



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: 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

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	CR4CK'D
Contact Name	Jackson Long
Contact Title	Jr. Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	3/12/2023	Jackson Long	N/A

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.
- Medium:** Indirect or partial threat to business processes.
- Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
- Informational:** No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- There were efforts towards Web Application Sanitization. Which slowed the process of command injections.

Summary of Weaknesses

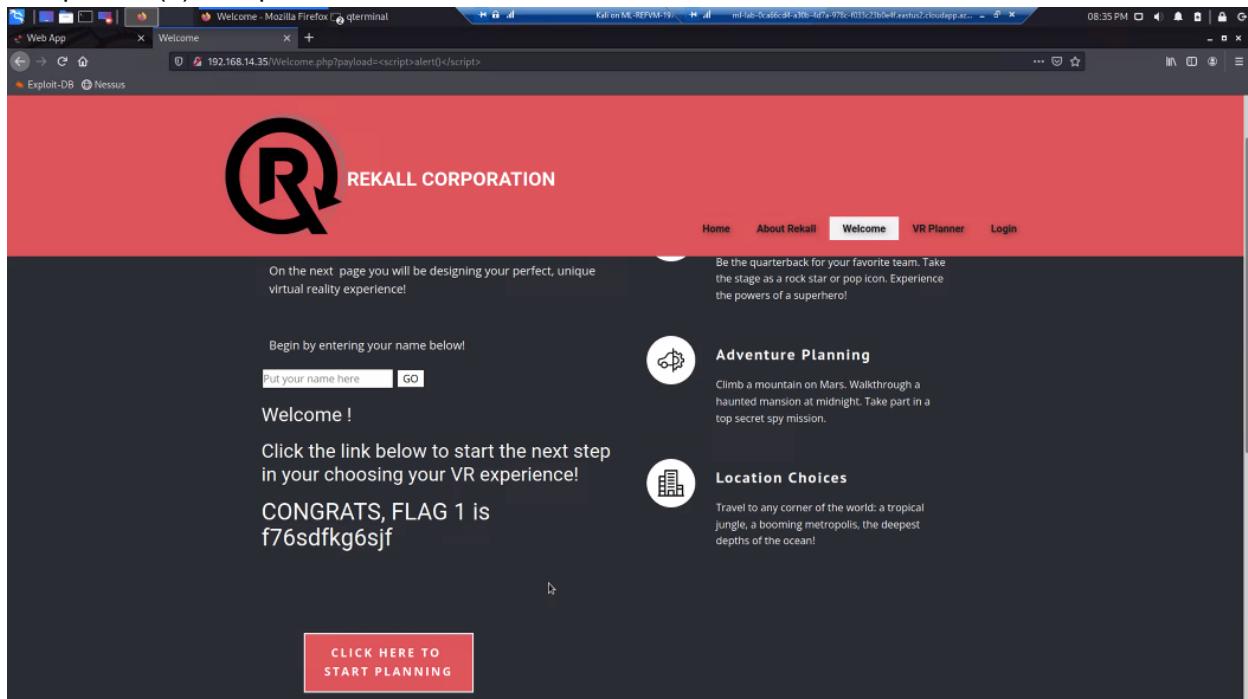
We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Weak passwords/password policy.
- Little effort in sanitizing user input validation.
- Weak firewall settings to block certain traffic requests and responses.
- Multiple open ports allowing for shells to be open.
- Found login credentials from Github, and used those to gain access to a shell.

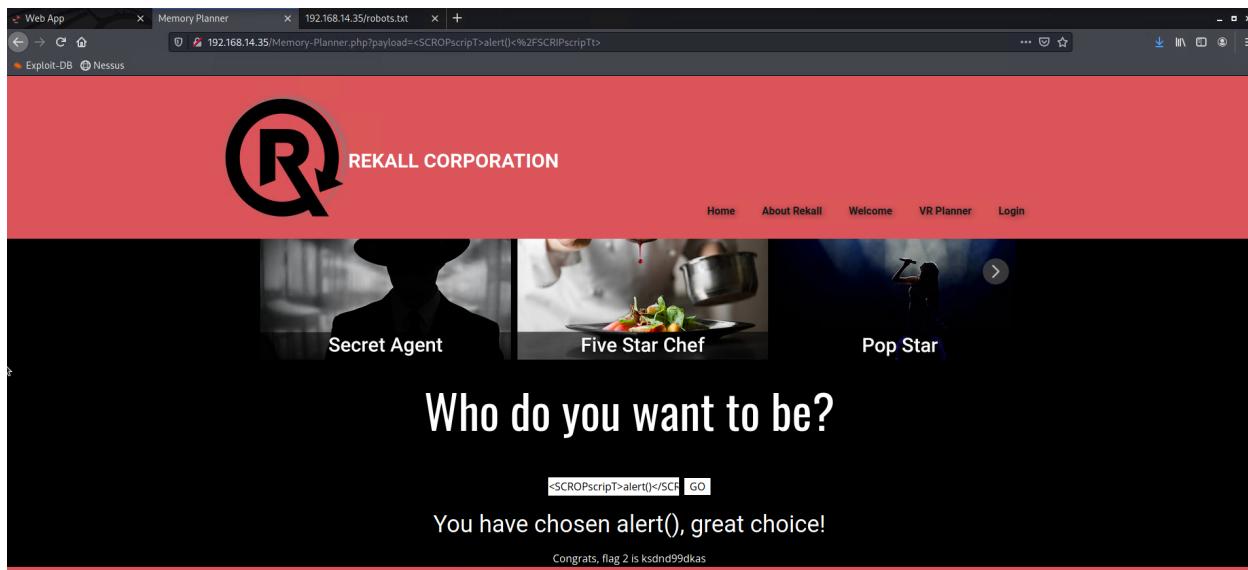
Executive Summary

Beginning stages of our penetration test were targeting/exploiting Rekall's Web-Application. Our first attack (C4) began by exploiting the "Name" field inside Rekall's "Welcome" page, by typing in a Javascript to give us an Alert Response. The same exploit was used on the "Memory-Planner" character entry field. Using the same exploit in the comments field on the comments page but modifying it; CR4CK'D was able to store scripts and allow users to pull data.

Using javascript CR4CK'D was able to successfully create an alert on Rekall Corps 'Welcome Page' <script>alert(1)</script> was run to achieve this.



Reflected XSS



Stored XSS Input

The screenshot shows a Mozilla Firefox browser window with the address bar set to 192.168.14.35/comments.php. The page displays a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the header, a large black section contains the text "Please leave your comments on our website!" and "CONGRATS, FLAG 3 is sd7fk1nctx". A red box highlights the text "<h1><script>alert(1)</script></h1>". Below this, a table lists three entries from the database:

#	Owner	Date	Entry
1	bee	2023-03-03 01:53:30	show me popup
2	bee	2023-03-03 01:55:10	test
3	bee	2023-03-03 01:56:26	\h1

Using test.jpg.php in both upload fields CR4CK'D was able to bypass user input whitelist

The screenshot shows a Mozilla Firefox browser window with the address bar set to 192.168.14.35/Memory-Planner.php. The page features a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (highlighted), VR Planner, and Login. The main content area has a large black background with the text "Choose your Adventure by uploading a picture of your dream adventure!". Below this, there is a form with a "Please upload an Image" label, a "Browse..." button, and a message "No file selected.". A "Upload Your File!" button is also present. At the bottom of the page, a message says "Your image has been uploaded here. Congrats, flag 5 is mmssd173g". Three circular images are displayed at the bottom: a sunset over water, a snowy mountain peak, and a forest scene.

Please upload an image:

Browse... test.jpg.php

Upload Your File!

Your image has been uploaded here. Congrats, flag 6 is Id8skd62hdd

Using SQL Injection on the Login page, CR4CK'D was able to access a successful login by using (any password or '1'='1')

*Untitled - Notepad

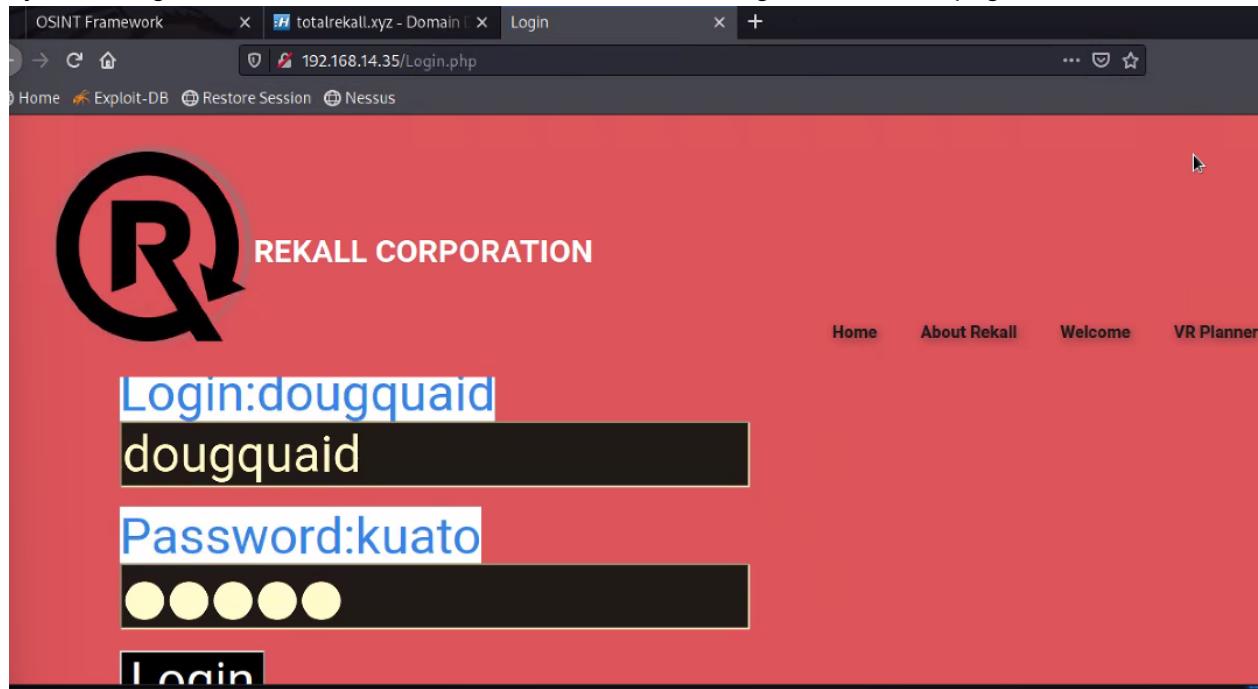
User= anything "Jackson"

Password= Jackson' or '1'='1

Login

Congrats, flag 7 is bcs92sjk233

By searching the HTML, C4 was able to find credentials to log into an admin page



Output from CURLing

```
root@kali: ~/Documents/day_1 ~ | root@kali: ~ | ↵
└─(root㉿kali)-[~]
# curl -v http://192.168.14.35/About-Rekall.php
*   Trying 192.168.14.35:80 ...
*   Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 12 Mar 2023 22:34:05 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=tmdccqedhvhh4rlu7d543g8iv4; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<

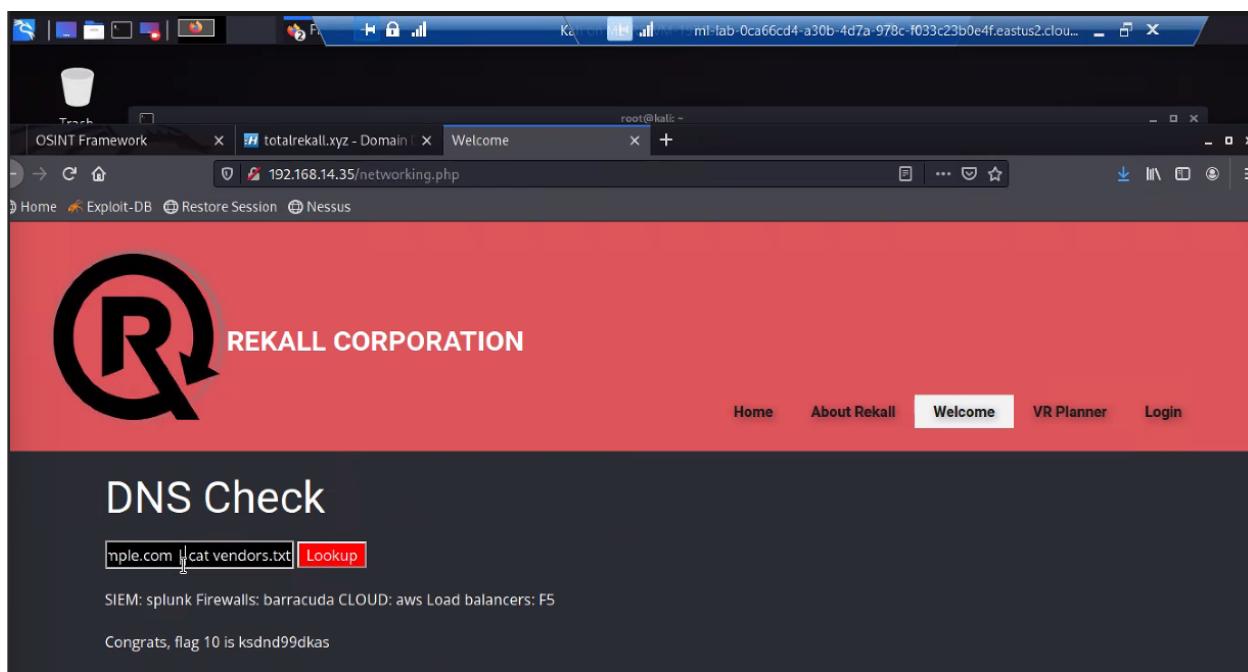
<!DOCTYPE html>
<html style="font-size: 16px;">
<head>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta charset="utf-8">
  <meta name="keywords" content="">
  <meta name="description" content="">
  <meta name="page_type" content="np-template-header-footer-from-plugin">
  <title>About Rekall</title>
  <link rel="stylesheet" href="nicepage.css" media="screen">
<link rel="stylesheet" href="About-Rekall.css" media="screen">
  <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script>
  <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>
  <meta name="generator" content="Nicepage 4.0.3, nicepage.com">
  <link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto: " data-bbox="115 800 886 938"/>
```

Found the robots.txt by adding /robots.txt at the end of the URL



User-agent: GoodBot
Disallow:
User-agent: BadBot
Disallow: /
User-agent: *
Disallow: /index/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkduffky23

Stored XSS to gain access to company information



MX-Record Checker field input to search the /etc/passwd

```
root:x:0:root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin  
/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin  
/nologin sync:x:4:65534:sync:/bin:/sync games:x:5: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:/usr/sbin/nologin www-data:x:33:33:www-  
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

By searching the etc/passwd, we were able to find a user “melina” and bruteforce her password which was also “Melina”

Enter your Administrator credentials!

Login:

Password:

Login

Successful login! flag 12 is [hsk23oncsd](#) , also the top secret legal data located here:
[HERE](#)

Executive Summary Day Two

By accessing the OSNIT Framework, C4 was able to pull sensitive information from the database.

```

Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
DNSSEC: Please query the RODS 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: +1.4886958800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-03-00T03:39:02.02 <<<

Queried whois.godaddy.com with "totalrecall.xyz"...
Domain Name: totalrecall.xyz
Registry Domain ID: D273189417-CNIC
Registrant ID: CR534509110
Registrar URL: https://www.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2024-02-02T10:16:16Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4886242595
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp/clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp/clientDeleteProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp/clientDeleteProhibited
Registrar Registration ID: CR534509109
Registrant Organization: sshUser alice
Registrant Street: #8692hsksasd Flagi1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone Ext: +1.7702229999
Registrant Phone Ext:
Registrant Fax Ext:
Registrant Fax Ext:
Registrant Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrecall.xyz
Registrant Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization: sshUser alice
Admin Street: #8692hsksasd Flagi1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrecall.xyz
Registrant Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization: sshUser alice
Tech Street: #8692hsksasd Flagi1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309

```

We were also able to gain an Address Lookup for IPs and more

Domain Dossier Investigate domains and IP addresses

domain or IP address: totalrecall.xyz

domain whois record DNS records traceroute

network whois record service scan go

user: anonymous [20.10.233.35]
balance: 32 units
[log in](#) | [account info](#)

[CentralOps.net](#)

Do you see Whois records that are missing contact information?
[Read about reduced Whois data due to the GDPR.](#)

Address lookup
canonical name: [totalrecall.xyz](#).
aliases
addresses: [34.102.136.180](#)

Domain Whois record
Queried [whois.nic.xyz](#) with "totalrecall.xyz"...

Domain Name: TOTALREKALL.XYZ
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2023-02-03T14:04:18Z

IP Match Case Match Diacritics Whole Words 1 of 7 matches

By searching on crt.sh, we were able to pull the certificate information for the website totalrecall.xyz

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name
	6095738632	2022-02-02	2022-05-03	flag3-7euweld.totalrecall.xyz	flag3-7euweld.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-05-03	flag3-7euweld.totalrecall.xyz	flag3-7euweld.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095204351	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095204151	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2023. All rights reserved.

We were able to find a GitHub repository that contained sensitive information and HTML code

File	Description	Last Updated
assets	Added site backup files	last year
old-site	Added site backup files	last year
README.md	Update README.md	last year
about.html	Added site backup files	last year
contact.html	Added site backup files	last year
index.html	Added site backup files	last year
robots.txt	Added site backup files	last year
xampp.users	Added site backup files	last year

main → site / xampp.users

totalrecall Added site backup files

1 contributor

1 lines (1 sloc) | 46 Bytes

```
1 trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

21.

Summary Vulnerability Overview

Vulnerability	Severity
Web App- Reflective XSS	Medium
Web App- Stored XSS	Medium
Web App- Stored XSS	Medium
Web App- Exposed Sensitive Data	Critical
Web App- Local File Inclusion	High
Web App- Local File Inclusion	High
Web App- Exposed Sensitive Data	Critical
Web App- Exposed Sensitive Data	Critical
Web App- Exposed Sensitive Data	Critical
Web App- Command Injection	Critical
Web App- Command Injection	Critical
Web App- Brute Force Attack	Critical
Linux- Open Source Vulnerability	Critical
Linux- Domain Ping	Low
Linux- Open Source Vulnerability	Low
Linux- Network Mapping Scan	Medium
Windows- Exposed Sensitive Data	Critical
Windows- Password Guess	Critical
Windows- Vulnerability FTP port 21	Critical
Windows- Vulnerability port 110	Critical

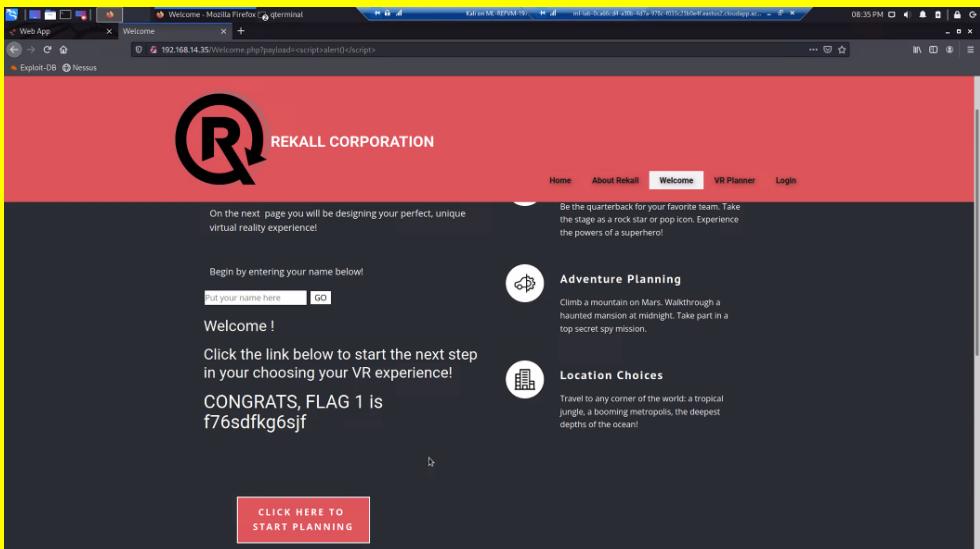
The following summary tables represent an overview of the assessment findings for this penetration test:

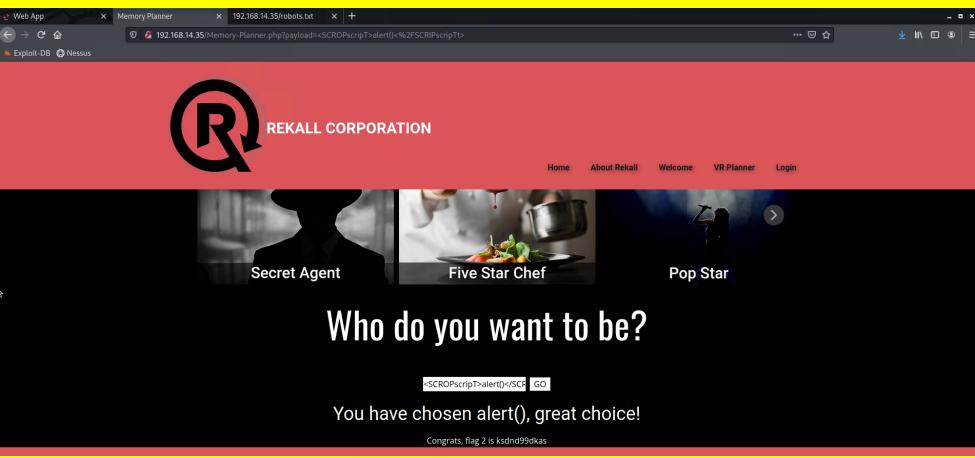
Scan Type	Total
	172.22.117.20
	192.168.13.10
	192.168.13.11
Hosts	192.168.13.12
	192.168.13.14
	192.168.13.1
	192.168.14.34

Ports	80, 8080, 22, 5901, 6001, 10000, 10001, 3306, 53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 21, 25, 106, 110, 443, 79
-------	--

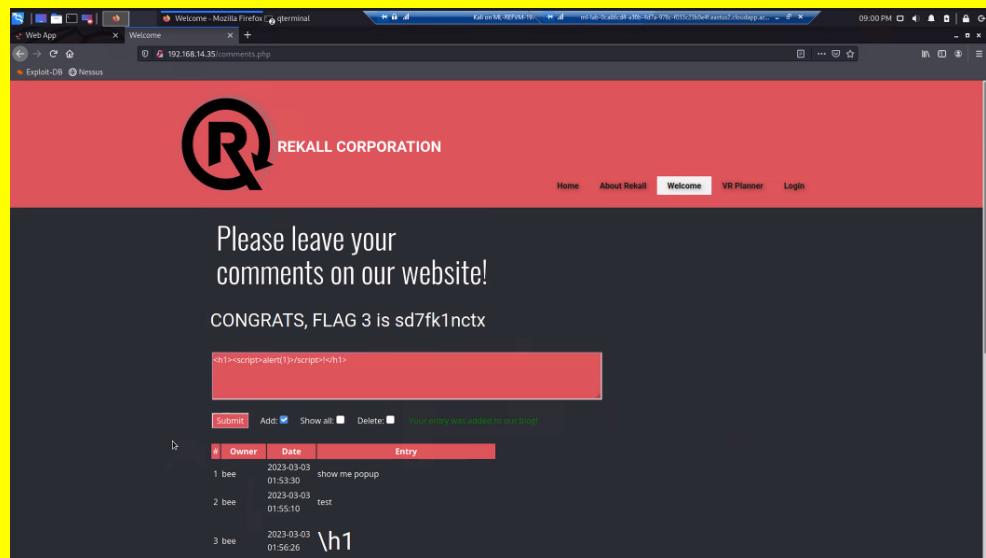
Exploitation Risk	Total
Critical	12
High	2
Medium	4
Low	2

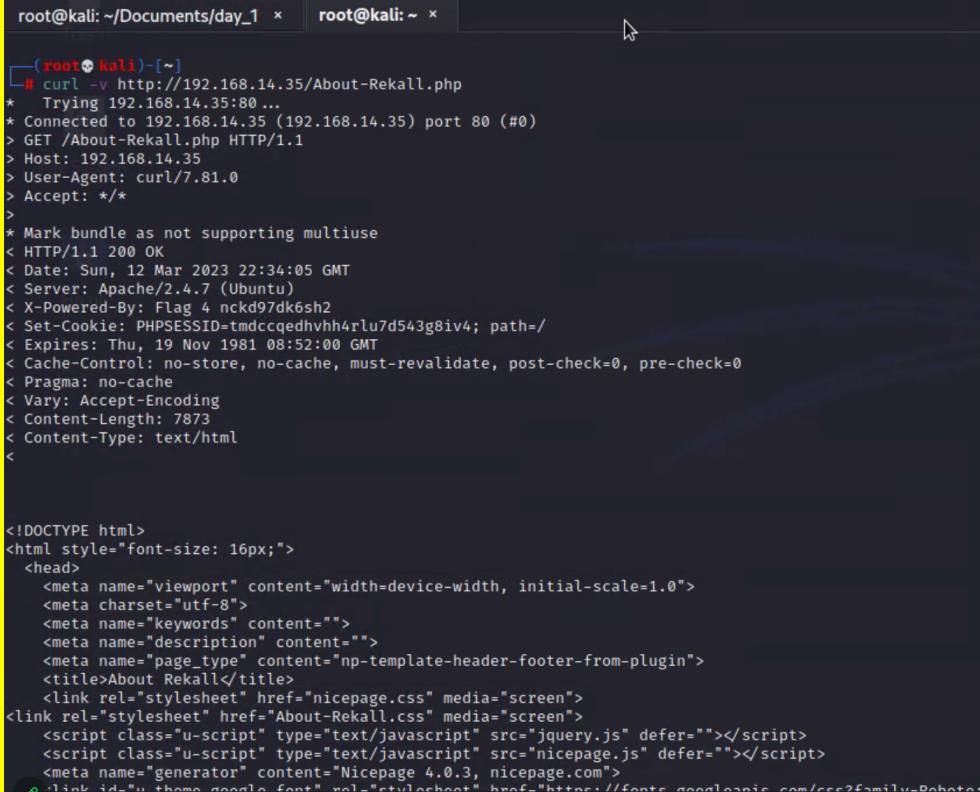
Vulnerability Findings

Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Cross-site scripting is when an attacker injects malicious code into a website that is then executed on a victim's browser. <script>alert(1)</script> was the script used.
Images	 <p>The screenshot shows a Firefox browser window with the URL <code>192.168.14.35/Welcome.php?payload=<script>alert(1)</script></code>. The page displays the Rekall Corporation logo and a red header bar. Below the header, there is a message about designing a virtual reality experience. A search bar contains the injected payload. To the right, there are sections for 'Adventure Planning' and 'Location Choices' with descriptions and icons. At the bottom, a red button says 'CLICK HERE TO START PLANNING'.</p>
Affected Hosts	192.168.14.35
Remediation	User input sanitizing

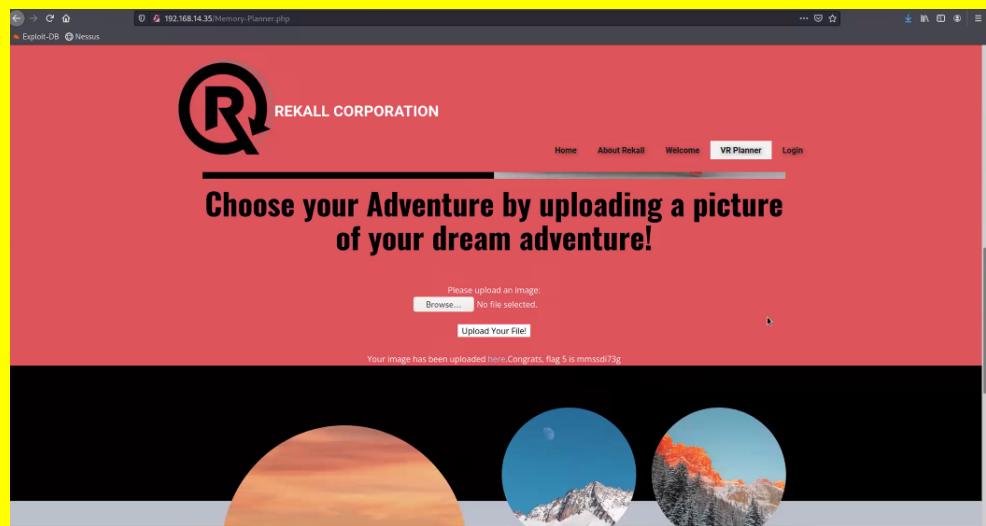
Vulnerability 2	Findings
Title	Reflective XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Most commonly found through links, this attack occurs when a script is 'reflected' off a web app to a victim's browser
Images	 A screenshot of a web browser window. The address bar shows '192.168.14.35/Memory_Planner'. The main content area displays the Rekall Corporation homepage with a large 'Who do you want to be?' question. Below it, there is a form field containing the payload '<SCRIPT>alert()</SCRIPT>' and a 'GO' button. A message below the button says 'You have chosen alert(), great choice!'. At the bottom of the page, a footer message reads 'Congrats, flag 2 is ksdnd99ekas'.
Affected Hosts	192.168.14.35
Remediation	Reflective XSS is difficult to remedy fully, but you can protect yourself similarly to stored XSS by sanitizing against impactful inputs

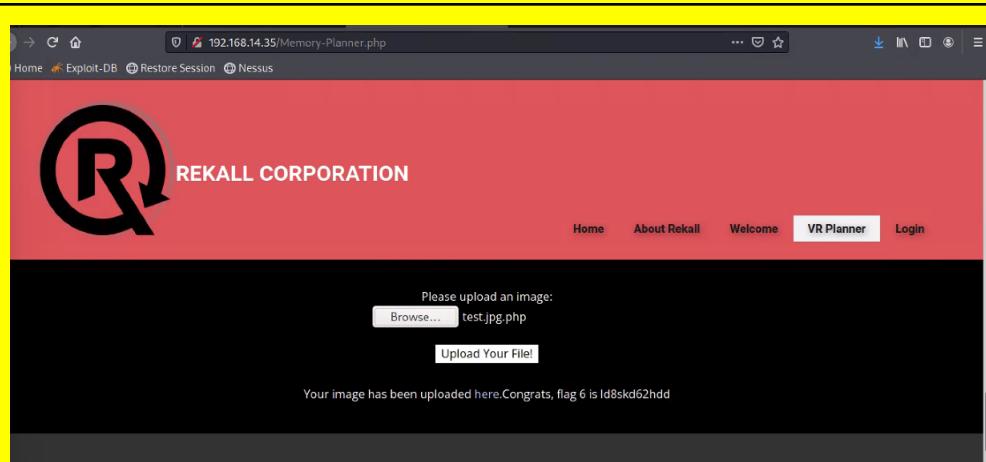
Vulnerability 3	Findings
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Stored XSS is potentially more dangerous than Reflective because the inputs are stored in the targets server

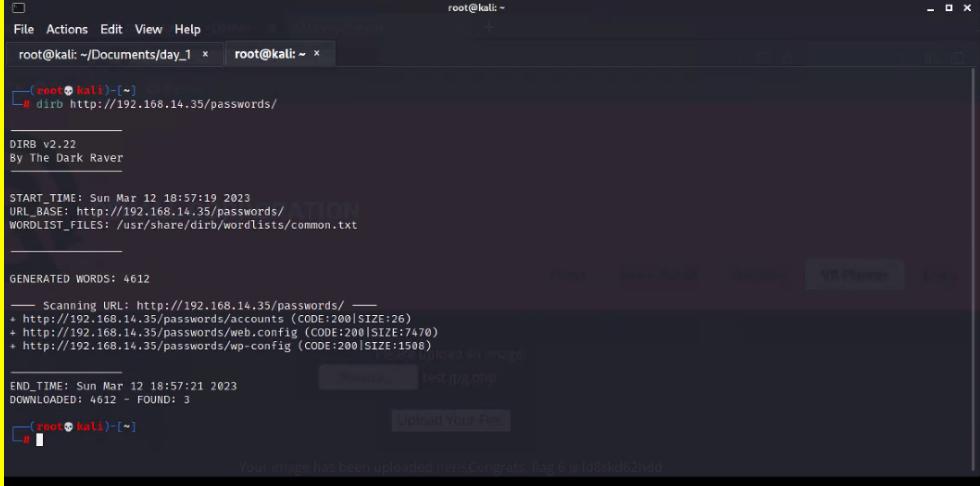
Images	 <p>The screenshot shows a web browser window with the title "Welcome - Mozilla Firefox". The address bar indicates the URL is 192.168.14.35/comments.php. The page has a red header with the "REKALL CORPORATION" logo. Below the header, there is a message: "Please leave your comments on our website!" followed by "CONGRATS, FLAG 3 is sd7fk1nctx". A red box highlights a comment entry from user "3 bee" at 01:56:26 which contains the payload "<h1><script>alert()</script></h1>". Below the comment form, there is a table with columns: #, Owner, Date, and Entry. The table shows three entries:</p> <table border="1"><thead><tr><th>#</th><th>Owner</th><th>Date</th><th>Entry</th></tr></thead><tbody><tr><td>1</td><td>bee</td><td>2023-03-03 01:53:30</td><td>show me popup</td></tr><tr><td>2</td><td>bee</td><td>2023-03-03 01:55:10</td><td>test</td></tr><tr><td>3</td><td>bee</td><td>2023-03-03 01:56:26</td><td>\h1</td></tr></tbody></table>	#	Owner	Date	Entry	1	bee	2023-03-03 01:53:30	show me popup	2	bee	2023-03-03 01:55:10	test	3	bee	2023-03-03 01:56:26	\h1
#	Owner	Date	Entry														
1	bee	2023-03-03 01:53:30	show me popup														
2	bee	2023-03-03 01:55:10	test														
3	bee	2023-03-03 01:56:26	\h1														
Affected Hosts	192.168.14.35																
Remediation	WAF can be used in a Stored XSS attack because it can filter traffic in the app.																

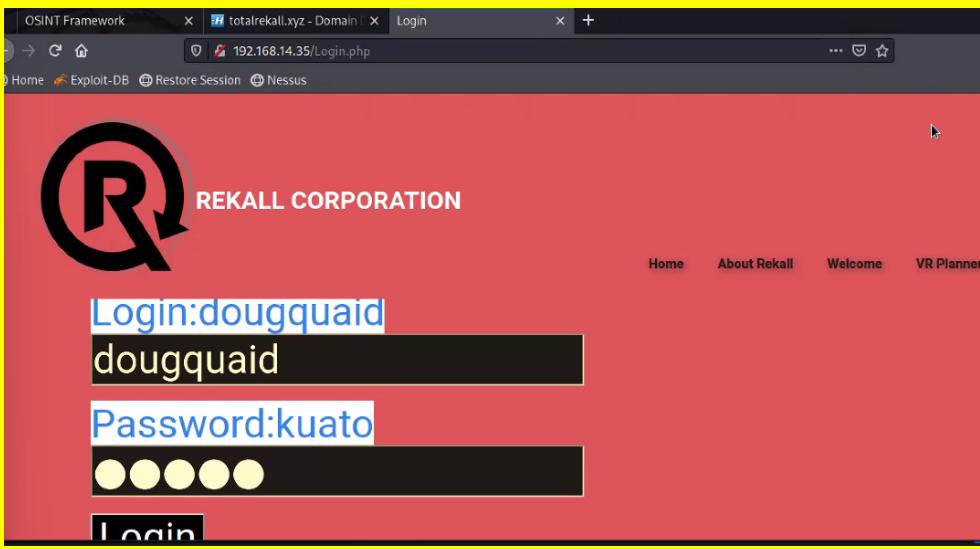
Vulnerability 4	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Using cURL, we were able to find sensitive data in plaintext format
Images	
Affected Hosts	192.168.14.35
Remediation	Encrypt sensitive data such as hashes, keys, and any other data that should not be viewed by those without credentials for viewing.

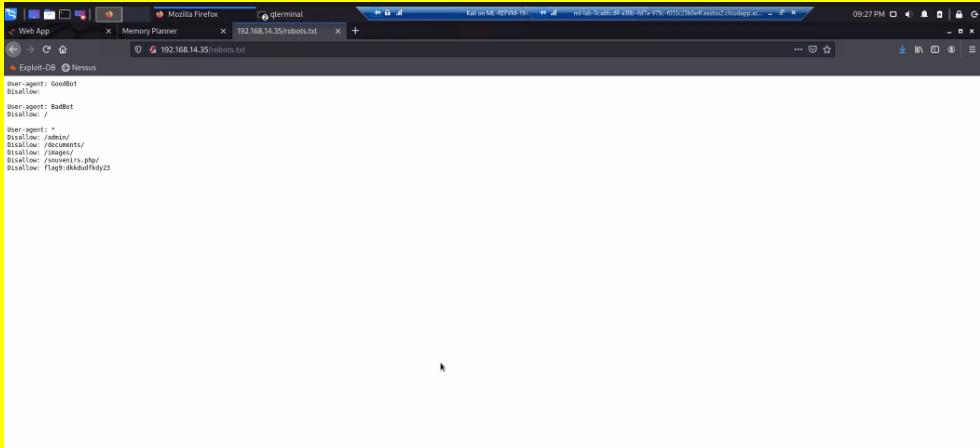
Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	An attack includes a path or hidden value in an input field. We were able to upload a malicious script by adding .jpg to make it appear as an image.

Images	 <p>The screenshot shows a web browser window for '192.168.14.35/Memory-Planner.php'. The header features the 'REKALL CORPORATION' logo and navigation links for Home, About Rekall, Welcome, VR Planner (which is highlighted in blue), and Login. Below the header, a large red banner displays the text 'Choose your Adventure by uploading a picture of your dream adventure!'. A file upload form is present with a placeholder 'Please upload an image.' and a 'Browse...' button. The message 'No file selected.' is displayed below the button. An 'Upload Your File!' button is located below the input field. At the bottom of the page, a message says 'Your image has been uploaded here. Congrats, flag 5 is mmssd73g' next to three circular thumbnails of landscapes.</p>
Affected Hosts	192.168.14.35
Remediation	Only allow images to be submitted to the field.

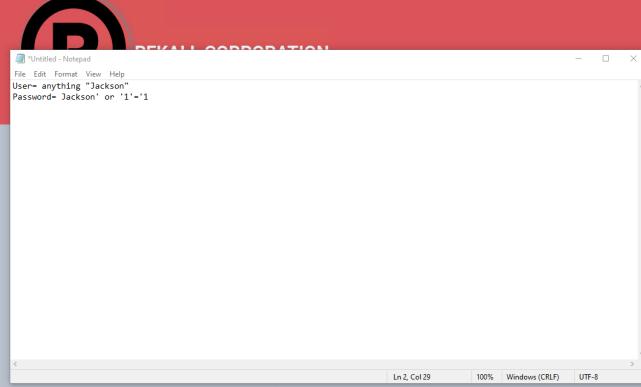
Vulnerability 6	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Similar to before, but because it was a .php page, we simply bypassed the parameter by including .php in the file upload.
Images	 <p>The screenshot shows a web browser window for '192.168.14.35/Memory-Planner.php'. The header features the 'REKALL CORPORATION' logo and navigation links for Home, Exploit-DB, Restore Session, and Nessus. Below the header, a large red banner displays the text 'Choose your Adventure by uploading a picture of your dream adventure!'. A file upload form is present with a placeholder 'Please upload an image.' and a 'Browse...' button. The message 'test.jpg.php' is displayed in the input field. An 'Upload Your File!' button is located below the input field. At the bottom of the page, a message says 'Your image has been uploaded here. Congrats, flag 6 is ld8skd62hdd'.</p>
Affected Hosts	192.168.14.35
Remediation	Strengthen the parameters to only allow certain files to be uploaded

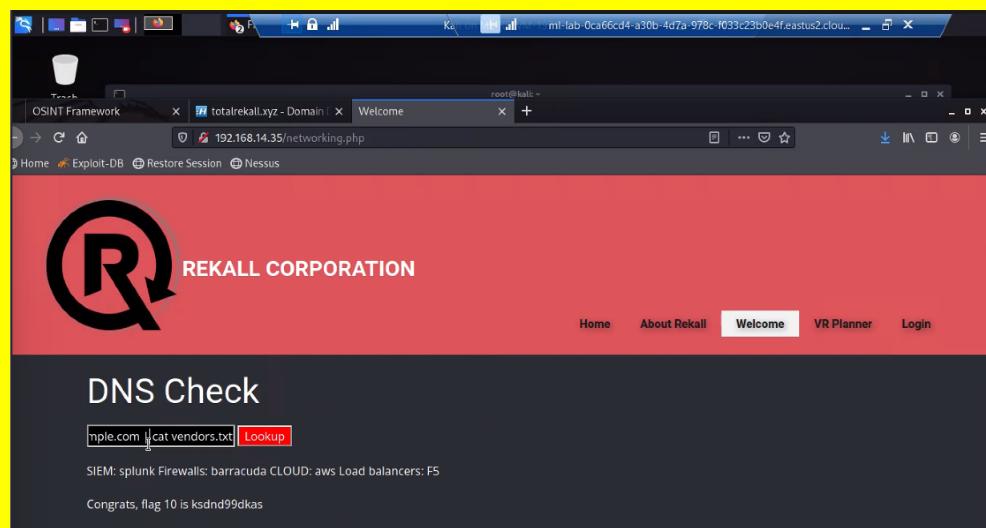
Vulnerability 7	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	We were able to use Dirb and locate a passwords directory. After cURLing, we found credentials for Thor and were able to login.
Images	 <p>The terminal output shows the following:</p> <pre> File Actions Edit View Help root@kali: ~/Documents/day_1 × root@kali: ~ × [root@kali ~]# dirb http://192.168.14.35/passwords/ DIRB v2.22 By The Dark Raver START_TIME: Sun Mar 12 18:57:19 2023 URL_BASE: http://192.168.14.35/passwords/ WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt GENERATED WORDS: 4612 Scanning URL: http://192.168.14.35/passwords/ + http://192.168.14.35/passwords/accounts (CODE:200 SIZE:26) + http://192.168.14.35/passwords/wp-config (CODE:200 SIZE:7470) + http://192.168.14.35/passwords/wp-config (CODE:200 SIZE:1508) END_TIME: Sun Mar 12 18:57:21 2023 DOWNLOADED: 4612 - FOUND: 3 [root@kali ~]# </pre> <p>Your image has been uploaded here. Congrats, flag 6 is id8skd62hdd</p>
Affected Hosts	192.168.14.35
Remediation	A web application firewall can be used to keep the HTML secure

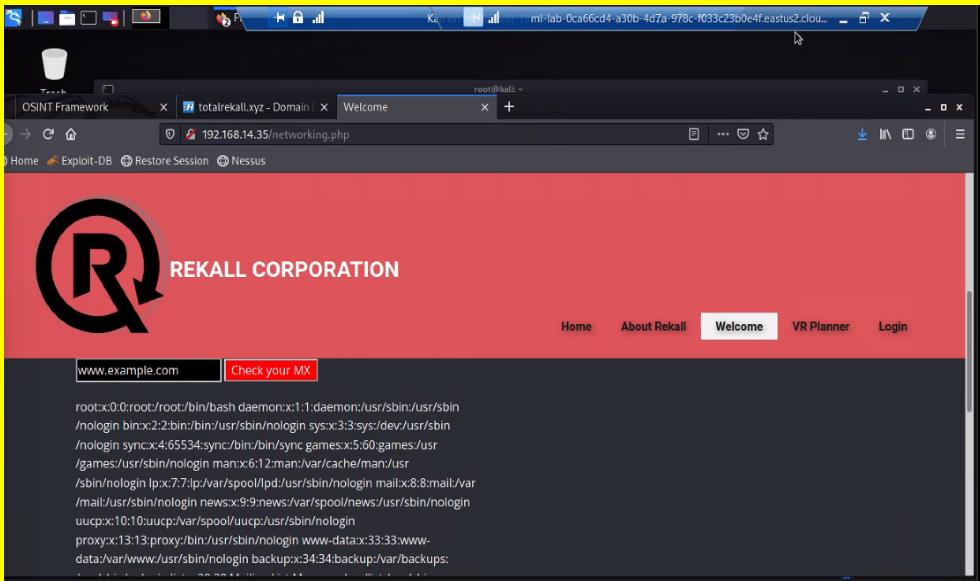
Vulnerability 8	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Password/Username hidden in the HTML lines
Images	
Affected Hosts	192.168.14.35
Remediation	Keep user and password credentials stored in a secure encrypted location.

Vulnerability 9	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Located the robots.txt directory on the web app by searching through the URL
Images	
Affected Hosts	192.168.14.35
Remediation	Refrain from using the robots.txt to hide information from search results

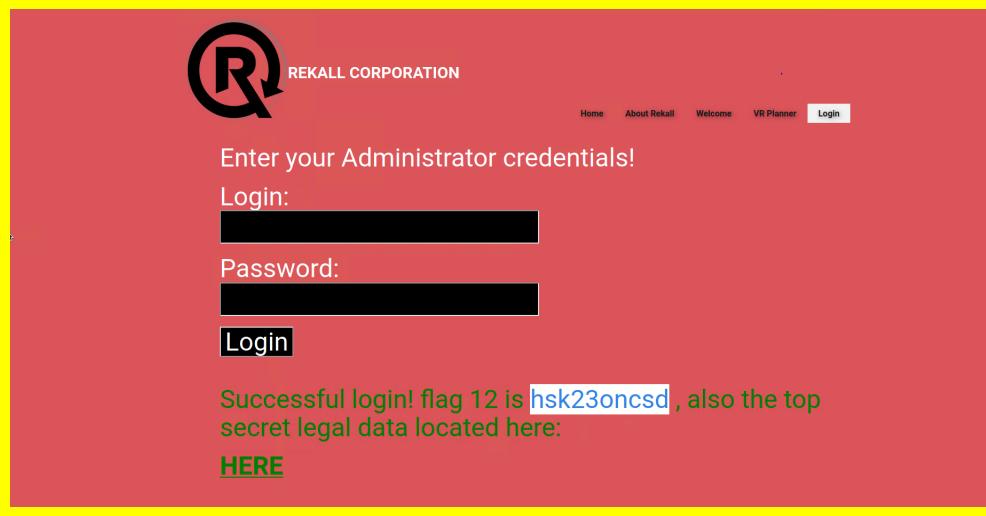
Vulnerability 10	Findings
Title	Command injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Using a SQL injection in the password field to make the password used 'true'

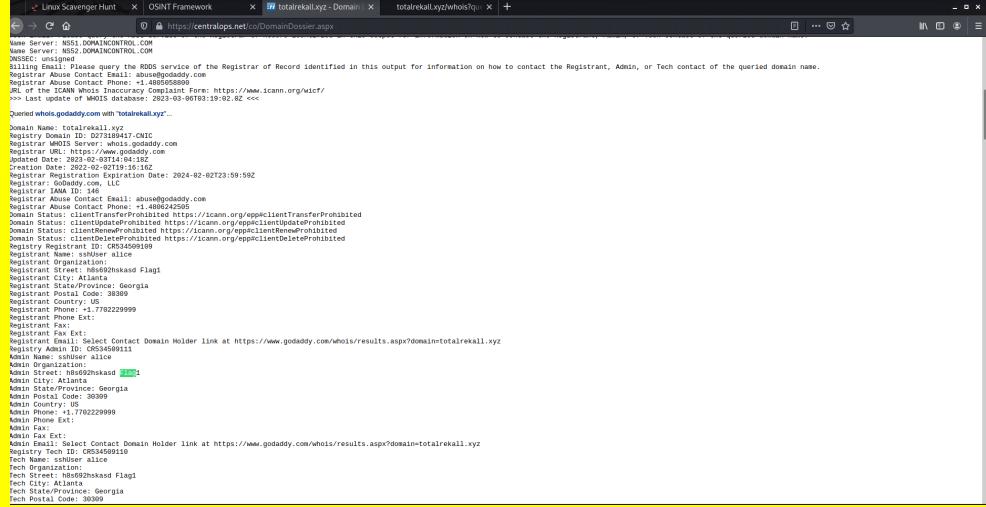
Images	
Affected Hosts	192.168.14.35
Remediation	Input validation/sanitization

Vulnerability 11	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	In the DNS Check field, we were able to use simple Command injections to locate the secret vendors.txt file
Images	
Affected Hosts	192.168.14.35
Remediation	Sanitizing as always the input and parameterized queries as well as whitelisting and using a WAF.

Vulnerability 12	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	In the MX field, we were able to do something similar by searching the /etc/passwd file by modifying the command injection
Images	 A screenshot of a browser window showing a command injection exploit. The URL is 192.168.14.35/networking.php. The page displays a list of users from the /etc/passwd file. A red box highlights the user 'root' entry: root:x:0:0:root:/root:/bin/bash. Below the list is a command-line interface showing the output of the command 'cat /etc/passwd'. The output includes the root password 'root:password'. The browser interface shows tabs for 'OSINT Framework', 'totalrekall.xyz - Domain', and 'Welcome'.
Affected Hosts	192.168.14.35
Remediation	Sanitizing as always the input and parameterized queries as well as whitelisting and using a WAF.

Vulnerability 13	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	By searching the /etc/passwd in the previous vulnerability, we were able to find a user 'Melina'. By using brute force techniques, we found the password was also 'Melina'.

Images	
Affected Hosts	192.168.14.35
Remediation	Enforce stricter passwords in the company. Brute force attacks can take years at a time with stronger passwords with required special characters.

Vulnerability 14	Findings
Title	Open Source Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	By searching OSNIT, we were able to pull sensitive 'WHOIS' company data
Images	
Affected Hosts	Totalrecall.xyz
Remediation	Important data or information should never be stored in plaintext, key encryptions can prevent this information from being leaked or obtained by attackers

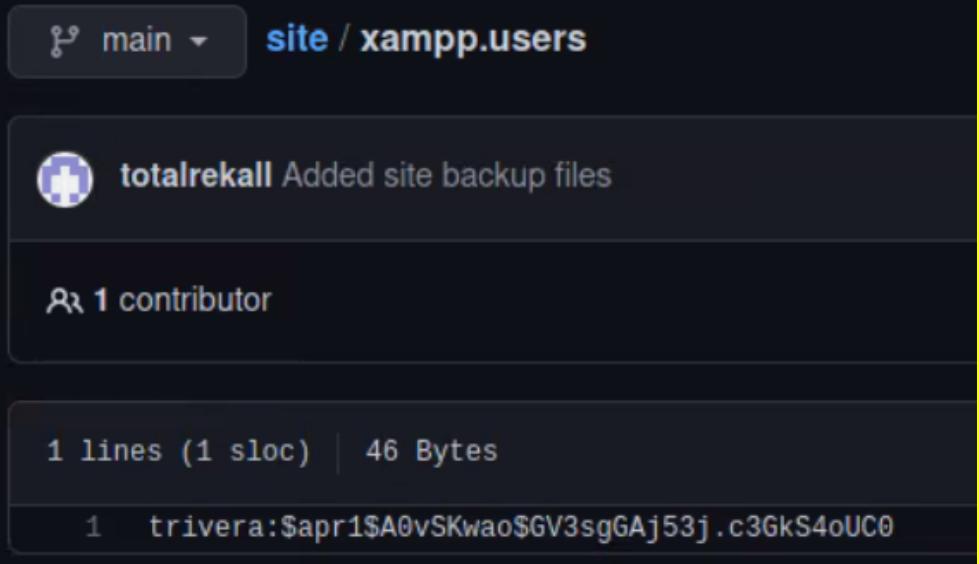
Vulnerability 15	Findings
Title	Domain Ping
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Pinging isn't bad and is a useful tool to see if the server is responding, but can be used in a DDOS attack on the server as well
Images	<pre> LAPTOP-[REDACTED] MINGW64 ~ \$ ping totalrekall.xyz Pinging totalrekall.xyz [34.102.136.180] with 32 bytes of data: Reply from 34.102.136.180: bytes=32 time=17ms TTL=115 Reply from 34.102.136.180: bytes=32 time=14ms TTL=115 Reply from 34.102.136.180: bytes=32 time=17ms TTL=115 Reply from 34.102.136.180: bytes=32 time=14ms TTL=115 Ping statistics for 34.102.136.180: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 14ms, Maximum = 17ms, Average = 15ms </pre>
Affected Hosts	Totalrekall.xyz
Remediation	Having strong firewalls in place to help filter what data comes into the server can help prevent a DOS attack. Load balancers also help strengthen the server.

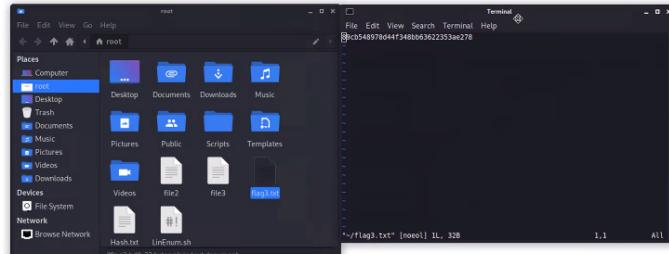
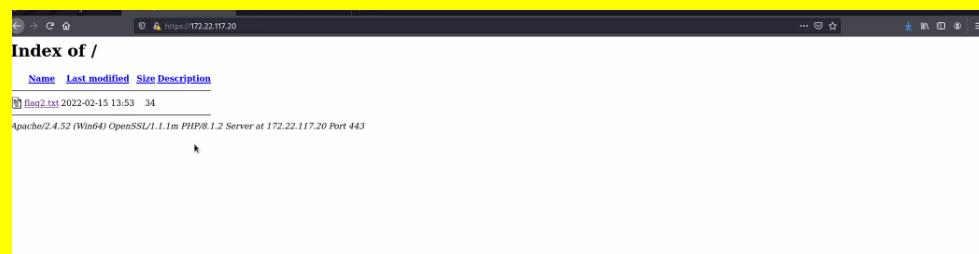
Vulnerability 16	Findings																																				
Title	Open Source Vulnerability																																				
Type (Web app / Linux OS / Windows OS)	Linux OS																																				
Risk Rating	Low																																				
Description	Searched on Cert.sh to pull the certificates for totalrekall.xyz																																				
Images	<p>The screenshot shows the crt.sh Identity Search interface. The search term 'totalrekall.xyz' is entered. The results table displays five certificates:</p> <table border="1"> <thead> <tr> <th>Certificates</th> <th>certah ID</th> <th>Logged At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching identities</th> <th>Issuer Name</th> </tr> </thead> <tbody> <tr> <td>6095738637</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag37rewind totalrekall.xyz</td> <td>flag37rewind totalrekall.xyz</td> <td>CNAME, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>6095204433</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>CNAME, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>6095204133</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>CNAME, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td>www.totalrekall.xyz</td> <td>www.totalrekall.xyz</td> <td></td> </tr> </tbody> </table>	Certificates	certah ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name	6095738637	2022-02-02	2022-02-02	2022-05-03	flag37rewind totalrekall.xyz	flag37rewind totalrekall.xyz	CNAME, CN=ZeroSSL RSA Domain Secure Site CA	6095204433	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	CNAME, CN=ZeroSSL RSA Domain Secure Site CA	6095204133	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	CNAME, CN=ZeroSSL RSA Domain Secure Site CA					www.totalrekall.xyz	www.totalrekall.xyz	
Certificates	certah ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name																														
6095738637	2022-02-02	2022-02-02	2022-05-03	flag37rewind totalrekall.xyz	flag37rewind totalrekall.xyz	CNAME, CN=ZeroSSL RSA Domain Secure Site CA																															
6095204433	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	CNAME, CN=ZeroSSL RSA Domain Secure Site CA																															
6095204133	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	CNAME, CN=ZeroSSL RSA Domain Secure Site CA																															
				www.totalrekall.xyz	www.totalrekall.xyz																																

Affected Hosts	Totalrecall.xyz
Remediation	Stronger firewalls and multiple encryption methods can be used to keep this open source information from harming the company.

Vulnerability 17	Findings
Title	Network Maping
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	The scan itself isn't a vulnerability, however weaknesses can be found with these Nmap scans such as open hosts and ports and
Images	<pre># nmap 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-03-15 19:19 EDT Nmap scan report for 192.168.13.10 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 3009/tcp open ajp13 3080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000080s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 3080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 30/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up (0.0000070s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE</pre>
Affected Hosts	192.168.13.0/24 192.168.13.10 192.168.13.11

	192.168.13.12 192.168.13.13 192.168.13.14 192.169.13.1
Remediation	Strong firewalls that can limit the rate at which a server can be pinged and making sure that exploitable ports are closed when not in use

Vulnerability 18	Findings																											
Title	Exposed Sensitive Data																											
Type (Web app / Linux OS / Windows OS)	Linux OS																											
Risk Rating	Critical																											
Description	C4 found a Github repository containing HTML code and login credentials																											
Images	 <p>The screenshot shows a GitHub repository page for a user named 'totalrecall'. The repository name is 'xampp.users'. It has 1 contributor. The file 'xampp.users' contains 1 line of code (1 sloc) and 46 bytes. The code itself is obfuscated: <code>1 trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0</code>. Below the file listing, there is a table of contents for the repository.</p> <table border="1"> <thead> <tr> <th></th> <th>Added site backup files</th> <th>last year</th> </tr> </thead> <tbody> <tr> <td>assets</td> <td>Added site backup files</td> <td>last year</td> </tr> <tr> <td>old-site</td> <td>Added site backup files</td> <td>last year</td> </tr> <tr> <td>README.md</td> <td>Update README.md</td> <td>last year</td> </tr> <tr> <td>about.html</td> <td>Added site backup files</td> <td>last year</td> </tr> <tr> <td>contact.html</td> <td>Added site backup files</td> <td>last year</td> </tr> <tr> <td>index.html</td> <td>Added site backup files</td> <td>last year</td> </tr> <tr> <td>robots.txt</td> <td>Added site backup files</td> <td>last year</td> </tr> <tr> <td>xampp.users</td> <td>Added site backup files</td> <td>last year</td> </tr> </tbody> </table>		Added site backup files	last year	assets	Added site backup files	last year	old-site	Added site backup files	last year	README.md	Update README.md	last year	about.html	Added site backup files	last year	contact.html	Added site backup files	last year	index.html	Added site backup files	last year	robots.txt	Added site backup files	last year	xampp.users	Added site backup files	last year
	Added site backup files	last year																										
assets	Added site backup files	last year																										
old-site	Added site backup files	last year																										
README.md	Update README.md	last year																										
about.html	Added site backup files	last year																										
contact.html	Added site backup files	last year																										
index.html	Added site backup files	last year																										
robots.txt	Added site backup files	last year																										
xampp.users	Added site backup files	last year																										
Affected Hosts	Totalrecall.xyz																											
Remediation	Having a stronger firewall implement rate limiting, only allowing X amount of pings to be sent.																											

Vulnerability 19	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Windows
Risk Rating	Critical
Description	Using credentials found in the Github repository to log in the server.
Images	 
Affected Hosts	172.22.117.0/24 172.22.117.10 172.22.117.20
Remediation	Do not post sensitive information on websites that are open source.

Vulnerability 20	Findings
Title	FTP port 21

Type (Web app / Linux OS / Windows OS)	Windows
Risk Rating	Critical
Description	FTP port 21 anonymous login enabled
Images	<pre>(root㉿kali)-[~/Desktop] └─# 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> flag3.txt ?Invalid command ftp> cat flag3.txt ?Invalid command ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (46.1595 kB/s) ftp> exit 221 Goodbye</pre> <pre>└─# nmap -A 172.22.117.20 Starting Nmap 7.92 (https://nmap.org) at 2023-01-11 21:45 Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00079s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp FileZilla ftppd 0.9.41 beta _ ftp-anon: Anonymous FTP login allowed (FTP code 230) _ _r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt _ ftp-bounce: bounce working! _ ftp-syst: SYST: UNIX emulated by FileZilla 25/tcp open smtp SLmail smtpd 5.5.0.4433 _ smtp-commands: rekall.local, SIZE 100000000, SEND, SOML _ This server supports the following commands. HELO MAIL 79/tcp open finger SLMail fingerd _ finger: Finger online user list request denied.\x0D</pre>
Affected Hosts	172.22.117.20

Remediation	Close port 21. Only use FTP when urgently necessary. Disable anonymous login
--------------------	--

Read Me:

This project was done in a group with John Wallace, and Tracy Skelton. We all contributed input on screenshots, remediation, and tactics.