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

Contact Information

Company Name	MAYURA LLC
Contact Name	SIVAYALINI PARTHIBAN
Contact Title	PENETRATION TESTER

Document History

Version	Date	Author(s)	Comments
001	01/19/2023	SIVAYALINI	

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.

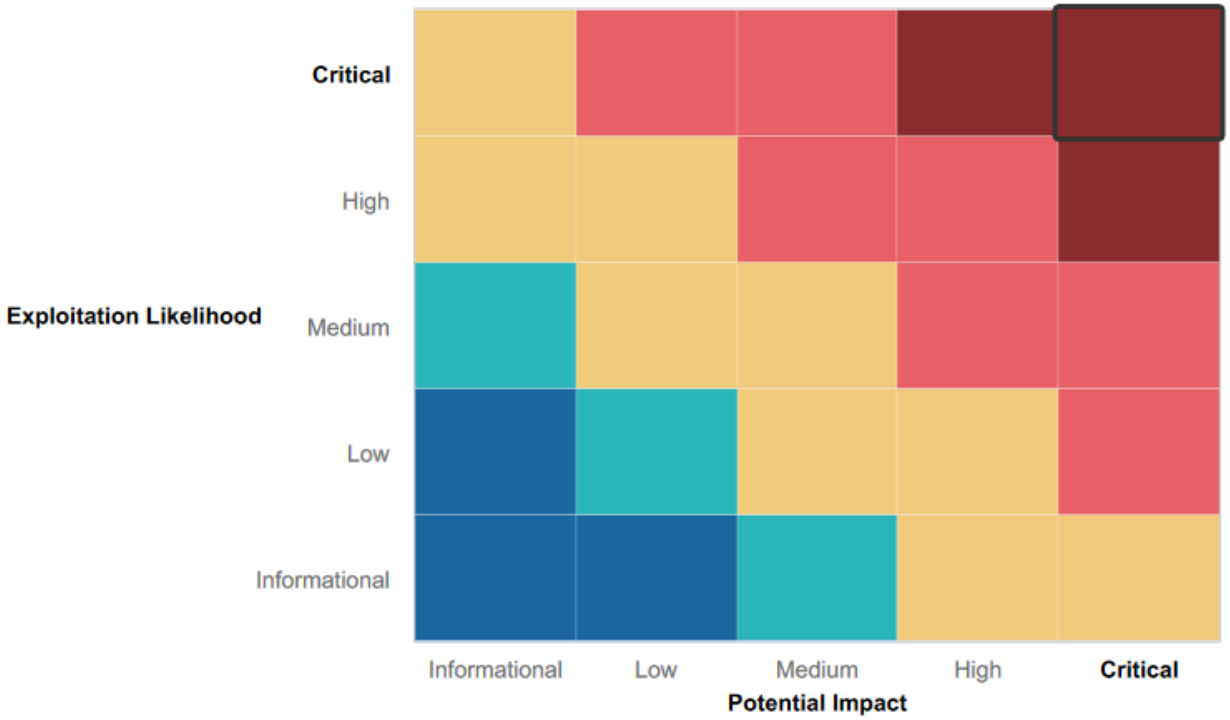
Executive Summary of Findings

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.

- Rekall using Metasploit and nmap that provides good security to prevent unauthorized access.
- No open source data.
- Ensures network availability to mitigate DDoS attack.

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.

- Rekall is vulnerable to XSS and SQL payload injection
- Apache web server is outdated.
- Slmail is vulnerable to exploits which allows access to shell.
- Open ports allow for ftp and unauthorized access.
- Password cracking and privilege escalation was very possible due to unauthorized access.
- User Credentials was found publicly in github.

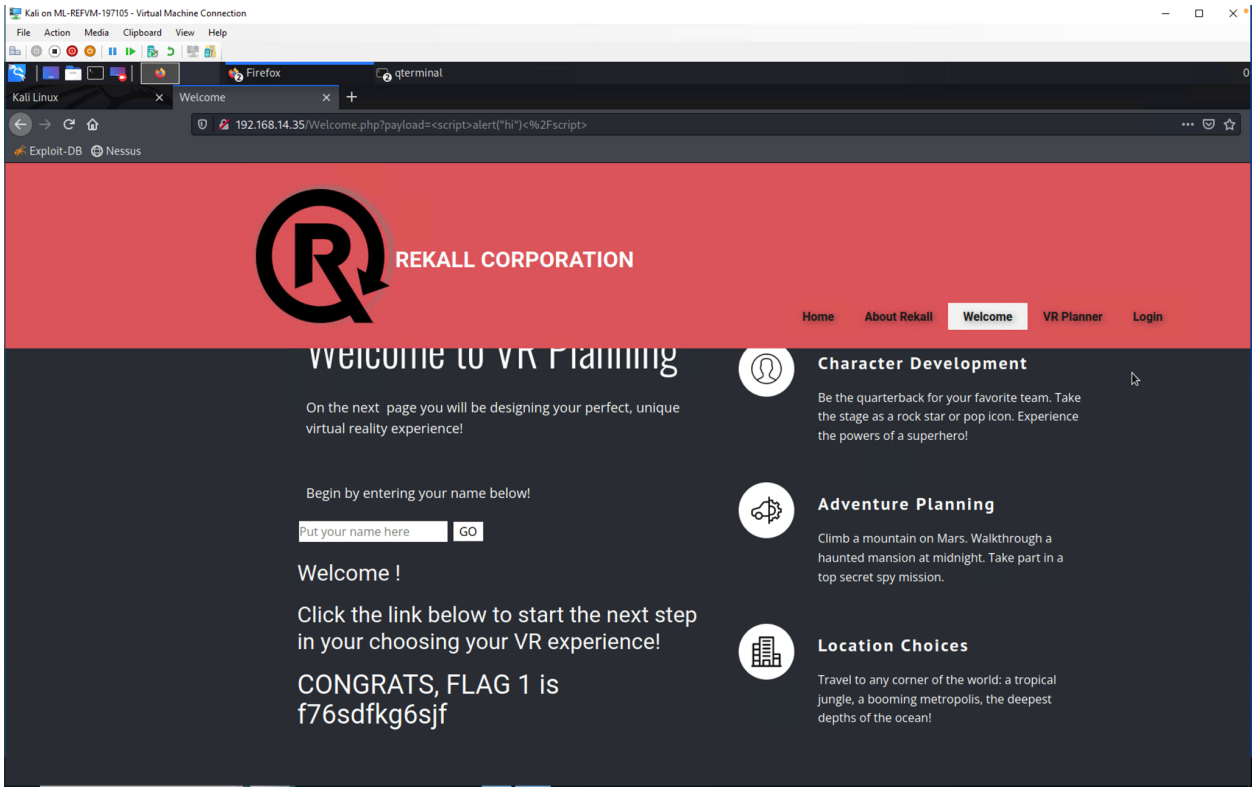
Executive Summary

During the entire Penetration testing for the Rekall's systems, we are able to identify several vulnerabilities that could affect Rekall's financial system and can also be harmful to the long-term stability of an organization. We were able to access Rekall servers/systems, and we were able to exfiltrate sensitive data.

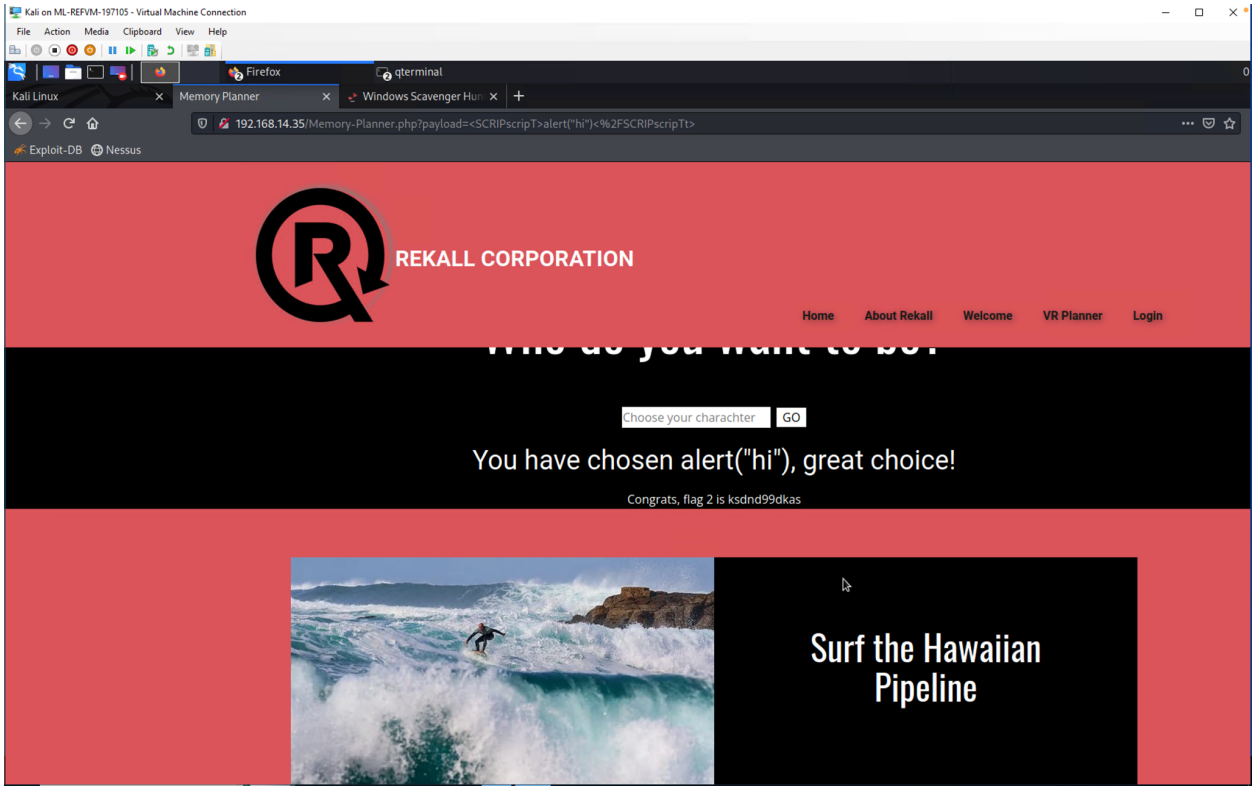
VULNERABLE TO MALICIOUS SCRIPT

- Rekall's site is vulnerable to XSS reflected attack as malicious scripts can run on the Welcome page.php, Memory planner.php page and XSS stored attack on comments.php page.
- Rekall's site is vulnerable to SQL injection attacks on the Login.php and Networking.php pages.
- It is also vulnerable to Local file inclusion on VR planner page.

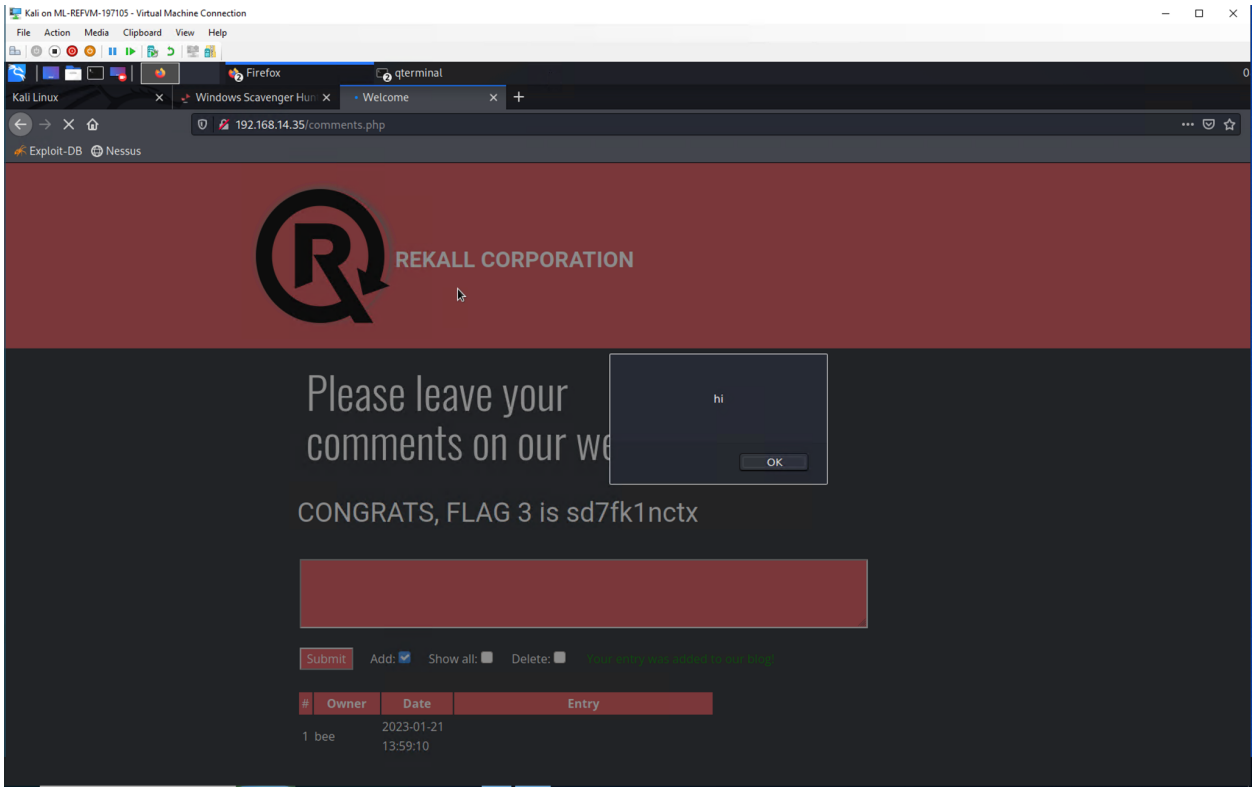
XSS REFLECTED ATTACK ON WELCOME.PHP PAGE



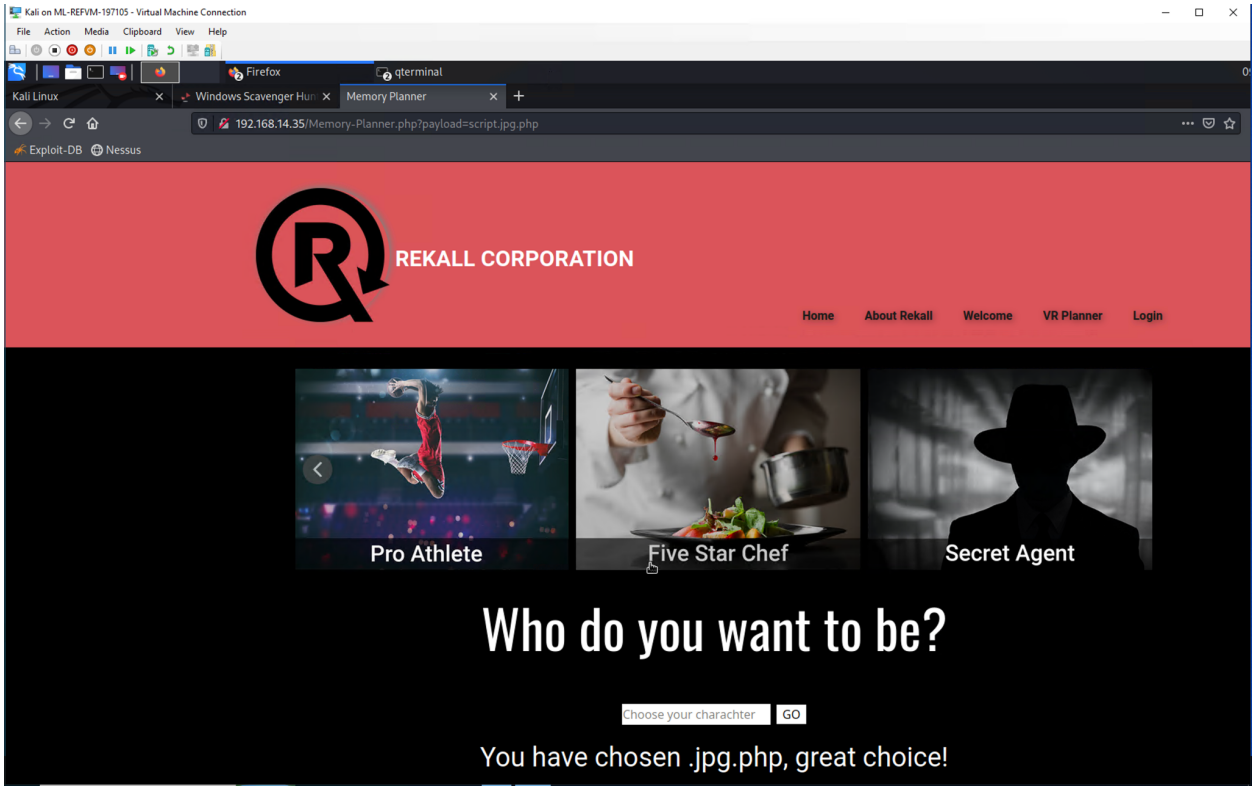
XSS REFLECTED ATTACK ON MEMORY-PLANNER.PHP



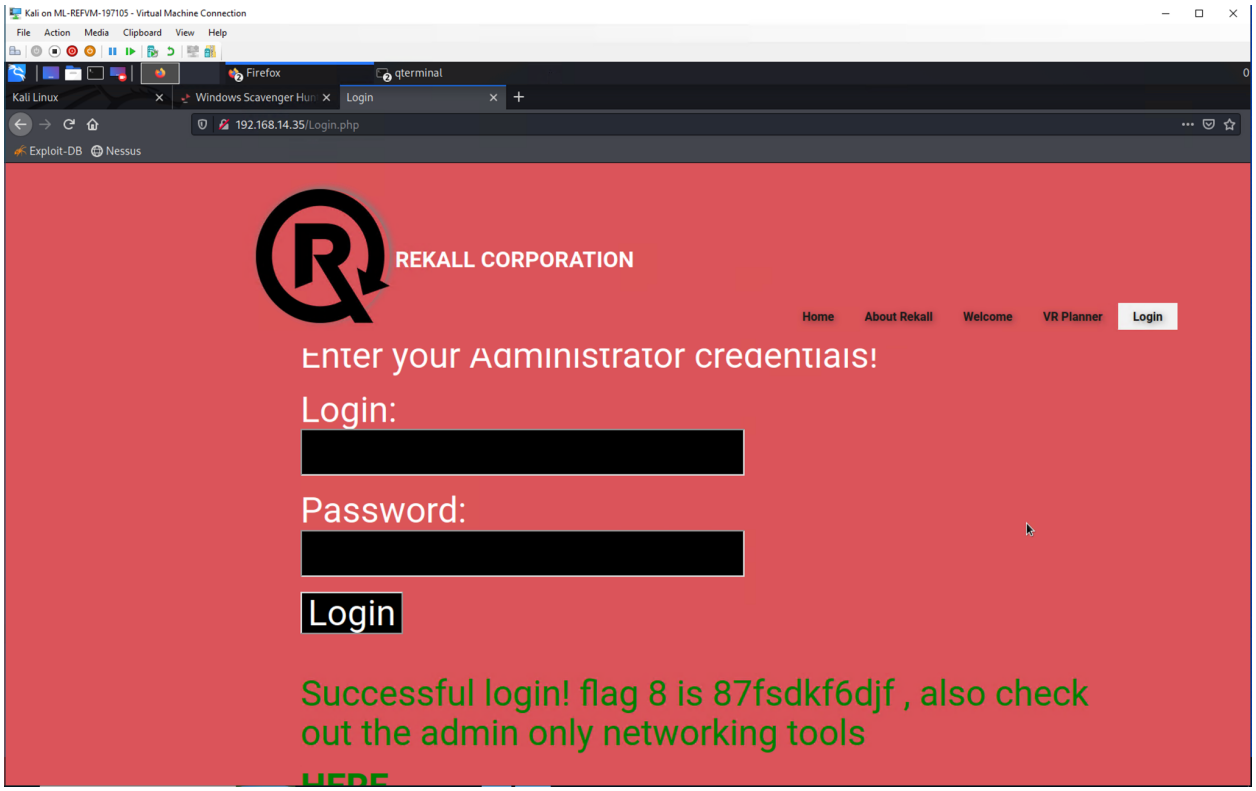
XSS STORED ATTACK ON COMMENTS.PHP PAGE



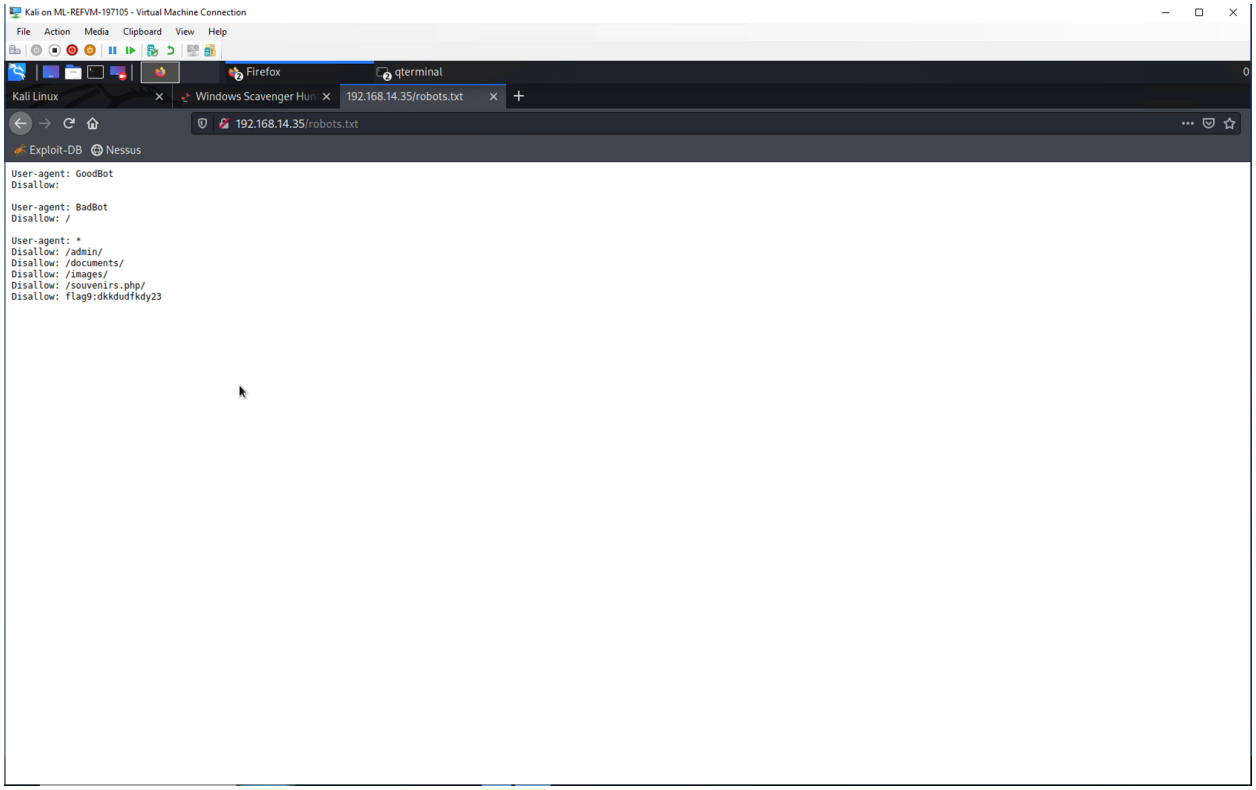
LOCAL FILE INCLUSION ON MEMORY-PLANNER.PHP PAGE



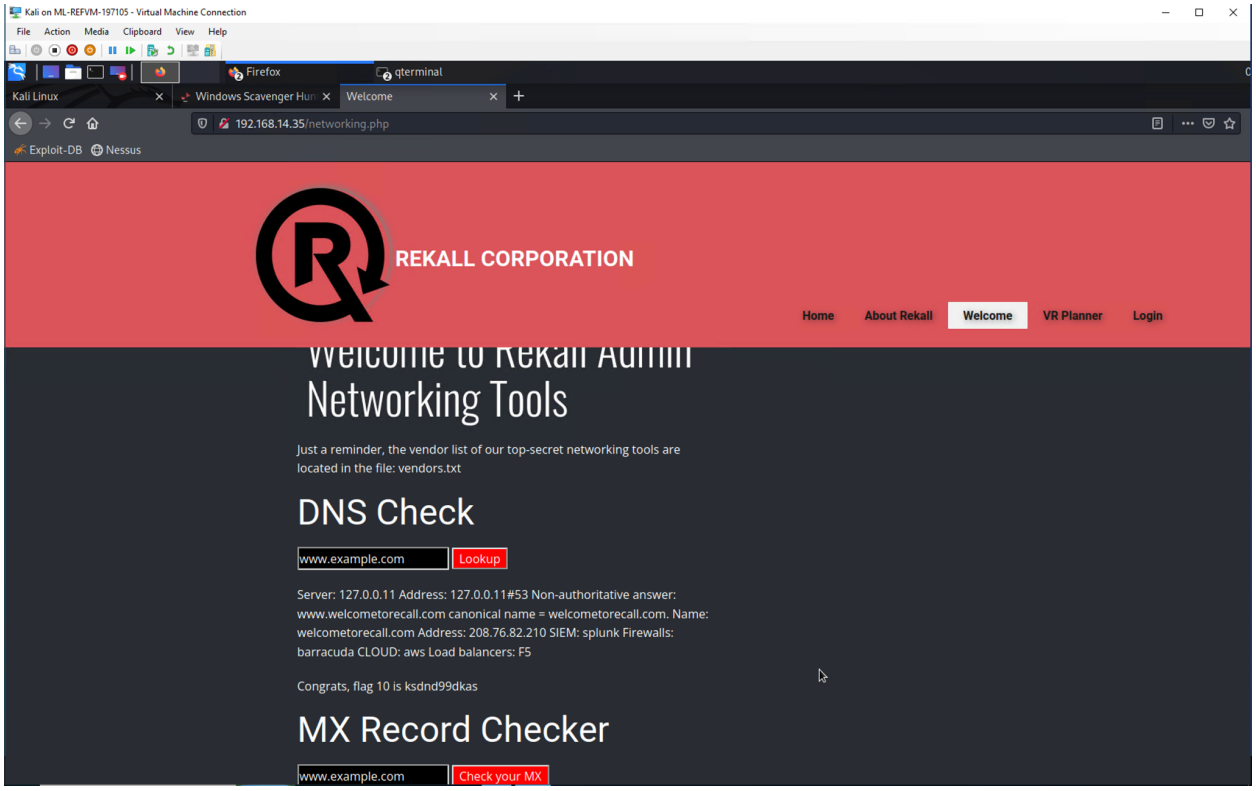
SENSITIVE DATA EXPOSURE ON LOGIN.PHP



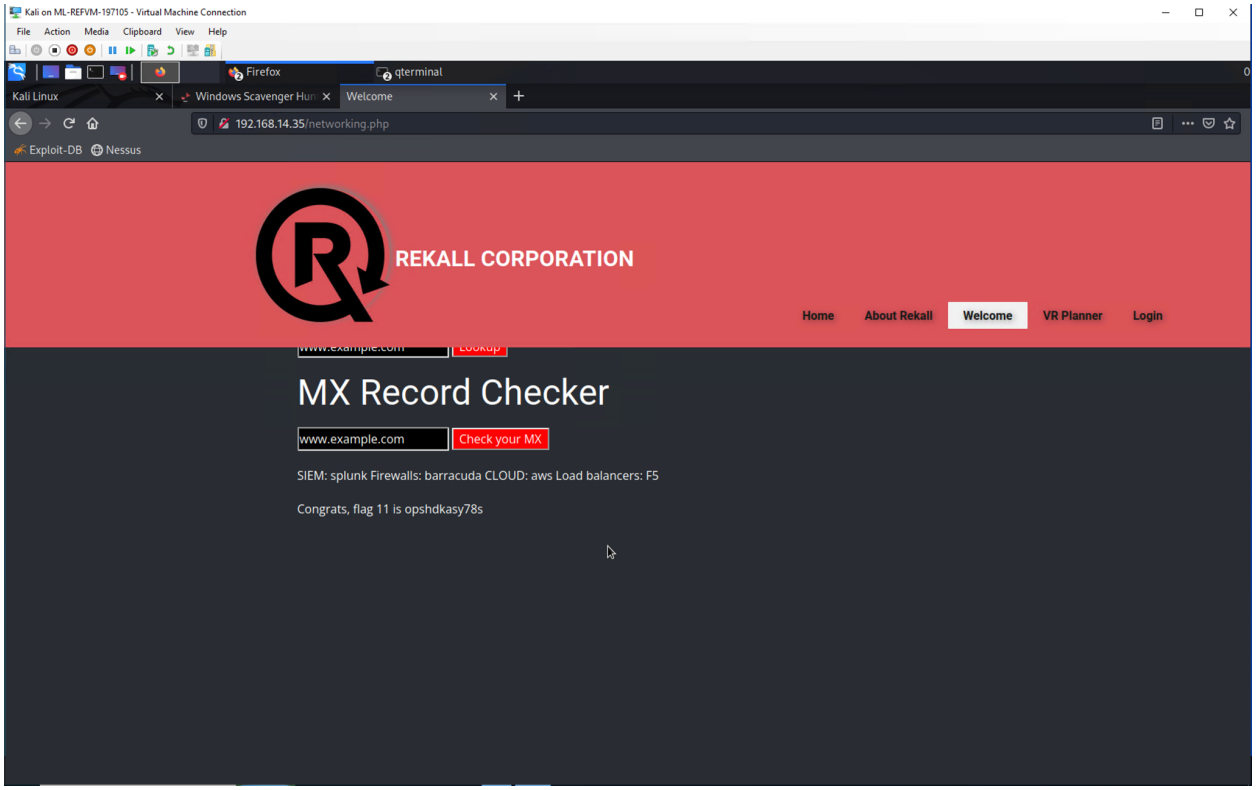
SENSITIVE DATA EXPOSURE ON ROBOTS.TXT



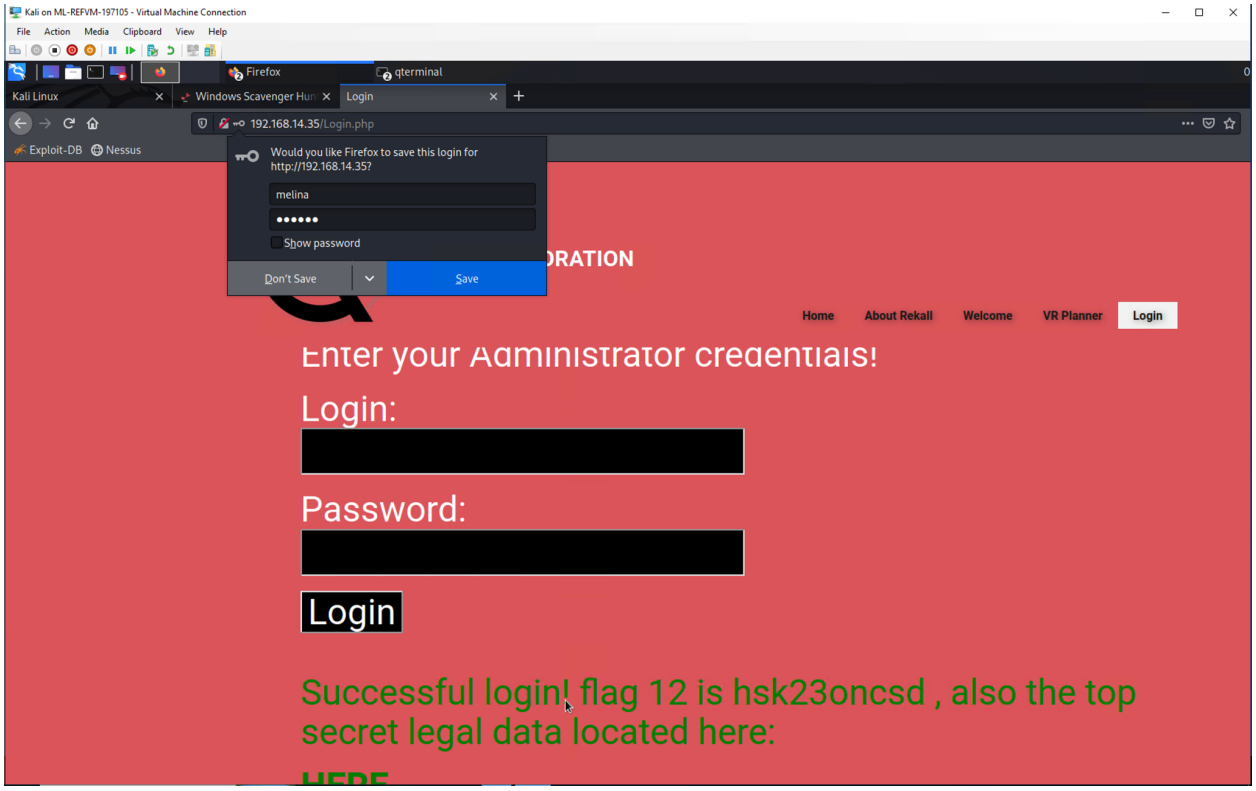
COMMAND INJECTION ON NETWORKING.PHP PAGE



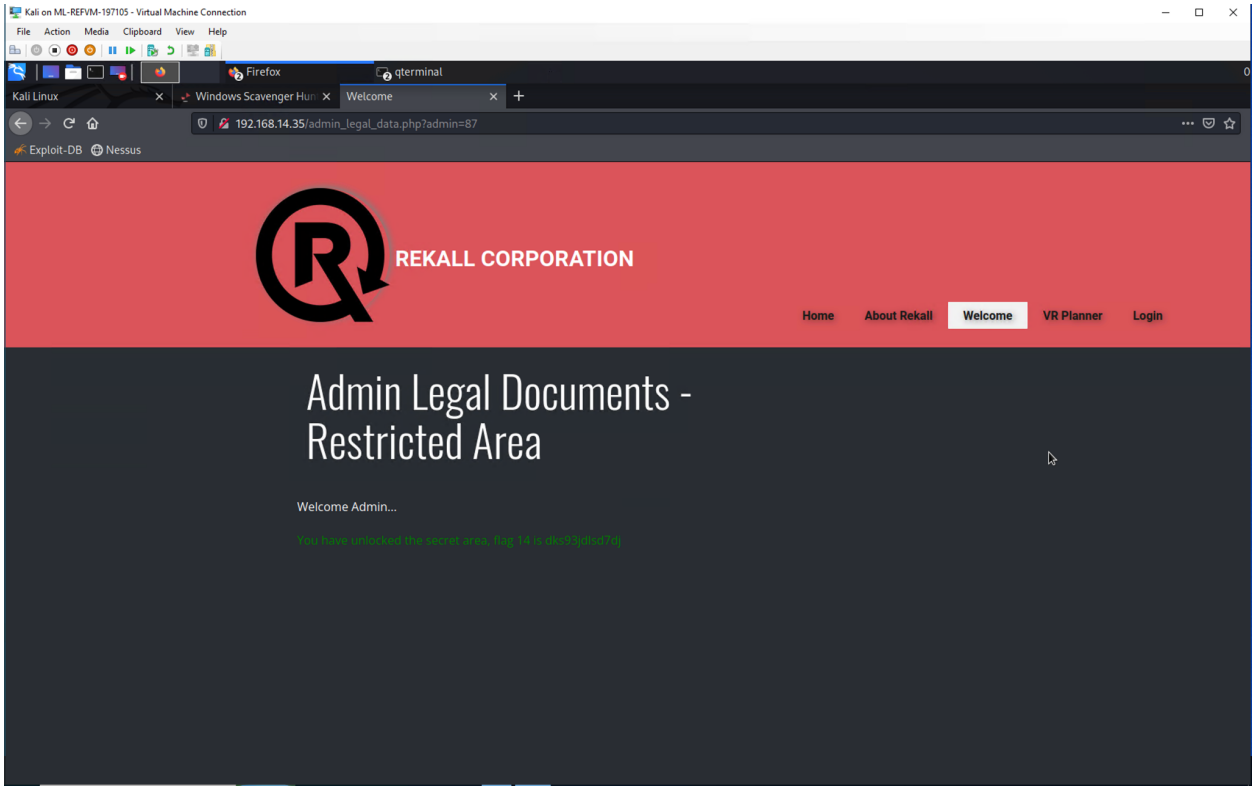
COMMAND INJECTION NETWORKING.PHP PAGE



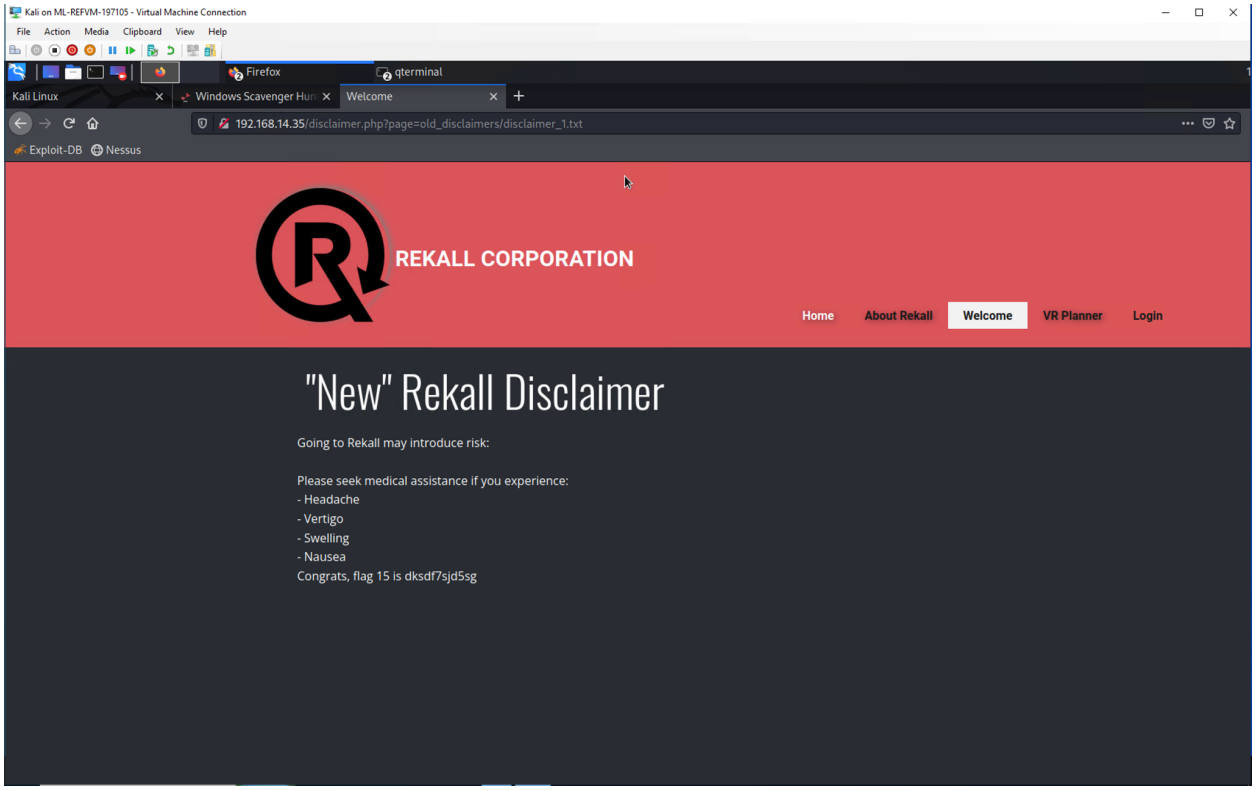
BRUTE FORCE ATTACK ON LOGIN.PHP



SESSION MANAGEMENT ON ADMIN_LEGAL_DATA.PHP



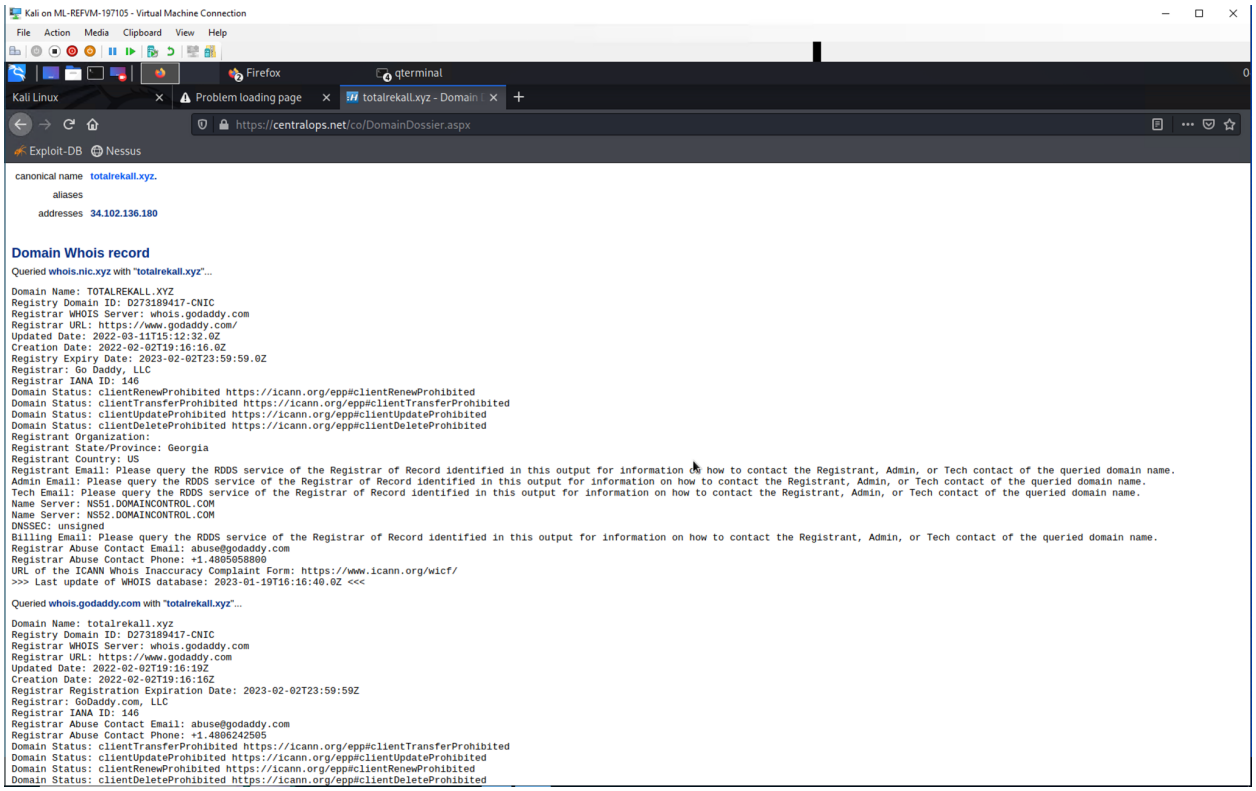
DIRECTORY TRAVERSAL ON DISCLAIMER.PHP



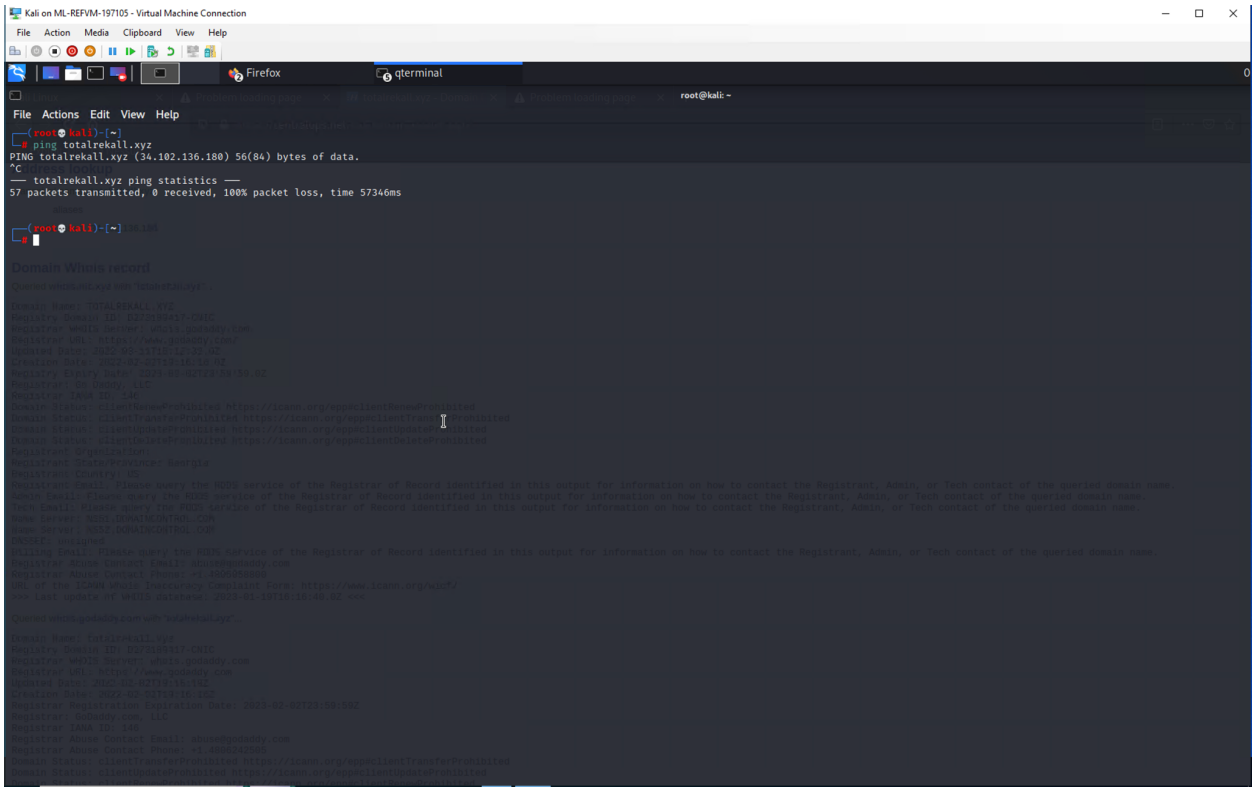
The Linux OS environment was the next testing environment, Mayura Pentesting group was successfully able to reveal the host, and with stolen credentials escalated privileges to root.

- Using OSINT open source data are exposed and using crt.sh stored certificate are exposed.
- By scanning the ports it was determined there are six hosts and one running Drupal.
- Apache Strusts(Out of date) - Critical vulnerability was found by running Nessus scan.

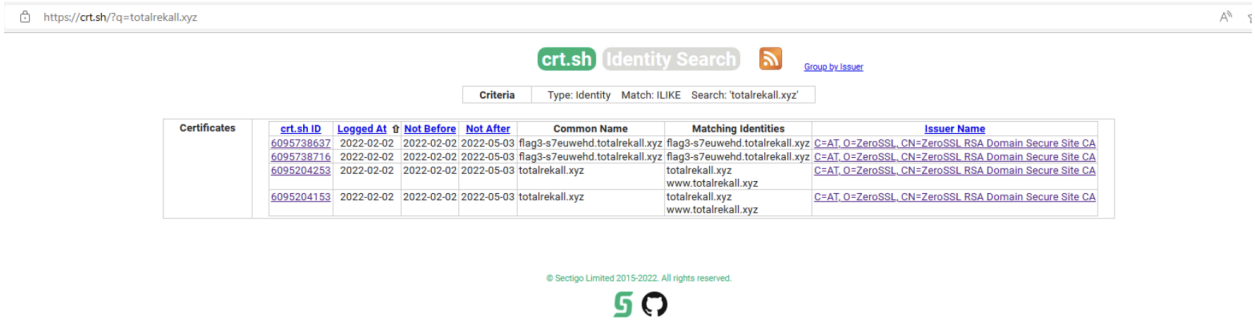
OPEN SOURCE EXPOSED DATA on Domain Dossier Webpage



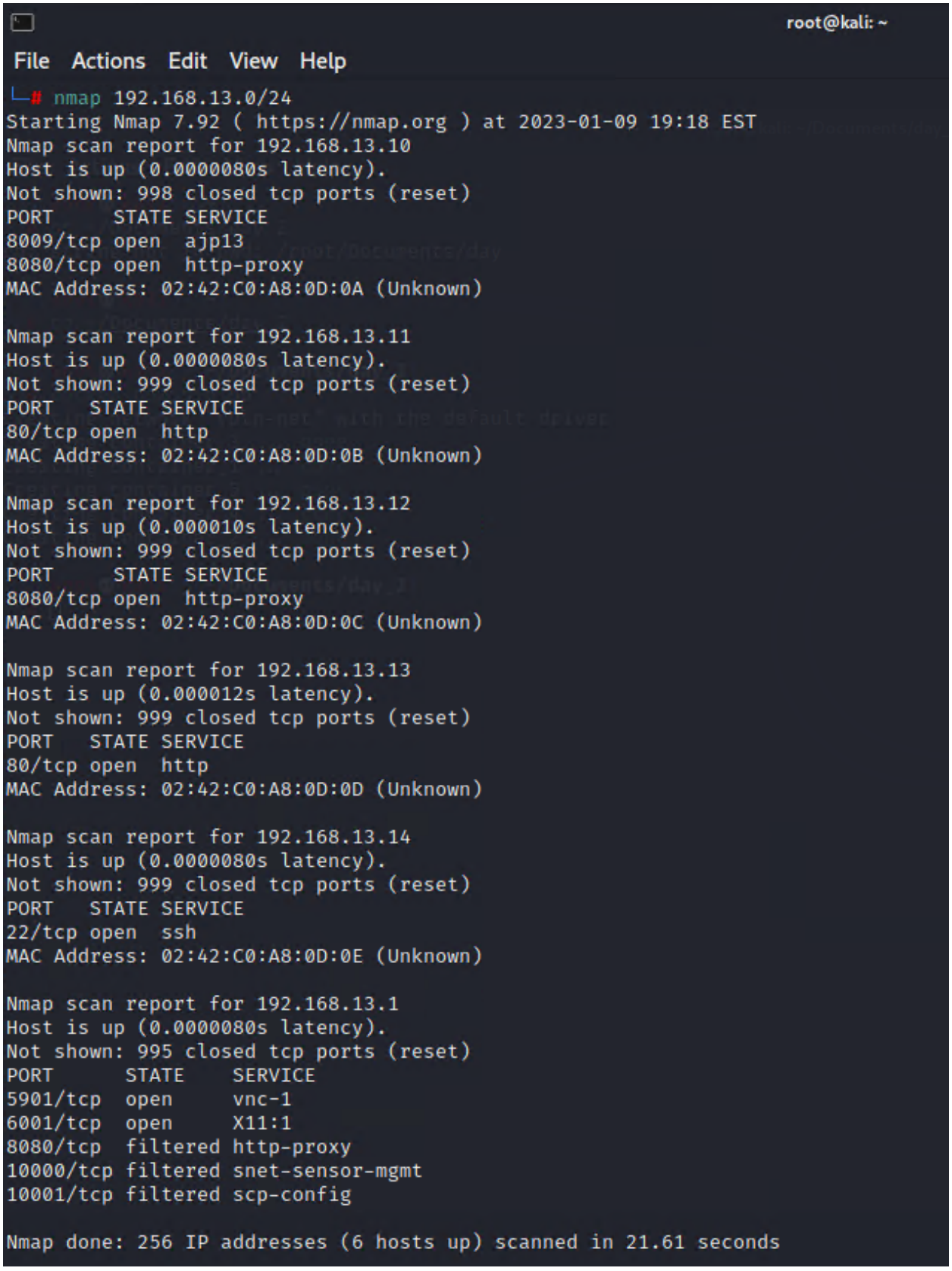
PING totalrekall.xyz



OPEN SOURCE EXPOSED DATA ON CRT.SH



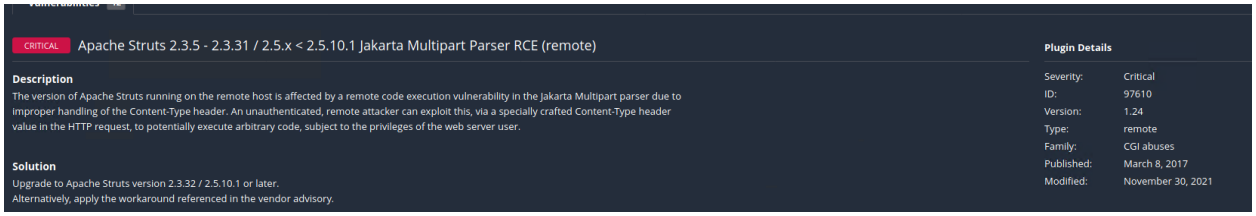
PORT SCANNING FOUND 6 HOSTS



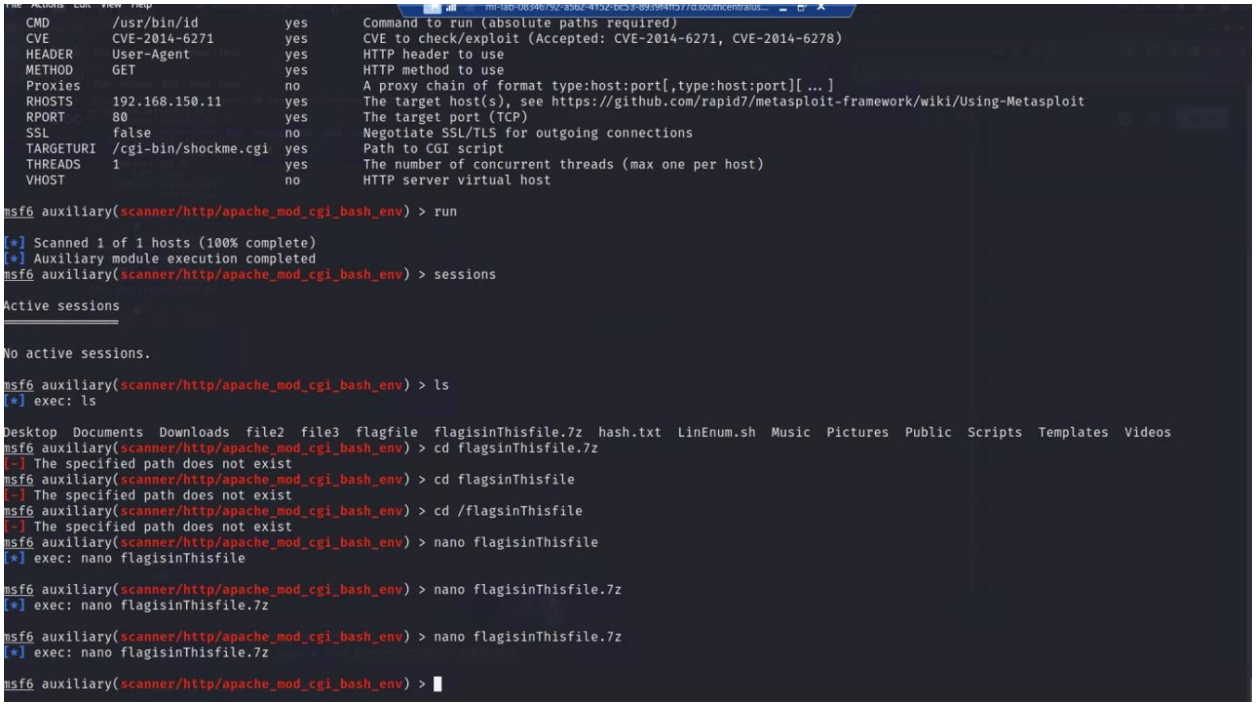
AGGGRESSIVE NMAP SCAN FOUND THE TRACEROUTE

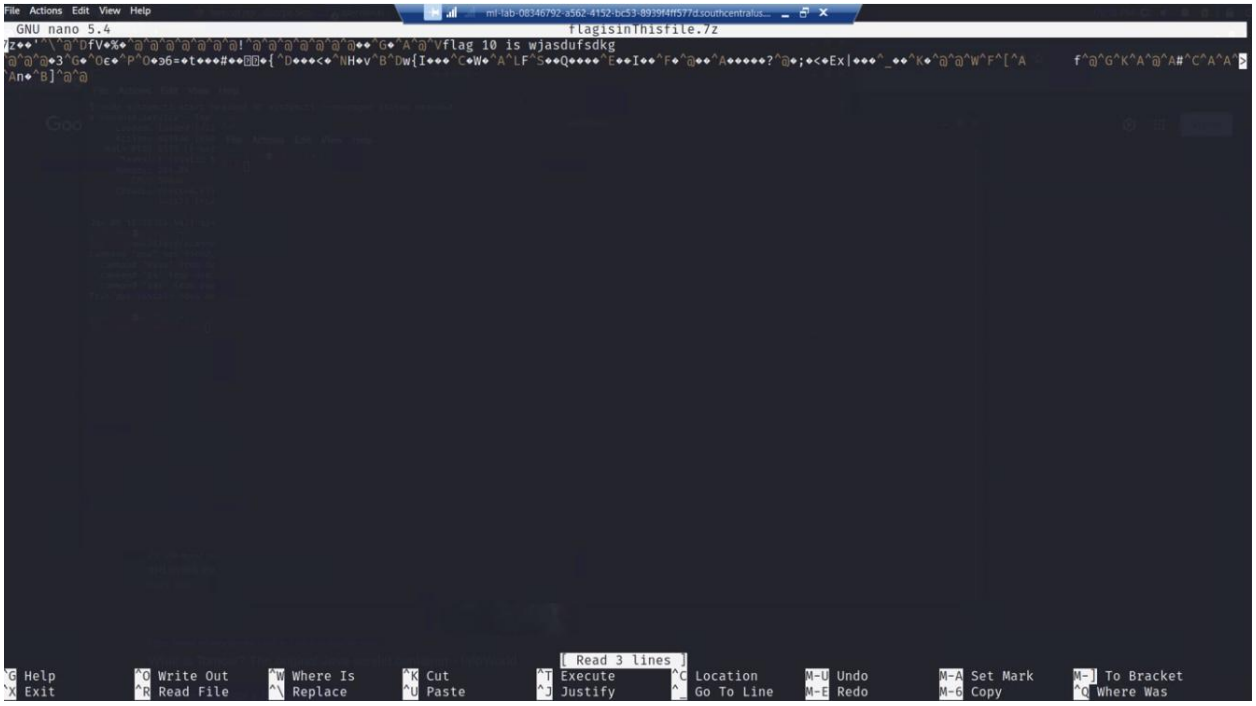
```
Nmap scan report for 192.168.13.13
Host is up (0.000024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/-
o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 35.005 days (since Mon Dec  5
19:27:38 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good
luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.02 ms 192.168.13.13
```

APACHE STRUTS - CRITICAL VULNERABILITY



NESSUS SCAN FOUND THE HOST IS VULNERABLE TO STRUSTS





The WINDOWS OS environment was the next testing environment. Mayura Penetration testing team successfully found the user credentials stored within the HTML source code of the Login.php page.

- User credentials were actually stored in the Github repository which can be used for unauthorized access to the system.
- FTP port 21 was open and vulnerable , port 110 used for SLMail service.
- Using Metasploit access can be gained to password hash file, which we cracked and helped for reverse shell creation.
- Meterpreter can display directories on public Windows directories.

Summary Vulnerability Overview

Vulnerability	Severity

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

Scan Type	Total
Hosts	
Ports	

Exploitation Risk	Total
Critical	0
High	0
Medium	0

Low	0

Vulnerability Findings

Vulnerability 1	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 2	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 3	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	

Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 4	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 5	Findings
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 6	Findings
Title	

Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Vulnerability 7	**Findings**
Title	
Type (Web app / Linux OS / WIndows OS)	
Risk Rating	
Description	
Images	
Affected Hosts	
Remediation	

Add any additional vulnerabilities below.