Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

<u>Student Note</u>: Complete all sections highlighted in yellow.

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	Elite Encryption Group
Contact Name	Juliana Rodrigues
Contact Title	Elite Tester

Document History

Version	Date	Author(s)	Comments
003	4/3/24	Juliana Rodrigues	Updated Day 3 Vulnerability Findings
002	4/1/24	Juliana Rodrigues	Updated Day 2 Vulnerability Findings
001	3/28/24	Juliana Rodrigues	Updated Day 1 Vulnerability Findings

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.

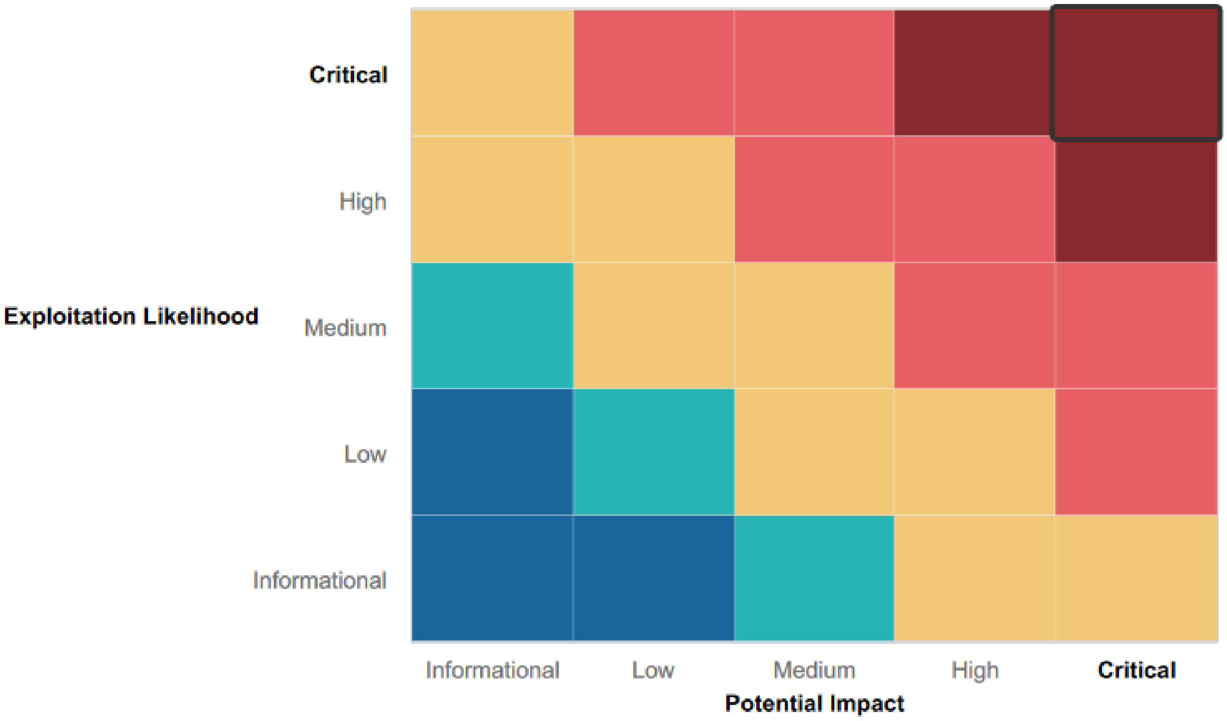
Executive Summary of Findings

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.

- Nmap/Metasploit/Hashcat professional tools were used, preventing unauthorized access.

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.

- Web application is vulnerable to XSS and SQL payload injections.
- Credentials were stored in the HTML source code of the web app.
- IP addresses displayed potential vulnerabilities.
- Credentials were stored in a public Github repository.
- “Anonymous” user was able to bypass via FTP; no password needed.

Executive Summary

During our first assessment, the Elite Encryption Group analyzed Rekall’s Web Application. We discovered several security vulnerabilities, which included SQL injection risks, the execution of malicious script through XSS, local file inclusions through file uploads, and vulnerability to command injections.

Our second assessment revealed other security vulnerabilities that could compromise the business, allowing sensitive information to be accessed by the public and vulnerable to exploits. This included exposure to open source data which was accessible through OSINT, the discovery of a stored certificate, credentials that were stored in the HTML source code, along with a public Github repository accessible to the public.

During our third Linux assessment, we discovered several security vulnerabilities within the Rekall Corporation. These vulnerabilities granted unauthorized access to sensitive information; five publicly accessible IP addresses were found to be exposed as a result of our examination into the Rekall environment. Furthermore, we discovered that user credentials were stored in a GitHub repository, allowing for illegal access to the web host's directories and files. Potential vulnerabilities, such as open ports, were discovered by scanning IP addresses within Rekall.

Our final assessment through Windows OS revealed open ports on the network that were vulnerable to exploits, in addition, credentials that were located through a password hash file and then cracked. We would like to highlight two additional key vulnerabilities of our assessment; the ability to view Tasks in Windows Task Schedule and the ability to display public Window directories via Meterpreter.

In summary, our assessment highlighted critical security flaws that could have serious implications for Rekall’s data integrity and confidentiality. Immediate remediation is recommended to safeguard against unauthorized access and potential breaches.

Summary Vulnerability Overview

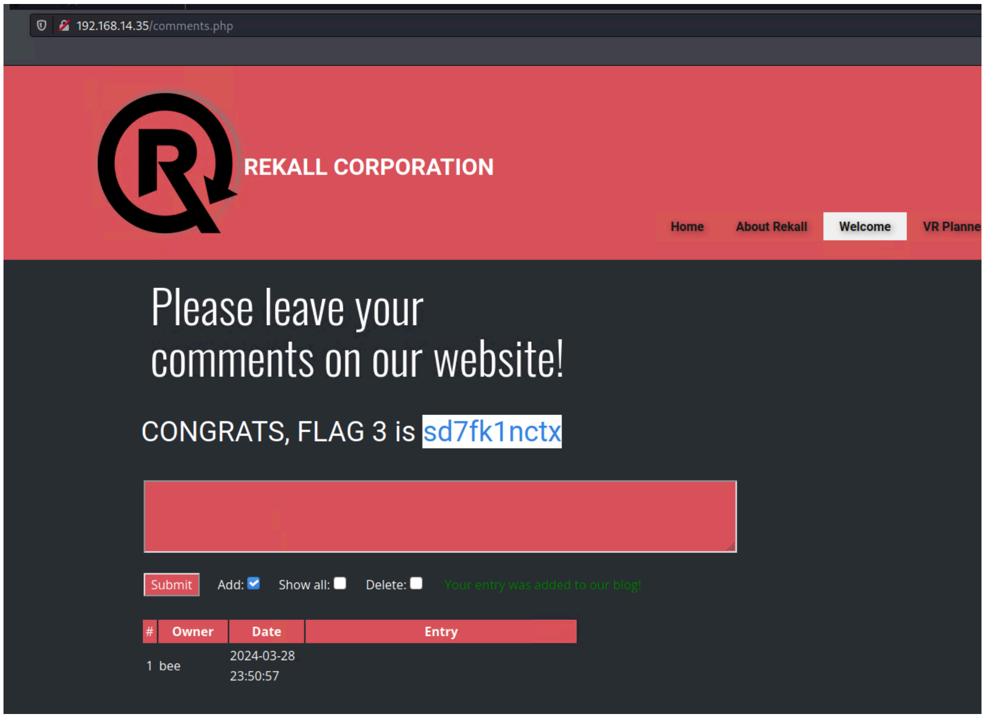
Vulnerability	Severity
XSS Script	Critical
Data Exposure	Critical
Command Injection	Critical
Aggressive nMap Scan	Critical
Certificate Search	Medium
Open Source Exposure	Medium
Public Credential Access	Critical
nMap Subnet Scan	Critical
Anonymous FTP	Critical

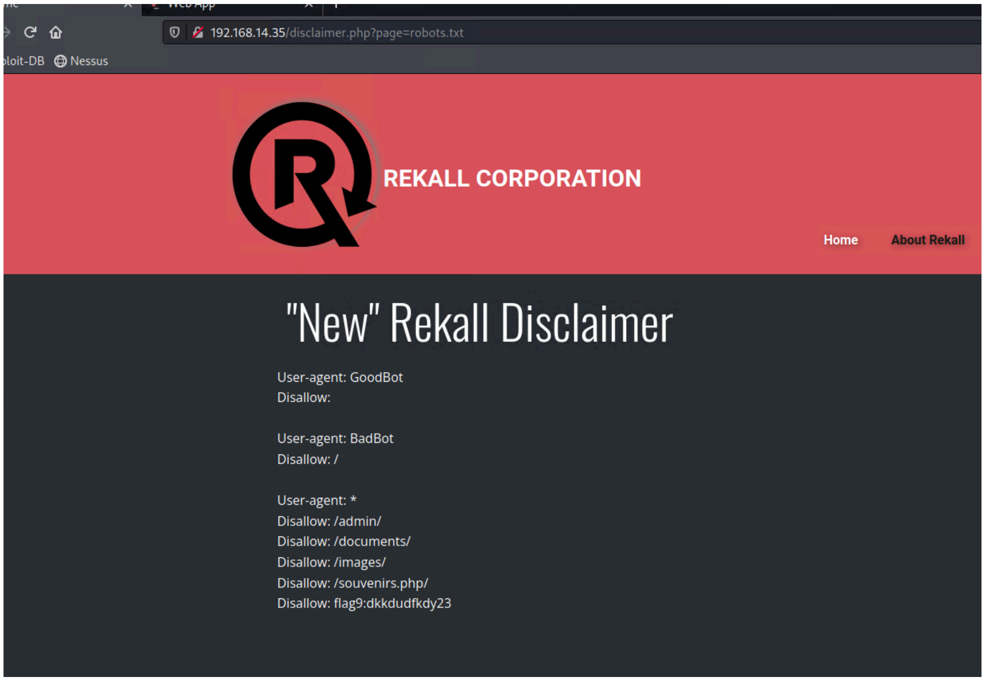
The following summary tables represent an overview of the assessment findings for this penetration test:

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

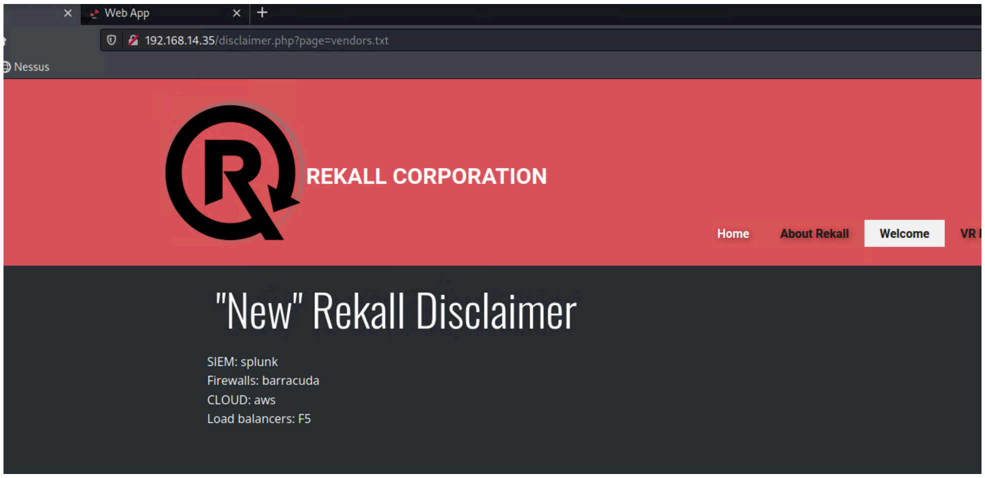
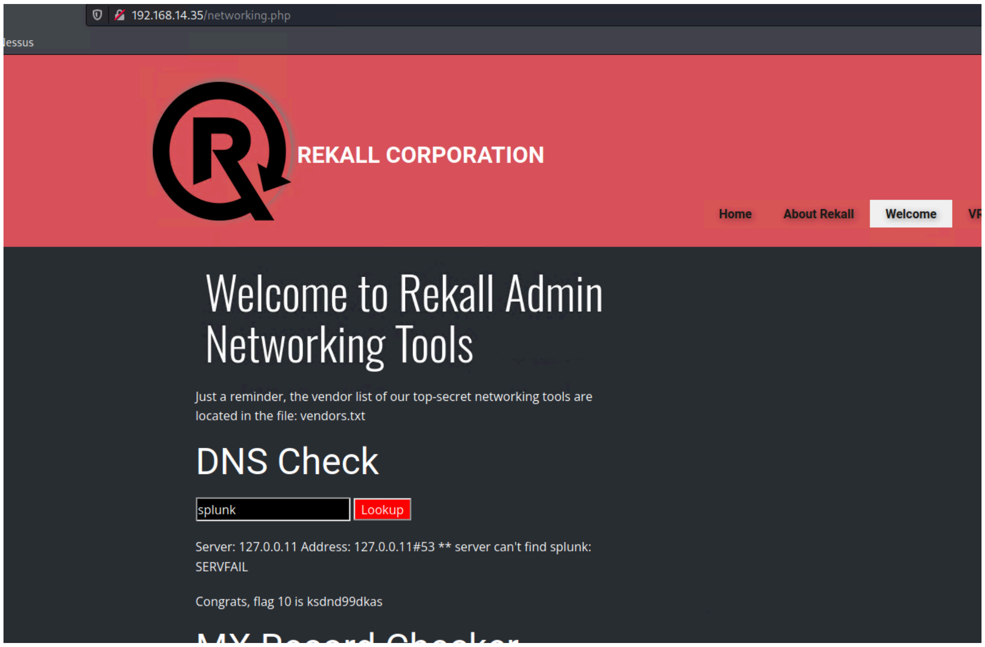
Exploitation Risk	Total
Critical	7
High	0
Medium	2
Low	0

Vulnerability Findings

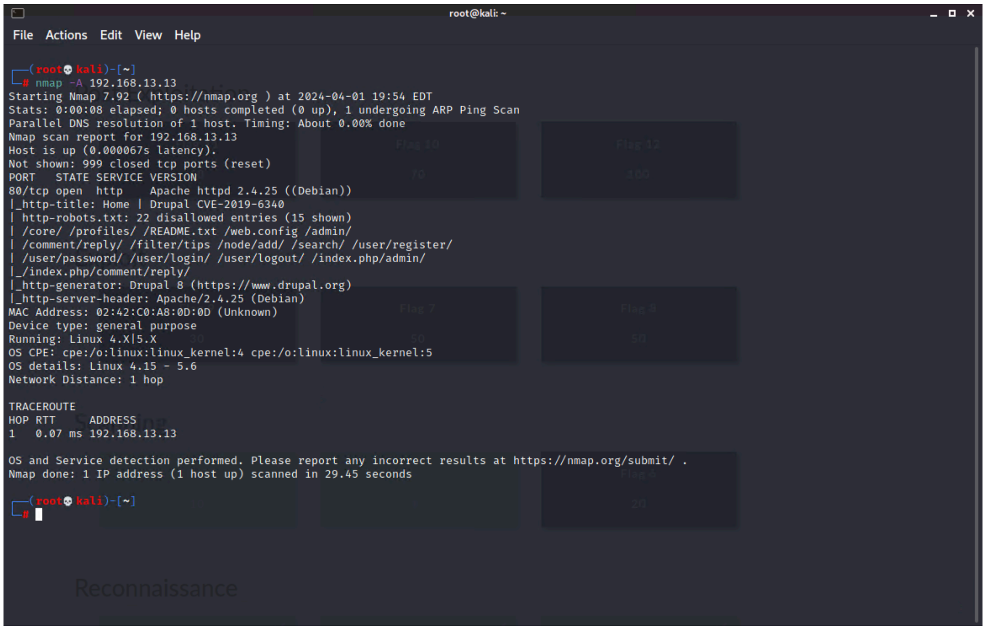
Vulnerability 1	Findings
Title	XSS Script
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	When accessing 192.168.14.35/comments.php, entering <script>alert(“Hi”)</script> will reveal flag 3.
Images	 192.168.14.35/comments.php REKALL CORPORATION Home About Rekall Welcome VR Planne Submit Add: ☑ Show all: □ Delete: □ Please leave your comments on our website! CONGRATS, FLAG 3 is sd7fk1nctx Your entry was added to our blog! # Owner Date Entry 1 bee 2024-03-28 23:50:57
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disable script code injection.

Vulnerability 2	Findings
Title	Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	A robots.txt file tells search engine crawlers which URLs the crawler can access on your site. Visiting 192.168.14.35/disclaimer.php?page=robots.txt will reveal flag 9.
Images	 Web App oloit-DB Nessus REKALL CORPORATION Home About Rekall 192.168.14.35/disclaimer.php?page=robots.txt "New" Rekall Disclaimer User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35
Remediation	Do not store sensitive information in robots.txt or other publicly accessible files; instead, use authentication procedures.

Vulnerability 3	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Able to input “splunk” in DNS Check which revealed flag 10. This was by navigating to /disclaimer.php?page=vendors.txt through /networking.php.

Images	 Web App Nessus REKALL CORPORATION Home About Rekall Welcome VR 192.168.14.35/disclaimer.php?page=vendors.txt "New" Rekall Disclaimer SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5  lessus REKALL CORPORATION Home About Rekall Welcome VR 192.168.14.35/networking.php Welcome to Rekall Admin Networking Tools Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check splunk Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 ** server can't find splunk: SERVFAIL Congrats, flag 10 is ksdnd99dkas MX Record Checker
Affected Hosts	192.168.14.35
Remediation	Use input validation to prevent unauthorized access.

Vulnerability 4	**Findings**
Title	Aggressive nMap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran nmap -A 192.168.13.13 which was identified as the host running DRUPAL. This was found by performing an nMap scan on 192.168.13.0/24 which revealed 5 hosts with exposed IP addresses.

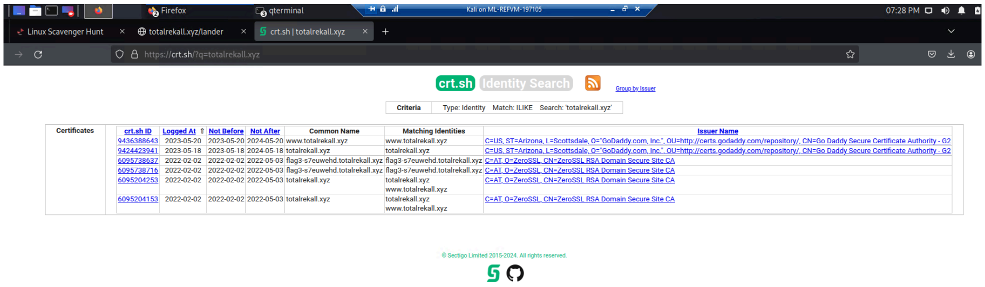
Images	
Affected Hosts	192.168.13.13
Remediation	Prevent nmap scan from providing real details; should reveal misleading details, or restrict information from being returned altogether.

```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-01 19:54 EDT
Stats: 0:00:08 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.13.13
Host is up (0.000067s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 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)
|_http-server-header: Apache/2.4.25 (Debian)
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
HOP RTT     ADDRESS
1   0.07 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.45 seconds

┌──(root💀kali)-[~]
└─#
```

Vulnerability 5	**Findings**
Title	Certificate Search
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Using crt.sh on totalrekall.xyz reveals flag 3 as a stored certificate.
Images	
Affected Hosts	34.102.136.180
Remediation	Safeguard data to prevent it from being revealed by the crt.sh website.

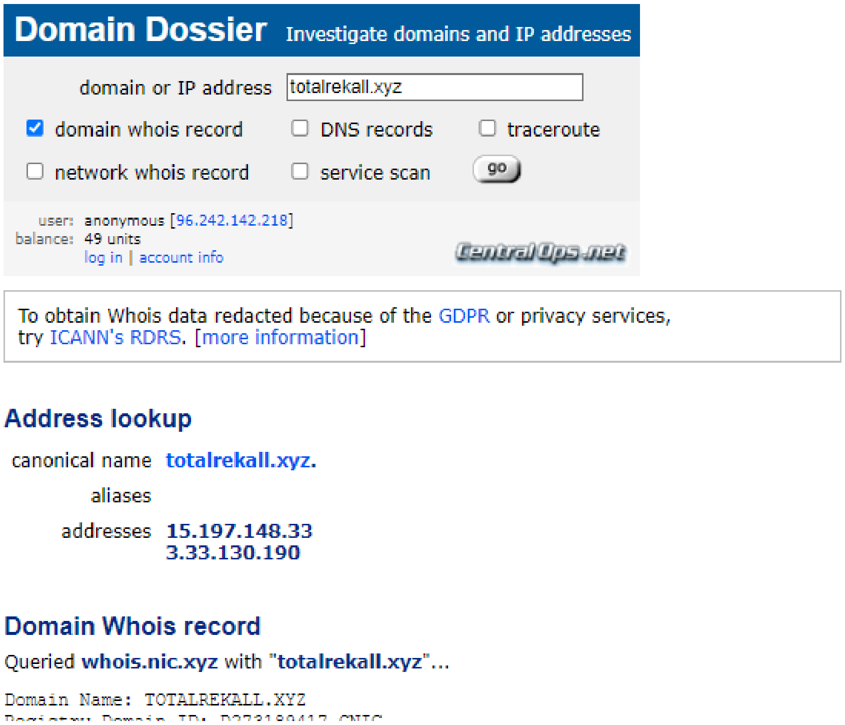
https://crt.sh/?q=totalrekall.xyz

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

Certificates

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

© Sectigo Limited 2015-2024. All rights reserved.

Vulnerability 6	Findings
Title	Open Source Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Used Domain Dossier > WHOIS record against totalrekall.xyz to access sensitive information, which revealed flag 1.
Images	

Domain Dossier Investigate domains and IP addresses

domain or IP address: totalrekall.xyz

☑ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan

user: anonymous [96.242.142.218]
balance: 49 units
log in | account info

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]

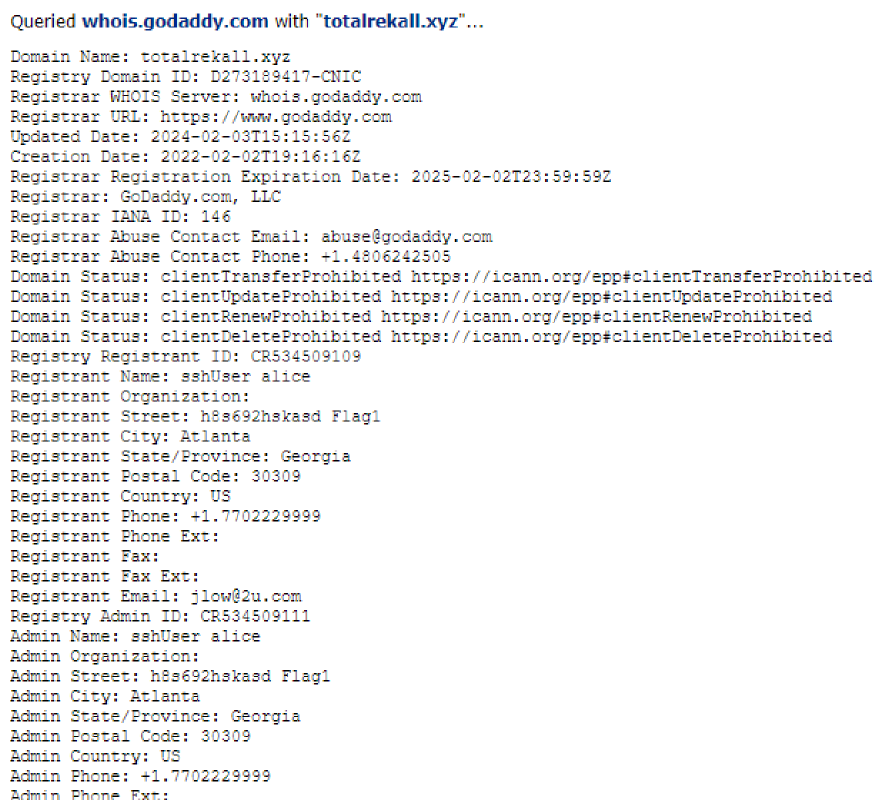
Address lookup

canonical name **totalrekall.xyz.**
aliases
addresses **15.197.148.33**
3.33.130.190

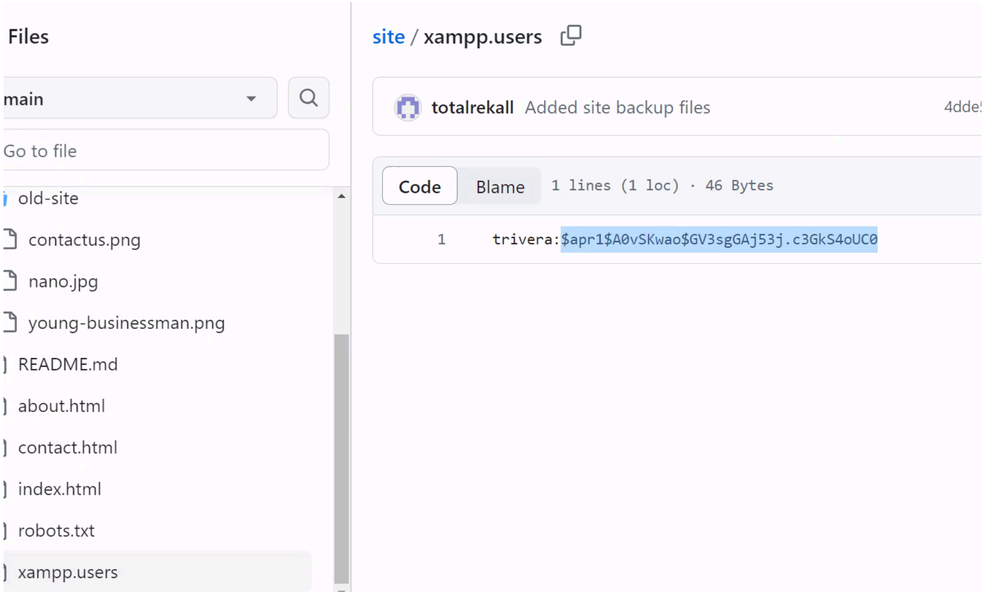
Domain Whois record

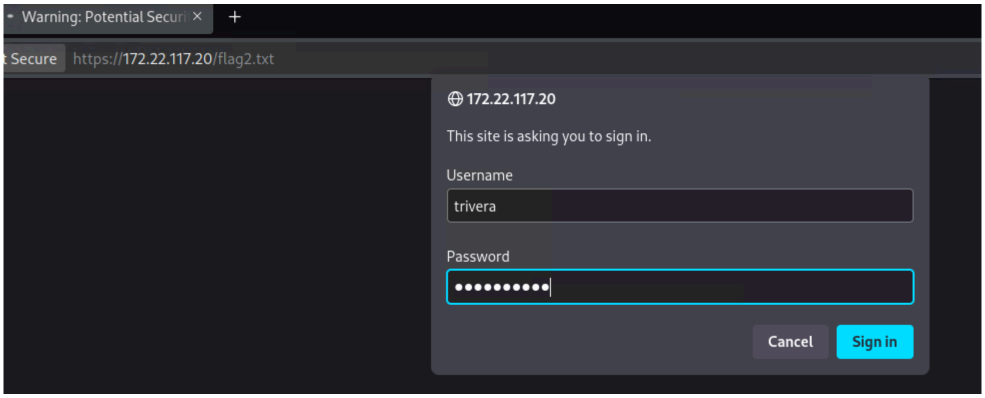
Queried **whois.nic.xyz** with "**totalrekall.xyz**"...

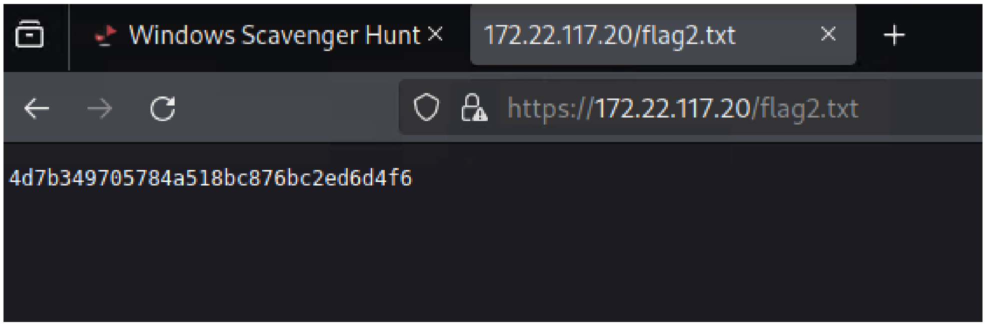
```
Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
```

	 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: 2024-02-03T15:15:56Z 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: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999 Admin Phone Ext:
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Safeguard data to prevent it from being exposed to the public.

Vulnerability 7	**Findings**
Title	Public Credential Access
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Credentials were found in totalrekall Github public repository. In the xampp.users page of the site repository, flag 1 was revealed.

Images	 Files main Go to file old-site contactus.png nano.jpg young-businessman.png README.md about.html contact.html index.html robots.txt xampp.users site / xampp.users totalrekall Added site backup files 4dde! Code Blame 1 lines (1 loc) · 46 Bytes `trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0`
Affected Hosts	172.22.117.0
Remediation	Safeguard the credentials in a secure place; no access to the public.

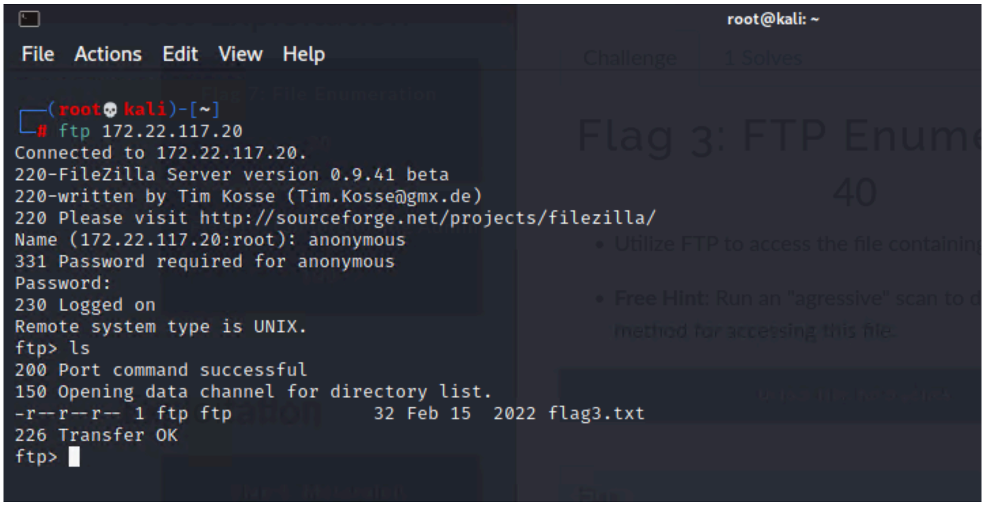
Vulnerability 8	**Findings**
Title	nMap Subnet Scan
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	After performing an aggressive nmap scan of 172.22.117.20, it revealed port 80 open; which was placed into the browser as https://172.22.117.20/flag2.txt and credentials from flag1, revealed flag2.
Images	 Warning: Potential Securi × + t Secure https://172.22.117.20/flag2.txt 172.22.117.20 Cancel Sign in This site is asking you to sign in. Username: trivera Password: ••••••••••

<table>
<tr><th></th><th>

Windows Scavenger Hunt
172.22.117.20/flag2.txt
https://172.22.117.20/flag2.txt

4d7b349705784a518bc876bc2ed6d4f6</th></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.20</td></tr>
<tr><td><b>Remediation</b></td><td>Input two-factor authentication or encourage stronger passwords.</td></tr>
</table>

<table>
<tr><th>Vulnerability 9</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Anonymous FTP</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>While using FTP to gain access to 172.22.117.20, the credentials allowed “anonymous” to be entered and successfully logon. When viewing the repository (ls), flag3.txt file was revealed.</td></tr>
<tr><td><b>Images</b></td><td>



```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> █
```

</td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.20</td></tr>
<tr><td><b>Remediation</b></td><td>Disable access to FTP with “anonymous” and other dummy names; password should be required as no password entered allowed access too.</td></tr>
</table>