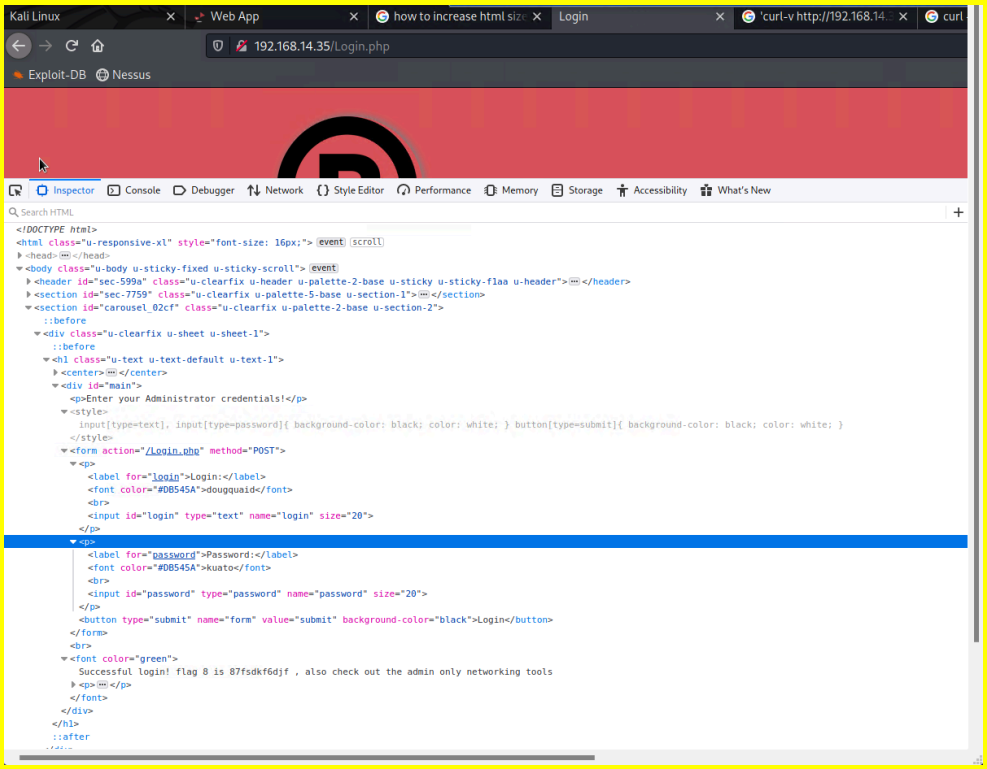
Vulnerability 6	Findings
Title	File upload PHP disguised as a JPG
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Critical
Description	Creation of a fake PHP file that is disguised as a JPG. This then is uploaded into the location upload option on the webpage. Once the PHP script is uploaded you can then navigate to the script via the

	URL.http://192.168.14.35/uploads/script.jpg.php?cmd=ls The “ls” cmd will now show an output.
Images	
Affected Hosts	192.168.14.35
Remediation	File Validation once again would be a solution to this. It does not only check the file extensions but also the contents. This would not allow a php file to be disguised as a jpg.

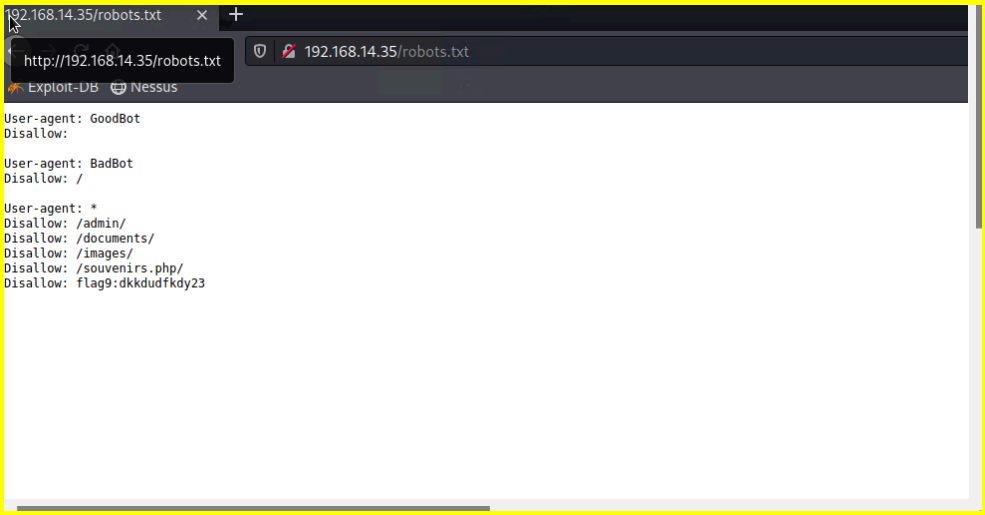
Vulnerability 7	Findings
Title	SQL Injection In the Login.PHP
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	High Risk
Description	Entering 1’ OR 1’ = 1’ into the password section is a way of bypassing authentication checks and to gain unauthorized access. This is a simple way of manipulating SQL that is then executed by the application.

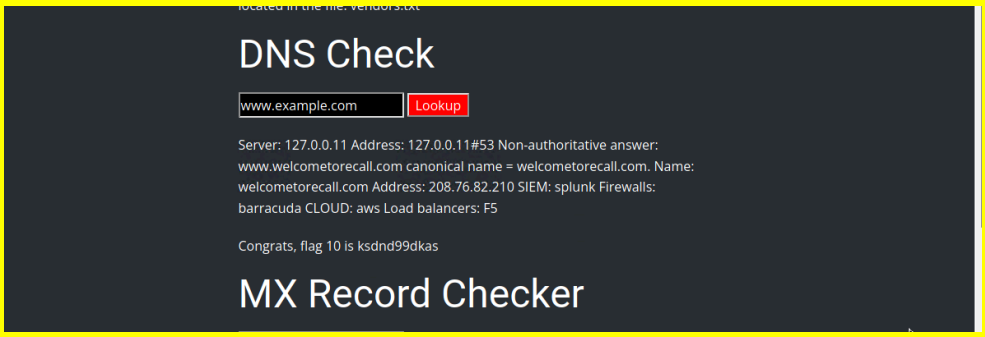
Images	
Affected Hosts	192.168.14.35
Remediation	Input validation would prevent this from happening. This would set queries to prevent unwanted SQL injection attacks. This would set restrictions on the user input.

Vulnerability 8	Findings
Title	Credentials in the Login.php
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	High Risk
Description	Looking into the HTML source code you can see that both the username and password are hardcoded into the login.php page. Inspecting both elements for the username and password both show this information to anyone inspecting the page.

Images	
Affected Hosts	192.168.14.35/networking.php
Remediation	Avoid storage of credentials in any of the HTML files

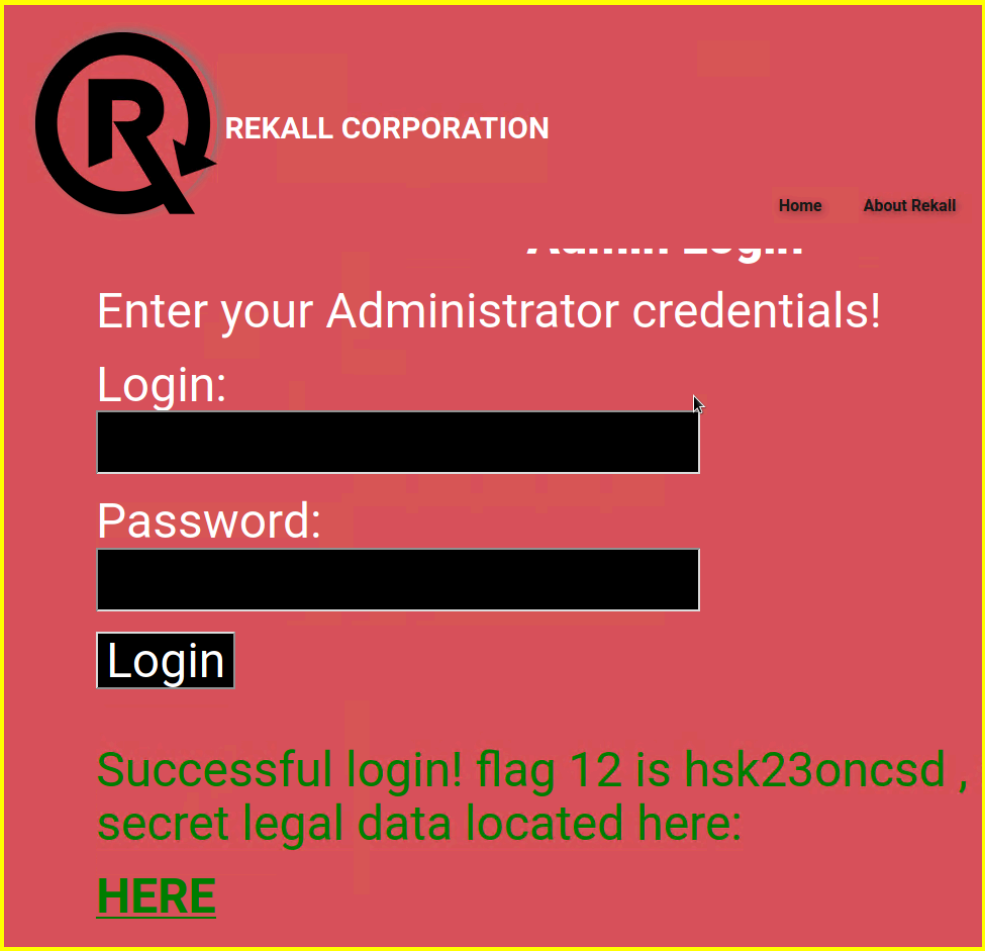
Vulnerability 9	Findings
Title	Information Via Robots.txt
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Medium
Description	Using 192.168.14.35/robots.txt will aid in finding potential vulnerabilities or hidden resources on the server. This could provide enough information to target specific files that could be used to exploit a website further.

Images	
Affected Hosts	192.168.14.35
Remediation	Implementation of user controls can help restrict who can see potential sensitive directories and files. Setting the allow to disallow would not permit public crawlers access to contents in the public directories.

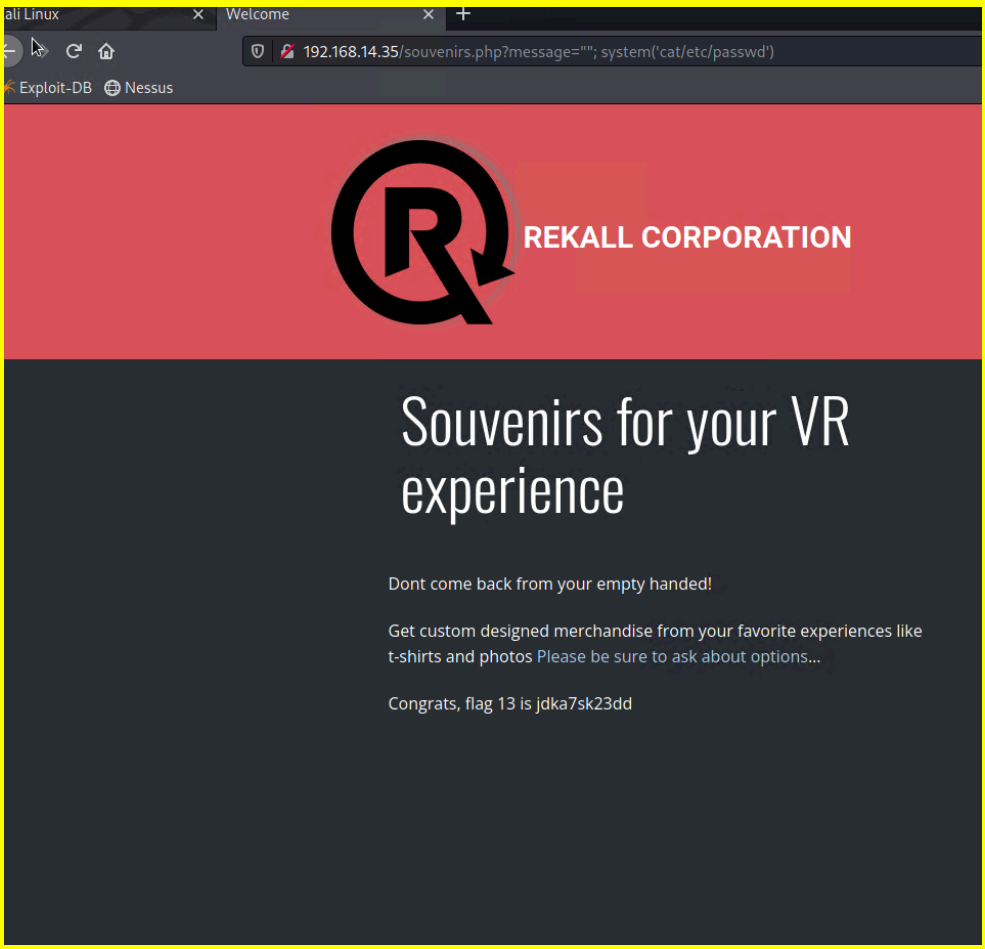
Vulnerability 10	Findings
Title	Command Injection in networking.php 192.168.14.35
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	High Risk
Description	This allows for command injection via a dns feature on 192.168.14.35/networking.php. using the && cat vendors.txt the attacker can now execute commands on the server to see a file.
Images	
Affected Hosts	192.168.14.35
Remediation	Use of safe APIS can be implemented in a way to stop executing shell commands from users.

Vulnerability 11	Findings
Title	Command injection VIA DNS 192.168.14.35
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	High
Description	Entering a website name into the MX Record checker will provide the firewalls and next flag. Because the && cat command is running, any website name will work in the search bar.
Images	
Affected Hosts	192.168.14.35/networking.php
Remediation	Use of safe APIS can be implemented in a way to stop executing shell commands from users.

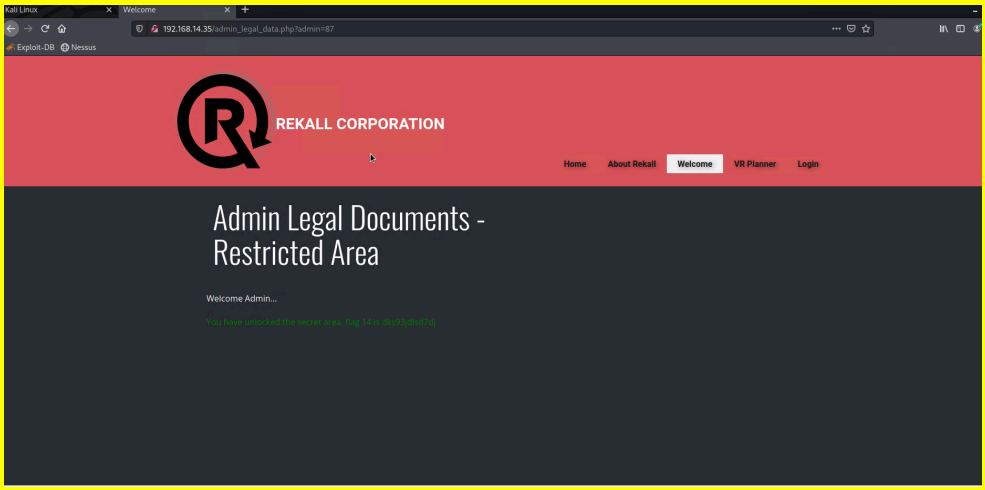
Vulnerability 12	Findings
Title	Authentication bypass via Command Injection in login.php
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	Critical
Description	Using the etc/password command we can then see all the usernames and passwords for login data. One of the usernames melina has melina set as her password as well. When entered into the login field the flag and important admin data are revealed also.

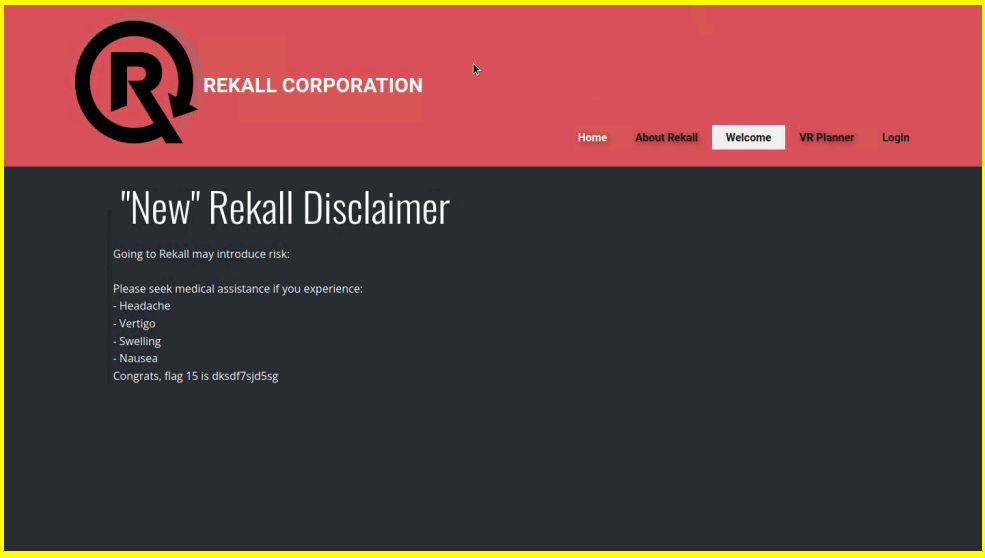
Images	
Affected Hosts	192.168.14.35/login.php
Remediation	The use of simple access controls can help limit who can see and access sensitive data such as etc/passwd files.

Vulnerability 13	Findings
Title	PHP injection VIA souvenirs.php 192.168.14.35
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	High Risk
Description	By manipulating a PHP flaw and then injecting payloads into the URL such as system('cat/etc/passwd') they can then access sensitive files like /etc/passwd getting access to the password file.

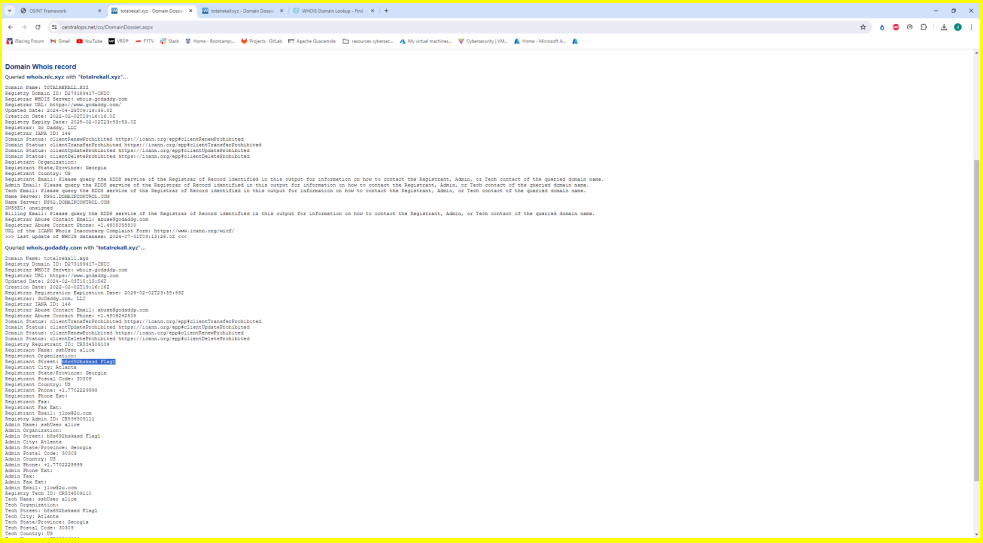
Images	
Affected Hosts	192.168.14.35/souvenirs.php
Remediation	Access Controls to certain sensitive files need to be set in place. This would restrict all access to sensitive files like /etc/passwd.

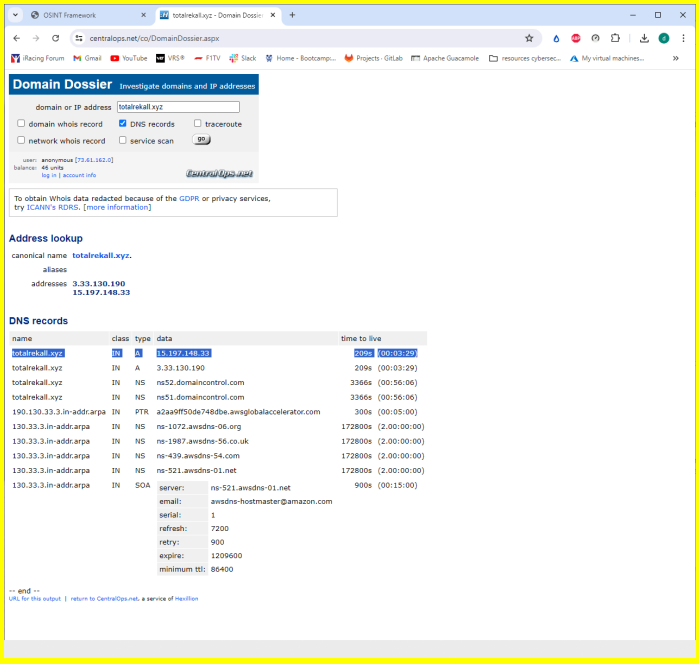
Vulnerability 14	Findings
Title	Brute Force Admin Legal Data
Type (Web app / Linux OS / WIndows OS)	Web APP
Risk Rating	High Risk
Description	Through the use of burp suite we use the brute force attack to enumerate valid session ids. When entering that session ID of 87 into the URL we were able to then access admin legal data and flag 14.

Images	
Affected Hosts	192.168.14.35/admin_legal_data.php
Remediation	Session expiry would stop inactive sessions from staying online. Any suspicious activity in the future then could be monitored and if need be access can be revoked from the user.

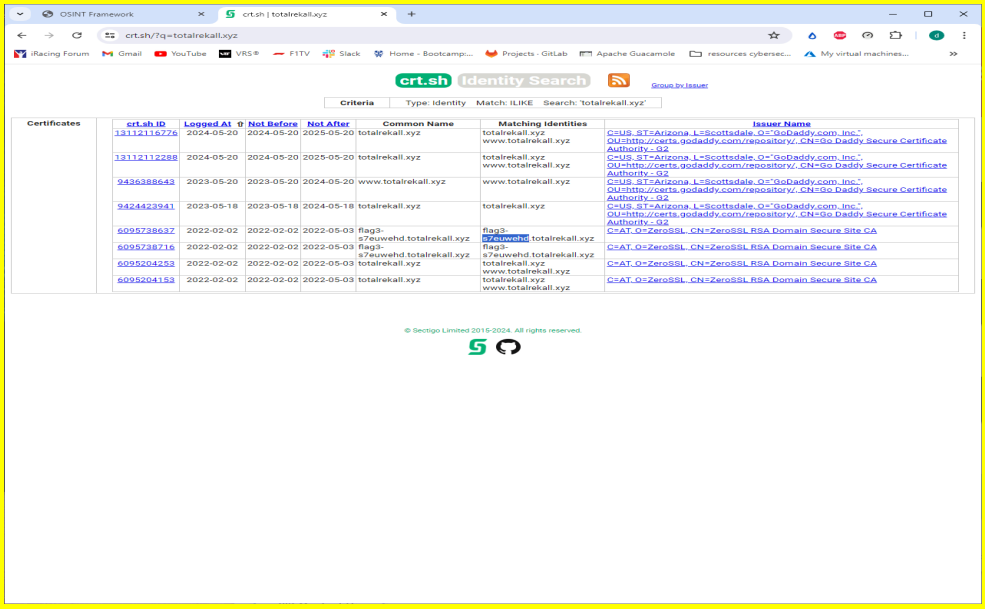
Vulnerability 15	Findings
Title	Path Traversal Via Disclaimer.php
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	High Risk
Description	This vulnerability is used by using path traversal on 192.168.14.35/disclaimer.php? page=old_disclaimers/disclaimer_1.txt. This then allows unauthorized access to any sensitive files that are in the disclaimers_1.txt file
Images	

Affected Hosts	192.168.14.35/disclaimer.php
Remediation	Restriction of sensitive files and adding permissions to files and such directories. This will add an extra layer of security and only allow certain roles and individuals to have access.

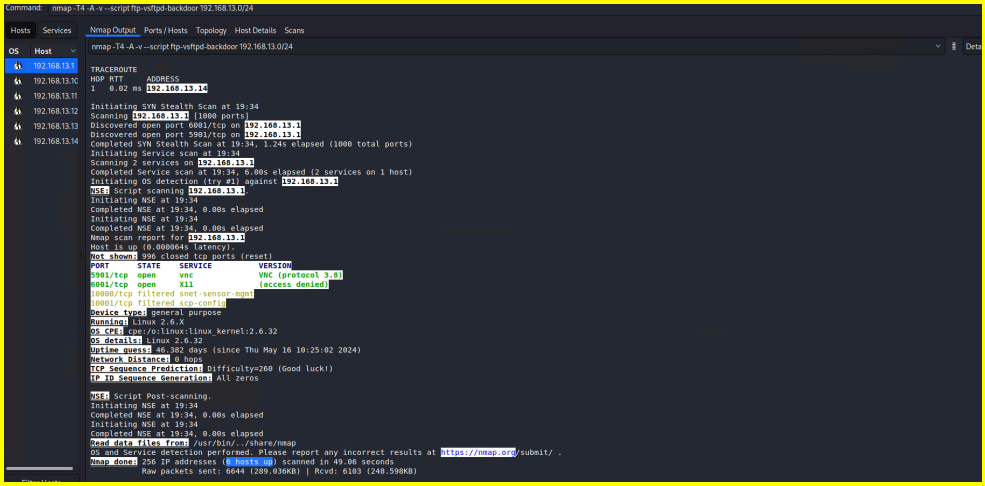
Vulnerability 16	**Findings**
Title	Exploitable WHOIS Information Disclosure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Go to https://centralops.net/co/DomainDossier.aspx and type in the URL (totalrekall.xyz), checkmark the box “whois domain records” and press enter
Images	
Affected Hosts	192.168.14.35
Remediation	This vulnerability allows an attacker to gather sensitive information about the domain totalrekall.xyz using the WHOIS service provided by centralops.net. By submitting the domain name to the WHOIS query and checking the "whois domain records" box, an attacker can obtain details such as the domain registrar, registrant contact information, and registration dates. This information can be used for social engineering attacks, targeted phishing campaigns, or to gain insights into potential security weaknesses associated with the domain registration.

Vulnerability 17	Findings
Title	DNS Information Leakage via CentralOps
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	This vulnerability allows an attacker to gather DNS-related information about the domain totalrekall.xyz using the Domain Dossier service provided by centralops.net. By submitting the domain name to the DNS query and checking the "DNS records" box, an attacker can obtain details such as DNS servers, MX records, and other DNS configurations. This information can be used to map the network infrastructure, identify potential points of entry, or facilitate targeted attacks against the domain's DNS infrastructure.
Images	
Affected Hosts	192.168.14.35
Remediation	Limiting access to DNS information to only approved users.

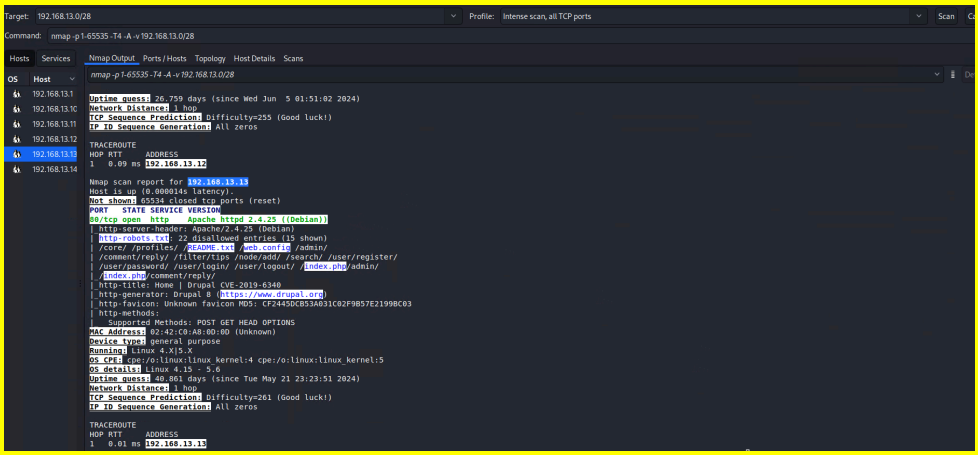
Vulnerability 18	Findings
Title	SSL Information leak

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	This vulnerability allows an attacker to gather SSL certificate information for the domain totalrekall.xyz using the Certificate Search service provided by crt.sh. By submitting the domain name to the search query, an attacker can obtain details such as issued SSL certificates, including their validity period, subject names, and issuer information. This information can potentially reveal details about the domain's security posture, certificate expiration dates, and historical changes in certificate configurations.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement proactive certificate management practices to ensure timely renewal and replacement

Vulnerability 19	**Findings**
Title	Nmap Assessment
Ty0pe (Web app / Linux OS / WIndows OS)	Network
Risk Rating	High
Description	Running an NMAP or Zenmap scan on the IP range 192.168.13.0/24

	reveals multiple hosts within the subnet. The scan returns 6 hosts, excluding the scanning system itself. The correct number of hosts identified is 5, as per the vulnerability assessment criteria. This vulnerability highlights potential risks associated with network enumeration and the exposure of active hosts within the specified IP range.
Images	
Affected Hosts	192.168.13.0/24
Remediation	Enabling firewall rules to limit access on the network.

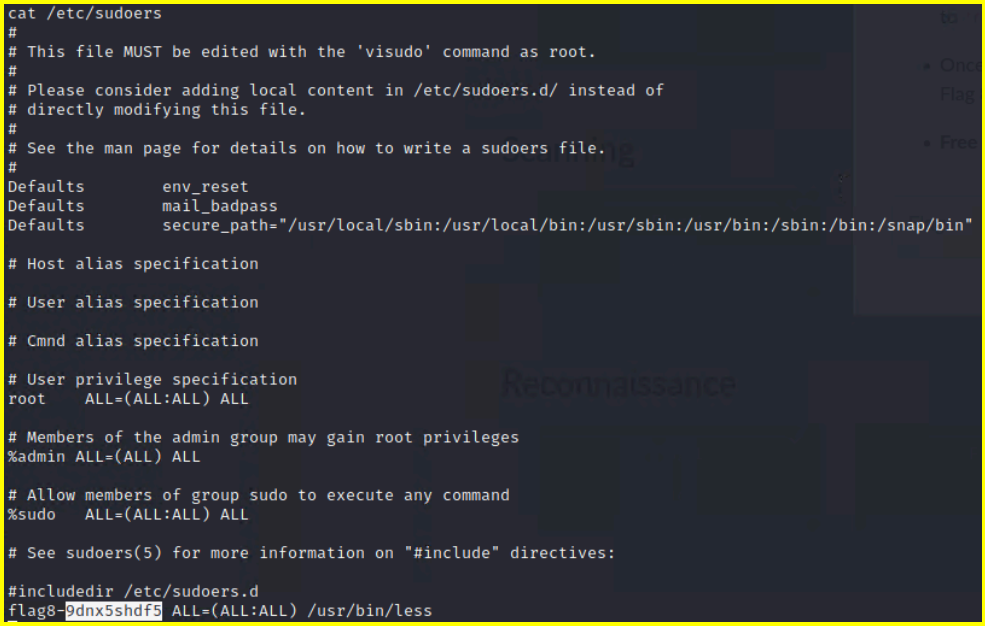
Vulnerability 20	Findings
Title	Drupal Via Intense Scan
Type (Web app / Linux OS / WIndows OS)	Network
Risk Rating	High
Description	Using Zenmap, an intense scan was conducted on the IP address 192.168.13.13 within the specified IP range (192.168.13.0/24 or 192.168.13.0/28). This scan revealed detailed information about the open TCP ports on the target host. Specifically, it was discovered that 192.168.13.13 is running the Drupal content management system (CMS). Drupal is a popular web application framework and CMS known for its extensive use in creating a variety of websites and web applications.

Images	
Affected Hosts	192.168.13.13
Remediation	Regularly update and patch Drupal installations to mitigate known vulnerabilities.

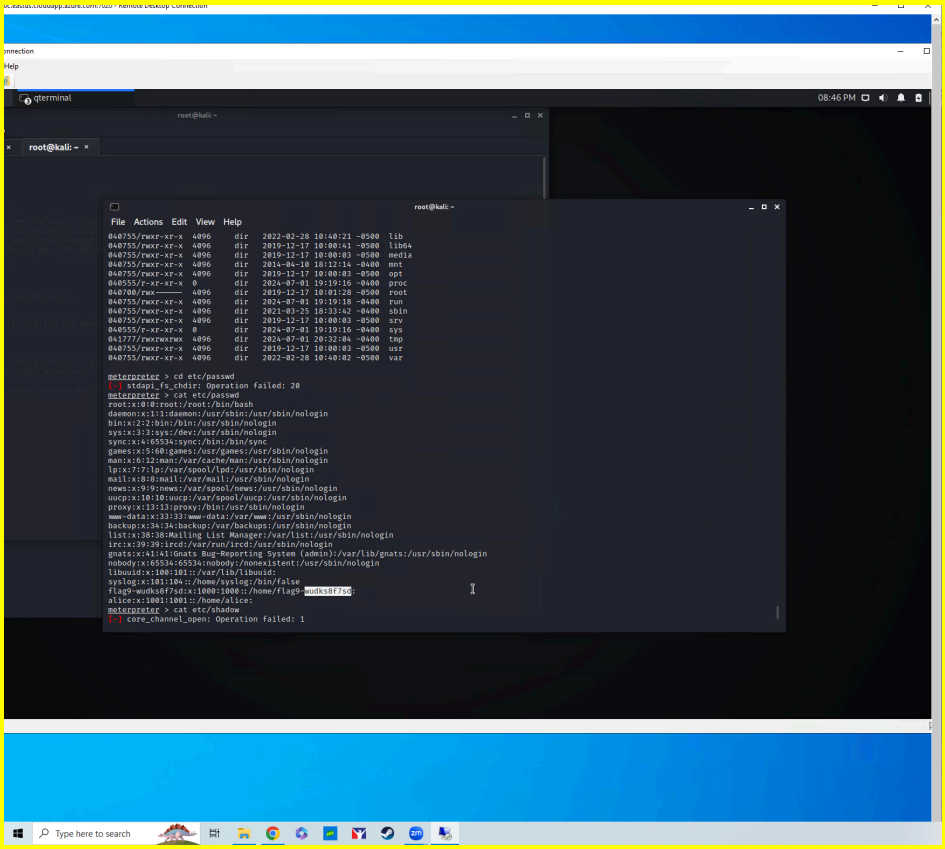
Vulnerability 21	**Findings**
Title	Nessus Scan Vulnerability
Type (Web app / Linux OS / WIndows OS)	Network
Risk Rating	Critical
Description	Run a basic network scan against 192.168.13.13 in Nessus. There will be one critical vulnerability, the flag is that vulnerability's ID.
Images	
Affected Hosts	192.168.13.13
Remediation	Assess all vulnerabilities on nessus scan and address all the issue.

Vulnerability 22	Findings
Title	Remote File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	An exploit in a Tomcat server running on IP address 192.168.13.10 was utilized via the Metasploit Framework (msfconsole). The specific module exploit/multi/http/tomcat_jsp_upload_bypass was employed to gain unauthorized access to the server. After Gaining access using the command 'find / -type f -iname '*flag*.txt' the flag is then found.
Images	
Affected Hosts	192.168.13.10
Remediation	Updating a patching the Tomcat server should help mitigate potential vulnerabilities with remote file inclusion.

Vulnerability 23	Findings
Title	Shellshock Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical

Description	The Shellshock vulnerability affects web applications running on servers using the Apache HTTP Server with CGI scripts that use the Bash shell. Exploiting this vulnerability allows attackers to use commands by injecting malicious code used by bash. To exploit this vulnerability using Metasploit: exploit/multi/http/apache_mod_cgi_bash_env_exec
Images	
Affected Hosts	192.168.13.11
Remediation	Ensure all versions of Bash are updated to fix the shellshock vulnerability.

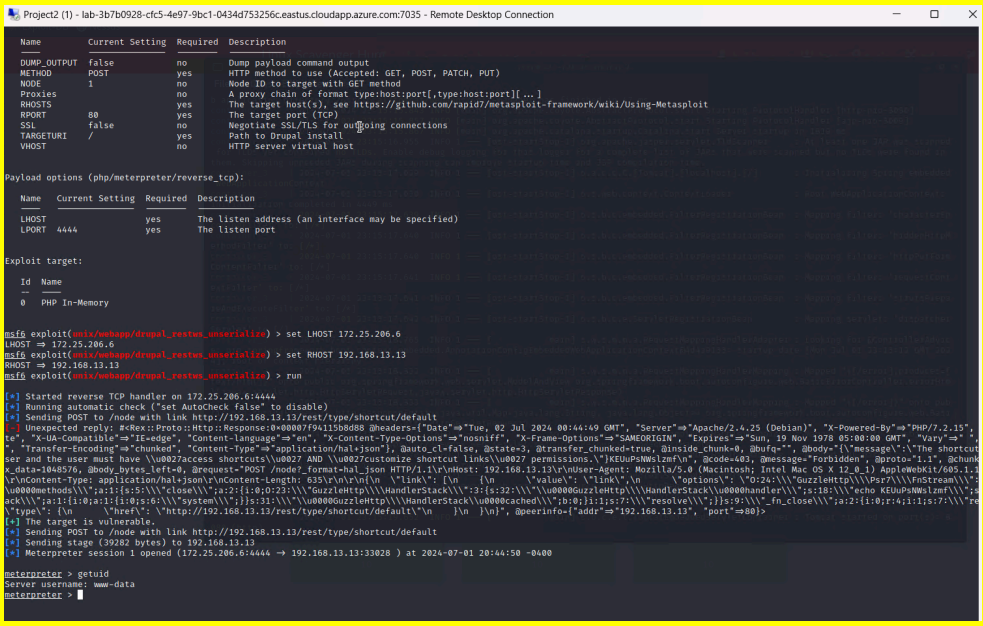
Vulnerability 24	Findings
Title	File Permissions on /etc/passwd
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	After gaining access using meterpreter. The vulnerability is then found in the /etc/passwd file. Using the command cat /etc/passwd we were able to access sensitive information finding the flag.

Images	
Affected Hosts	192.168.13.11
Remediation	Updating file permissions will help to ensure that no one unauthorized can have access to any sensitive files.

Vulnerability 25	Findings
Title	Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	*exploit multi/http/struts2_content_type_ognl* The vulnerability in Apache Struts2 framework mishandles the Content-Type header, enabling remote attackers to execute arbitrary code on the server. This exploit can result in complete compromise of the affected system.

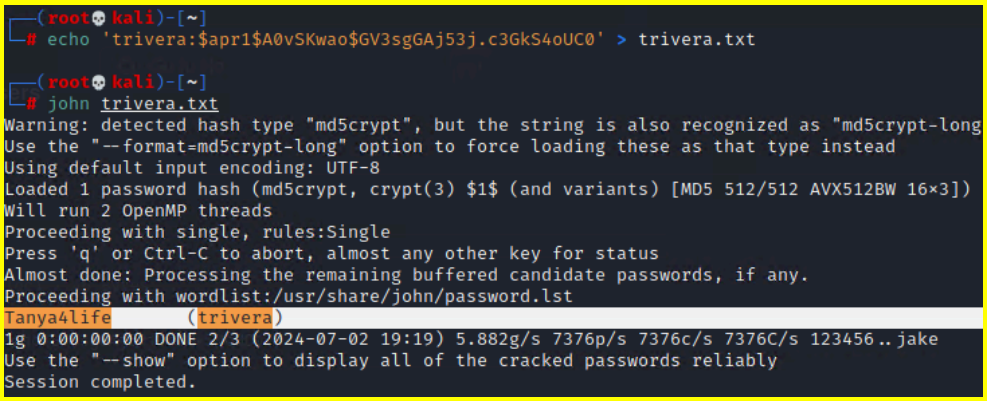
Images	
Affected Hosts	192.168.13.11
Remediation	Ensure that the Apache Struts2 framework is updated to the latest patched version, which addresses the vulnerability.

Vulnerability 26	Findings
Title	Drupal Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	unix/webapp/drupal_restws_unserialize The vulnerability unix/webapp/drupal_restws_unserialize is found in the Drupal RESTful Web Services (RESTWS) module. It occurs because the module doesn't handle user input correctly. This oversight could allow attackers to inject PHP objects or execute arbitrary code on the server.

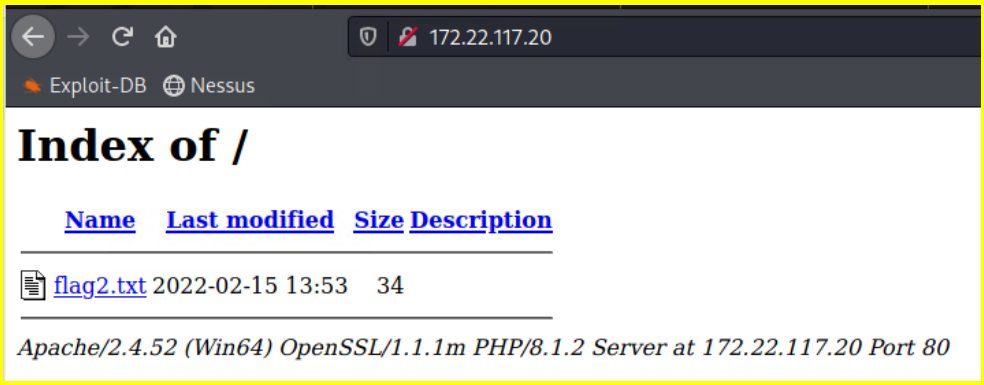
Images	
Affected Hosts	192.168.13.11
Remediation	Implement proper input validation and sanitization mechanisms within the application code.

Vulnerability 27	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Gained unauthorized access to the system using the credentials of 'Alice' with password 'Alice', obtained via Whois Domain command. Exploiting CVE-2019-14287 via 'sudo -u#-1' to elevate privileges to root.
Images	

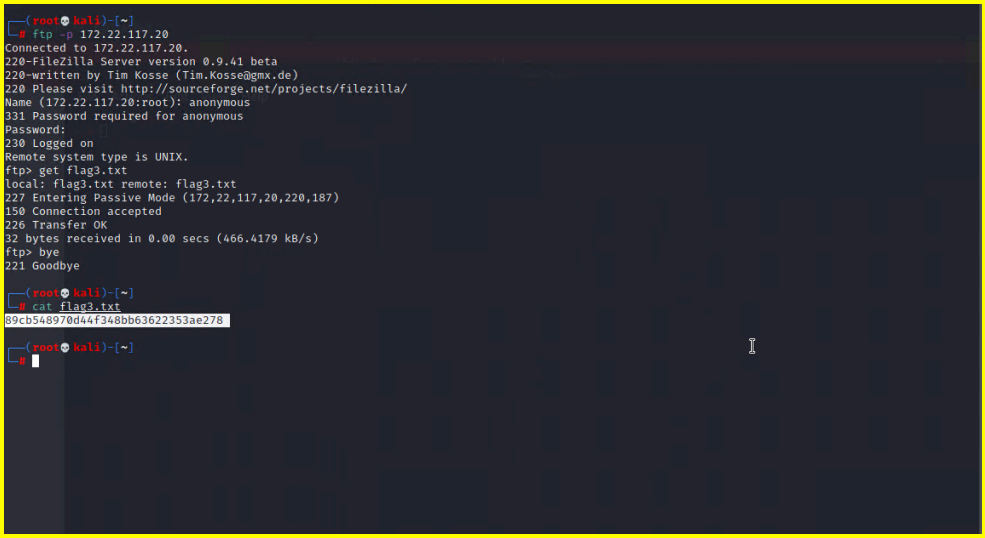
Affected Hosts	192.168.13.11
Remediation	Password management and requiring users to have complex passwords.

Vulnerability 28	Findings
Title	Credentials on Public GitHub Repository
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Credentials for accessing the XAMPP application were found exposed on the public GitHub repository of totalrekall. These were then extracted and cracked with the tool John The Ripper.
Images	
Affected Hosts	192.168.14.35
Remediation	Reset any and all passwords that are associated with the github repository leak. Enforcing a policy for 2fa or multi factor authentication to also increase security.

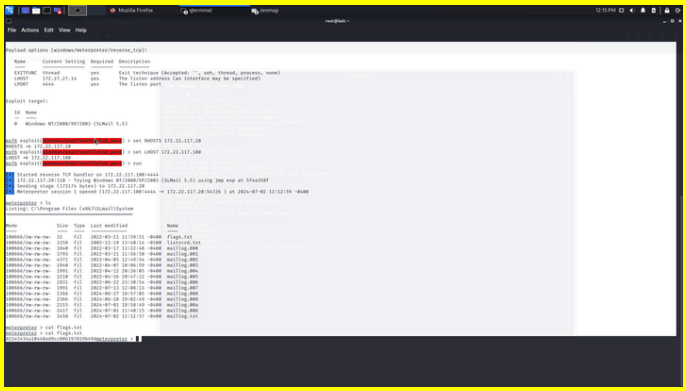
Vulnerability 29	Findings
Title	Compromised Credentials
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical

Description	Access to flag 2 on 172.22.117.20 was gained without proper authentication using credentials obtained from Vulnerability 28. Using Firefox on Kali Linux, access to an index page revealed flag 2.
Images	
Affected Hosts	172.22.117.20
Remediation	Changing compromised passwords and enforcing a MFA policy will enhance and add extra layers of security.

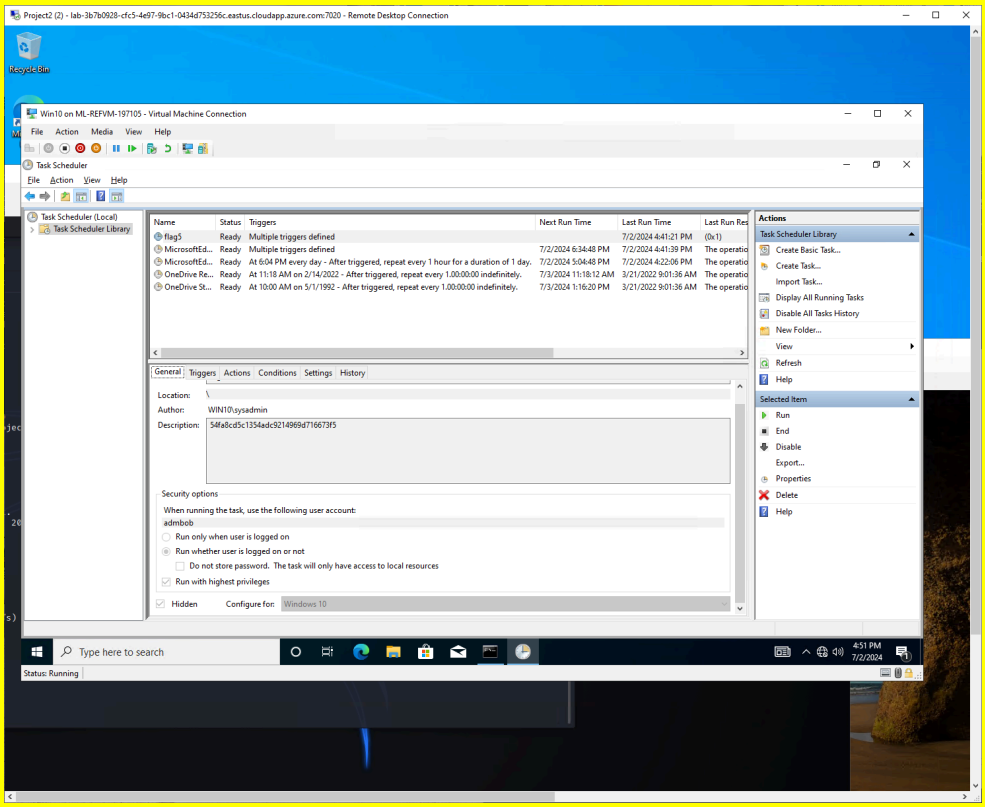
Vulnerability 30	Findings
Title	FTP Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Flag is accessed using the FTP (File Transfer Protocol) method ftp -p 172.22.117.20.

Images	
Affected Hosts	172.22.117.20
Remediation	Changing permissions on the FTP server to only allow authorized users. Regularly auditing users to see whos inactive to potentially clear out and active authorized users.

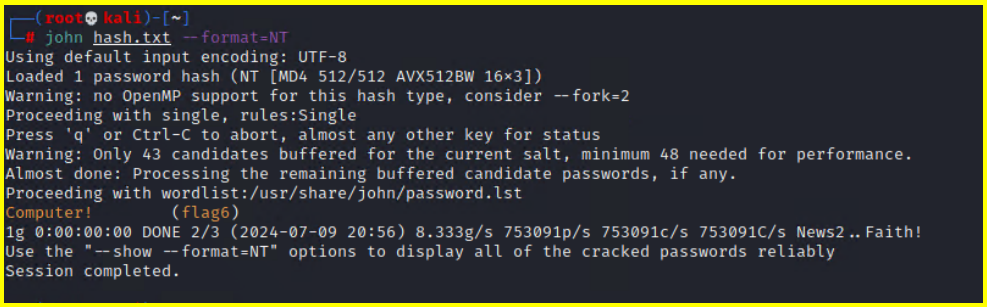
Vulnerability 31	Findings
Title	Remote Code Execution Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Medium
Description	Using the exploit module exploit/windows/pop3/seattlelab_pass in Metasploit, attackers can remotely execute code on the system at IP 172.22.117.10 This exploit targets vulnerabilities in the SLMail service. The flag for this vulnerability was found after using the ‘ls’ command in the system.

Images	
Affected Hosts	172.22.117.10
Remediation	Updating the SLmail service and OS to help patch the known vulnerability. The deployment of an IDS system would help to detect unauthorized attempts and any potential malicious activity.

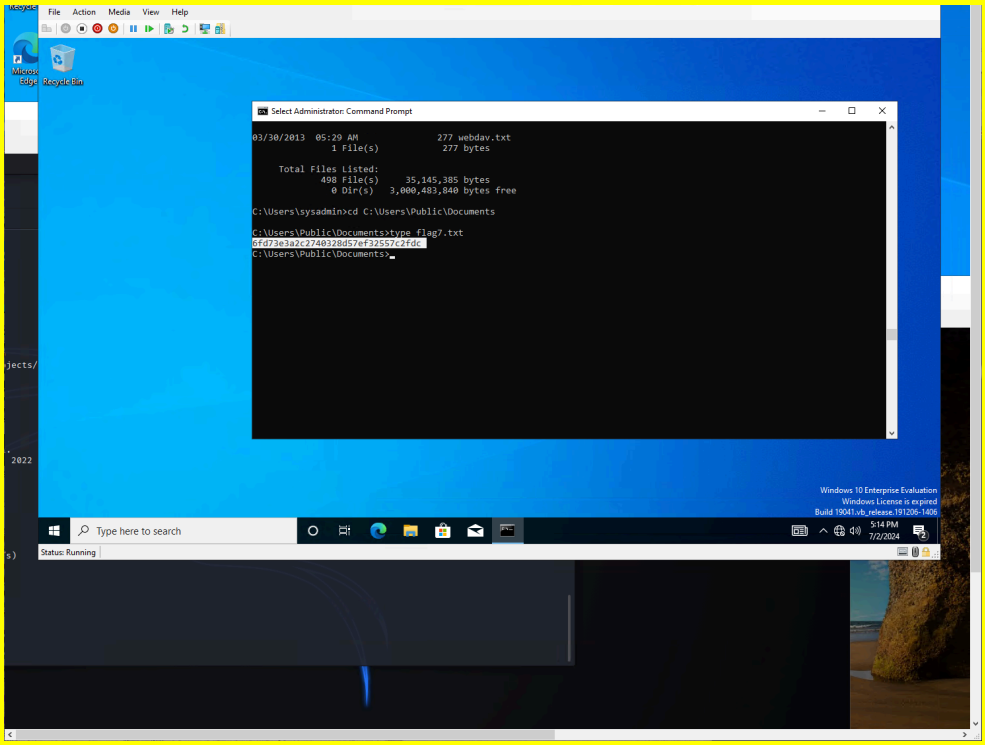
Vulnerability 32	Findings
Title	Scheduled tasks in the Windows 10 Machine
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low
Description	This flag was accessible by using the task scheduler in the affected system. Once in we were able to find the flag in the scheduled tasks.

Images	
Affected Hosts	172.22.117.10
Remediation	Limit the abscess to the task scheduler to authorized users only.

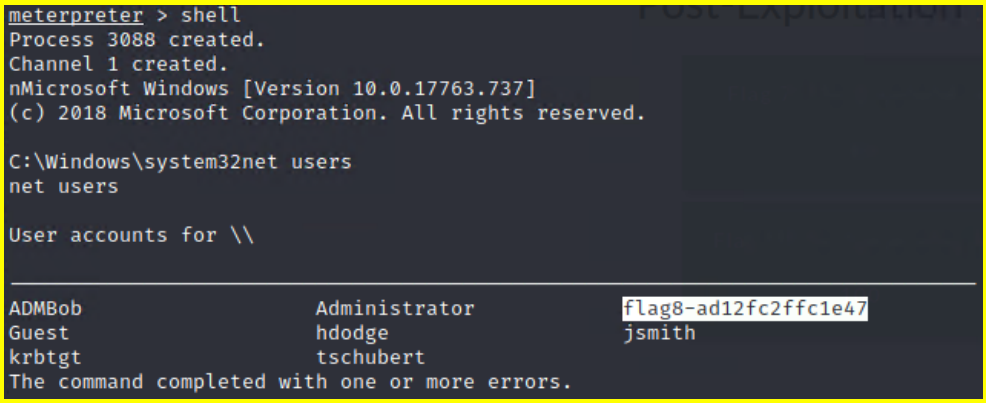
Vulnerability 33	Findings
Title	Unauthorized access using Kiwi and Password Cracking With John The Ripper
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using the Metasploit module exploit/windows/pop3/seattlelab_pass, access to the system was successfully gained. Once inside, the lsa_dump_sam command in Kiwi loaded the hash for flag 6. Using the NTML format in John the Ripper, we successfully decrypted the password, which was found to be "Computer!"

Images	
Affected Hosts	172.22.117.10
Remediation	Conduct regular checks to find and fix security issues in your network and systems. This will help find vulnerabilities and any potential upgrades or patching can be done.

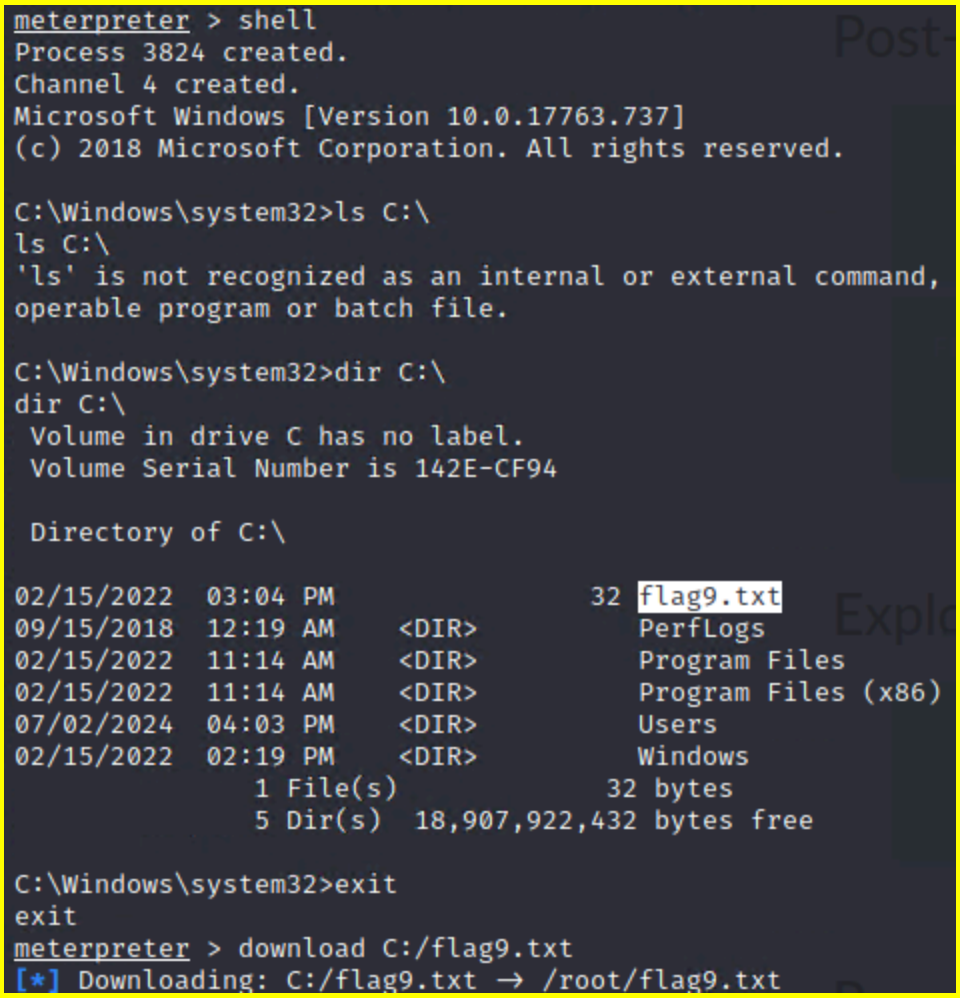
Vulnerability 34	Findings
Title	Sensitive Data In Public User Documents
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	After Navigating to the C:\Users\Public\Documents” in the windows 10 machine were then able to access sensitive data in a public file finding the flag.

Images	
Affected Hosts	172.22.117.10
Remediation	Implement strict access controls to limit who can view or modify files in the "C:\Users\Public\Documents" directory.

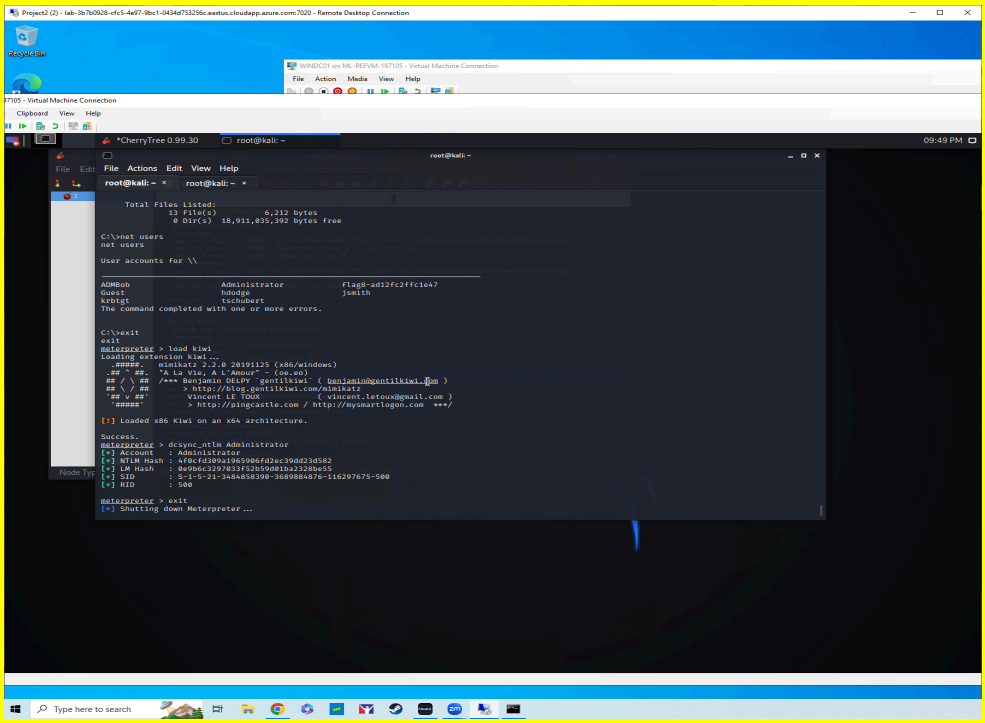
Vulnerability 35	Findings
Title	Metasploit Exploit Unauthorized Access On The Windows 10 Machine
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	To exploit this vulnerability on a Windows 10 machine, a meterpreter session must be active. Use the Metasploit module exploit/windows/local/wmi (alternatively, psexec can also be used) to execute the exploit. Access is granted using the credentials obtained via a Kiwi dump in the meterpreter session: username = admbob, password = Chargeme!, SmbDomain = WIN10.

Images	
Affected Hosts	172..22.117.10
Remediation	Apply all available security patches and updates to the Windows 10 operating system and relevant applications to mitigate known vulnerabilities.

Vulnerability 36	Findings
Title	File Access on Windows DC10
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	This vulnerability allows unauthorized access to sensitive files on the Windows DC10 machine. By accessing a shell on the machine, running dir C:\ reveals the presence of the flag9.txt file. Using Metasploit's download command, the file is retrieved from C:\ and saved to the local system's home directory. The contents of flag9.txt are then viewed using the cat command.

Images	 bnv
Affected Hosts	172.22.117.10
Remediation	Implement strict access controls to limit who can access sensitive files and directories on Windows DC10.

Vulnerability 37	Findings
Title	Admin Password Hash
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	This vulnerability allows retrieving the Administrator password hash from the WINC01 system using Metasploit's Meterpreter tool. By using Meterpreter, you can run net users to get a list of users, including Administrator. After using a tool called Kiwi within Meterpreter, running

	dcsync_ntlm Administrator fetches the password hash for the Administrator account.
Images	
Affected Hosts	172.22.117.10
Remediation	Limiting access to tools like meterpreter and kiwi to only authorized users.