| Cybersecurity |
| --- |
| Penetration Test Report |

Rekall Corporation

Penetration Test Report

**Student Note: Complete all sections highlighted in yellow.**

# 

## Confidentiality Statement

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

Table of Contents

[Confidentiality Statement 2](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative](#_4i7ojhp) 10

[Summary Vulnerability Overview 1](#_2xcytpi)3

Vulnerability Findings [1](#_1ci93xb)4

# 

## Contact Information

| **Company Name** | RED |
| --- | --- |
| **Contact Name** | Chris Akatcherian |
| **Contact Title** |  |

## 

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 11/7/2024 | chris akatcherian |  |

# 

## 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:

Chart

Description automatically generated with medium confidence

### 

### 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.

● Certain Web Application input fields were well protected against basic XSS exploits and

required farthing probing

● RED’s did not have success attempting SQL injections against the web page.

● Basic protections were in place in certain areas, making it harder for RED’s to

successfully complete exploits such as Local File inclusion and in some cases XSS scripting.

● Many input fields had proper input validation

### Summary of Weaknesses

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

● Web app is vulnerable to several attacks including XSS scripting, Local File inclusion, and

command injections leaving vulnerable data to be easily accessed by a threat actor, as well

as the potential to upload malicious scripts to be stored on the Rekall’s servers.

● Linux and Windows machines were both found to have several cases of sensitive data

exposure, leaving important information easily accessible to threat actors that may have

compromised the system.

● Several open ports were discovered with basic nmap scans, revealing potential

vulnerabilities throughout Rekall’s network.

● Old vulnerabilities were found on the Windows and Linux machines, including Shellshock,

SLMail pop3d, and Apache T omcat Remote Code Execution.

● Open source intelligence tools revealed information such as the ‘WHOIS’ data that could be

used by adversaries to further scan the network and discover vulnerabilities

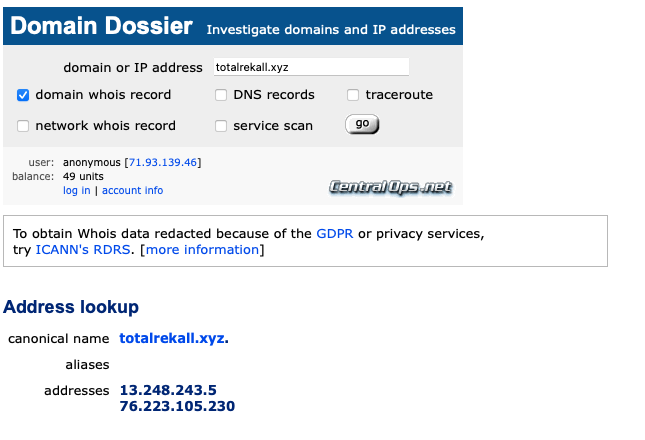
● Using kiwi, several important users' credentials were able to be retrieved and their

passwords cracked.

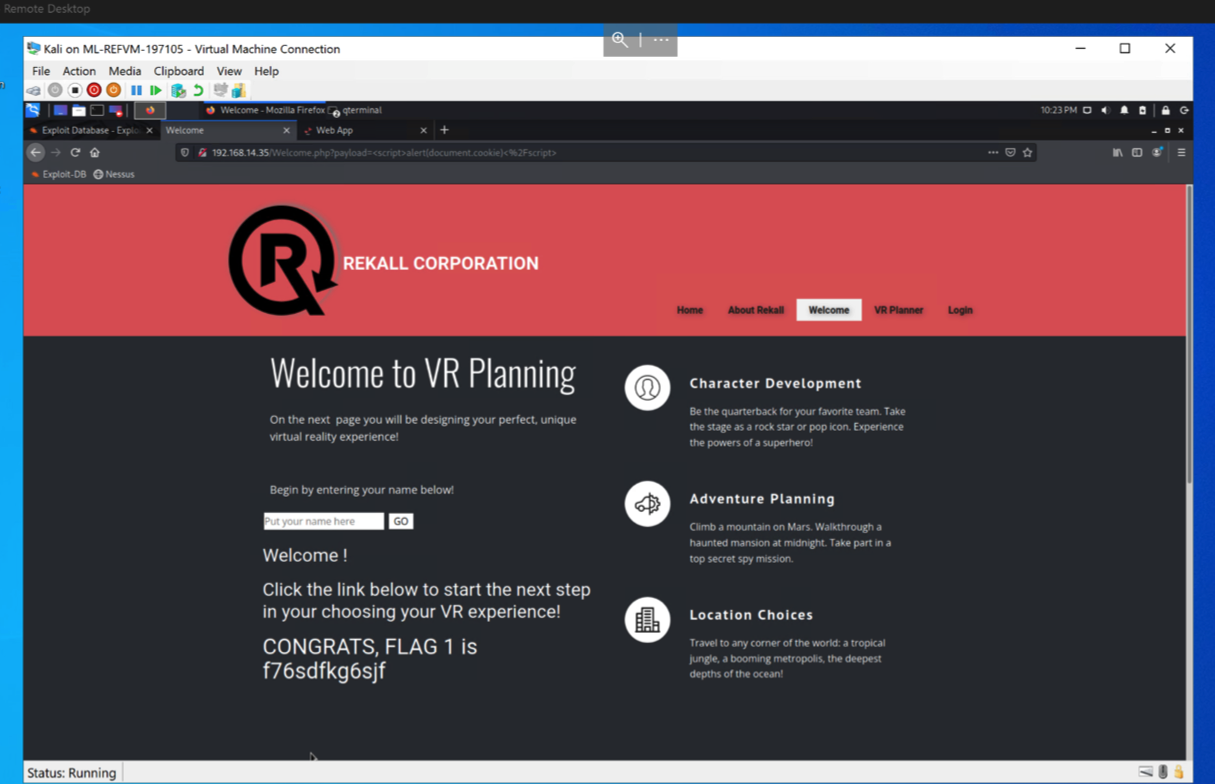
## Executive Summary

Day 1 (Web App)

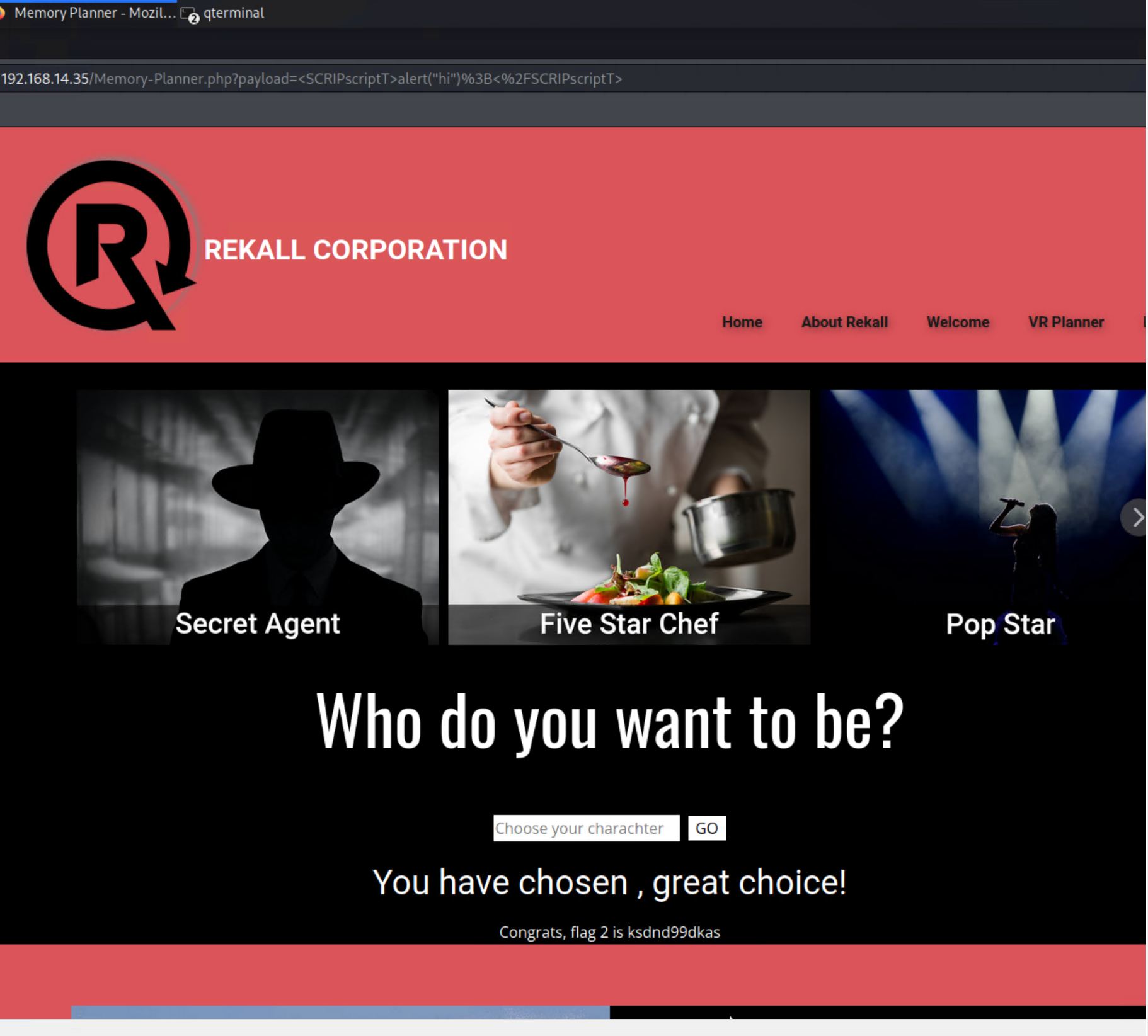
Using an open source Domain Dossier, RED was able to run a domain ‘WHOIS’ record of totalrekall.xyz and found info such as IP Adresses and the canonical name of the web app.



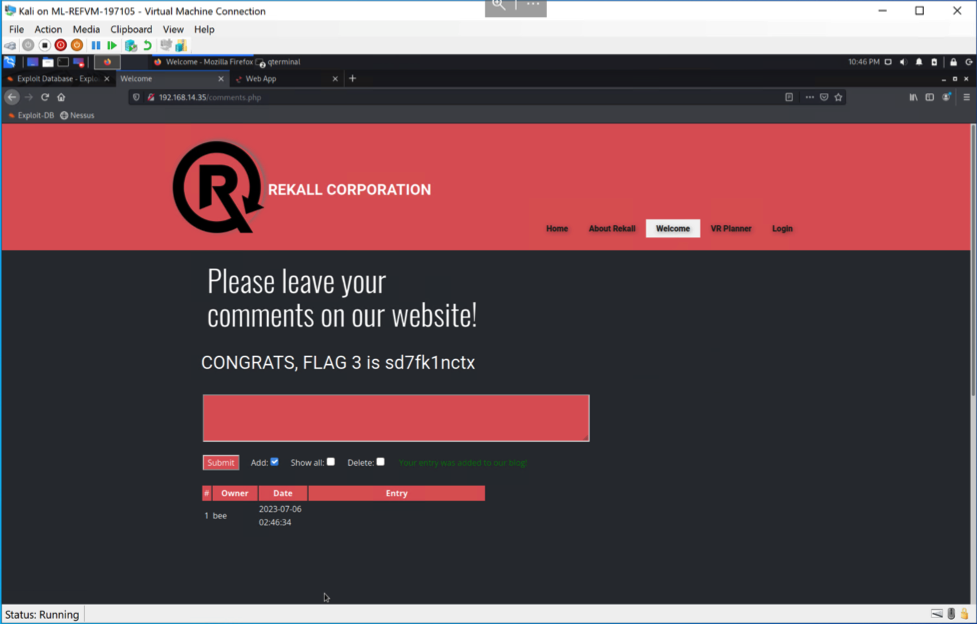
Using this information, RED was able to access the webapp through browser as well as through the command line. We started at the Rekall Corporation ‘Welcome’ page and attempted any XSS (Cross Site Scripting) vulnerabilities that we could find, and assessed that we were successfully create an alert by implementing a reflected XSS script.



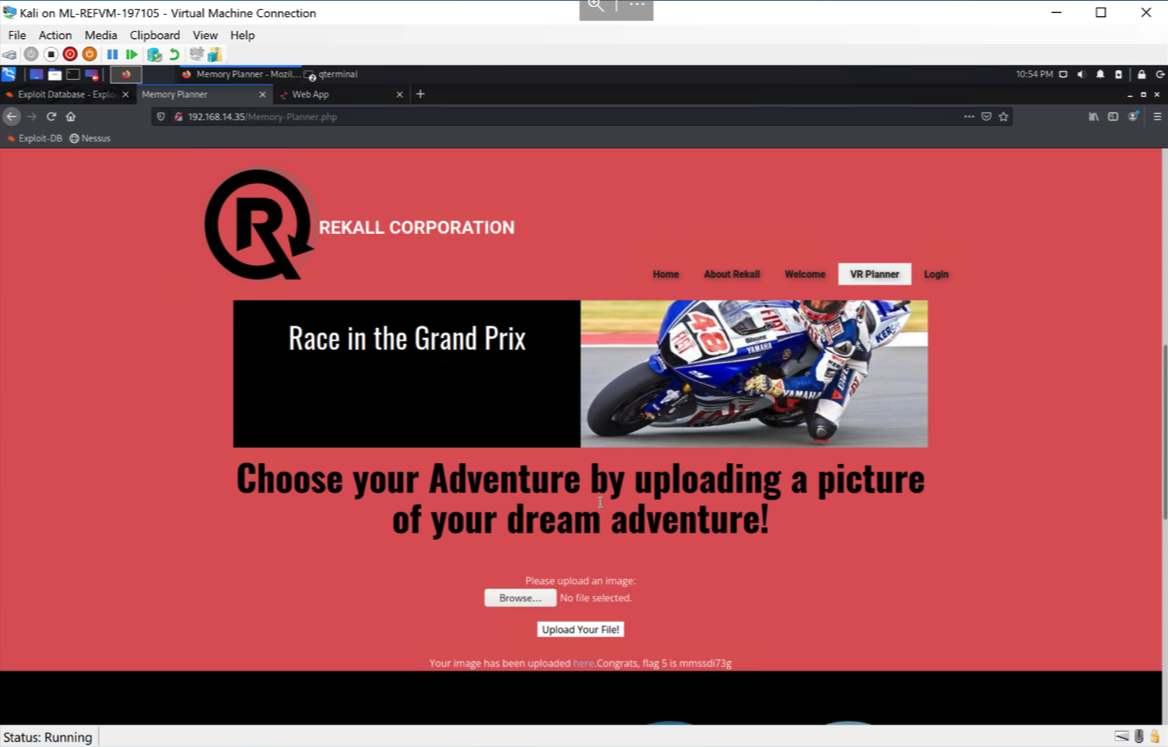
We then looked further on the web page and tried the same tactics (XSS scripts) and found that the exploit was successful as well on the ‘Memory Planner’ page.



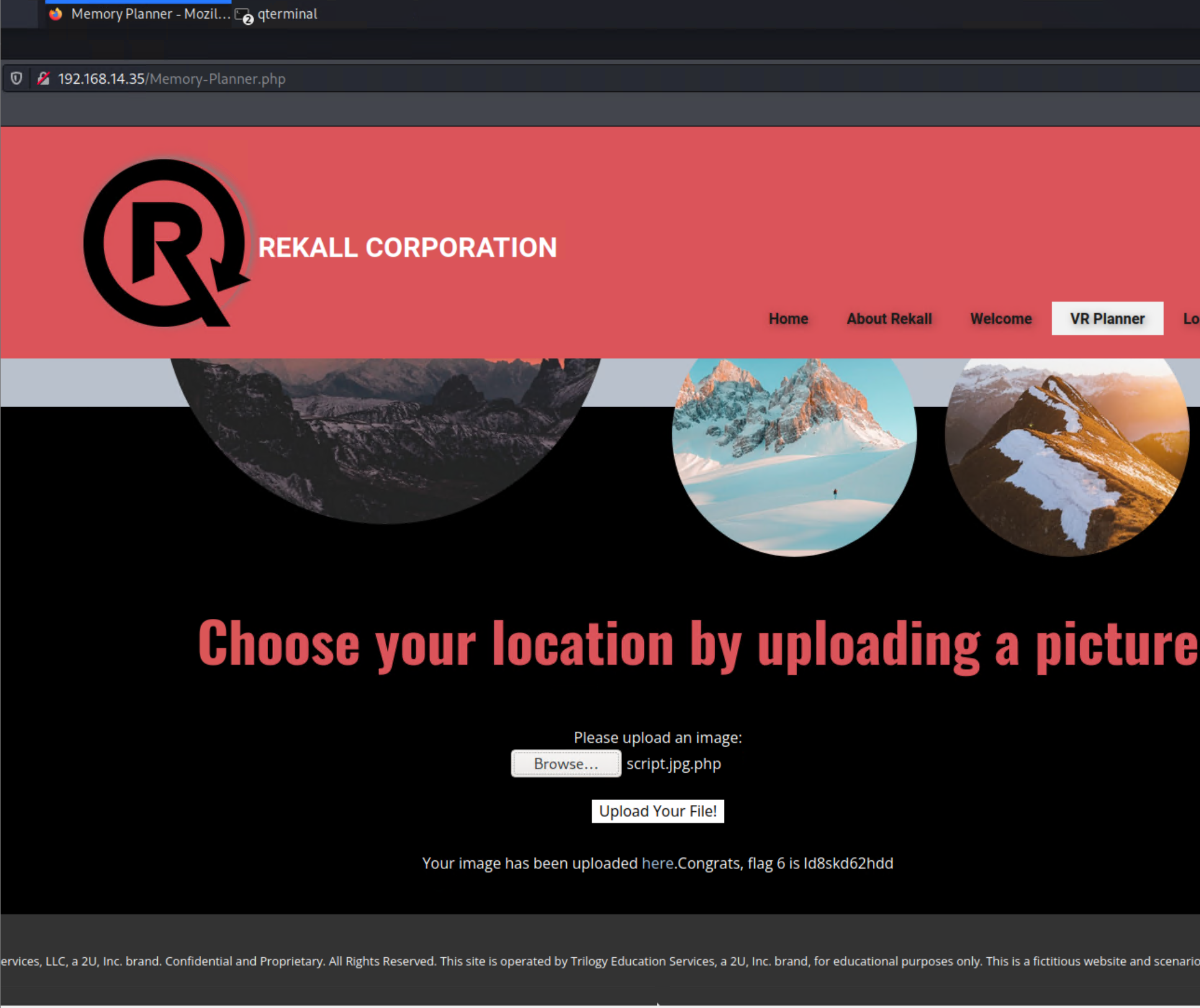
RED was also able to discover another XSS vulnerability within the ‘comments’ section.



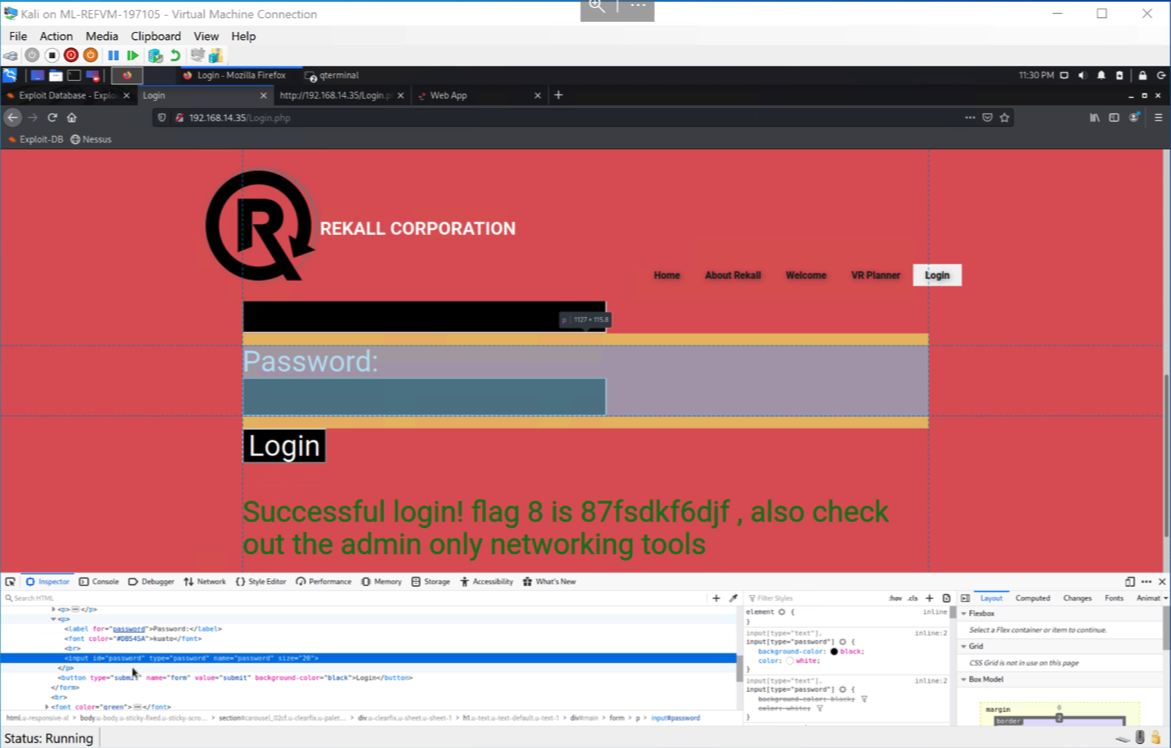
RED then came across a vulnerability within the ‘Memory Planner’ web page that could be used to upload malicious scripts that could go unnoticed. This is a Local File Inclusion Vulnerability.



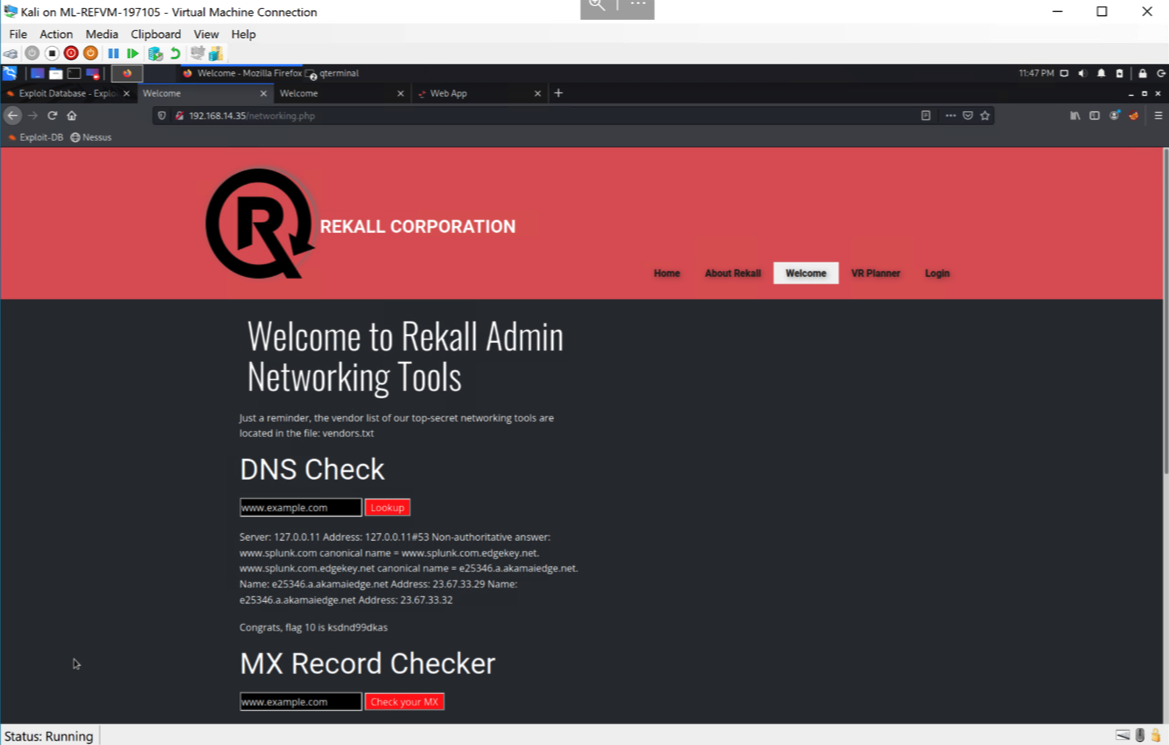
We then cam across another Local File Inclusion vulnerability within the same page. Unlike the last case this upload only allows ‘.jpg’ files. This can be easily bypassed by ending the malicious file with ‘.jpg.php’



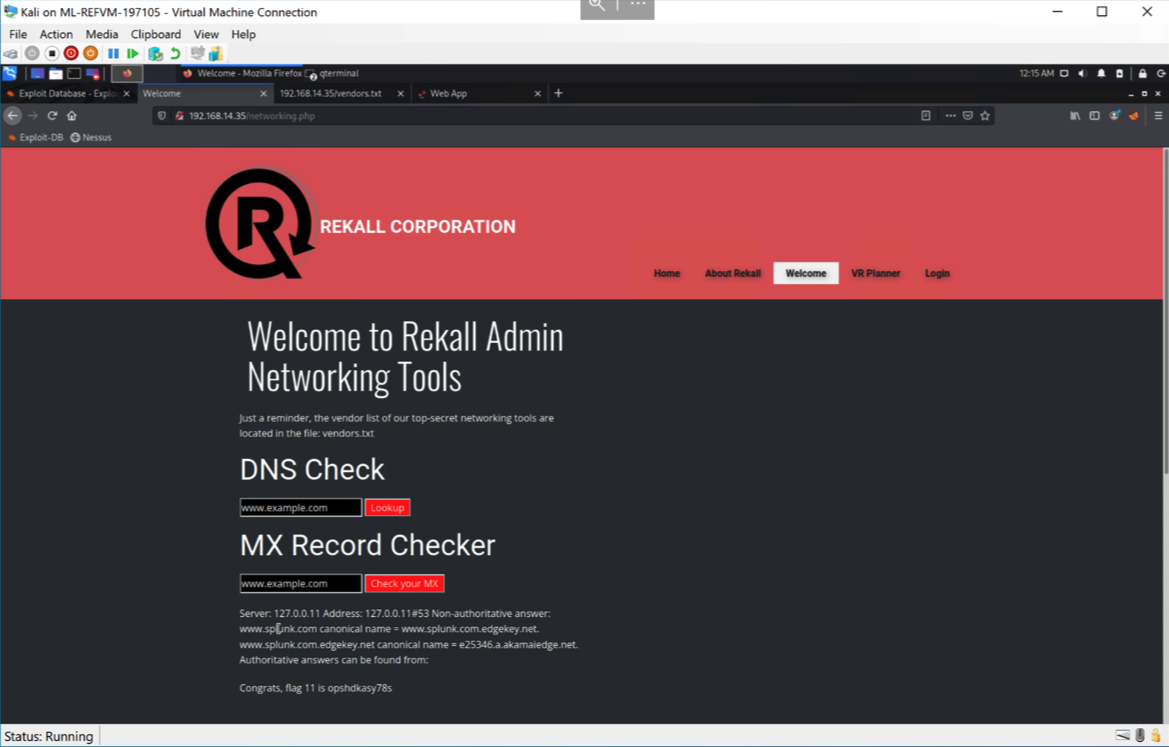
Navigating to the ‘Login.php’ page, RED was also able to discover sensitive data exposure located within the page source of the web page. Located in the page source was the username and Password of a specific user that were valid, allowing us to login.



Moving to the ‘Networking’ web page, RED was able to immediately discover a vulnerability as the web page reveals sensitive information within a ‘vendors.txt’ file containing a top-secret list. We then found there was a command injection vulnerability within the ‘DNS Check’ tool. Using this vulnerability, we were able to display the contents of the ‘vendors.txt’ file.



Just below the DNS check, there is another field called ‘MX Record Checker’ that RED was further able to exploit.



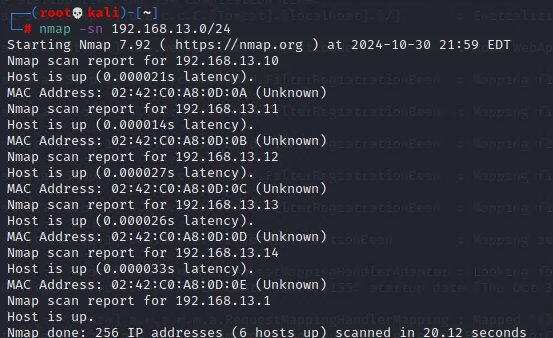
This concludes the findings of RED’s Day 1.

## 

## Day 2 (Linux)

## 

## During our reconnaissance we ran an nmap scan against the target IP Address (192.168.13.0/24) including the subnet /24 to run a scan across 256 host machines. We included the option -A with the scan to run an aggressive scan against the target IP.



## 

## Referring back to the scan, RED was able to run a Nessus scan for one of the machine found and found one critical the vulnerability for Apache Struts

## 

## Again, referring to the scan done earlier, RED’s looked for any vulnerabilities to

## be exploited on the target machine (192.168.13.10) using metasploit. After testing several

## exploits we found that there was an ‘Apache T omcat Remote Code Execution Vulnerability’

## (CVE-2017-12617) and successfully exploited the vulnerability to gain a Meterpreter session.

## 

## 

## 

## Looking at host 192.168.13.11 RED’s noticed there could potentially be a Shellshock

## vulnerability on the machine. RED’s attempted to exploit this vulnerability and found our

## attempt to be successful, resulting in us achieving a shell on the target machine.

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

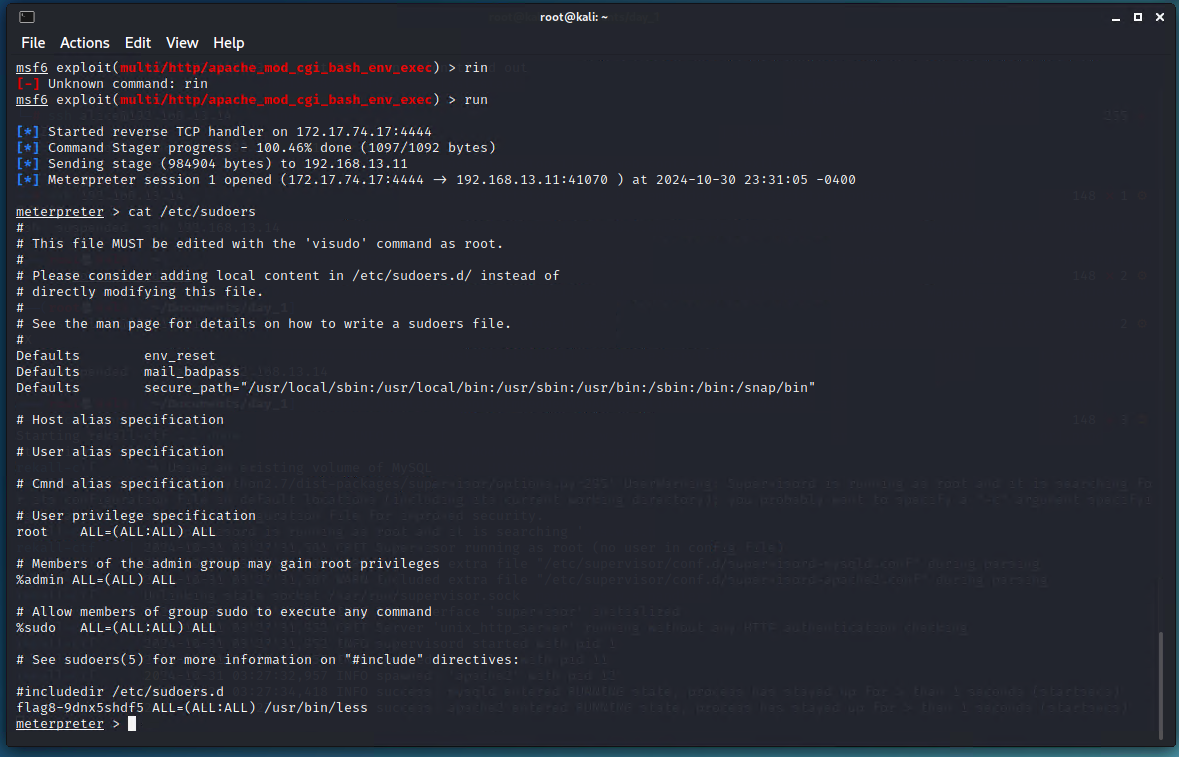
## 

## 

## 

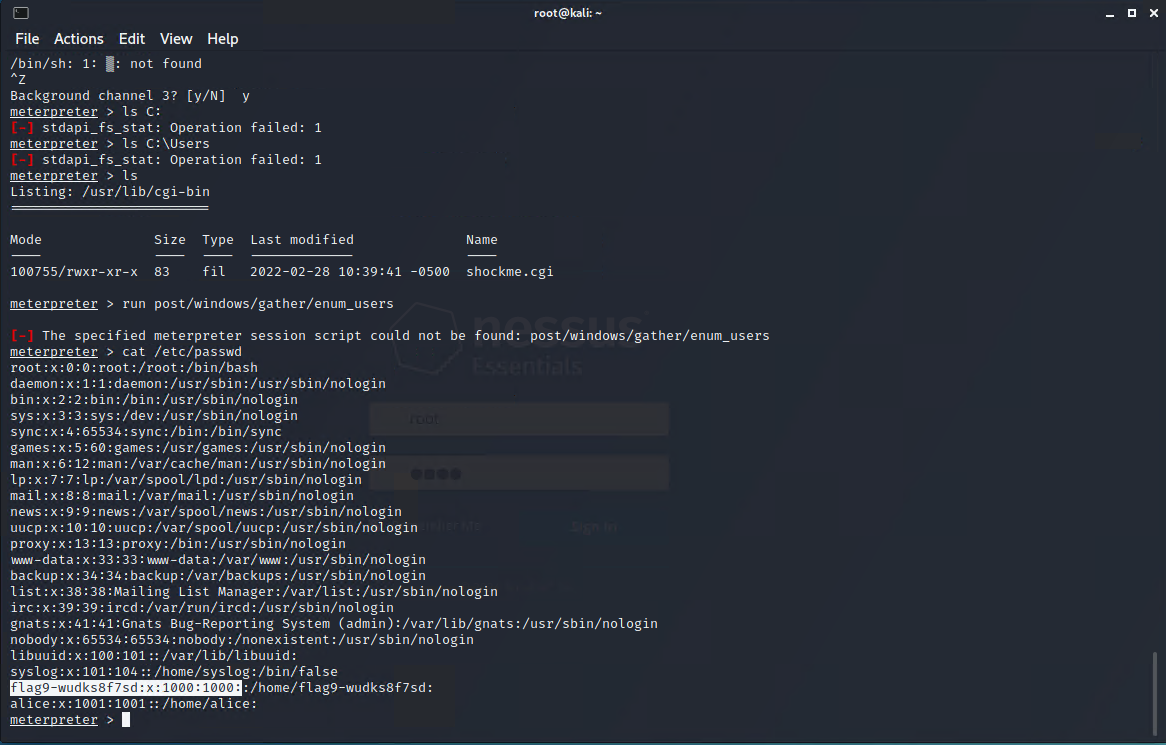
## 

## Evidence of successful Shellshock exploit:



Once inside the target machine (192.168.13.11), RED’s was able to access several

other user’s credentials through the etc/passwd file.



This concludes RED’s findings during day 2 of our testing.

## Day 3 (Windows)

Red began their investigation into Windows testing by investigating the totalrekall github page to discover any information that could help us during our testing. Inside of the github page we discovered a major vulnerability as a username and password hash was stored openly on the github and easily accessible by anybody.

Evidence of sensitive data exposure:

trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0

## 

## 

## After running our nmap scan against the host IP address (172.22.117.20), we discovered an

## open HTTP port on one of the Windows machines. After putting the IP address into a browser

## we were able to successfully connect using the credentials found from the github page

## previously. Inside we found a file named ‘flag2.txt’ and found sensitive data inside.

## 

## Evidence of sensitive data exposure/successful http connection:

## 

## 

## 

## During RED’s initial scan of the network we found that port 21 (FTP) was also open on

## the host IP address 172.22.117.20. After further analyzing we found that anonymous access

## was allowed onto the FTP server. With this discovery, we were able to successfully login

## anonymously to the FTP server.

## 

## 

## 

## RED’s also discovered port 110 open which is used by SLMAIL, as well as what version

## is being run (pop3d). Using this information RED’s used a metasploit exploit to

## successfully connect to the target machine (172.22.117.20) and gain a Meterpreter session.

## Evidence of SLMail pop3d exploit:

## 

## 

## Using the Meterpreter session that was created previously, RED’s was able to open a

## shell and successfully look at scheduled tasks on the host machine, as well as the ability to

## create or delete any tasks that were found.

## Scheduled Tasks exploit:

## 

## 

## 

## RED then backtracked out of the shell and back to the Meterpreter session in order to

## dump the credentials using a tool named ‘Kiwi’. using the command lsa\_dump\_sam, we were

## able to successfully pull many credentials from the system, including usernames and password

## hashes. After attempting to crack these passwords we successfully gained new credentials to

## the user ‘flag6’.

## 

## Evidence of Exploit:

## 

## 

## 

## 

## 

## 

## 

## RED began looking around the host machine (172.22.117.20) to see if there was any

## other sensitive data that could be found. Using the search tool we were able to discover another

## file within the ‘C:\Users\Public\Documents” directory named ‘flag7.txt’.

## Evidence of flag7.txt discovery:

## 

## 

## 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Reflected or Stored XSS Vulnerabilities on Multiple Web Pages | **High** |
| Command injection Vulnerabilities | **High** |
| Sensitive Data Exposure (Windows) | **Critical** |
| Local File Inclusion Vulnerabilities | **Critical** |
| Open Source Data Exposure | **Medium** |
| Apache T omcat Remote Code Execution Vulnerability (CVE-2017-12617) | **Critical** |
| Shellshock Vulnerability (Linux) | **Critical** |
| FTP Anonymous Login | **Critical** |
| Kiwi Credential Dump | **High** |
| Sensitive Data in user ‘C:\Users\Public\Documents’ Directory | **Medium** |
| SLMail pop3d Exploit | **Critical** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.20 192.168.13.10  192.168.13.11 192.168.13.12  192.168.13.13 192.168.13.14  192.168.14.35 |
| Ports | 21, 22, 80, 106, 110 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 6 |
| **High** | 3 |
| **Medium** | 2 |
| **Low** | 0 |

## Vulnerability Findings

| **Vulnerability 1** | **Findings** |
| --- | --- |
| **Title** | Reflected or Stored XSS Vulnerabilities on Multiple Web Pages |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Malicious script was successfully reflected or stored on multiple web pages on  totalrekall.xyz. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | User Input Validation  Escaping user input |

| **Vulnerability 2** | **Findings** |
| --- | --- |
| **Title** | Command injection Vulnerabilities |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | High |
| **Description** | Successfully viewed the contents of ‘vendors.txt’ which contained sensitive  information |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | User input validation  Sensitive information such as ‘vendors.txt’ should not be visible on the web  page to see publicly |

| **Vulnerability 3** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data Exposure (Windows) |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | Sensitive data was able to be collected pertaining to a Rekall’s Windows  machine, including user credentials found on the totalrekall github page that  were used to gain access to the FTP server |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Never leave important information such as user credentials on a github  page accessible to anyone  Restrict access to port 21  Salt Hashes |

| **Vulnerability 4** | **Findings** |
| --- | --- |
| **Title** | Local File Inclusion Vulnerabilities |
| **Type (Web app / Linux OS / WIndows OS)** | Web App |
| **Risk Rating** | Critical |
| **Description** | Successfully uploaded malicious php scripts on multiple sections of the  ‘memory-panner.php’ web page. |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35 |
| **Remediation** | ID Assignation  Do not permit file paths to be appended directly  Dynamic path concatenation |

| **Vulnerability 5** | **Findings** |
| --- | --- |
| **Title** | Open Source Data Exposure |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS  Web App |
| **Risk Rating** | Medium |
| **Description** | Through OSINT tools we successfully compiled information on the target  machine and web page that was useful during our investigation, and could  prove useful to a threat actor. Including the ‘WHOIS’ data of ‘totalrekall.xyz’ |
| **Images** |  |
| **Affected Hosts** | 192.168.14.35  192.168.13.11  192.168.13.12  192.168.13.13 |
| **Remediation** | Ensure no sensitive data is found in WHOIS records  Ensure no sensitive information can be found publicly |

| **Vulnerability 6** | **Findings** |
| --- | --- |
| **Title** | Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Successfully exploited Apache T omcat vulnerability allowing for Remote Code  Execution and retrieving a reverse shell session |
| **Images** |  |
| **Affected Hosts** | 192.168.13.10 |
| **Remediation** | Update to the latest version of Apache Struts |

| **Vulnerability 7** | **Findings** |
| --- | --- |
| **Title** | Shellshock Vulnerability |
| **Type (Web app / Linux OS / WIndows OS)** | Linux OS |
| **Risk Rating** | Critical |
| **Description** | Successfully exploited a Shellshock Vulnerability found on a Linux machine,  resulting in gaining a shell at root level. |
| **Images** |  |
| **Affected Hosts** | 192.168.13.11 |
| **Remediation** | Update to the latest version of bash |

| **Vulnerability 8** | **Findings** |
| --- | --- |
| **Title** | FTP Anonymous Login |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | RED’s found that anonymous login was enabled onto FTP and was  able to successfully connect using the anonymous login. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Disable Anonymous authentication on FTP |

| **Vulnerability 9** | **Findings** |
| --- | --- |
| **Title** | Kiwi Credential Dump |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | High |
| **Description** | After gaining a Meterpreter shell, RED’s successfully dumped many  different user credentials using a tool named ‘kiwi’. Allowing us to crack  another user’s password hash and gain access to another account. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Salt Password hashes  LSAAS Protected Mode  Ensure Windows is up to date |

| **Vulnerability 10** | **Findings** |
| --- | --- |
| **Title** | Sensitive Data in user ‘C:\Users\Public\Documents’ Directory |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Medium |
| **Description** | Once RED’s compromised the Windows machine, we discovered  sensitive information being stored inside the user ‘Public’ which can be  accessed by anyone on the system. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Never store sensitive information in user ‘Public’ as anyone has the credential  access to be able to access these files  Always be weary of who has read, write, and execute privileges on directories  or files containing sensitive information |

| **Vulnerability 11** | **Findings** |
| --- | --- |
| **Title** | SLMail pop3d Exploit |
| **Type (Web app / Linux OS / WIndows OS)** | Windows OS |
| **Risk Rating** | Critical |
| **Description** | After discovering the version of SLMail to be pop3d, RED’s  successfully deployed a metasploit module and was successful in their exploit  attempts, resulting in RED’s gaining a Meterpreter session on the host  machine. |
| **Images** |  |
| **Affected Hosts** | 172.22.117.20 |
| **Remediation** | Disable & Remove SLMail as it has known vulnerabilities and is an outdated  service  Restrict or close access to port 110 |