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	Big Bad Industries
Contact Name	Sir Big Bad III
Contact Title	Biggest and Baddest

Team

Team Member	Author(s)
001	Michael Meadow
002	Leon Mosburg
003	Michael Gorin
004	Ryan Fernandez
005	Chris Maurer
006	Marc Villanueva
007	Matt Kamimura
008	Nicholas Martin
009	Camden Hassanpour

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.

192.169.14.35
192.168.13.10
192.168.13.11
192.168.13.12
192.168.13.13
192.168.13.14
172.22.117.10
172.22.117.20

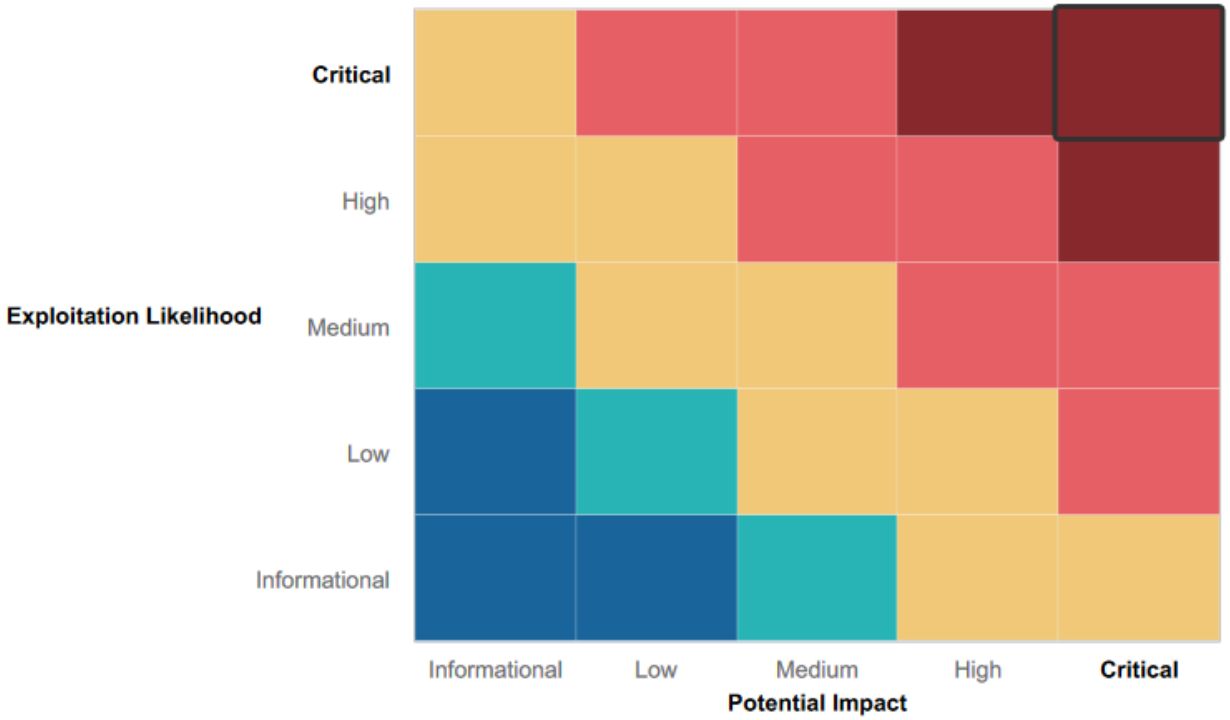
Executive Summary of Findings

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.

Day 1

- XSS exploits on certain web application input fields were protected against basic attacks
- Input fields have some input sanitization rules implemented
- Attacking the webpage via SQL injection has little success
- Local File Inclusion attacks have very little success on the webpage
- Defacement of webpage had no success

Day 2

- Principle of least privilege properly employed.
- SQL Injection attacks on the webpage had no success
- LFI attacks had no success on the webpage
- Input fields have proper input sanitization

Day 3

- Proper segregation of systems preventing DOS attacks
- Standard security measures in place for most of Rekall's systems
- Unable to directly access the Domain Controller machine

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.

Day 1

Web App

- Weak implementation of input sanitization
- Susceptible to numerous XSS vulnerabilities on multiple web pages
- Leak of sensitive user data
- Vulnerable to multiple local file inclusion vulnerabilities
- Vulnerable to SQL injection attacks on the login page
- Admin account login details exposed on the login page by viewing the HTML source
- Sensitive data was leaked by viewing the publicly accessible robots.txt
- Vulnerable to multiple command injection attacks
- Susceptible to brute force attacks on the login page. The login page does not have login rate limiting enabled.
- Vulnerable to PHP injection attacks
- Susceptible to directory traversal attacks on the networking page
- Vulnerable to a session management attack by broken access control (BAC)

Day 2

Linux server vulnerabilities

- Susceptible to standard reconnaissance techniques such as NMAP scanning
- IP addresses for these servers are exposed to the open internet
- Each identified vulnerability can be easily matched to a specific CVE, which then allows easy exploitation via Metasploit.
- Susceptible to multiple RCE exploits which allow attackers to run arbitrary commands
- The web application servers ran outdated unpatched versions of apache which were vulnerable to numerous exploits
- Outdated version of Drupal vulnerable to a CVE exploit
- Vulnerable to device enumeration using CIDR scans
- SSH password for Alice was very weak since she used her username as the password, which left the account susceptible to password guessing

Day 3

Windows vulnerabilities

- Using OSINT techniques, confidential information was found on Rekall's public Github repo
- Susceptible to HTTP enumeration
- Rekall's machines were vulnerable to FTP Enumeration
- Using information gained from the scan, an unpatched SLMail exploit was used to gain entry to a local administrator machine
- Once shell access was gained on the machine, a scheduled task could be created to allow an attacker to maintain persistent access
- Vulnerable to user enumeration
- Reuse of credentials between machines allowed lateral movement to compromise the domain controller after initial access.

Executive Summary

Web App

The web application suffers from multiple vulnerabilities primarily due to inadequate input sanitization protocols. These vulnerabilities have allowed for the exploitation of various command injection vectors, including PHP and SQL injections, posing significant risks such as unauthorized access to, exfiltration, or destruction of the database. Moreover, the presence of multiple input fields vulnerable to Cross-Site Scripting (XSS) payloads heightens the risk, particularly concerning client-side security.

Furthermore, lax validation mechanisms for image upload inputs have enabled the storage of potentially malicious scripts within the application via local file inclusion (LFI). Additionally, the inadvertent exposure of administrative credentials in plaintext within the HTML source code, along with weak password defenses susceptible to brute force attacks, severely compromises access controls.

Despite some efforts at input sanitization, these measures have proven ineffective against well-known escape commands, allowing for arbitrary code execution in critical components like DNS and MX lookup functionalities. Exploitation of remote code execution vulnerabilities further enables manipulation of uploaded files via LFI, potentially introducing malicious software into the server-side environment.

Directory traversal vulnerabilities, especially within the disclaimer section of the website, exacerbate the risk landscape by providing unfettered access to sensitive directories and files stored within the application's structure. Combined with the code execution vulnerability in the DNS lookup feature, unauthorized access to and retrieval of sensitive information are greatly simplified.

The discovery of PHP injection vulnerabilities underscores the urgent need for robust security measures throughout the application's codebase, as revealed through tools like Burp Suite.

Moreover, the compromise of the secret admin area due to inadequate security measures, coupled with exploitation of session manipulation vulnerabilities through tools like Burp Suite, underscores vulnerabilities in both access controls and session management protocols.

In summary, these vulnerabilities necessitate comprehensive security auditing and remediation efforts to strengthen the web application against potential exploits and protect sensitive data from unauthorized access or manipulation.

Linux Servers

Following the recon and enumeration process encompassing WHOIS, nmap, and SSL certificate examinations of totalrekall.xyz, our investigation discovered user SSH credentials and a publicly accessible IP address via port 21. While the disclosure of such information in the public domain may not immediately pose a threat, it does present a potential entry point for exploitation, as detailed in later sections of the report.

Subsequently identifying six available hosts through nmap scans on the discovered IP addresses, our team embarked on a thorough exploration to uncover vulnerabilities within the services identified during these scans. Once again, while the presence of open ports does not inherently pose a direct threat, the absence of anonymity combined with exposed services can lead to the discovery of exploitable systems. In this specific scenario, the 192.168.13.14 machine was accessed via port 22 (SSH) using credentials extracted from the WHOIS lookup, which included a notably inadequate password mirroring the username itself. Leveraging CVE-2019-14287, our team successfully rooted and compromised the machine.

Further examination through a Nessus scan on the 192.168.13.12 machine revealed the presence of CVE-2019-6340, subsequently leading to the compromise of the 192.168.13.13 machine. Enumeration via nmap of the 192.168.13.15 machine uncovered a potential remote code execution exploit targeting Apache Tomcat (CVE-2017-12617), enabling unauthorized root access to the machine.

Additionally, an enumeration scan of the 192.168.13.11 machine exposed a vulnerability susceptible to the shellshock exploit (CVE-2014-6278). Although this exploit did not immediately confer root privileges, it nonetheless provided access to numerous confidential files, including the sudoers list and the passwd file, laying the foundation for potential privilege escalation attempts.

During our investigation, it was discovered that the 192.168.13.15 machine was affected by vulnerability CVE-2017-5638. Leveraging Metasploit, we successfully exploited this vulnerability, resulting in the compromise of the machine.

Windows Servers

The penetration testing engagement conducted on Rekall's network unveiled several critical vulnerabilities and security weaknesses with significant implications for the organization's assets. Through Open Source Intelligence (OSINT) techniques, a username and hash was uncovered on Rekall's public GitHub repository, potentially exposing the organization to unauthorized access or exploitation.

Rekall's web servers were found susceptible to HTTP enumeration, which could disclose crucial information about the underlying server infrastructure and potentially expose security vulnerabilities. Additionally, vulnerabilities in FTP enumeration were identified, posing a risk of unauthorized access and the potential exploitation of FTP-related weaknesses.

Exploiting an unpatched SLMail vulnerability, attackers could gain entry to a local administrator machine, emphasizing the importance of promptly applying security patches and updates to mitigate the risk of known vulnerabilities being exploited. Subsequently, shell access to the compromised machine allowed the creation of a scheduled task, enabling persistent access even after remediation efforts.

The discovery of vulnerable user enumeration mechanisms and credential reuse between machines facilitated lateral movement within Rekall's network. This allowed attackers to compromise the domain controller, highlighting the urgency for implementing comprehensive security measures. These measures should include regular patch management, robust access controls, and employee security awareness training to mitigate the risks of potential cyber threats and their severe consequences, including data breaches and reputational damage.

Summary Vulnerability Overview

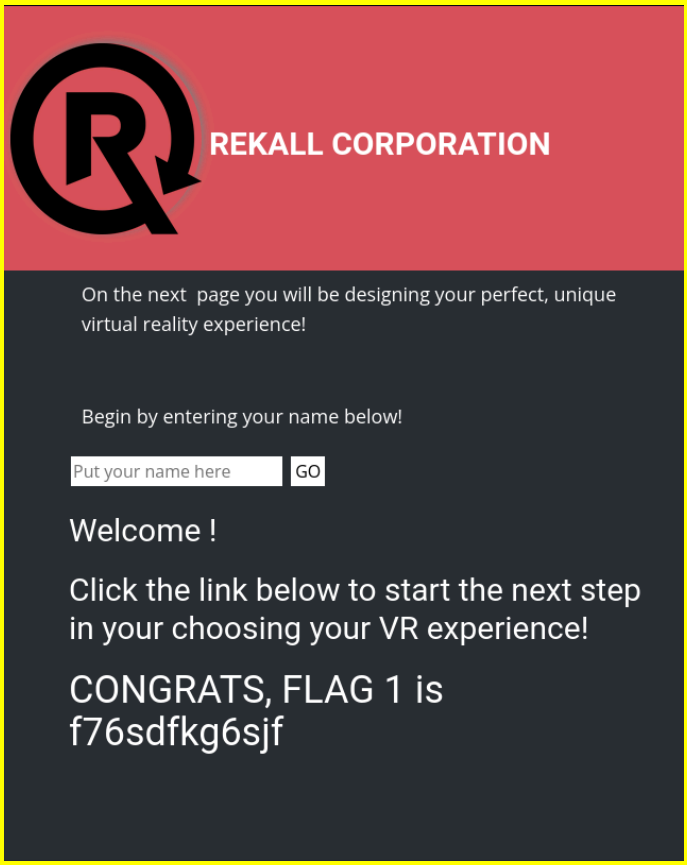
Vulnerability	Severity
DAY 1	
Webpage vulnerable to XSS attacks	Critical
Webpage vulnerable to SQL injection	Critical
Webpage vulnerable to LFI attacks	Critical
Sensitive user data exposure	Critical
Admin login credentials exposed on login page by viewing HTML	Critical
Directory traversal from the networking page	Critical
Weak login credentials, vulnerable to brute force attacks	High
DAY 2	
Vulnerable to Remote Command Execution attacks	Critical
Outdated Service versions on machines which are vulnerable to certain CVE exploits	Critical
SSH was exploited using weak user credentials, susceptible to password guessing	Critical
Linux servers vulnerable to NMAP scanning	High
IP addresses exposed to Public	High
Vulnerable to CIDR scans	High
DAY 3	
Unpatched systems leading to multiple CVE exploits	Critical
Credentials publicly hosted on GitHub	Critical
Poor security rules across systems	High
Information enumerated using OSINT	Low

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

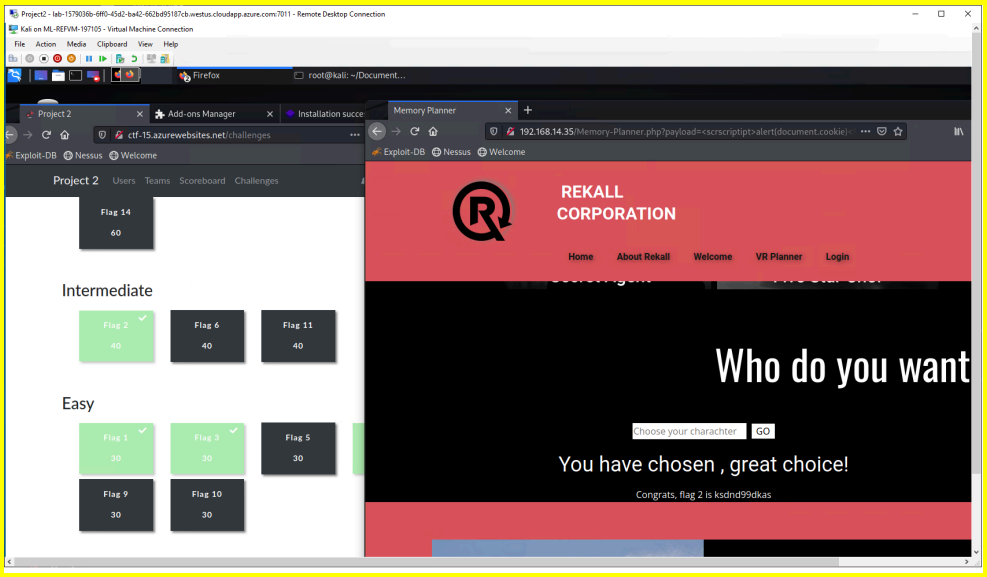
Scan Type	Total
Hosts	192.169.14.35 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20
Ports	21, 22, 25, 53, 79, 80, 88, 106, 110, 135, 139, 389, 445, 465, 593, 636, 3268, 3269, 4444, 8009, 8080

Exploitation Risk	Total
Critical	16
High	14
Medium	3
Low	3

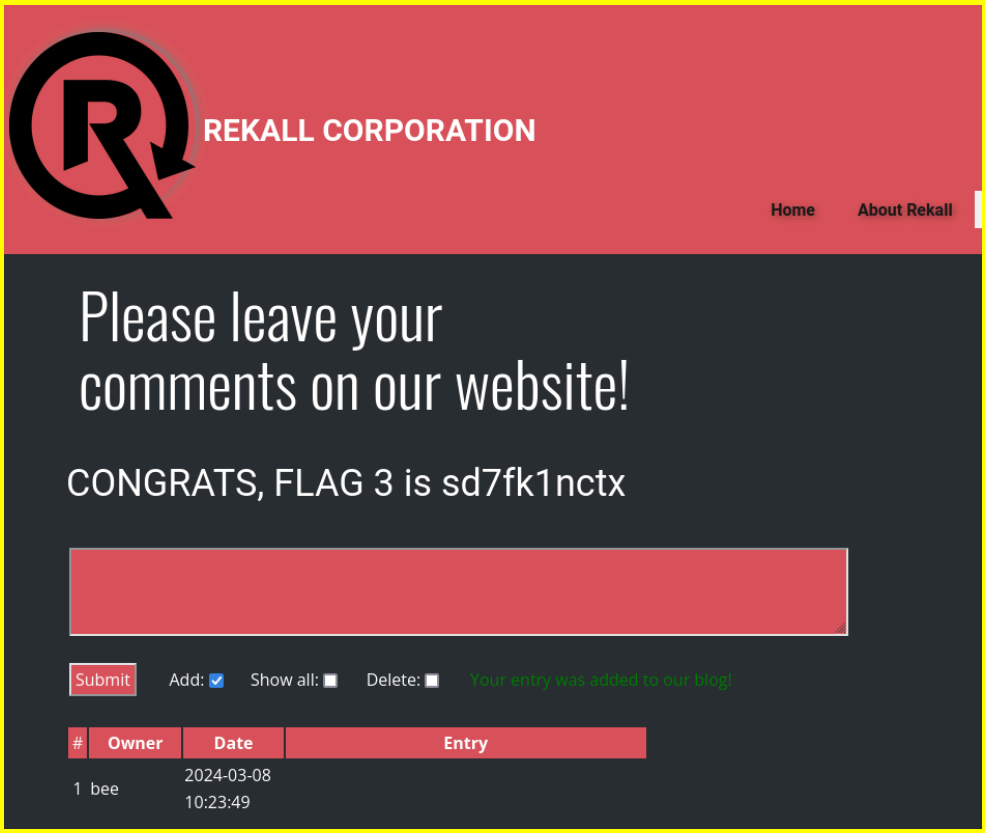
Day 1 Vulnerability Findings

Vulnerability 1	Findings
Title	Flag 01 - XSS Payload
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	In executing an XSS payload attack on `welcome.php`, we inject scripts into user-controlled content. When users access the page, these scripts execute in their browsers, allowing us to steal session cookies.
Images	

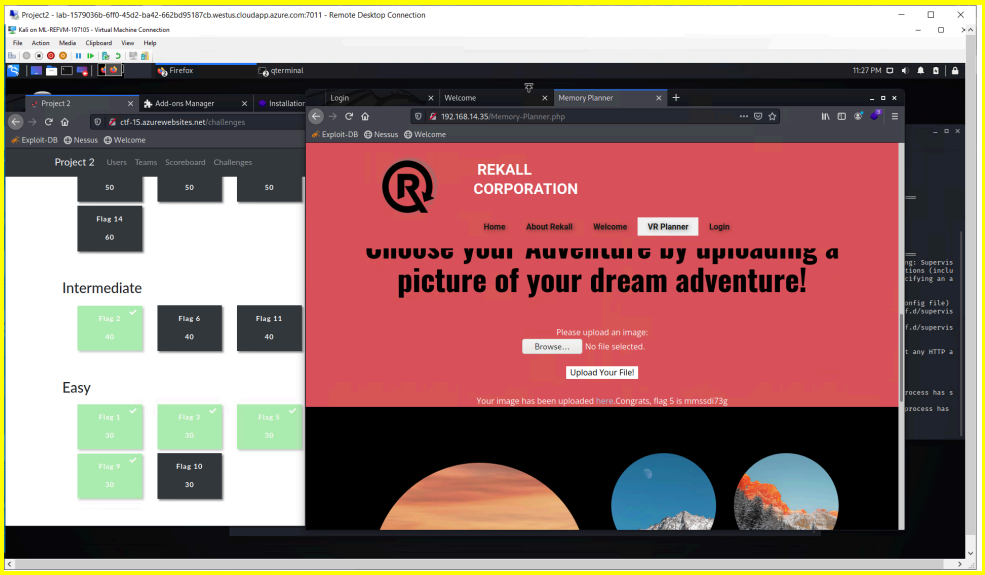
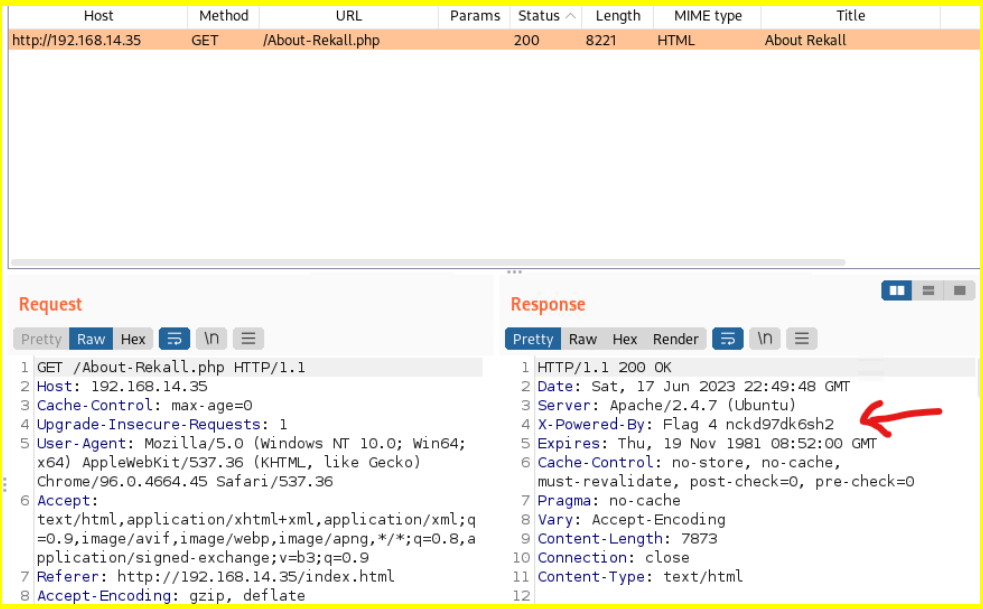
Affected Hosts	192.169.14.35
Remediation	Deploying a Web Application Firewall (WAF) can provide an additional layer of defense against XSS attacks by inspecting incoming web traffic and blocking malicious payloads in real-time. WAFs analyze HTTP requests and responses, enforcing security policies to filter out potentially harmful content before it reaches the web application. Implementation of a WAF complements other security measures and helps mitigate the risk of XSS vulnerabilities in web applications.

Vulnerability 2	**Findings**
Title	Flag 02 - XSS exploit through VR Planner page
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	On the VR planner page, we were able to run a script command as an input in the “Choose your character” box. This can possibly give us access to more directories and files in the database.
Images	
Affected Hosts	192.168.14.35
Remediation	Proper input sanitization to prevent specific inputs from being entered.

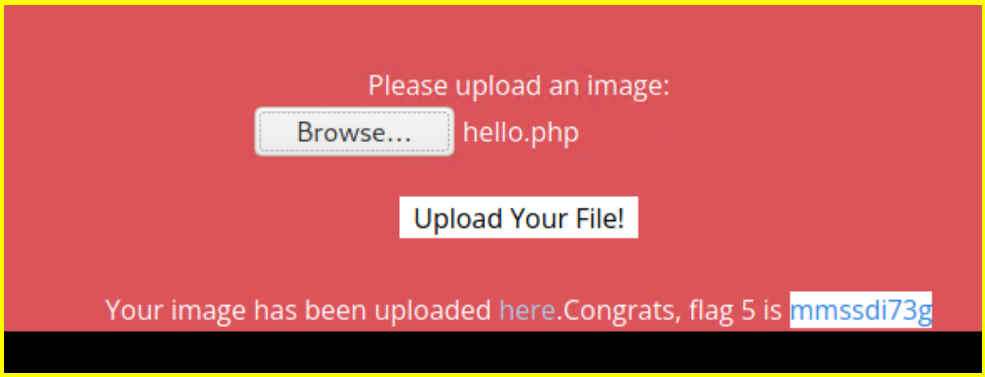
Vulnerability 3	**Findings**
Title	Flag 03 - Stored XSS

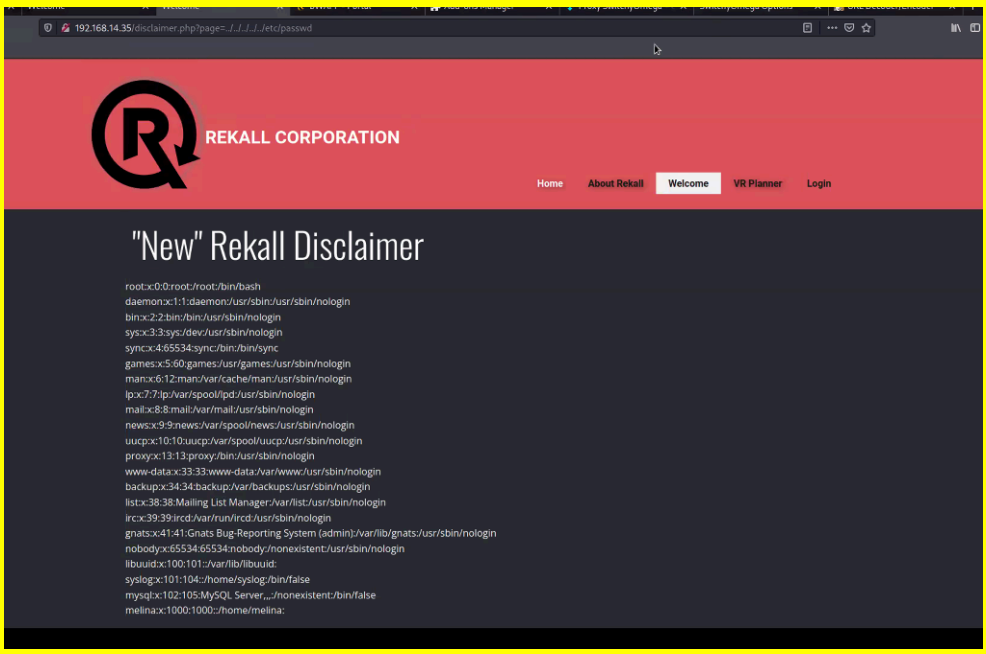
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Storing XSS payloads can lead to compromise of PII and access control tokens that attackers can leverage.
Images	
Affected Hosts	192.168.14.35
Remediation	Input validation and sanitization and/or content security policies.

Vulnerability 4	Findings
Title	Flag 04 - Local File Inclusion Exploit through Image Upload
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using the image upload tool on the VR Planner page, we were able to upload a script.php file with execute command code in it that allowed us to view the target file.

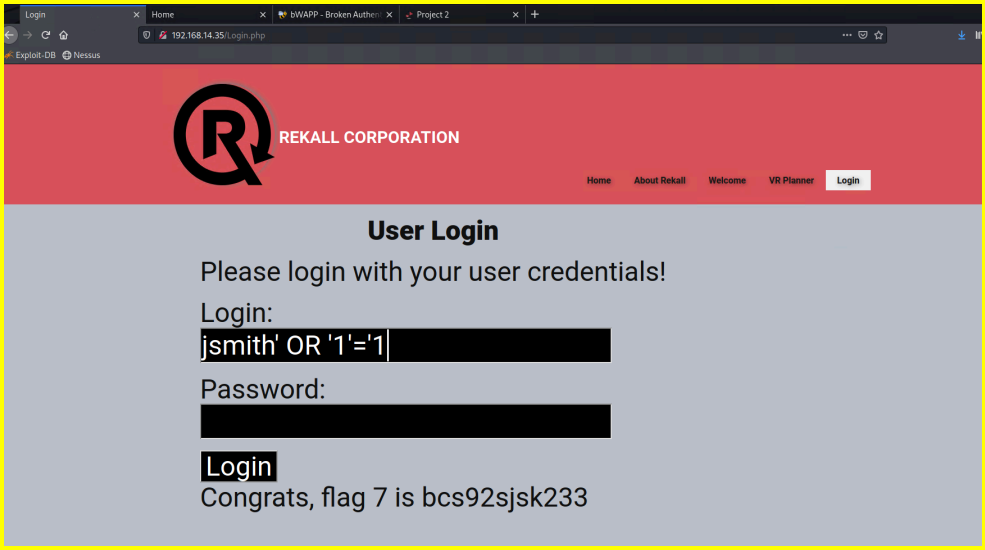
Images	 
Affected Hosts	192.168.14.35
Remediation	Implement strict file validation and sanitization checks on uploaded files, ensuring that only allowed file types and locations can be accessed or executed by the server.

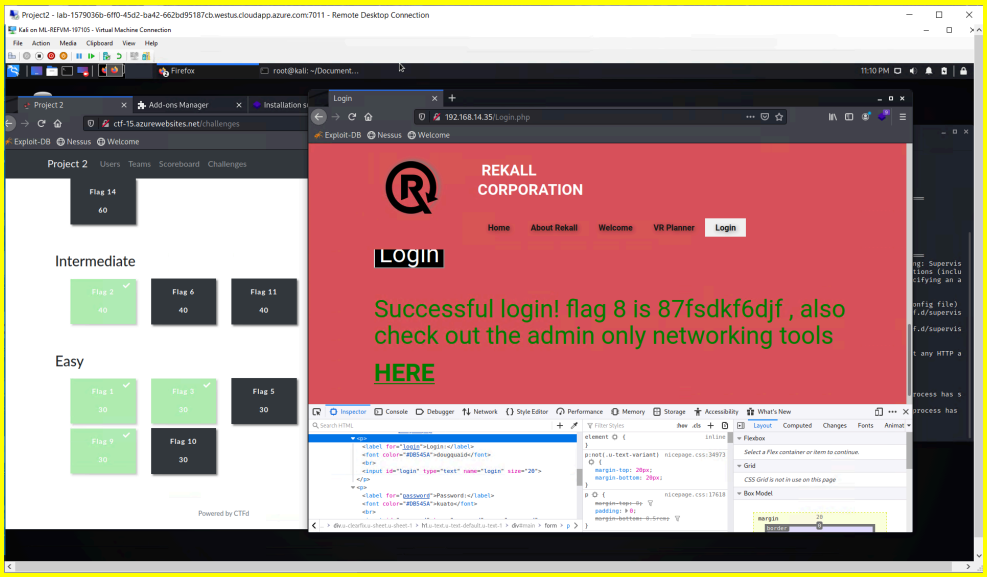
Vulnerability 5	Findings
Title	Flag 05 - Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Local File was uploaded bypassing security by adding “.jpg” in an arbitrary place within the filename.

Images	
Affected Hosts	192.168.14.35
Remediation	To defend against Local File Inclusion (LFI) exploits, avoid using user-controlled input directly in file paths or includes, employ whitelisting techniques for allowed file paths, and store sensitive files outside the web root directory to mitigate unauthorized access risks.

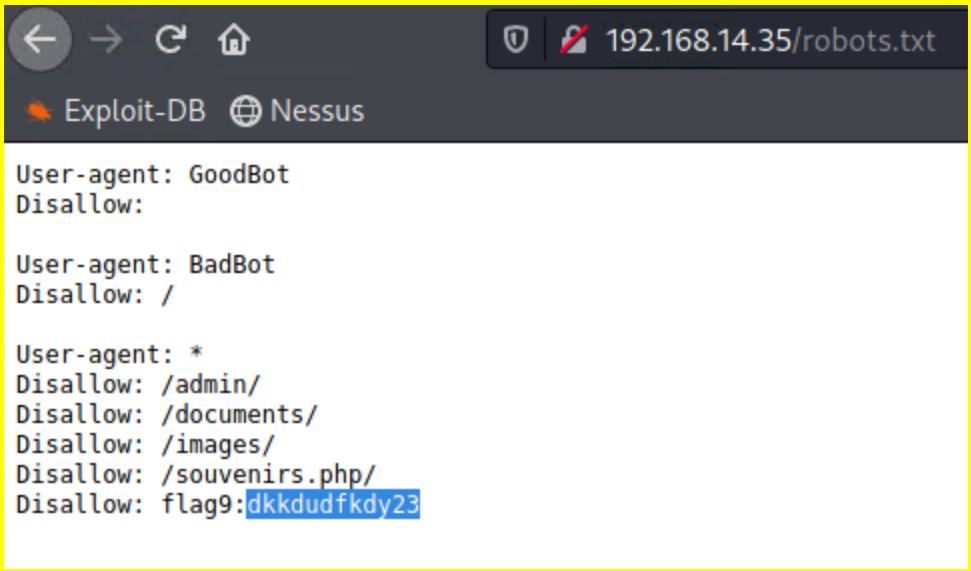
Vulnerability 6	Findings
Title	Flag 06 - LFI Accessible Through RCE
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	RCE on the DNS Lookup portion of the web app enabled access
Images	
Affected Hosts	192.169.14.35
Remediation	To mitigate LFI accessible through Remote Code Execution (RCE), enforce

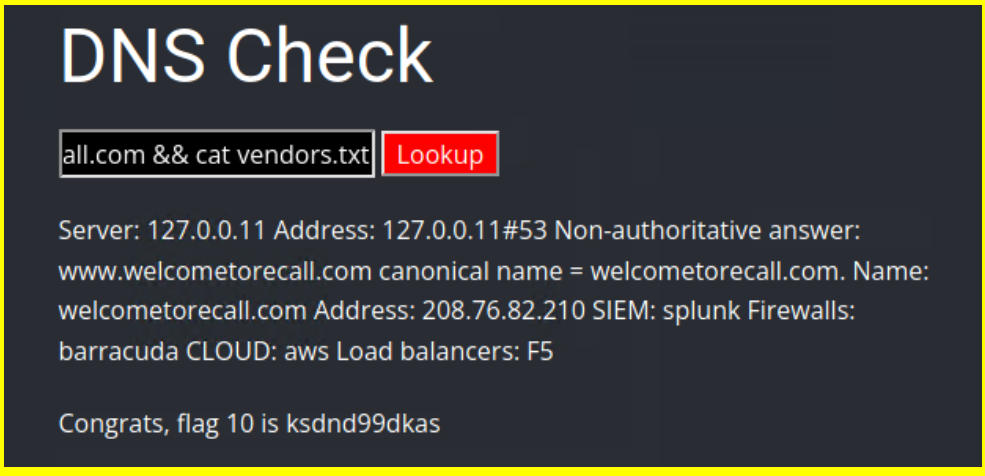
	proper input validation and sanitization to prevent unauthorized file inclusion attempts, and implement strict file system access controls to restrict access to sensitive directories and files, thereby minimizing the impact of potential exploitation. Additionally, consider deploying application-level security mechanisms such as web application firewalls (WAFs) to detect and block malicious file inclusion attempts in real-time.

Vulnerability 7	Findings
Title	Flag 07 - SQL Injection on the Login.php page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Lack of input sanitization allows an attacker to use SQL injection attacks to compromise Rekall's database.
Images	
Affected Hosts	192.168.14.35
Remediation	Aside from input sanitation, we suggest additional defenses such as: parameterized queries or prepared statements to separate SQL code from user input, implementing least privilege principles to restrict database user permissions, utilizing stored procedures or ORM frameworks to abstract database interactions, and employing web application firewalls (WAFs) to detect and block malicious SQL injection attempts.

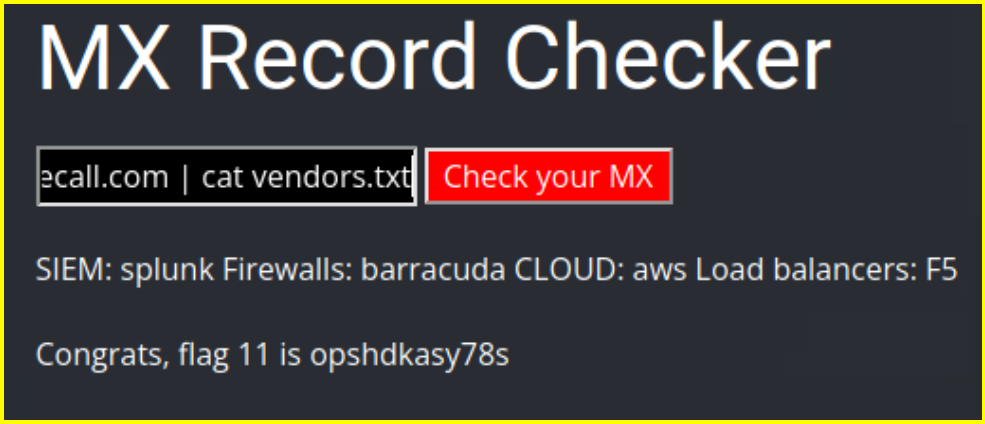
Vulnerability 8	Findings
Title	Flag 08 - Sensitive login information exposed in the HTML source of the Login page
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using developer tools on the browser, we are able to view the HTML code of the website which contains stored admin credentials which we then used to log into the admin section of the site.
Images	
Affected Hosts	192.168.14.35
Remediation	Recode the HTML portion of the site so that it doesn't include any credentials or public facing sensitive information.

Vulnerability 9	Findings
Title	Flag 09 - Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Vulnerable files exposed in robots.txt

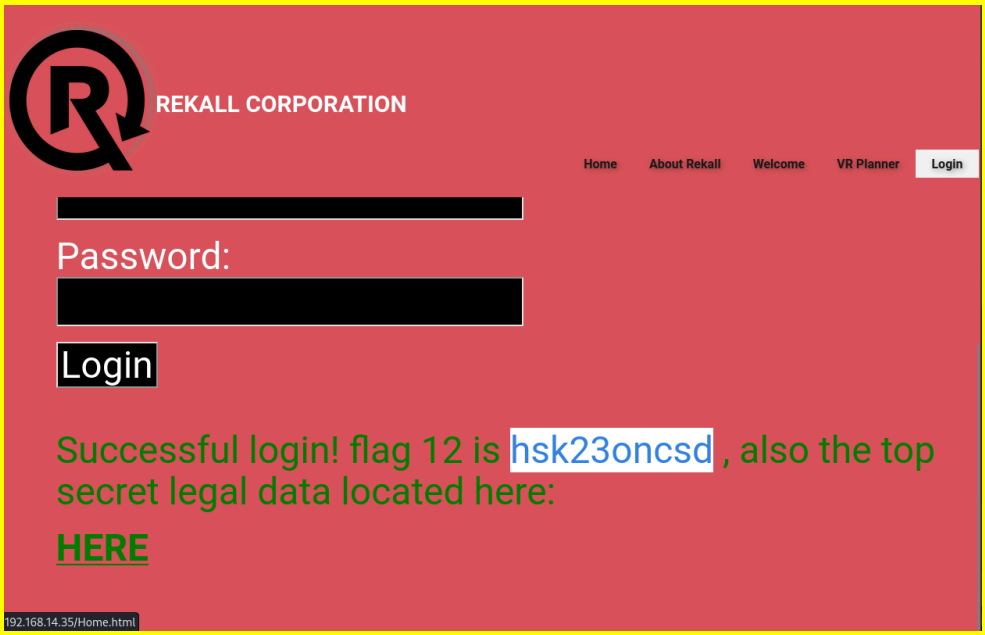
Images	
Affected Hosts	192.168.14.35
Remediation	Remove references to vulnerable files from robots.txt

Vulnerability 10	Findings
Title	Flag 10 - Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Lack of input sanitization allows command injection in the DNS checker form on Rekall's website, allowing arbitrary command execution.
Images	

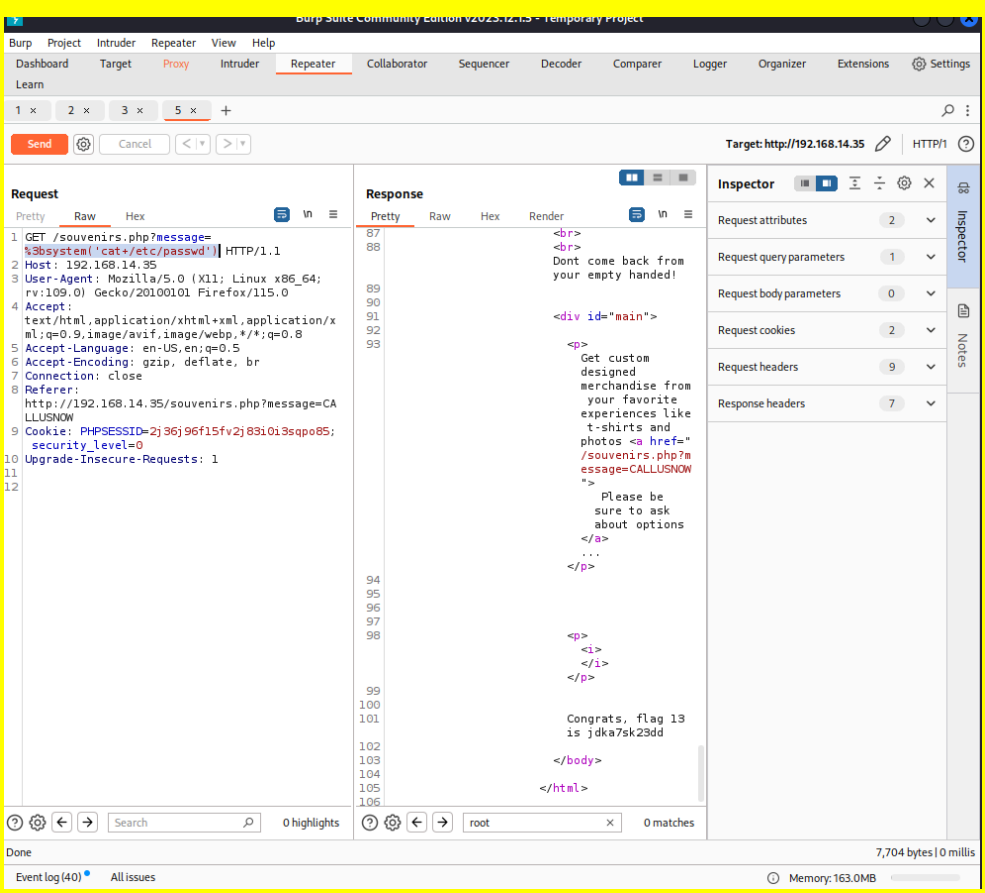
Affected Hosts	192.168.14.35
Remediation	Implement comprehensive input sanitization policies to prevent command injection.

Vulnerability 11	**Findings**
Title	Flag 11 - Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Command injection
Images	
Affected Hosts	192.168.14.35
Remediation	Comprehensive input sanitization rules to prevent command injection.

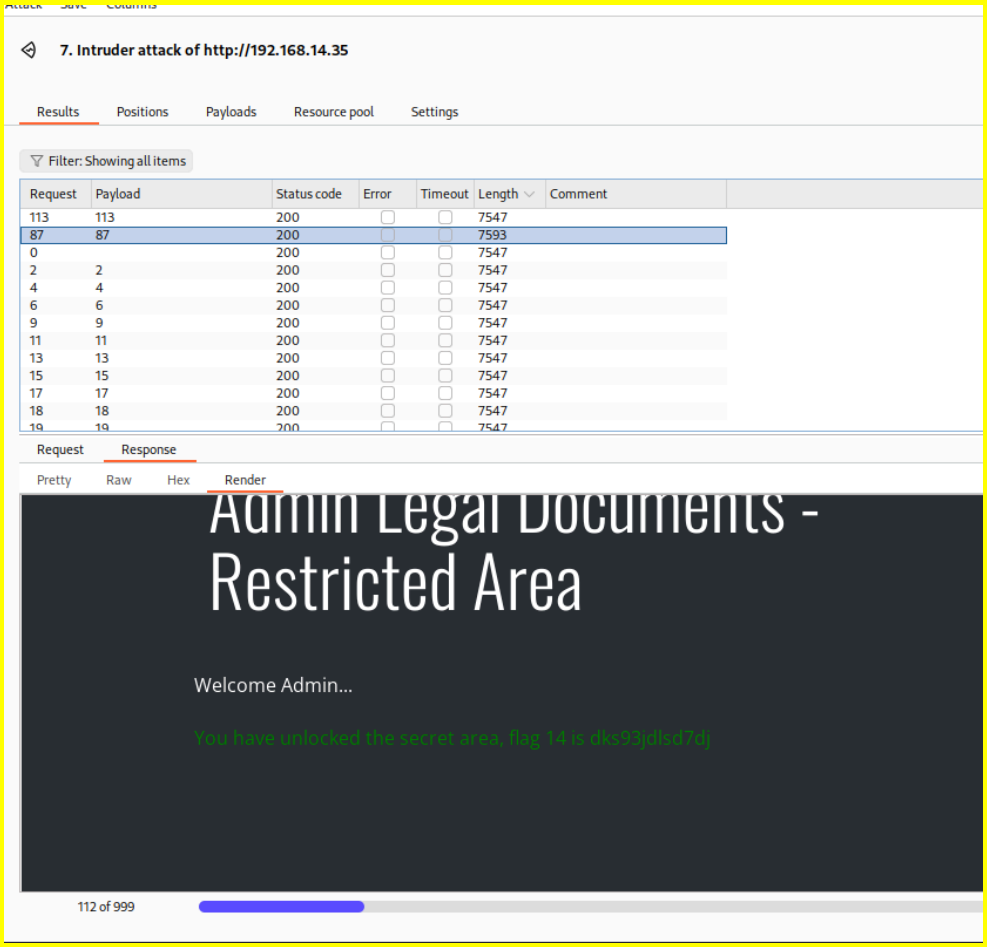
Vulnerability 12	**Findings**
Title	Flag 12 - Brute Force Attack on Rekall's Login Form
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Rate limiting is not implemented on the login form to mitigate brute force attacks.

Images	
Affected Hosts	192.168.14.35
Remediation	Stronger password policies, implementing multi-factor authentication (MFA) adds an extra layer of security beyond passwords, while rate limiting mechanisms throttle the number of login attempts, collectively mitigating brute force attacks by slowing down unauthorized access attempts and requiring additional verification for authentication.

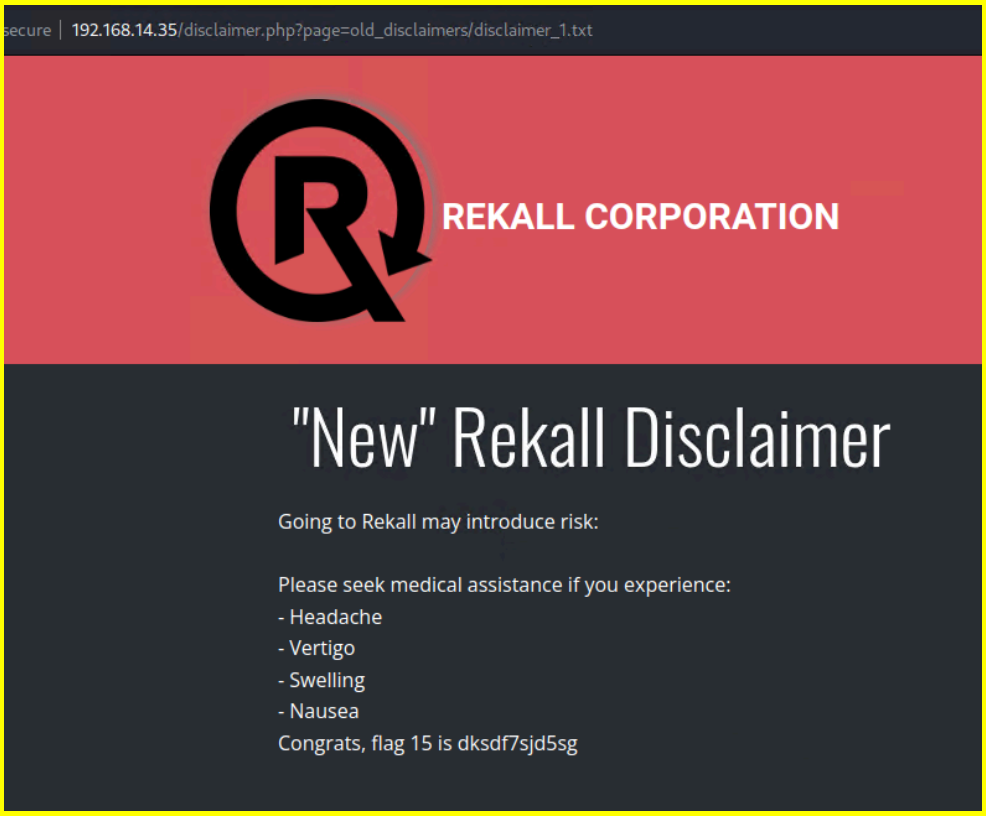
Vulnerability 13	Findings
Title	Flag 13 - PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Using Burp Suite we were able execute PHP injection on the souvenirs.php portion of the web app

Images	
Affected Hosts	192.168.14.35
Remediation	Incorporate a WAF, and/or utilize Input validation and sanitization.

Vulnerability 14	Findings
Title	Flag 14 - Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Exploitation of session management, using the Burp Suite intruder tool to brute force the session ID

Images	
Affected Hosts	192.168.14.35
Remediation	Utilize secure session handling practices such as implementing random and unique session identifiers, enforcing HTTPS for secure transmission, and regularly expiring and regenerating session tokens.

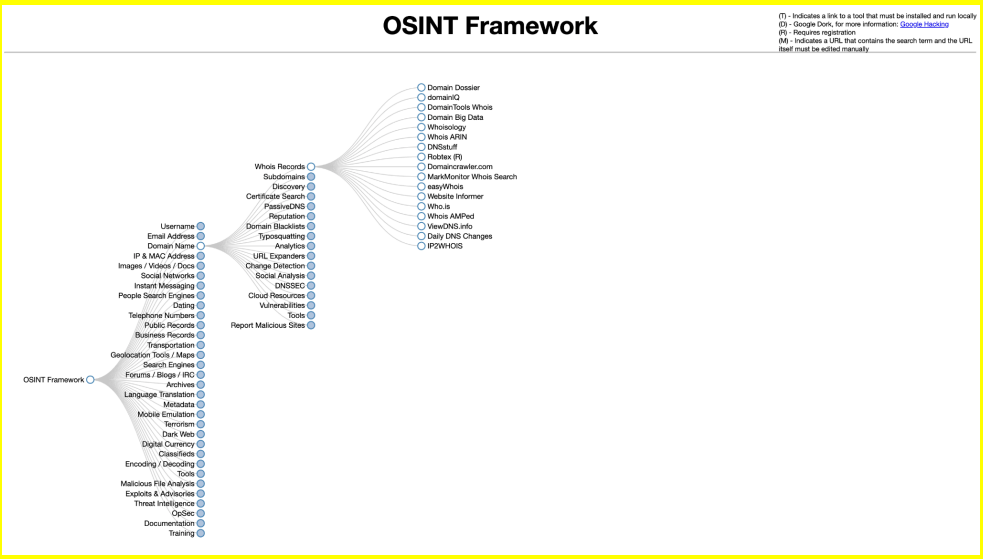
Vulnerability 15	Findings
Title	Flag 15 - Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using directory traversal techniques, viewed the content of the using to command injection exploits

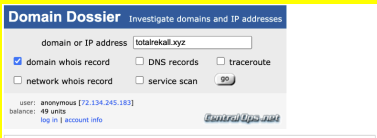
Images	
Affected Hosts	192.168.14.35
Remediations	Implementing access controls to restrict file system access based on user privileges, employing file system abstraction libraries or frameworks to abstract file operations, and configuring web server settings to deny access to sensitive directories and files.

Day 2 Vulnerability Findings

Vulnerability 1	Findings
Title	Flag 01 - Open Source Intelligence (OSINT) using WHOIS
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Used https://osintframework.com/ & https://centralops.net/co/DomainDossier.aspx

Images





To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

Address lookup

canonical name totalrekall.xyz.
aliases
addresses 15.197.148.33
3.33.130.190

Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2024-02-03T15:15:57.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2025-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2024-02-03T15:15:57.0Z
Creation Date: 2022-02-02T19:16:16.0Z
Registry Expiry Date: 2025-02-02T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod
Registrant Organization:
Registrant State/Province: Georgia
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-03-11T18:21:16.0Z <<<

Queried whois.godaddy.com with "totalrekall.xyz"...

Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
```

Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

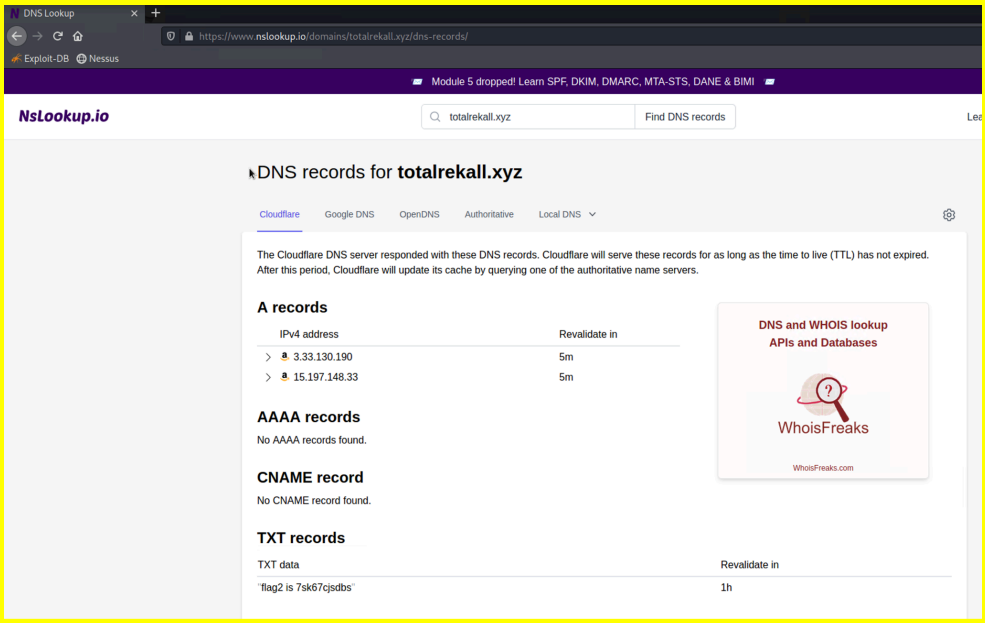
```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jlow@2u.com
Name Server: NS51.DOMAINCONTROL.COM
```

Queried **whois.godaddy.com** with "**totalrekall.xyz**"...

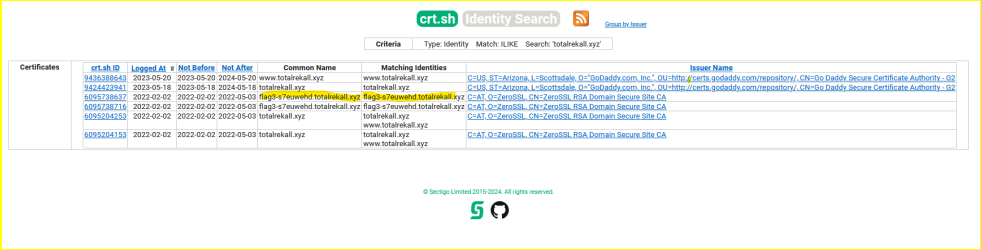
```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: h8s692hskasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jlow@2u.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-03-11T18:21:16Z <<<
```

Affected Hosts	Totalrekall.xyz

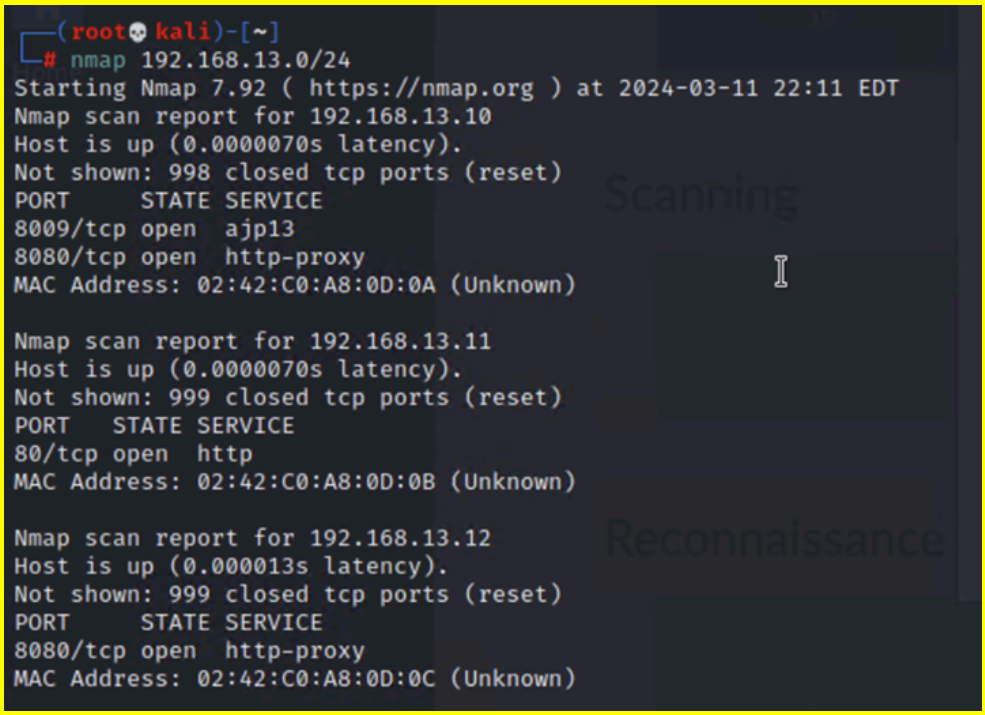
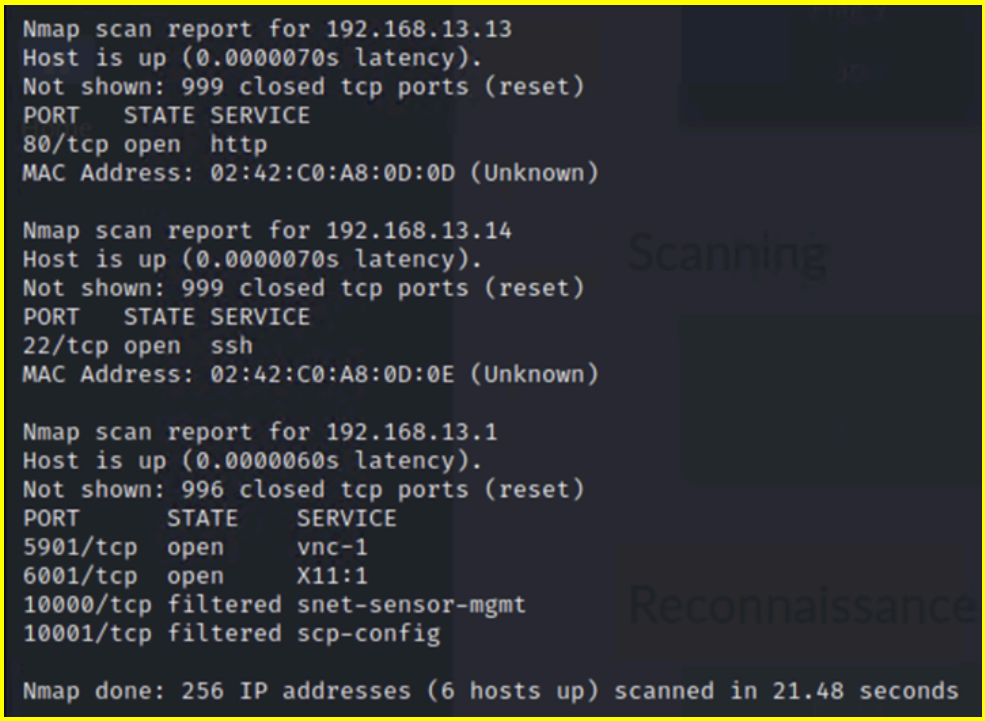
Remediation	Opt for domain registration privacy options that allow you to limit the disclosure of sensitive data.

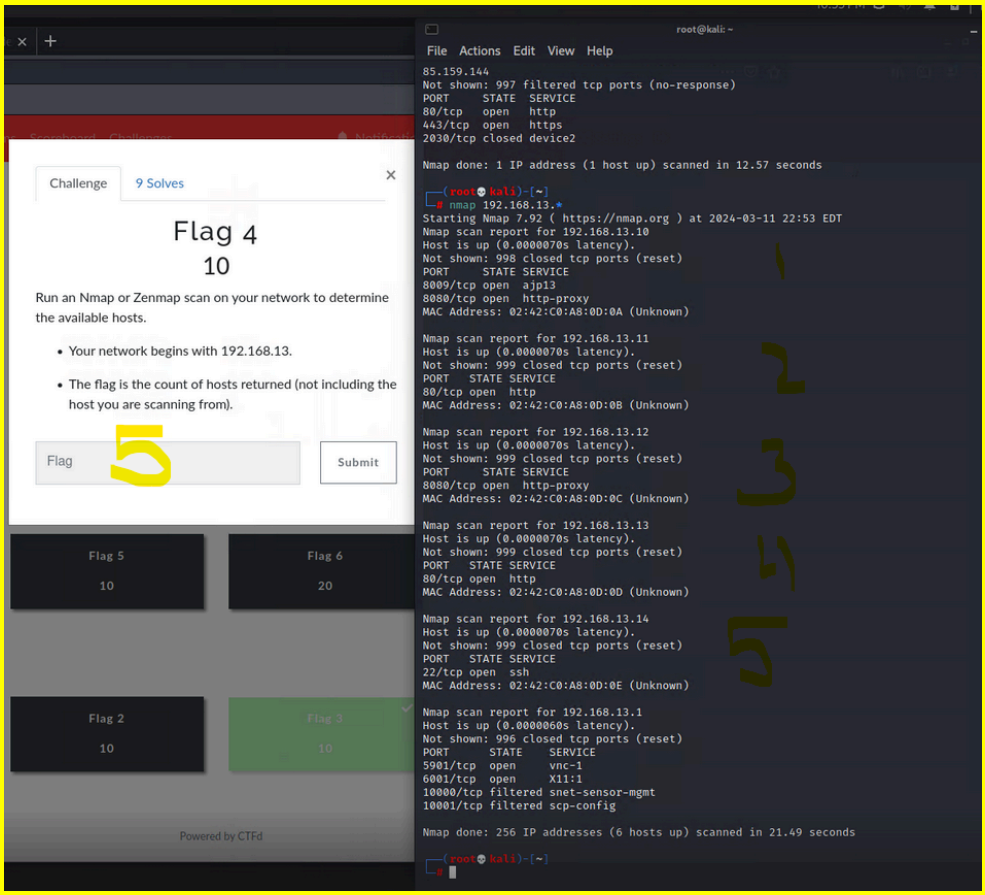
Vulnerability 2	Findings
Title	Flag 02 - SSL Research about totalrekall.xyz
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Informational
Description	Public facing IP for totalrekall.xyz found on nslookup.io
Images	
Affected Hosts	3.33.130.190
Remediation	Make DNS records private / implement proxies.

Vulnerability 3	Findings
Title	Flag 03 - Open Source Intelligence of SSL Certificates
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**

Description	Used crt.sh to look up certificates @ totalrekall.xyz
Images	
Affected Hosts	flag3-s7euwehd.totalrekall.xyz
Remediation	Restrict the publication of DNS records and maintain a minimum level of exposure

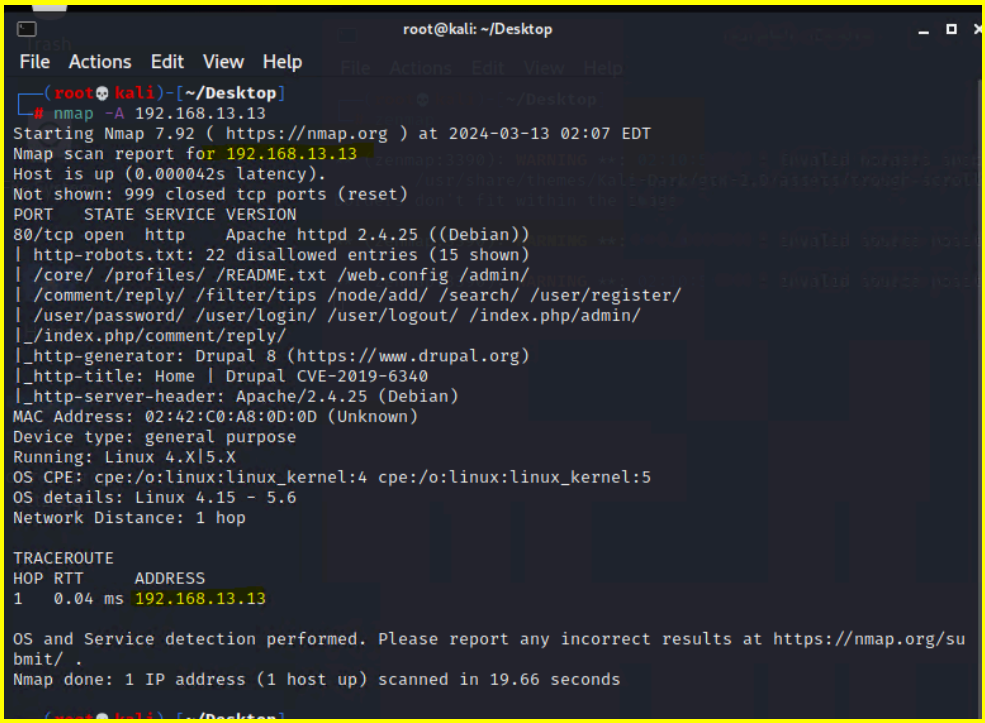
Vulnerability 4	Findings
Title	Flag 04 - Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Utilizing the Nmap scan, we detected five active hosts, enabling us to streamline our investigation and focus on testing and potentially exploiting these IP addresses.

Images	 



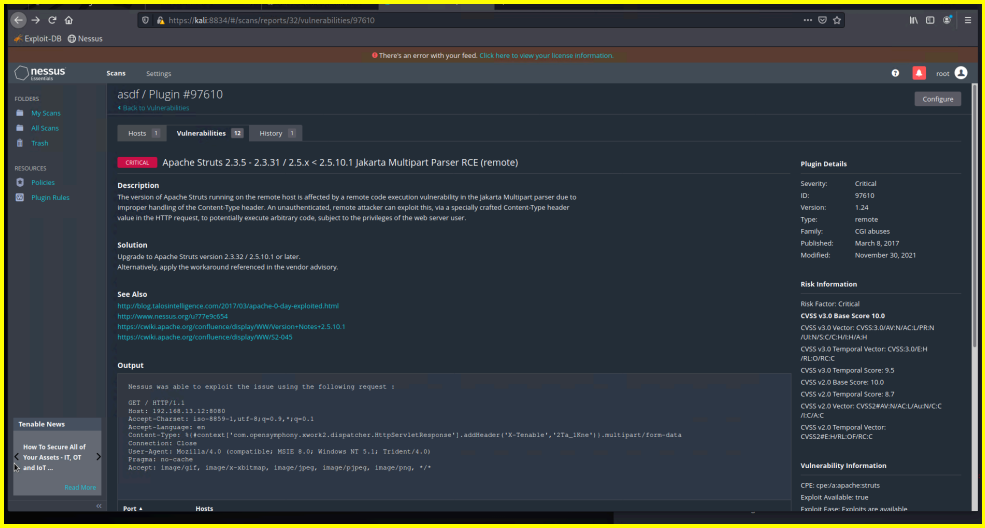
Affected Hosts	192.168.13.13
Remediation	Enhance firewall configurations or invest in a robust Intrusion Detection System (IDS) to bolster network security.

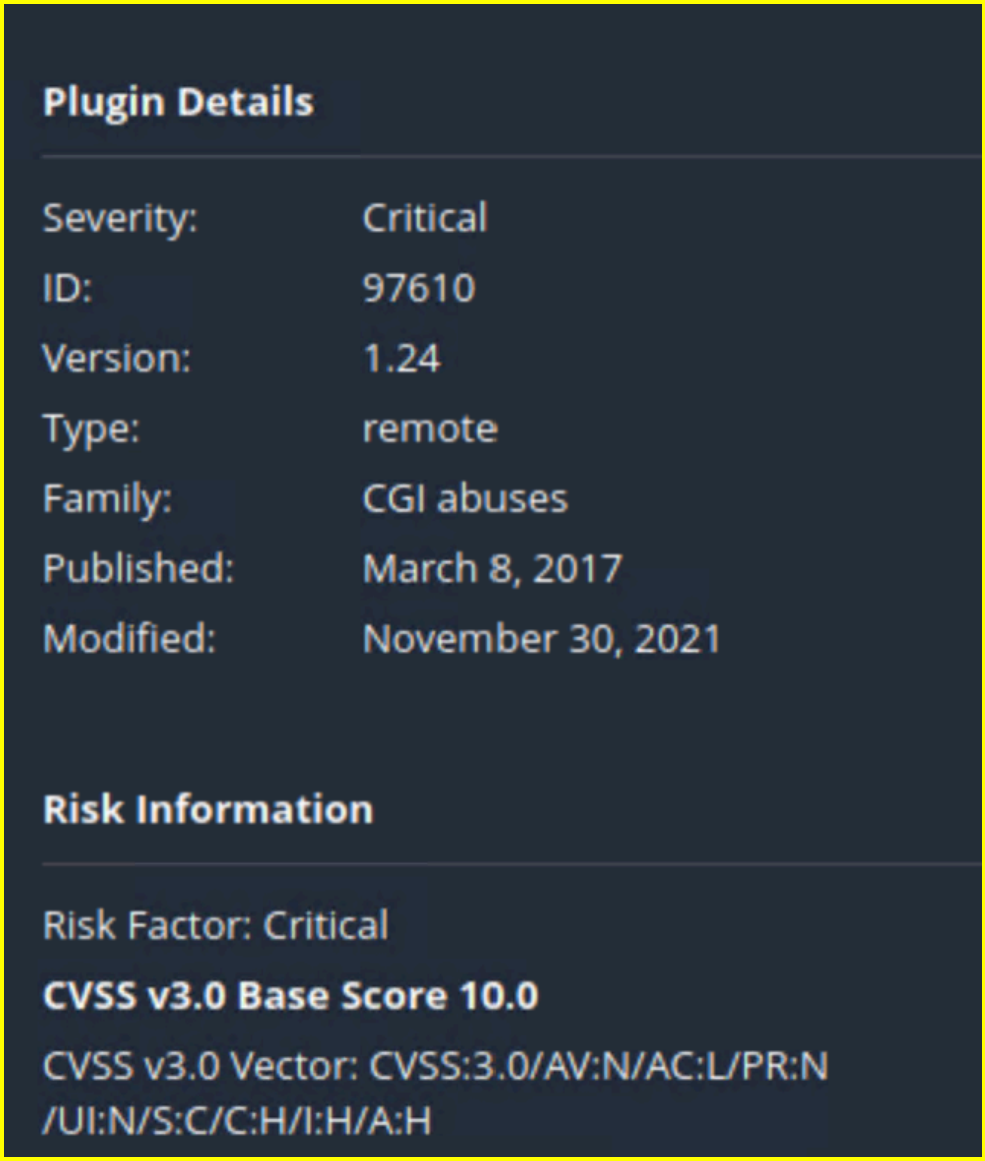
Vulnerability 5	Findings
Title	Flag 05 - Enumeration of open ports
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Low**
Description	IP Address from the NMAP scan

Images	
Affected Hosts	192.168.13.13
Remediation	Implement stricter firewall policies in addition to an IPS system if possible.

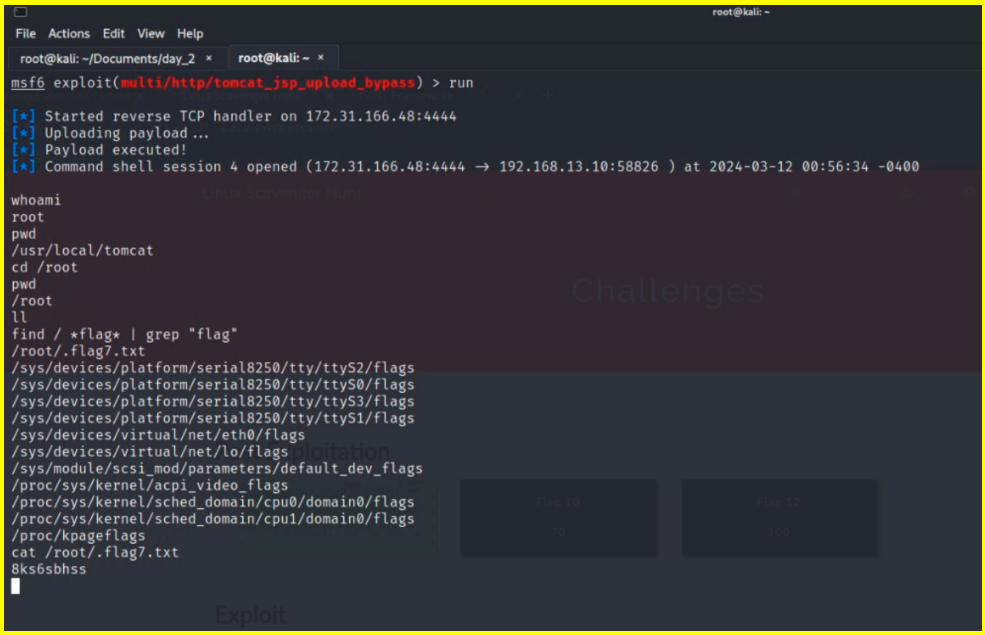
Vulnerability 6	Findings
Title	Flag 06 - Unpatched RCE vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	CVE-2017-97610: The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.

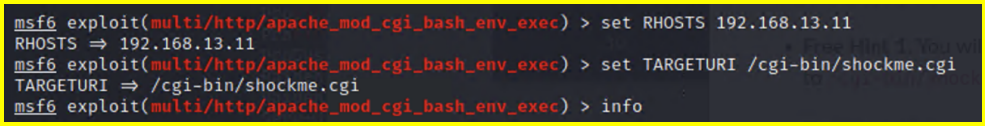
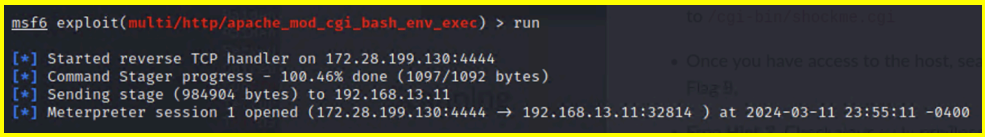
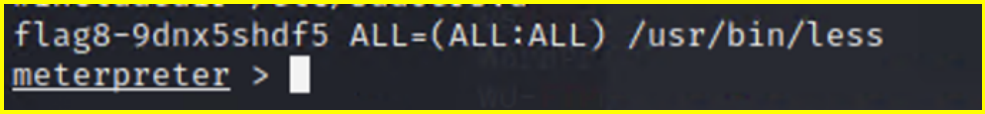
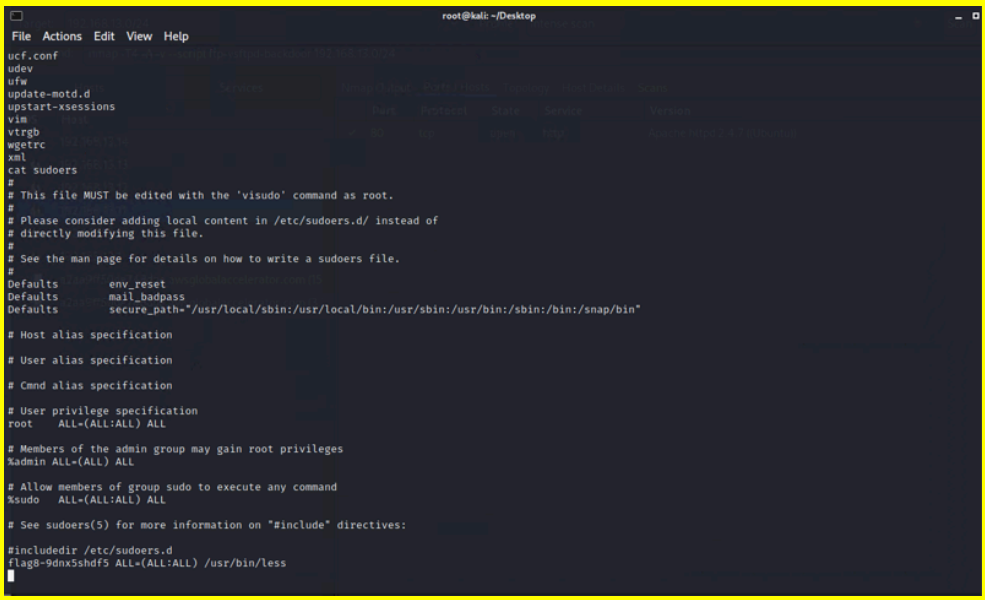
Images

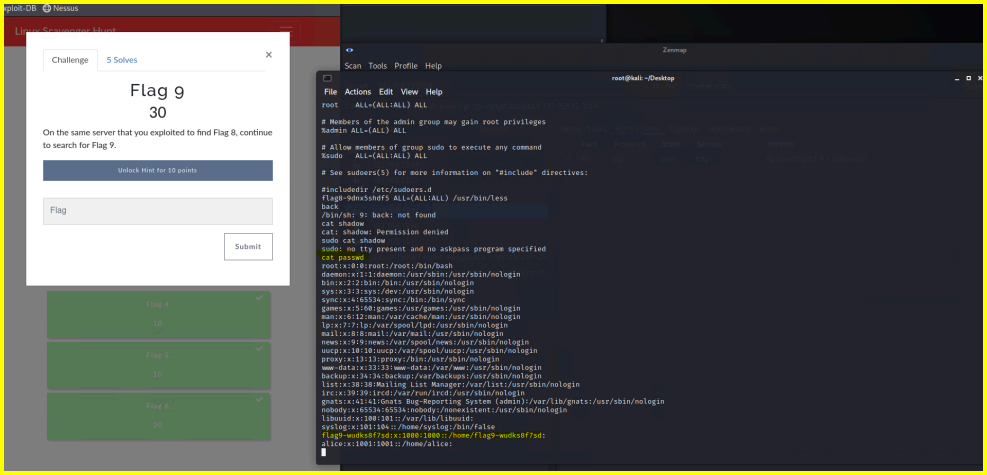
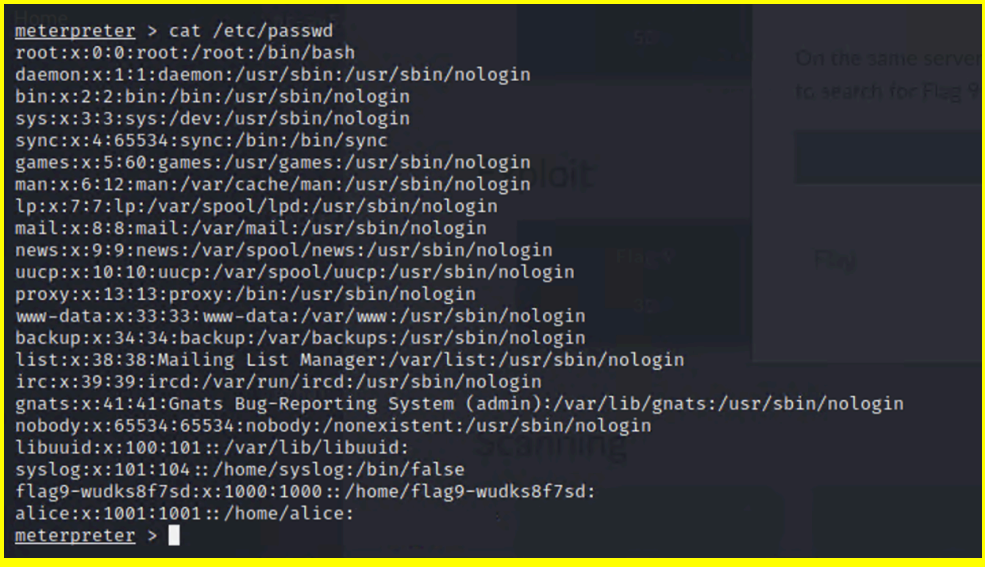


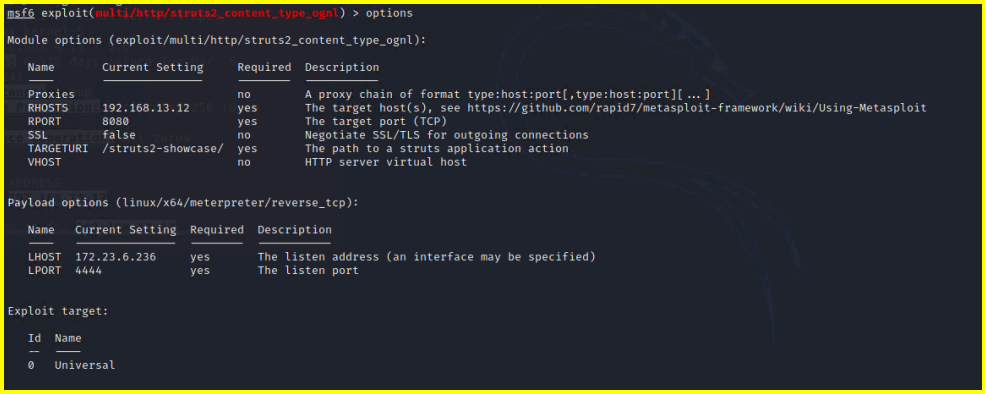
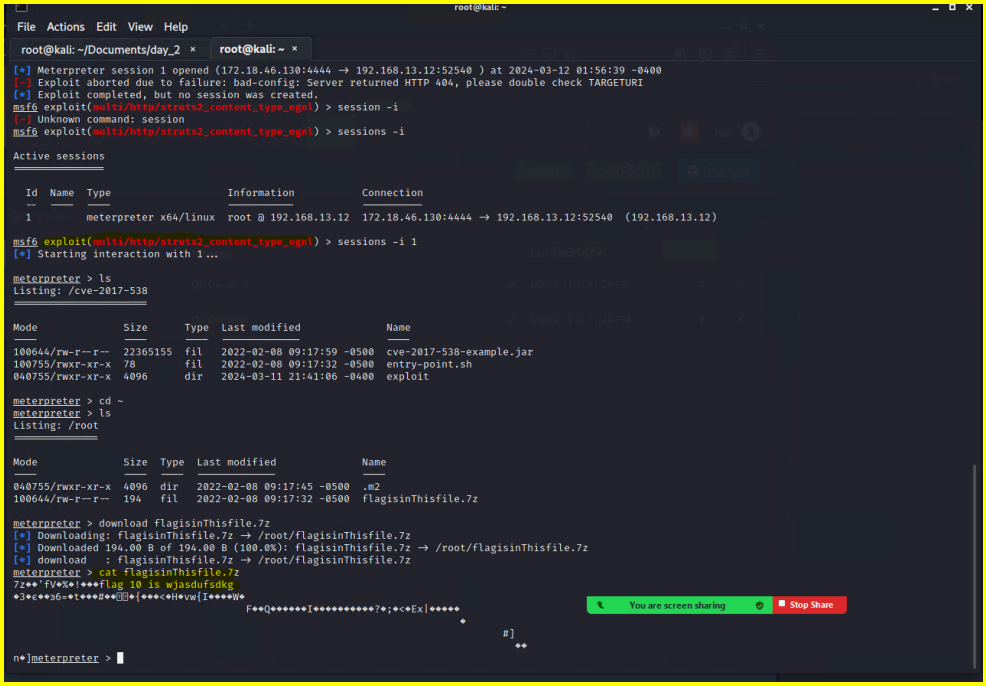


Affected Hosts	192.168.13.12
Remediation	Regularly update and patch all software. Monitor for new vulnerabilities and apply patches as soon as possible

Vulnerability 7	**Findings**
Title	Flag 07 - Unpatched RCE vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	CVE-2017-12617: When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.
Images	
Affected Hosts	192.168.13.10
Remediation	Patch systems to latest vendor versions

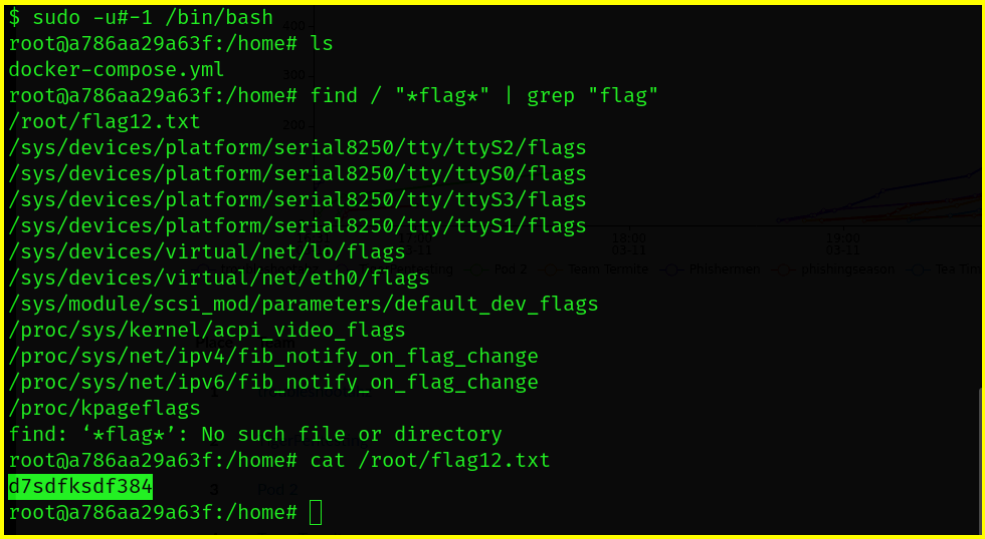
Vulnerability 8	Findings
Title	Flag 08 - Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	CVE-2014-6278: GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.
Images	   
Affected Hosts	192.168.13.11
Remediation	Update the firmware to the latest version according to developer

Vulnerability 9	Findings
Title	Flag 09 - Misconfigured privileges
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Using the Meterpreter session we opened onto the machine 192.168.13.11, we were able to navigate and dig through the system and also use our access to cat open the /etc/passwd file. This type of file access can allow us to view user credentials and privileges.
Images	 
Affected Hosts	192.168.13.11
Remediation	Auditing and updating permissions for who can access sensitive files like /etc/passwd and /etc/shadow so that only the highest privileged users can access these files, which will help mitigate attackers from stealing/modifying this information.

Vulnerability 10	Findings
Title	Flag 10 - Remote code execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	CVE-2017-5638: The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.
Images	 
Affected Hosts	192.168.13.12
Remediation	Requires proper configuration of the firewall and updating Apache Struts.

Vulnerability 11	Findings
Title	Flag 11 - Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	CVE-2019-6340: Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x before 8.5.11 and Drupal 8.6.x before 8.6.10. This can lead to arbitrary PHP code execution in some cases. A site is only affected by this if one of the following conditions is met: The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests, or the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7. (Note: The Drupal 7 Services module itself does not require an update at this time, but apply other updates associated with these services that are in use.)
Images	
Affected Hosts	192.168.13.13
Remediation	Regularly update Drupal and restrict the permissions of the www-data user to only what is necessary for operation

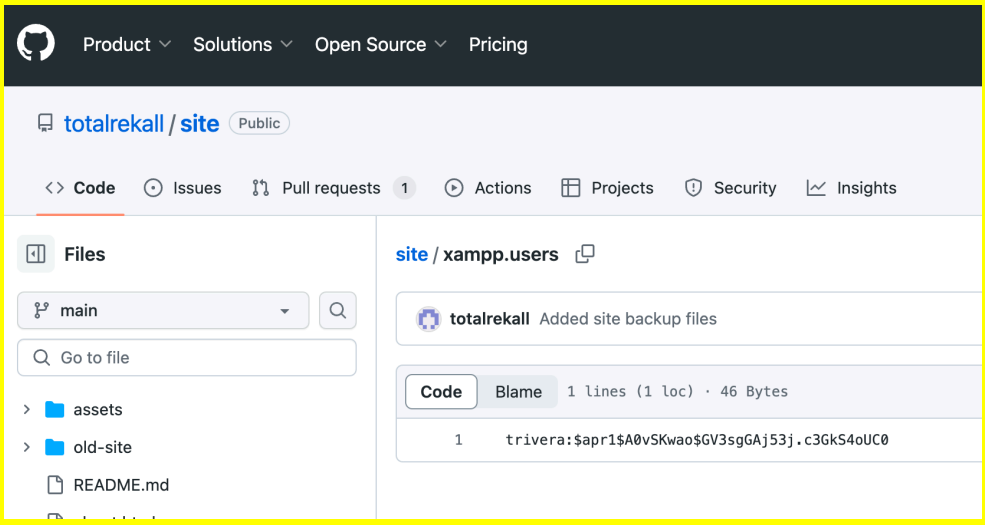
Vulnerability 12	Findings
Title	Flag 12 - Weak password / privilege escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Upon discovering an admin user's plaintext username, we initiated a brute-force attack by attempting "Alice" as the password. This successful login granted SSH access to the machine, then leveraging CVE-2019-14287 we were able to gain root access

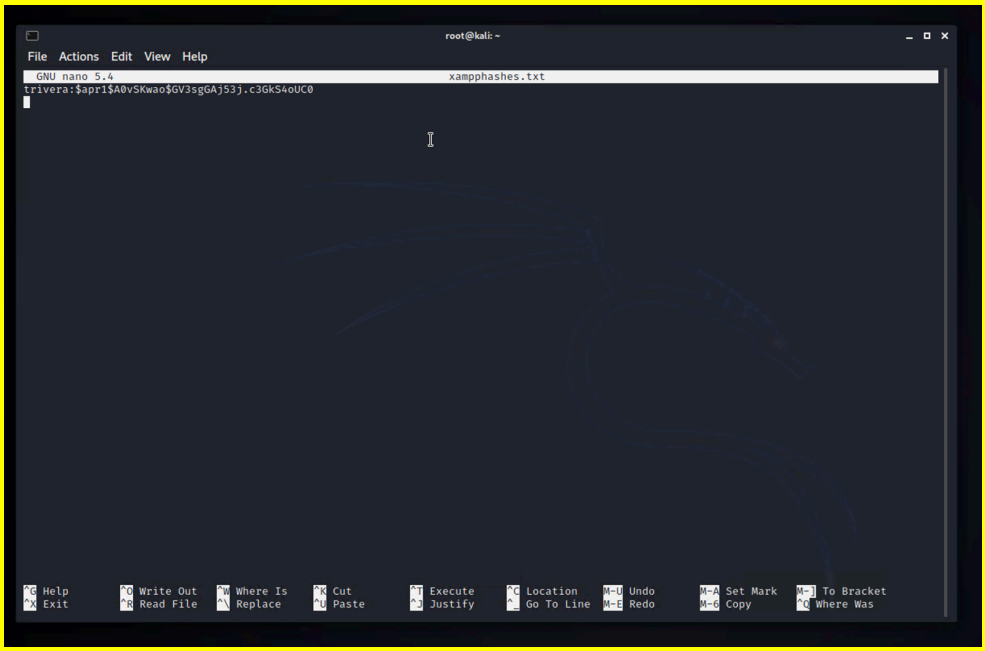
Images	
Affected Hosts	192.168.13.14
Remediation	Complex passwords should be mandated to mitigate some of the threat from this type of attack. MFA would have prevented this attack by requiring an additional authentication factor beyond just the weak password, such as a code sent to the user's mobile device. Even if the attacker guessed the password, they would still be unable to access the system without the secondary authentication method. Patch the systems to sudo 1.2.8 and above.

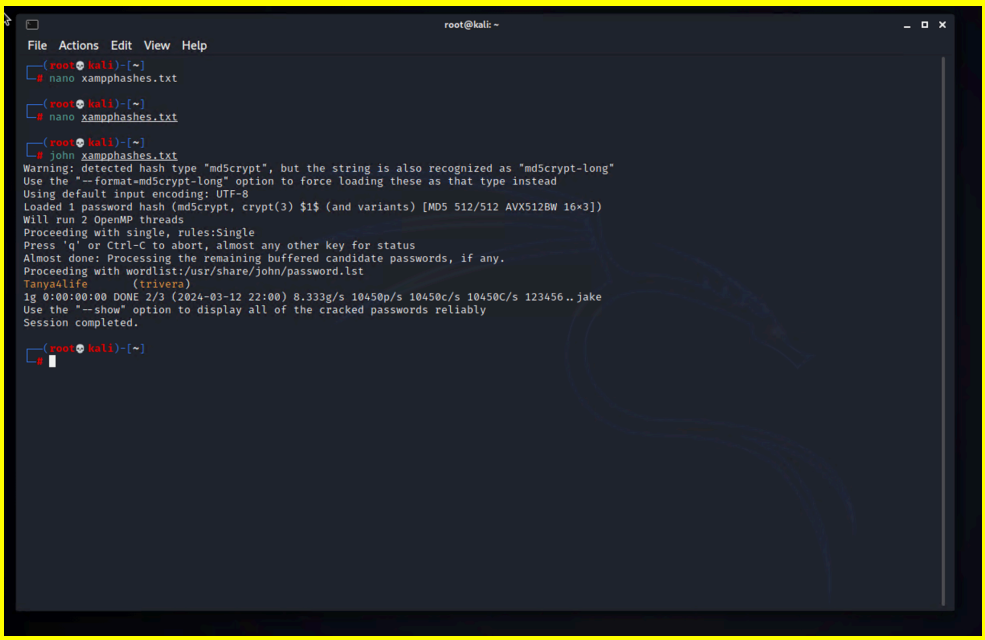
Day 3 Vulnerability Findings

Vulnerability 1	Findings
Title	Flag 01 - OSINT enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS / Web App
Risk Rating	High
Description	Exposed administrator password hash viewable on a public Github repo

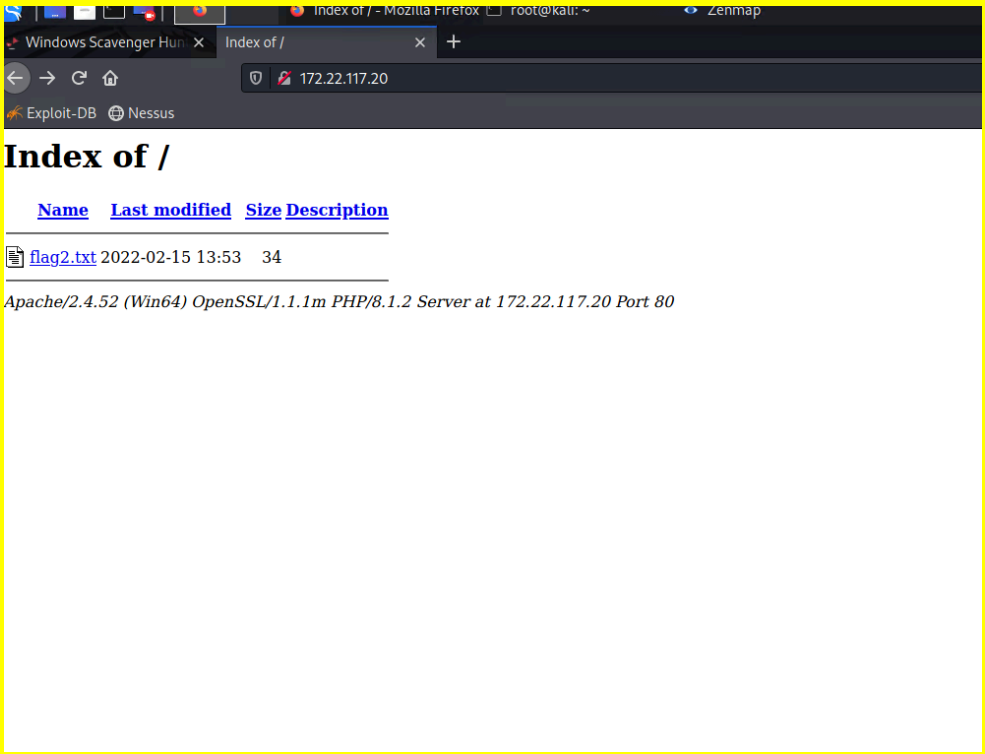
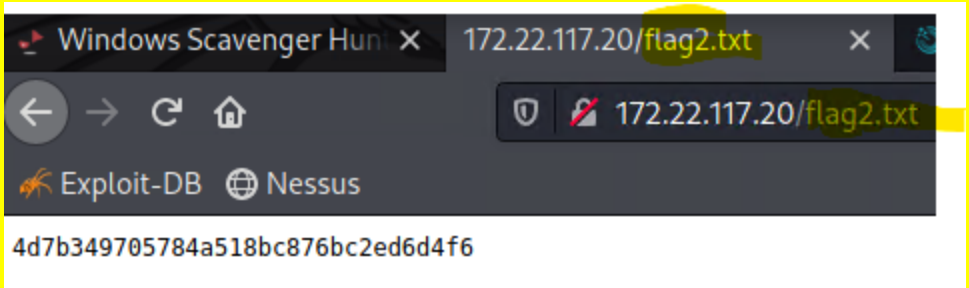
Images

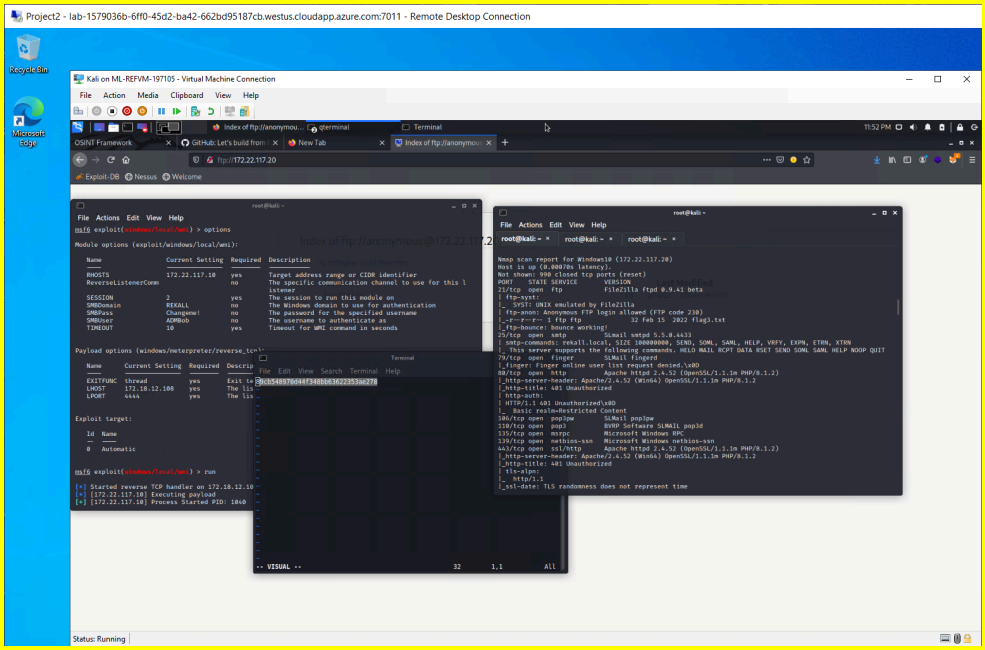
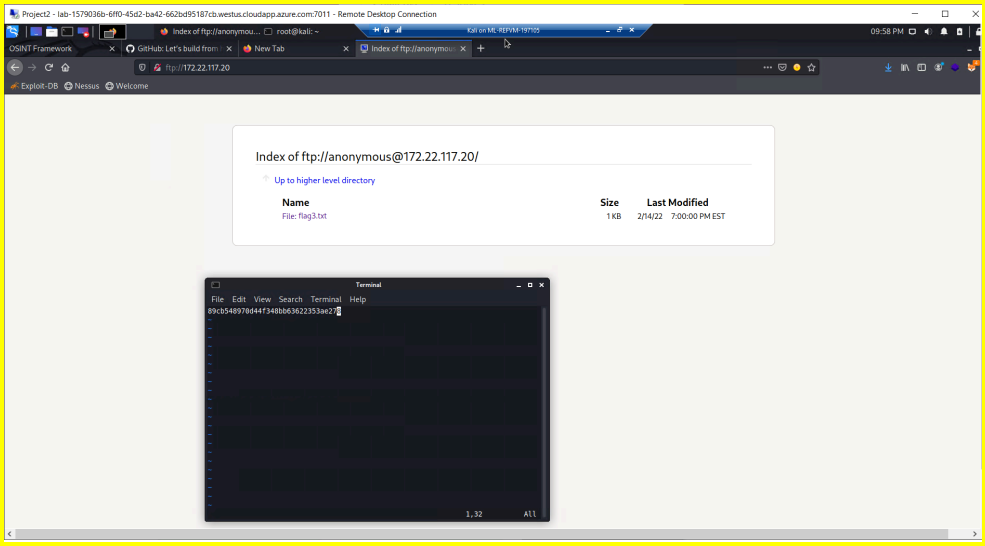




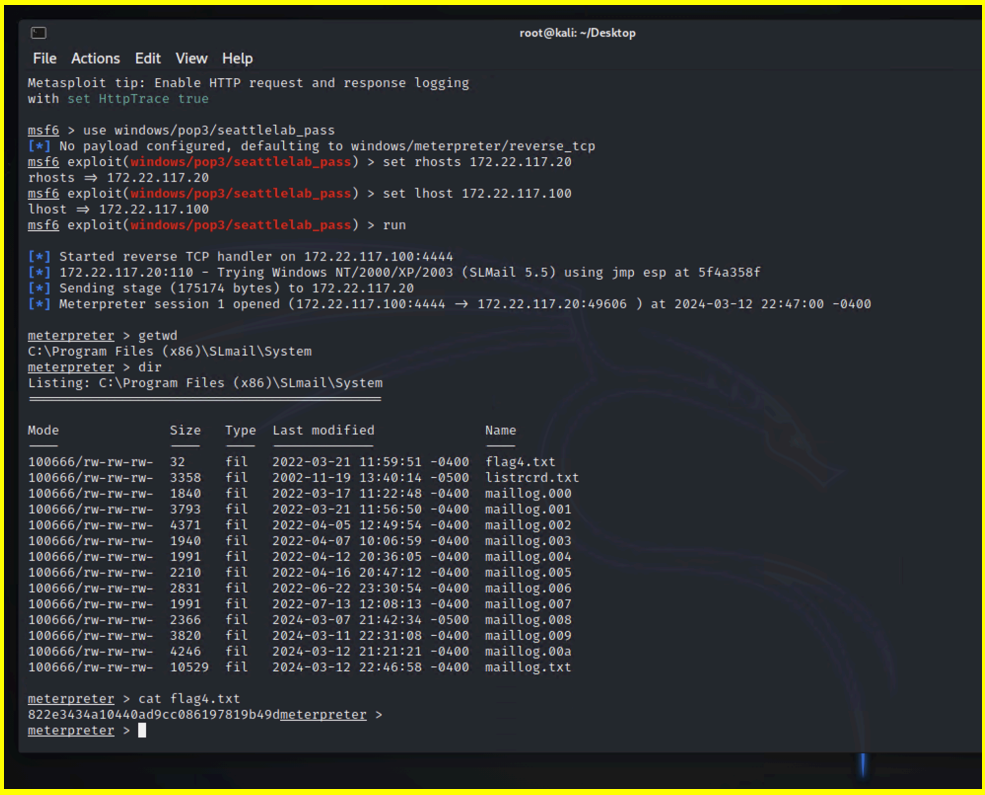


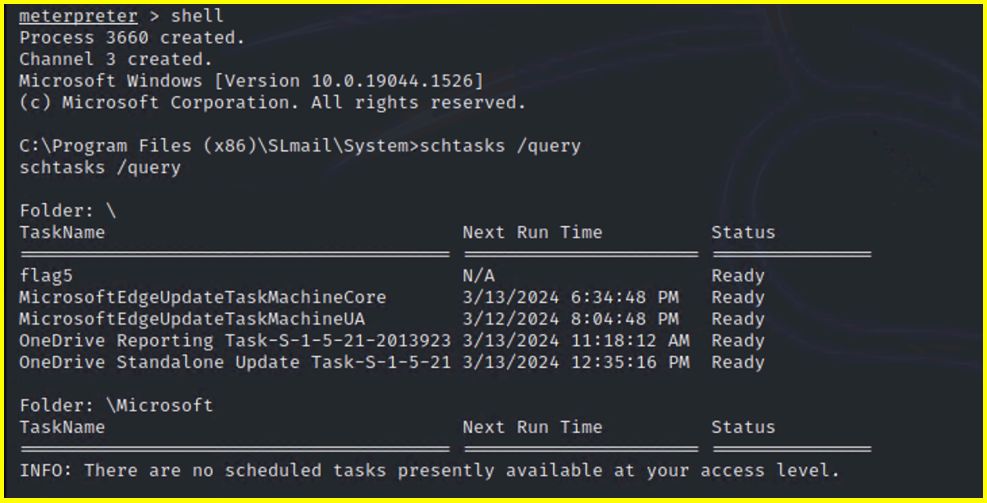
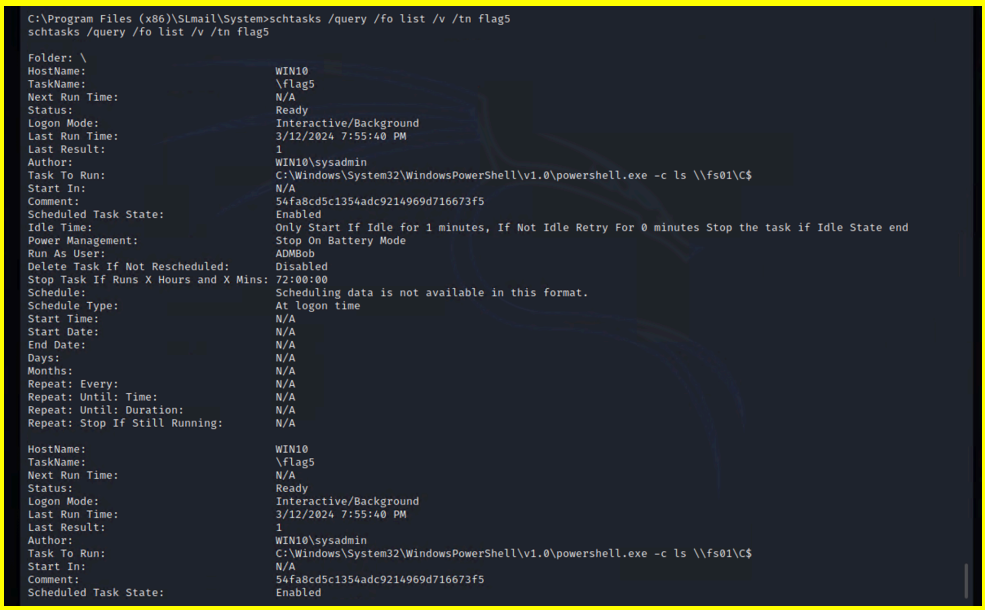
Affected Hosts	N/A
Remediation	Make the Github repo private, change the current password and enforce use of stronger passwords.

Vulnerability 2	**Findings**
Title	Flag 02 - HTTP enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Port 80 left open on the 172.22.117.20 machine allowed access to sensitive information
Images	 
Affected Hosts	172.22.117.20
Remediation	Firewall, reconfiguration of HTTP on 172.22.117.20 machine

Vulnerability 3	Findings
Title	Flag 03 - Anonymous FTP exploitation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using an aggressive NMAP scan, we were able to find out that machine 172.22.117.20 (WIN 10 Machine) was able to be accessed by anonymous FTP. We then opened a browser and entered the link ftp://anonymous:anonymous@172.22.117.20 which then gave us access to a file on the system.
Images	 

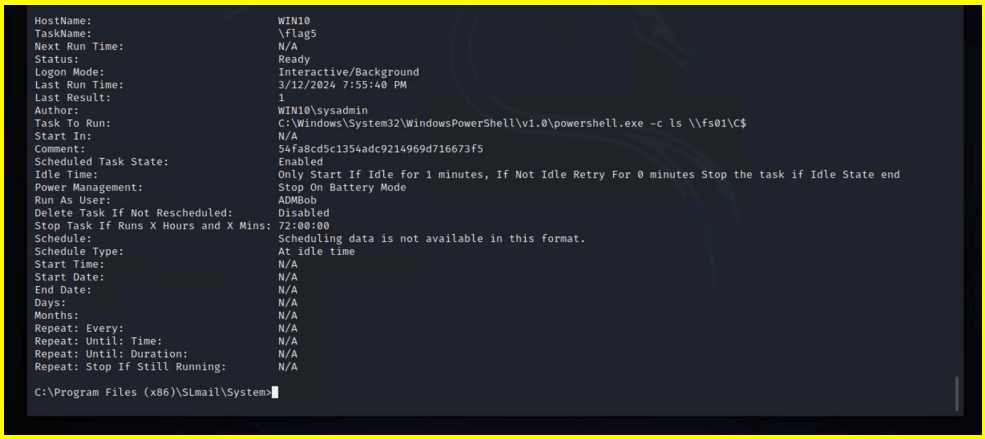
Affected Hosts	172.22.117.20
Remediation	Best practice would be to disable anonymous FTP access to the server so that unauthorized users are kept from gaining access. For long-term mitigation, using secure FTP protocols for these files and regularly monitoring the FTP logs for suspicious activity would help to further protect from attackers.

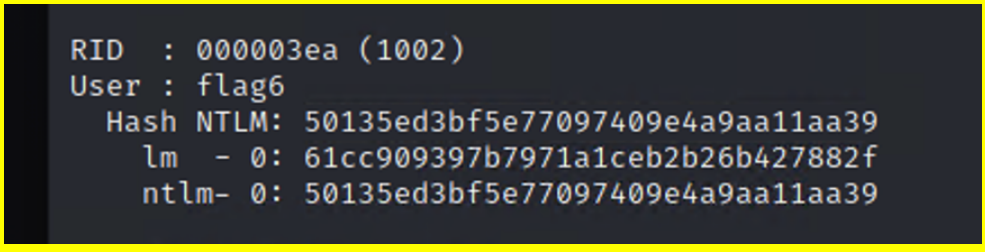
Vulnerability 4	Findings
Title	Flag 04 - Remote Buffer Overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Upon discovering a machine using the “slmail” service, we successfully leveraged CVE-2003-0264 to execute a remote buffer overflow and establish a shell. After this we were able to navigate through directories, extracting sensitive data from the system.
Images	
Affected Hosts	172.22.117.20
Remediation	Configure firewalls to restrict inbound and outbound traffic, minimizing the attack surface accessible to attackers using Metasploit, update services to vendor recommended versions.

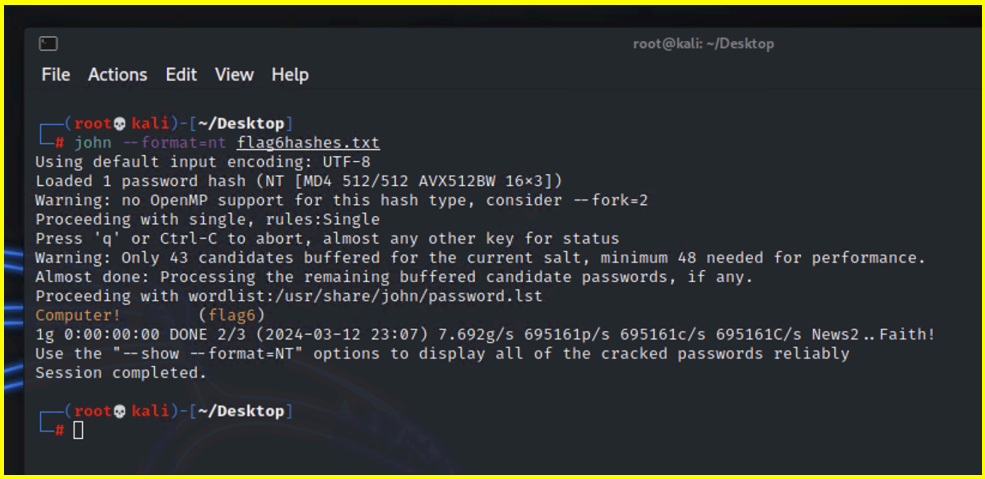
Vulnerability 5	Findings
Title	Flag 05 - Manipulation of scheduled tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Improper permissions on scheduled tasks and inspecting tasks revealed the flag
Images	 

```
meterpreter > shell
Process 3660 created.
Channel 3 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>schtasks /query
schtasks /query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
flag5                                    N/A                    Ready
MicrosoftEdgeUpdateTaskMachineCore       3/13/2024 6:34:48 PM   Ready
MicrosoftEdgeUpdateTaskMachineUA         3/12/2024 8:04:48 PM   Ready
OneDrive Reporting Task-S-1-5-21-2013923 3/13/2024 11:18:12 AM  Ready
OneDrive Standalone Update Task-S-1-5-21 3/13/2024 12:35:16 PM  Ready

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.
```

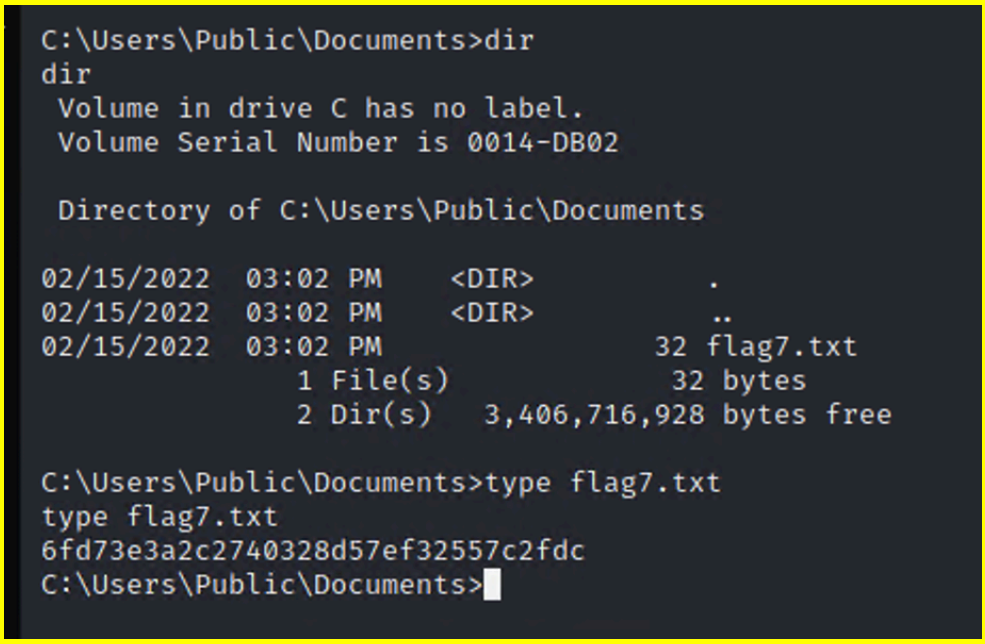
```
C:\Program Files (x86)\SLmail\System>schtasks /query /fo list /v /tn flag5
schtasks /query /fo list /v /tn flag5

Folder: \
HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        3/12/2024 7:55:40 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        3/12/2024 7:55:40 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
```

	
Affected Hosts	172.22.117.20
Remediation	Apply Principle of Least Privilege to task scheduling

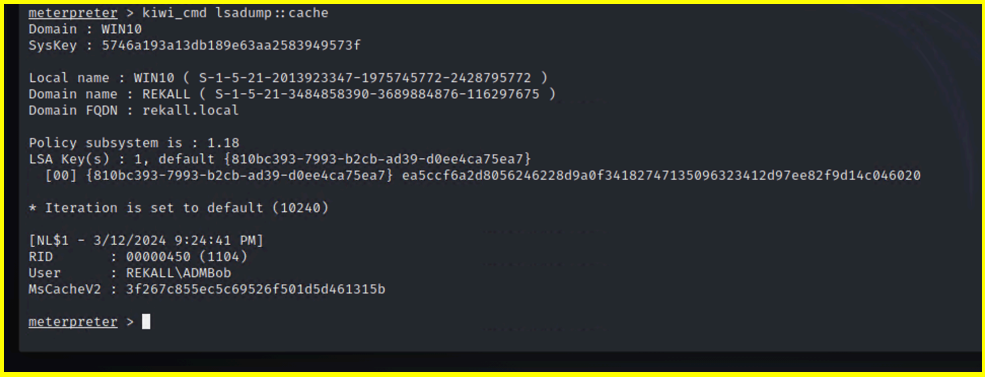
Vulnerability 6	Findings
Title	Flag 06 - LSADump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	After creating a Meterpreter session with the SLMail exploit on the Windows 10 machine, we loaded the Kiwi module so that the session would run Kiwi commands. From there, we ran kiwi_cmd lsadump::sam to dump the credentials, including usernames and password hashes, to the terminal. Flag 6 was a user named “flag6”, we used John the Ripper to crack the password hash and reveal the plain text password.
Images	



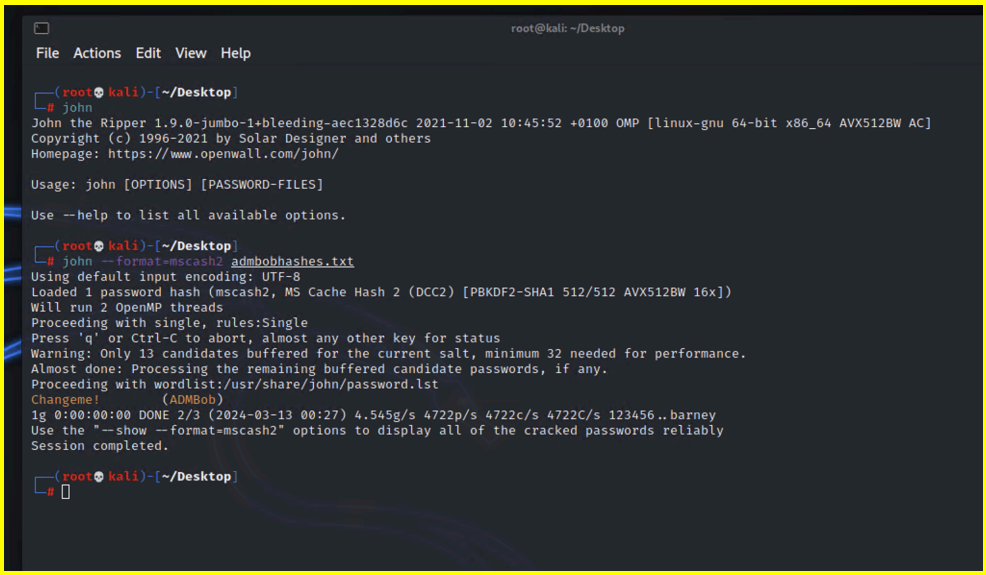
Affected Hosts	172.22.117.20
Remediation	Properly update and patch the system so that it is no longer vulnerable to simple LM and NTLMv1 protocols. Updated OS patches also contain protections for LSADump attacks and keep the sensitive data less accessible.

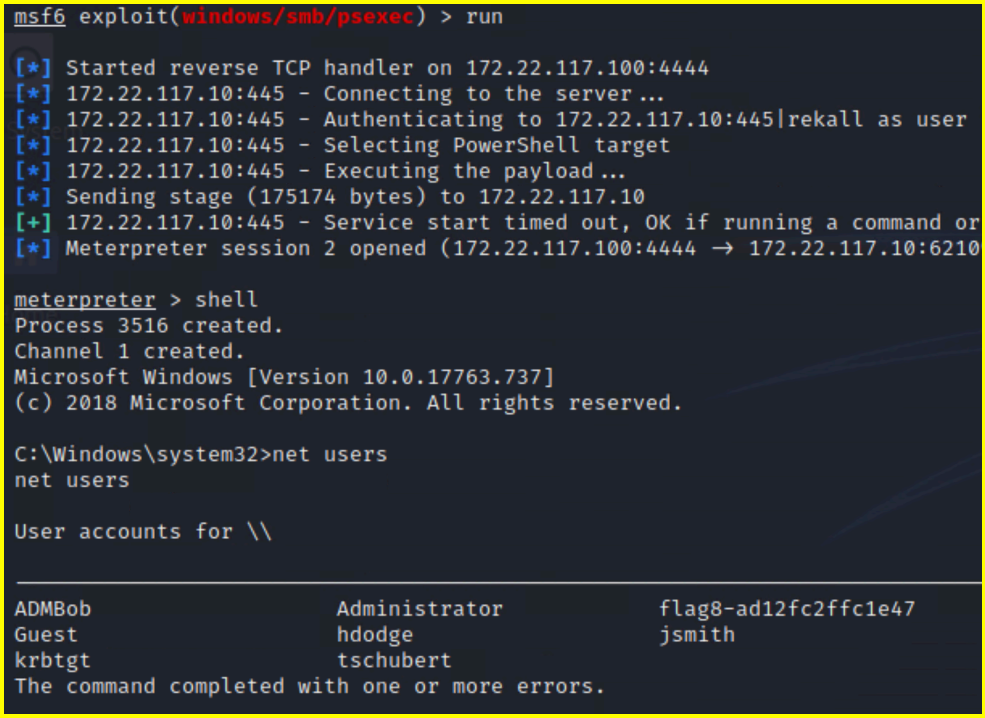
Vulnerability 7	Findings
Title	Flag 07 - File enumeration / sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Sensitive data exposure and located by searching the file system of the compromised machine
Images	

Affected Hosts	172.22.117.20 at C:\Users\Public\Documents
Remediation	Regularly audit file systems for sensitive information and adhere to least-privilege access principles

Vulnerability 8	**Findings**
Title	Flag 08 - Lateral Movement into WINDC machine
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using cracked credentials from the Windows 10 machine, we were then able to laterally move to the WINDC machine using Metasploit. First we set up a new session on 172.22.117.20 using the Metasploit (exploit/windows/smb/psexec), as well as using the credentials for user ADMBob. After opening that session, we backgrounded the session, then set up a payload using exploit/windows/local/wmi targeting the 172.22.117.10 machine using the same credentials. When we ran the exploit, this opened up a new Meterpreter session on the Domain Controller system.
Images	

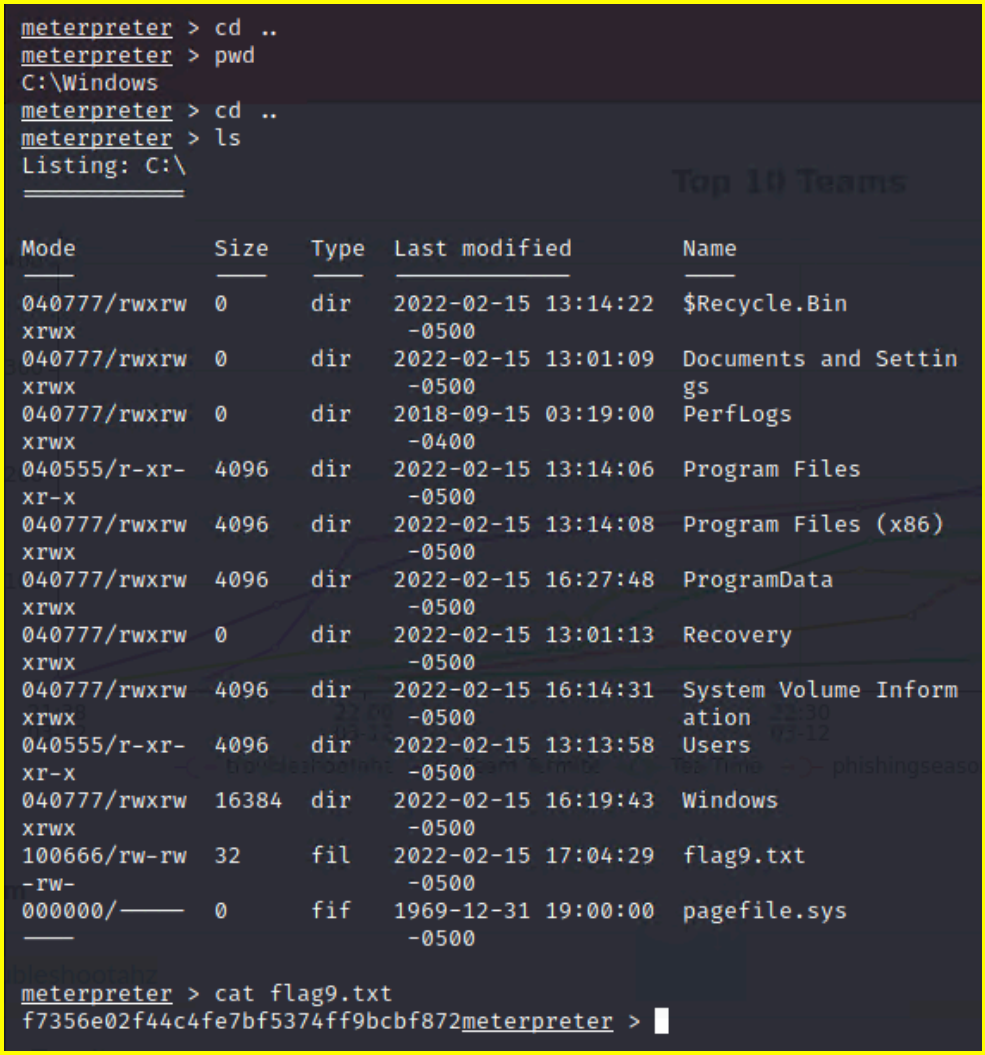
```
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
  [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f3418274713509632341 2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 3/12/2024 9:24:41 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```



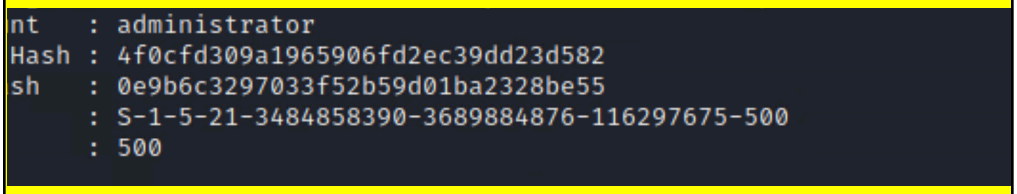


Affected Hosts	172.22.117.20,172.22.117.10
Remediation	Monitoring tools and Intrusion Prevention Systems can help mitigate these types of attacks. These can alert security teams to unauthorized access attempts while they monitor for any signs of lateral movement.

Vulnerability 9	Findings
Title	Flag 09 - File Enumeration / sensitive data exposure

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	The flag was found in a file named flag9.txt in root directory
Images	
Affected Hosts	172.22.117.10
Remediation	Implement proper access control and protect sensitive files

Vulnerability 10	Findings
Title	Flag 10 - Compromised Admin Password
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**

Description	The NTLM password hash of the Administrator account was revealed by DCSyncing the user with Kiwi
Images	
Affected Hosts	DCSyncing the Admin user revealed the NTLM hash using Kiwi
Remediation	Ensure password hashes are properly protected against tools such as Kiwi and implement more robust authentication methods