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

Contact Information

Company Name	**Mt. Zion CyberSecurity Group**
Contact Name	AbibTumbapo Subba
Contact Title	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

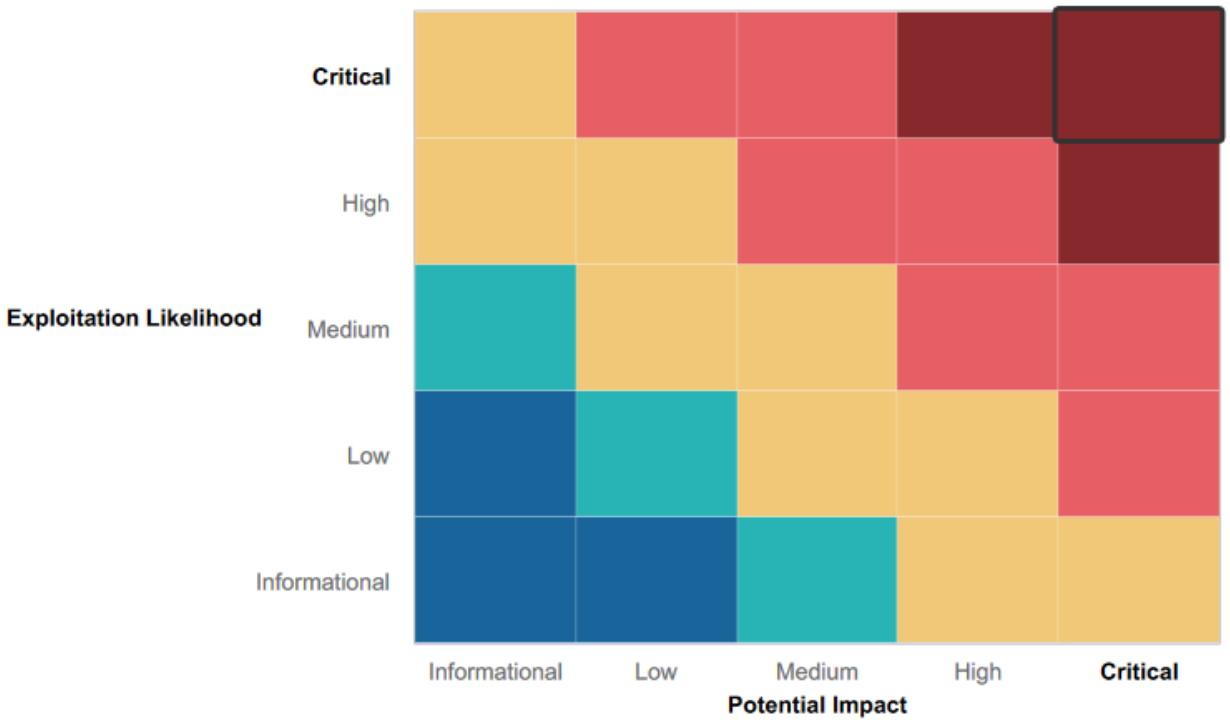
Grading Methodology

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 avaibility.
- 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 : *87fsdkf6djf)*	Critical
XSS Reflected (Flag: *f76sdfkg6sjf*)	Medium
XSS Stored (Flag : *sd7fk1nctx*)	Critical
Certificate Search via crt.sh (Flag : *s7euwehd*)	Medium
Public Directory Search (Flag : *96fd73e3a2c2740328d57efe2557c2fdc*)	Medium
Windows 10 Machine Task Scheduler (Flag: *54fa8cd5c1354adc9214969d716673f5*)	Medium
Sensitive Data Exposure- Robot.txt used to block certain urls (Flag :dkkdudfkdy23)	Low
SQL Injection (Flag : *bcs92sjsk233*)	Critical
SLMail Exploit port - 110 (Flag : *822e3434a10440ad9cc086197819b49d*)	Critical
User's Cracked Password using john hash.txt (Flag : *Tanya4Life*)	Critical
Shellshock on Web Server (Port - 80) (Flag : *9dnx5shdf5*)	Critical
Open Source Exposed Data (Flag : *h8s692hskasd*)	High
Local File Inclusion (Flag : *mmssdi73g*)	Critical
Command Injection (Flag : *ksdnd99kas*)	Critical
Nessus Scan Result (Flag : *97610*)	Critical
Privilege Escalation (Flag : *d7sdfk384*)	Critical
FTP Enumeration port - 21 (Flag : *89*cb548970d44f348bb63622353ae278)	Critical

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

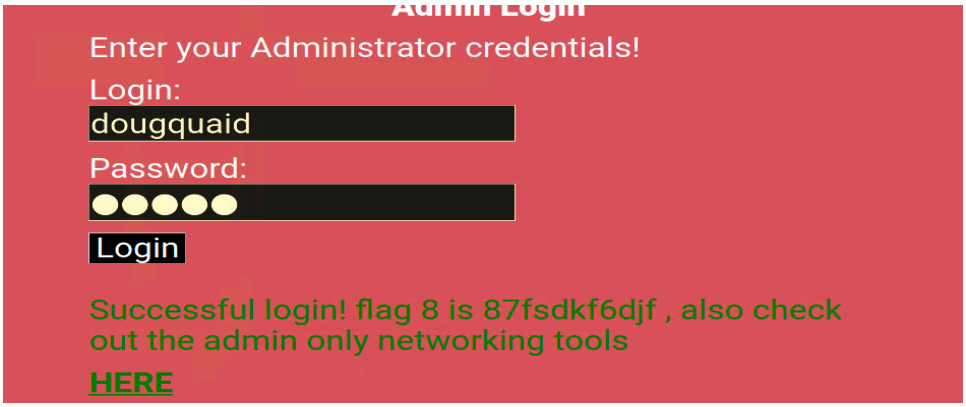
Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 110

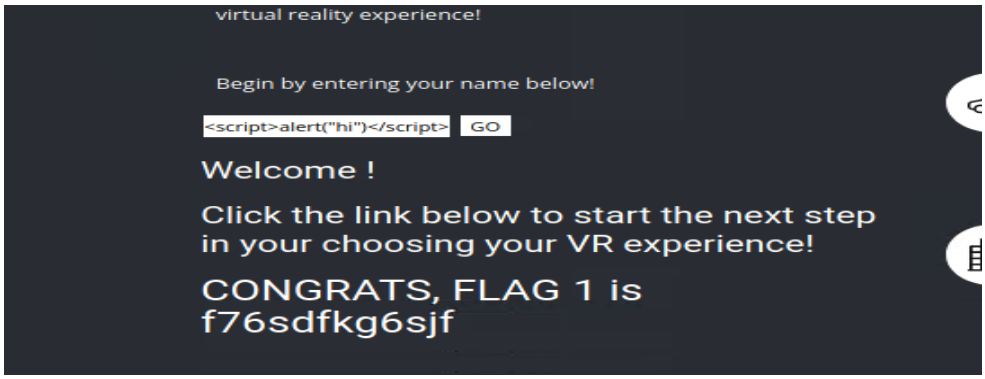
Exploitation Risk	Total
Critical	11
High	1
Medium	4
Low	1

Vulnerability Findings

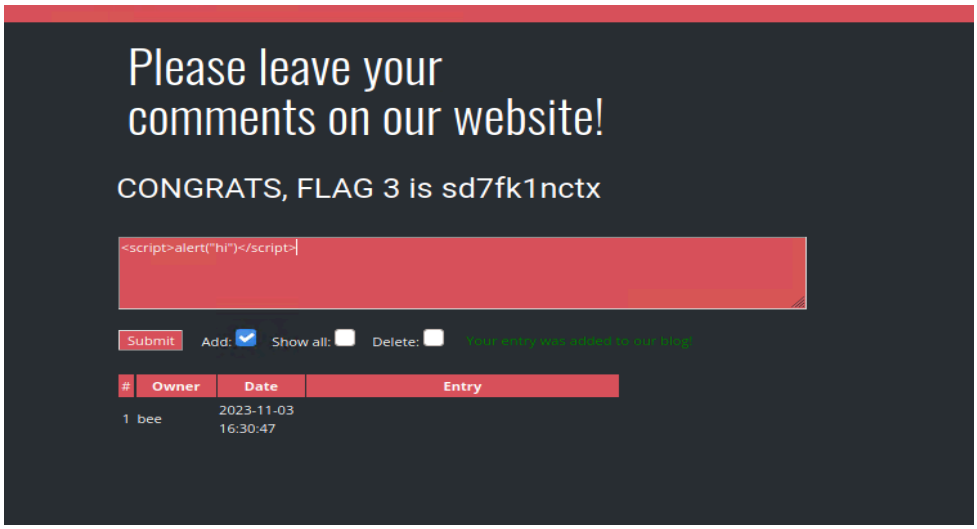
Vulnerability 1	Findings
Title	Sensitive Data Exposure Available in Admin plaintext on HTML
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	The username and password are in the HTML source code, discovered plain and simple /login.php (second field) information for an administrator.
Images	 

```
}
</style>

    <form action="/Login.php" method="POST">

        <p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />
        <input type="text" id="login" name="login" size="20" /></p>

        <p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />
        <input type="password" id="password" name="password" size="20" /></p>

        <button type="submit" name="form" value="submit" background-color="black">Login</button>

    </form>

    </br >

</div>
```

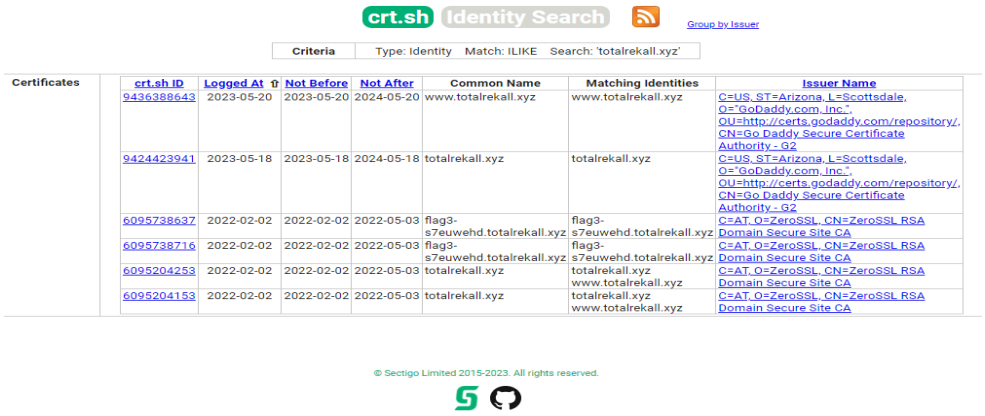
	
Affected Hosts	Web App
Remediation	Access the HTML code and delete these login details to resolve the issue.

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	
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	
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.

Images	
Affected Hosts	3.33.130.190 &15.197.148.33
Remediation	Safeguard data against exposure through the crt.sh website.

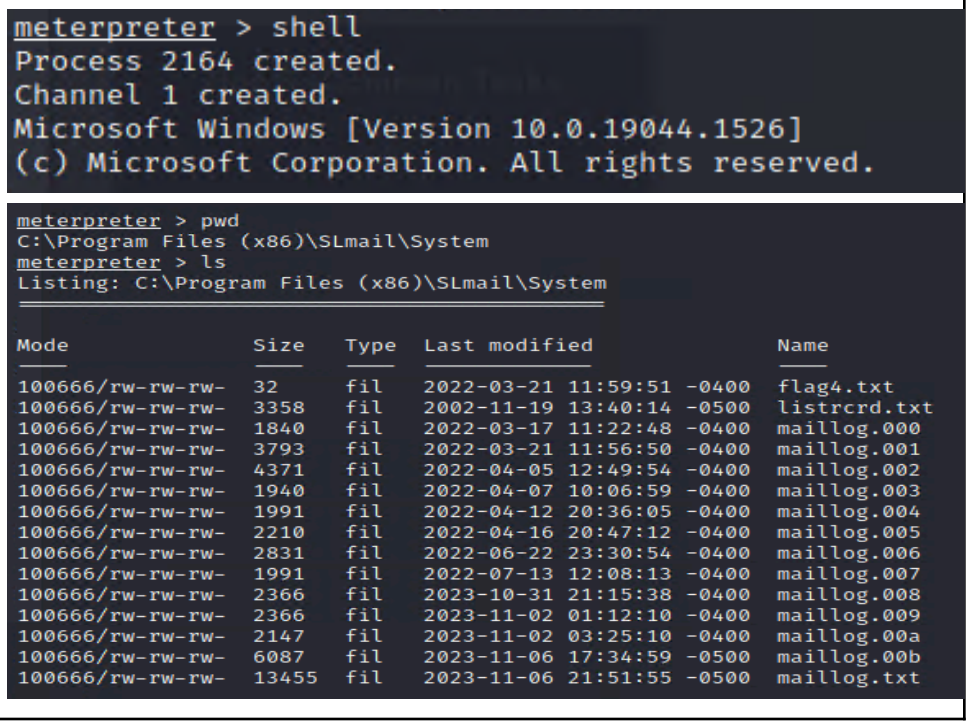
crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

Certificates

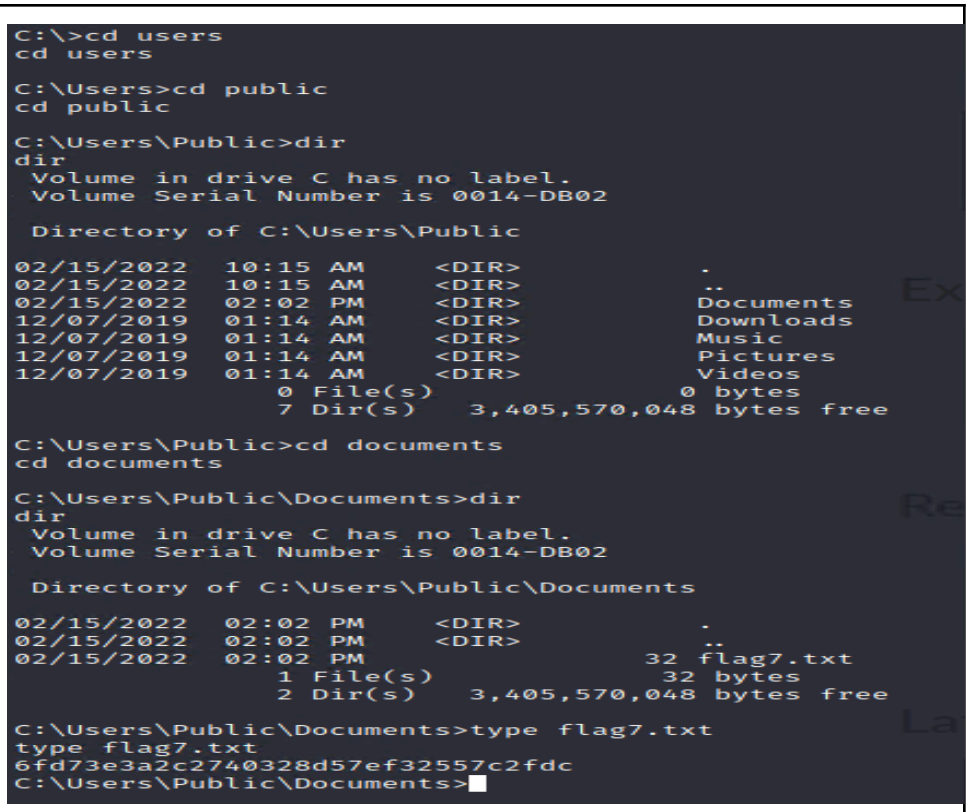
crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2023. All rights reserved.

Vulnerability 5	Findings
Title	Public Directory Search
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	Navigating to the Users\Public\Documents>directory, used the **'ls'** command in Meterpreter to display files.
Images	

```
meterpreter > shell
Process 2164 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.
```

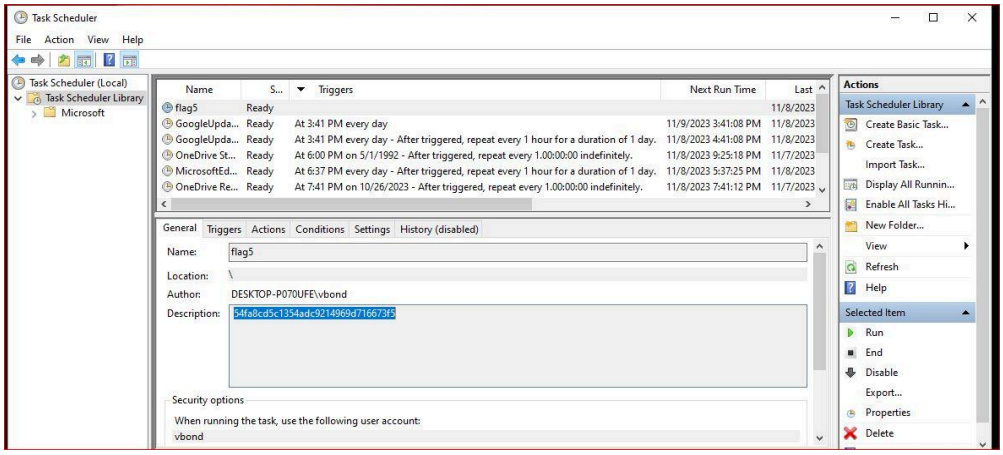
```
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

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   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
```

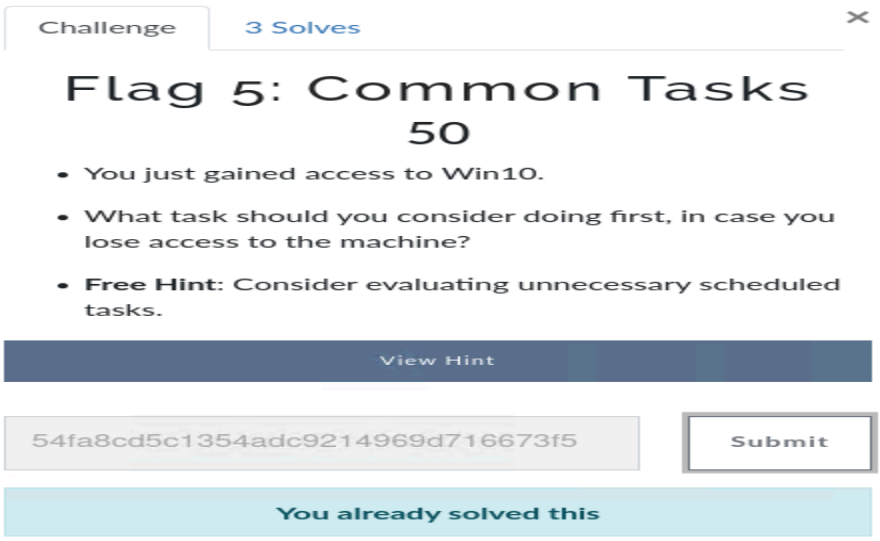
	
Affected Hosts	172.22.117.20
Remediation	Move sensitive files to more secure areas and/or restrict unauthorized access.

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	

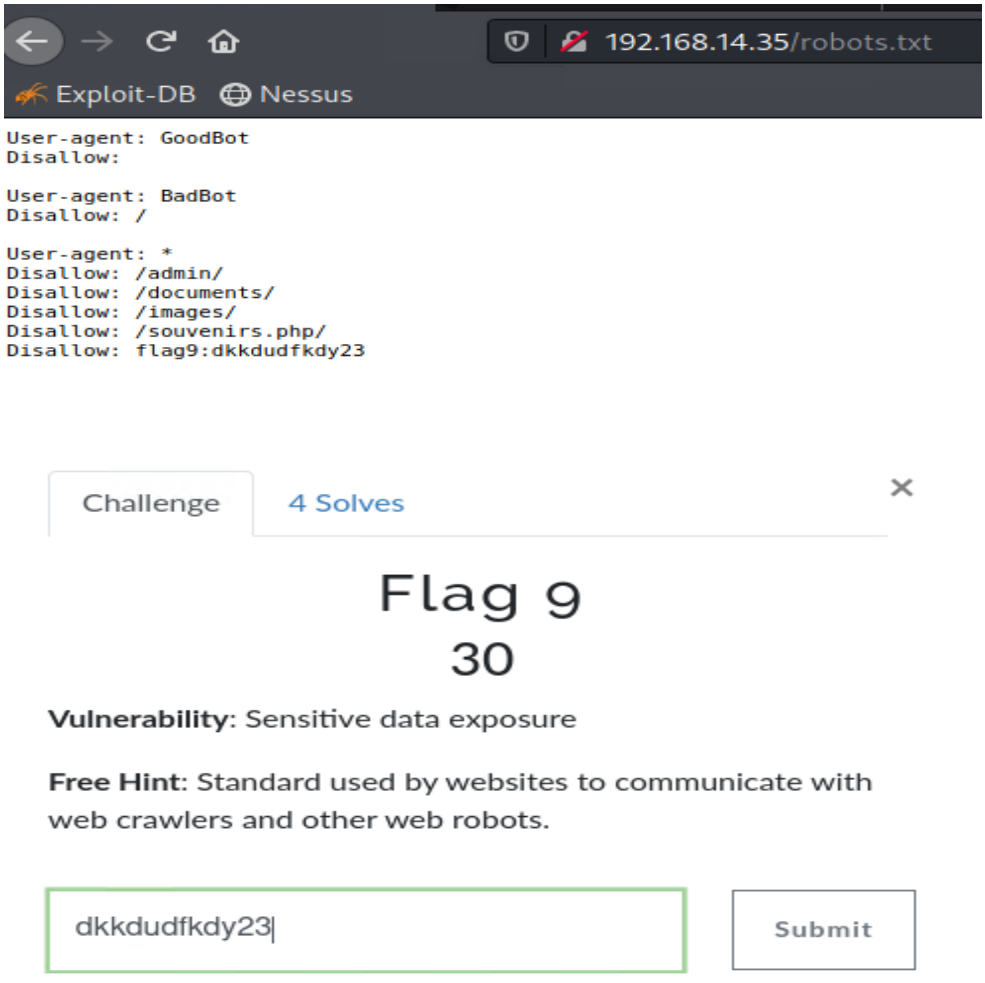
```
meterpreter > shell
Process 5060 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

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
```

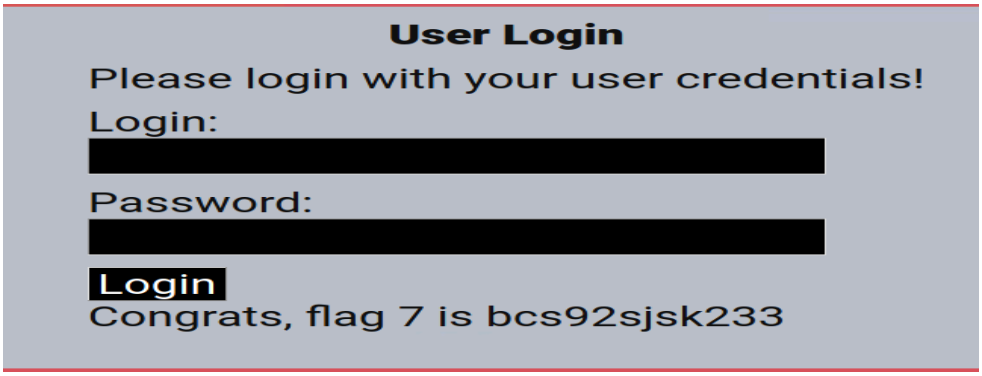


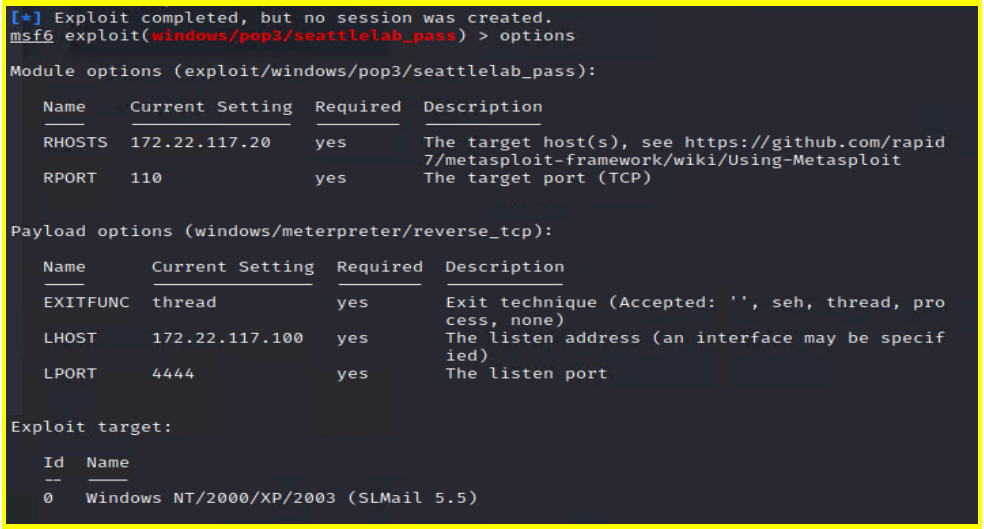
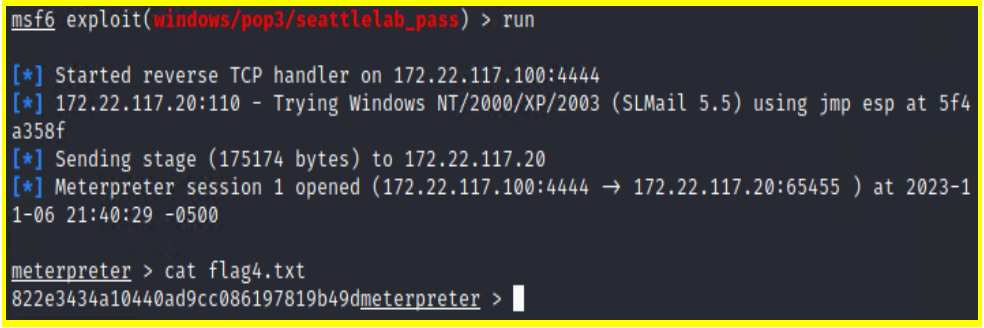


Affected Hosts	172.22.117.20
Remediation	Modify account permissions to limit unauthorized access.

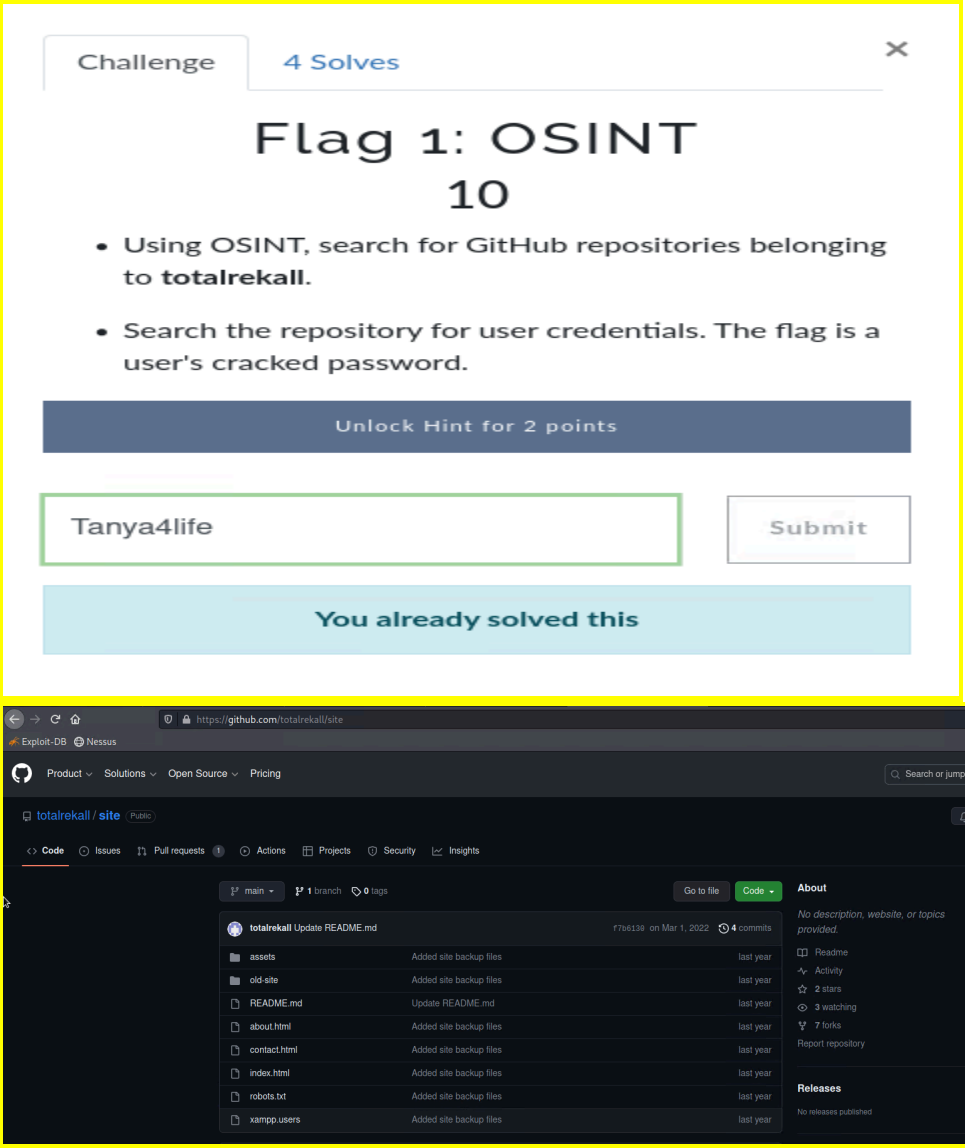
Vulnerability 7	Findings
Title	Sensitive Data Exposure - Robot.txt used to block certain urls.
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Access to the robots.txt webpage is not restricted. Robots.txt is used to attempt to block certain urls.
Images	
Affected Hosts	192.168.14.35
Remediation	Limit access to the robots.txt file to authorized users only.

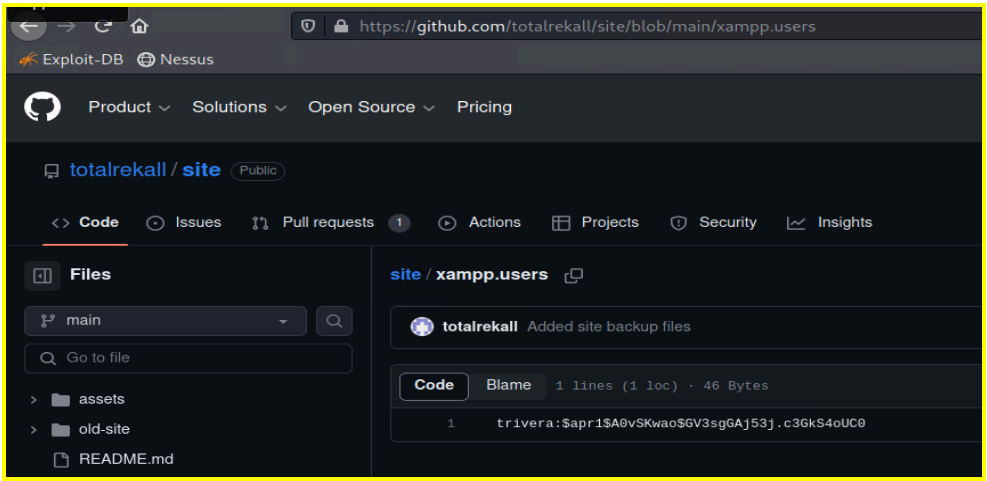
Add any additional vulnerabilities below.

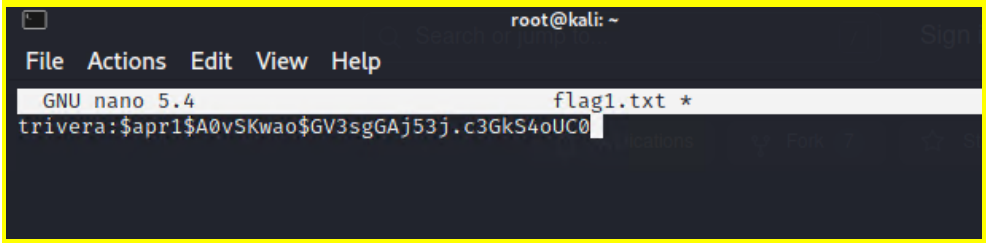
Vulnerability 8	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Successful exploitation took place when the toolbar intended for the password on the Login.php (first field) page accepted a payload to exploit using the following (“ok” or "1=1- -").
Images	 
Affected Hosts	192.168.14.35
Remediation	Strengthen web application defenses by rejecting direct input and incorporating character escaping to prevent security risks.

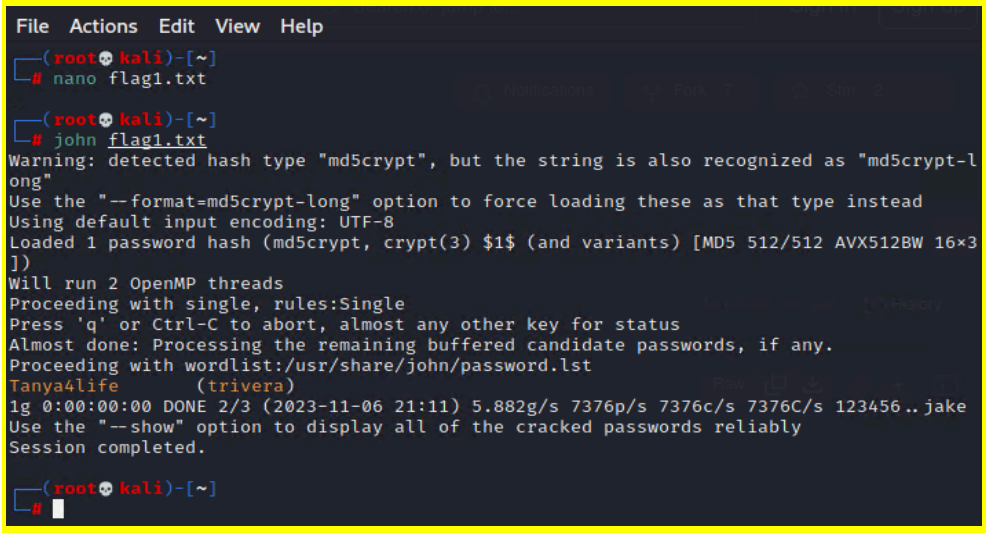
Vulnerability 9	Findings
Title	SLMail Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Through the strategic use of the windows/pop3/seattlelab_pass exploit within Metasploit, a vulnerability within SLMail's open port 110 was successfully exploited, leading to the establishment of a Meterpreter session with successful outcomes.
Images	  

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	

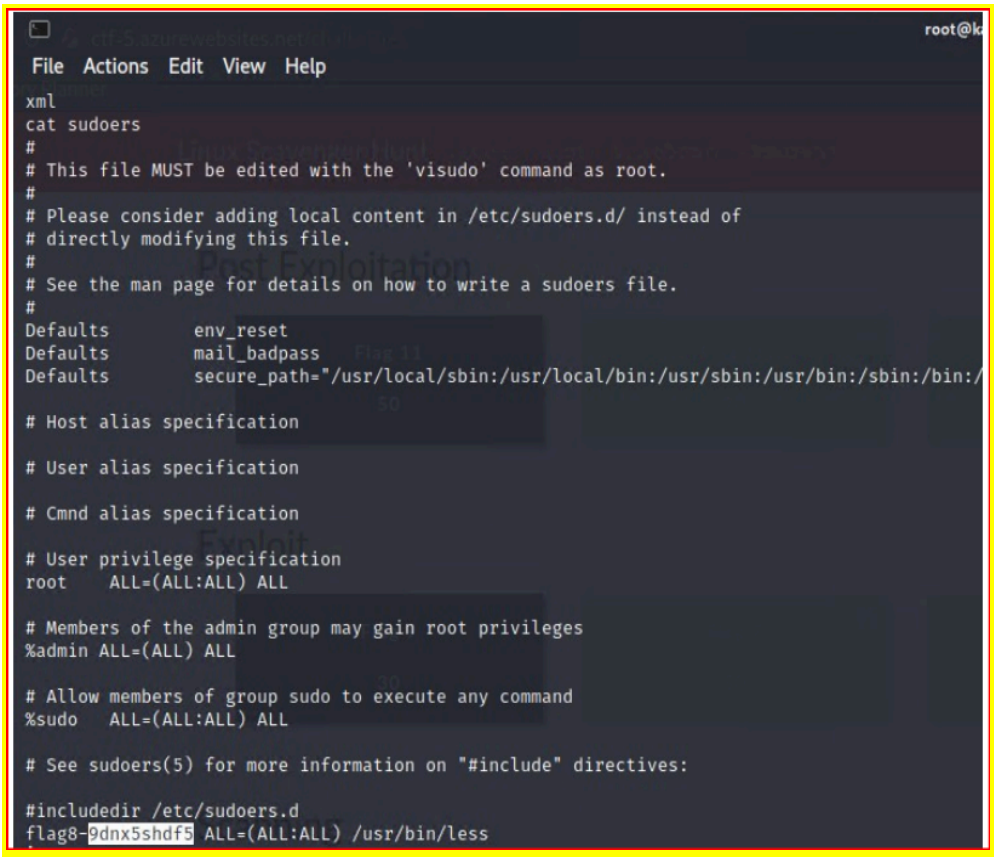






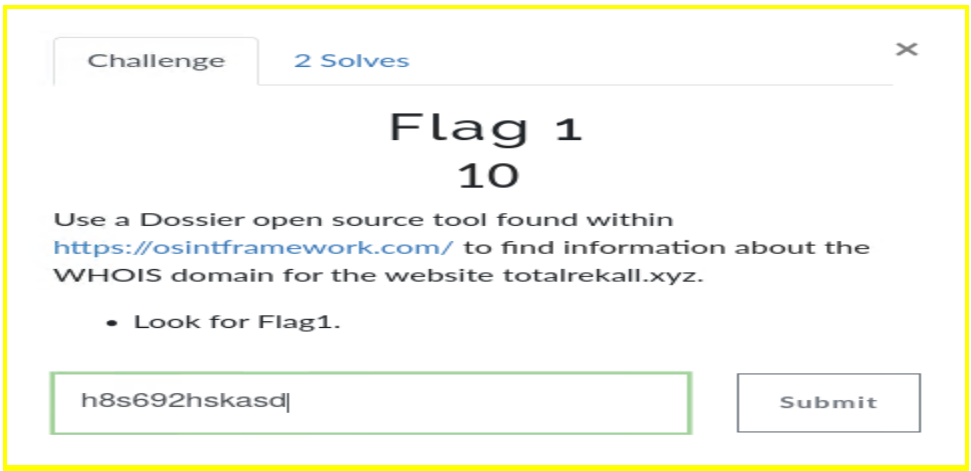
Affected Hosts	Total Rekall web server
Remediation	Implemented measures to deny access by removing any credentials from the GitHub repository.

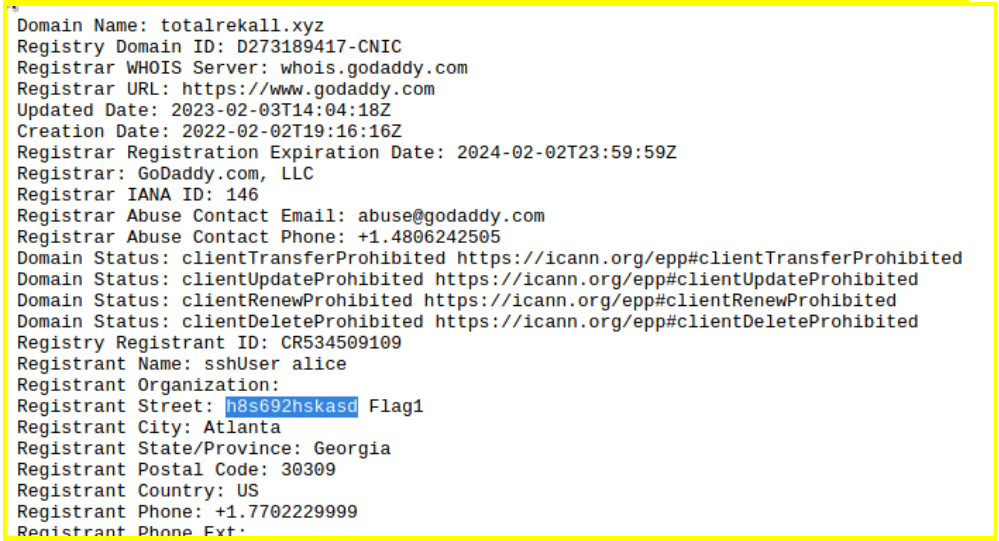
Vulnerability 11	Findings
Title	Shellshock on Web Server (Port - 80)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**

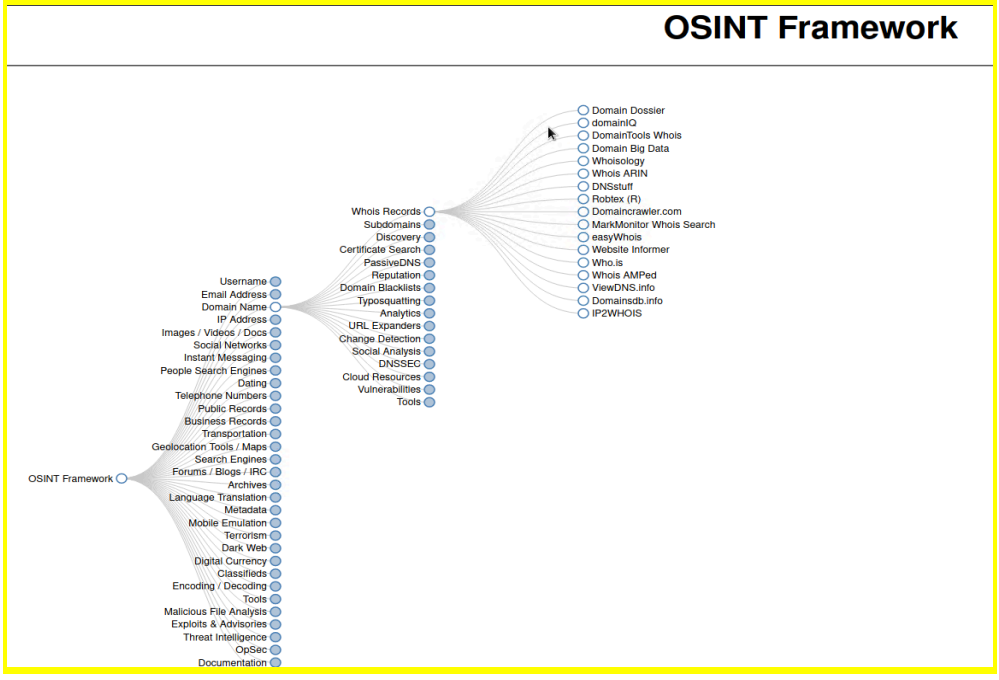
Description	Used exploit : Run MSF console, and search exploits that have Shellshock. Run MSF (exploit/multi/http/apache_mod_cgi_bash_env_exec) set target URI (the vulnerable webpage) : /cgi-bin-/shockme.cgi shell. Navigate to /etc/sudoers.d/ for root privileges file.
Images	
Affected Hosts	192.168.13.11
Remediation	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. orarom ALL = ALL, !/bin/su

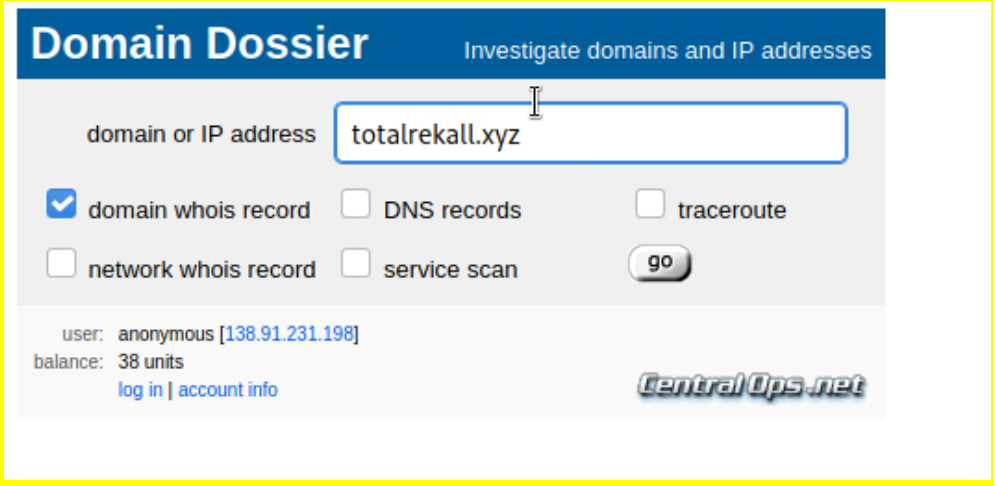
Vulnerability 12	Findings
Title	Open Source Exposed Data - open-source intelligence (OSINT)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Examined the WHOIS data using open-source intelligence (OSINT) on the domain dossier webpage to retrieve sensitive information for totalrekall.xyz.

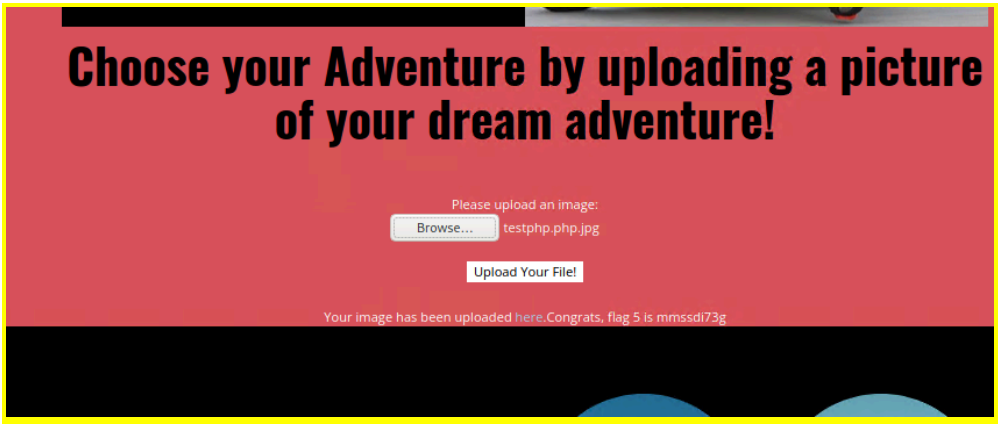
Images

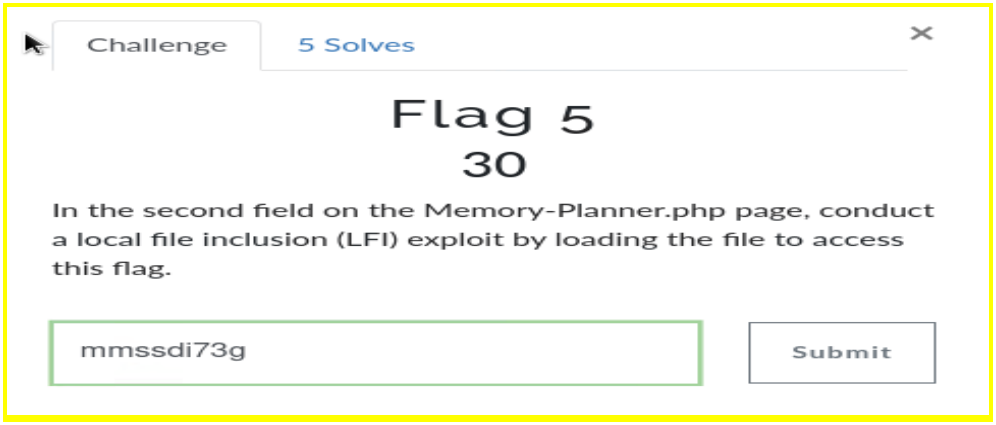


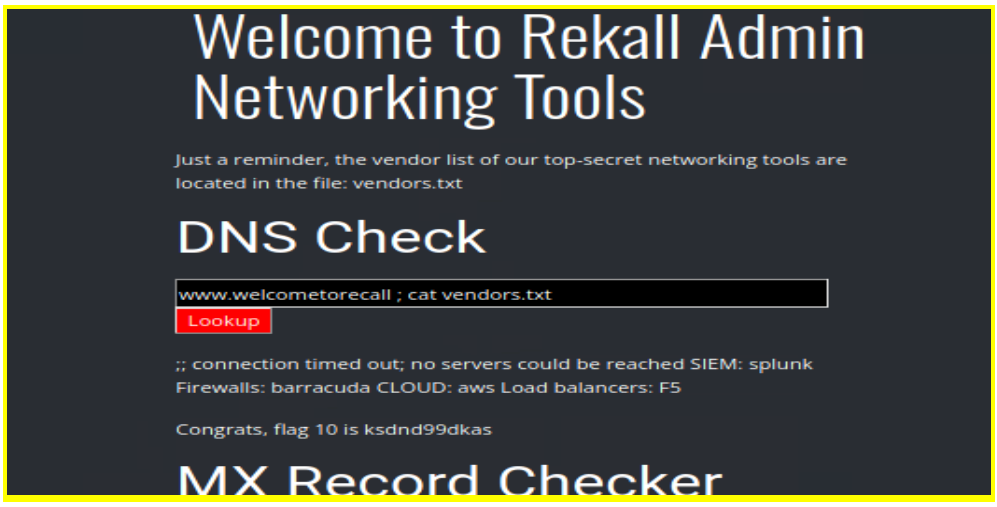




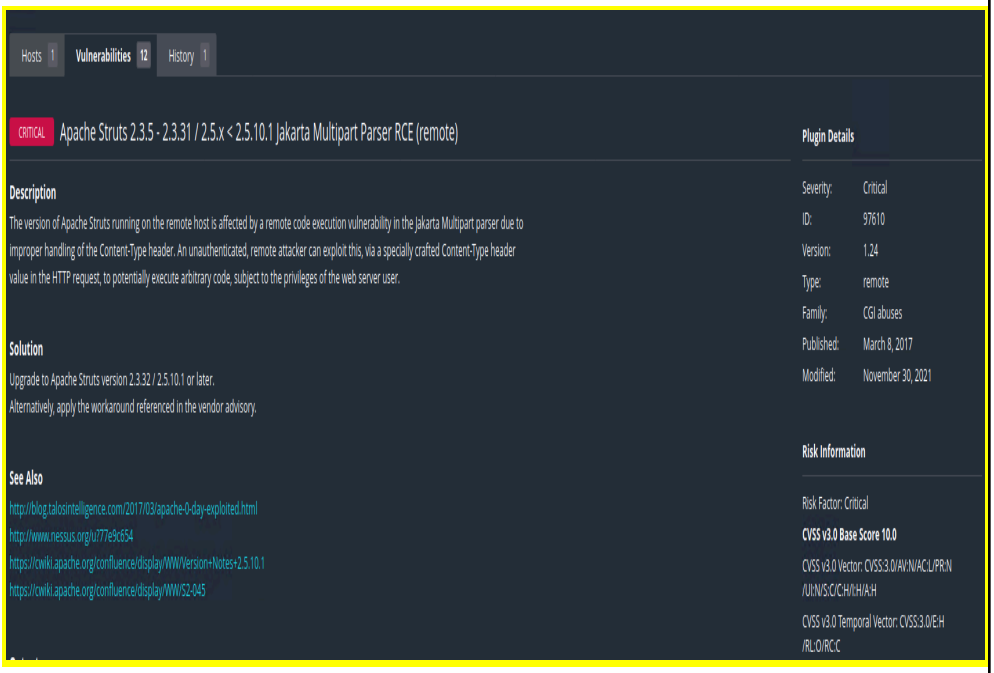
	
Affected Hosts	totalrekall.xyz
Remediation	Guard against the public exposure of sensitive data and initiate a comprehensive sanitization of WHOIS records to maintain privacy and security.

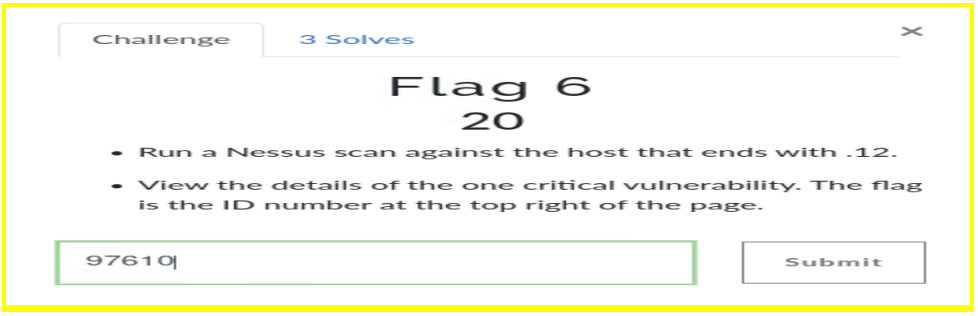
Vulnerability 13	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	A successful Local File Inclusion (LFI) was performed, resulting in the uploading of a ‘php’ file via the toolbar situated on the VR Planner page.
Images	

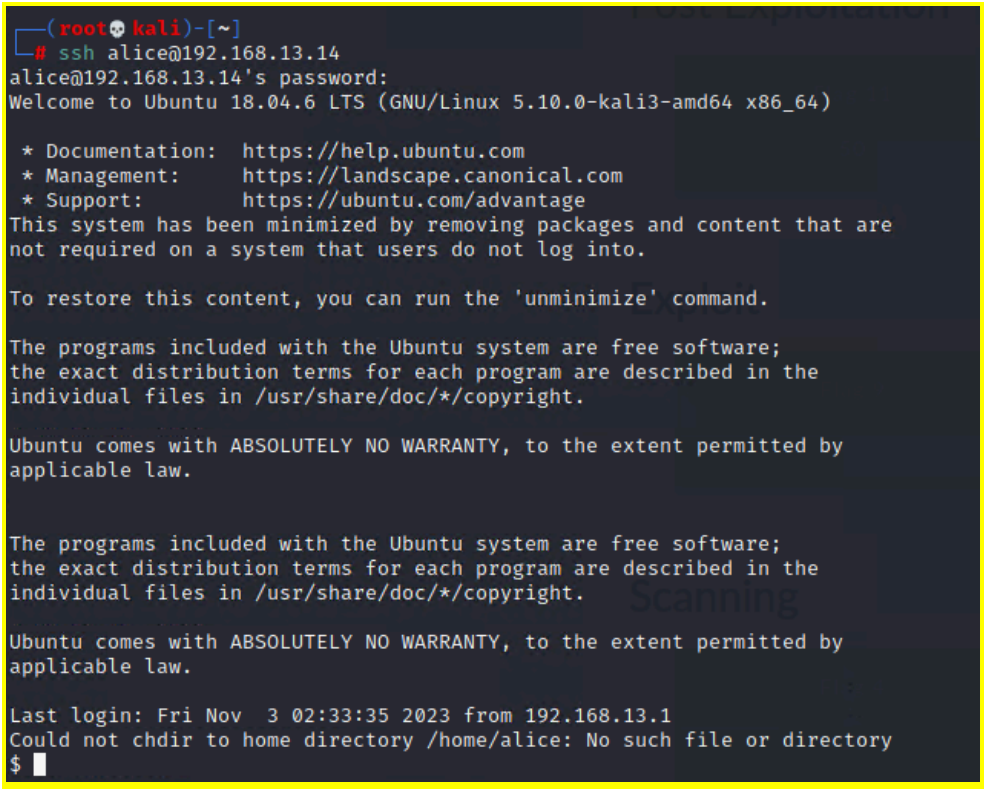
	
Affected Hosts	192.168.14.35
Remediation	Safeguard against direct appending of file paths, and if feasible, confine API access to permit inclusion solely from a designated directory and its subdirectories.

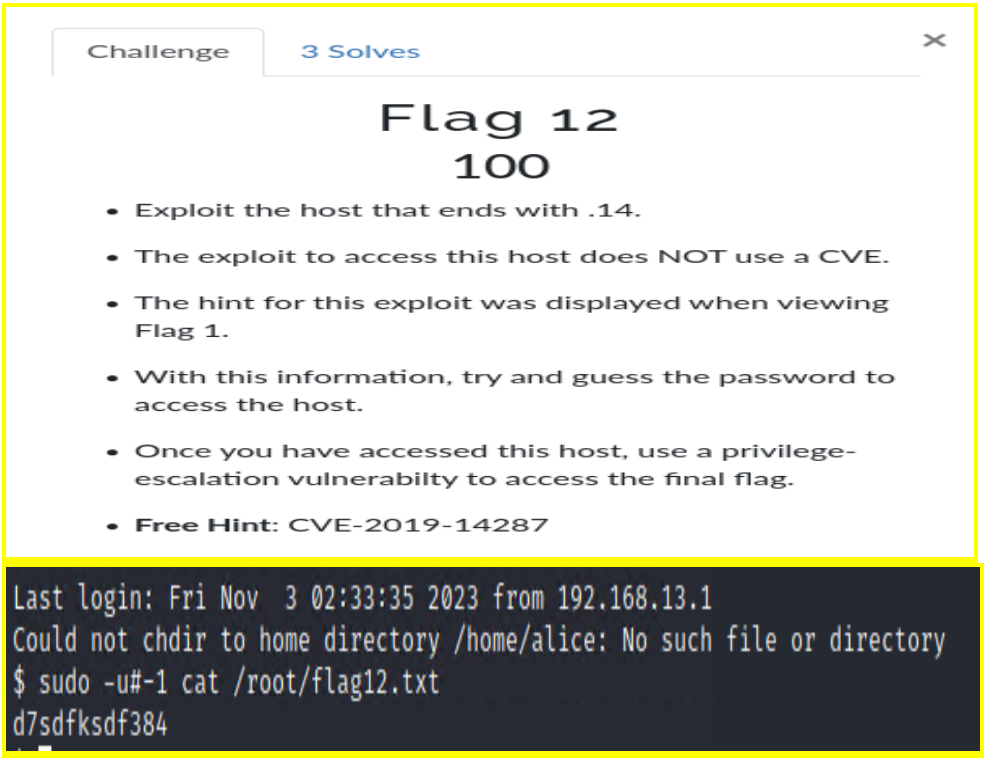
Vulnerability 14	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt. Payload to exploit: 'www.welcometorecall.com && cat vendors.txt'.
Images	

	
Affected Hosts	192.168.14.35
Remediation	Prevent the web application from accepting input directly and/or incorporate character escaping measures.

Vulnerability 15	Findings
Title	Nessus Scan
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	An Apache Struts vulnerability was uncovered during the Nessus scan.
Images	

	
Affected Hosts	192.168.13.12
Remediation	Keep Apache regularly updated.

Vulnerability 16	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	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.
Images	

	
Affected Hosts	192.168.13.14
Remediation	Secure the system by either closing port 22, strengthening credentials enforcement, and/or introducing 2-factor authentication.

Vulnerability 17	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Window OS
Risk Rating	**Critical**
Description	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.

Images

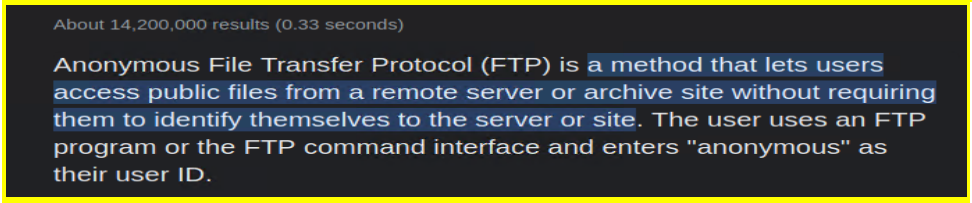
RESOLUTION

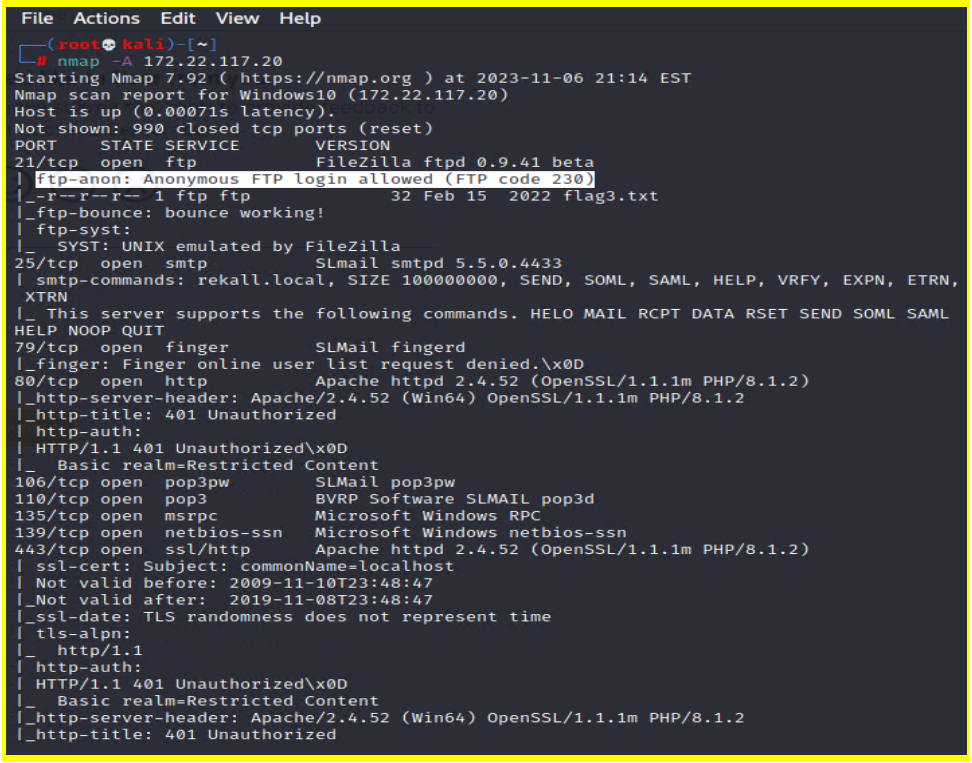
1. Click **Start**, select **Run**, and then enter `cmd` to give you a blank `c:\>` prompt.
2. Enter `ftp`.
3. Enter `open`.
4. Enter the IP address or domain that you want to connect to.
5. Enter your user name and password when prompted.

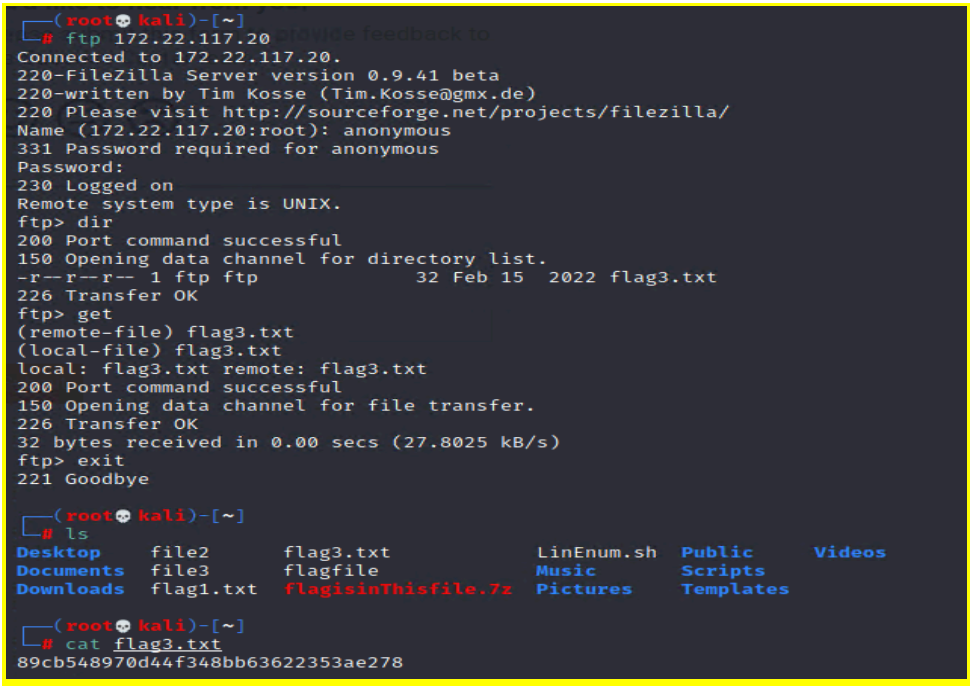
You can now send FTP commands to the server.

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
```







Affected Hosts	172.22.117.20
Remediation	Limit the accessibility to Port 21.