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

Contact Information

Company Name	Trevor’s Cybersecurity
Contact Name	Trevor Knauf
Contact Title	Chief Coordination Officer

Document History

Version	Date	Author(s)	Comments
001	4/24/2023	Trevor Knauf	2nd attempt

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.

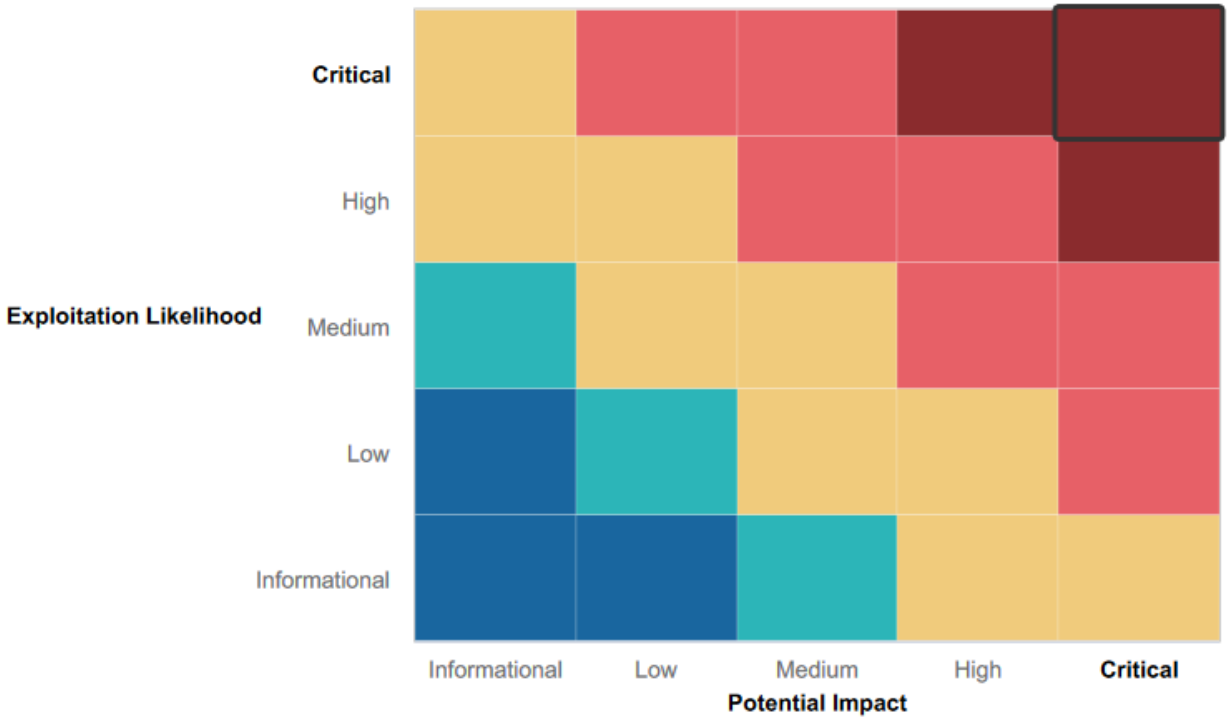
Executive Summary of Findings

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.

- Some level of input validation to stop data from being vulnerable.
- Strong strategy for denial of DDoS attacks
- Confidential information is hard to find

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 application is vulnerable to cross site scripting and SQL injection
- Users credentials stored in HTML source code
- Open ports which are vulnerable to attacks

Executive Summary

From the web application Rekall could very much benefit from a web application firewall to start off with. There were too many ways that an actor could find vulnerabilities and then attack them to gain sensitive data. In the web app we were able to exploit the company by using cross site scripting, SQL injection, PHP injection, and directory traversal. Using Nmap scans and Nessus also gave out very sensitive information about open ports and other vulnerabilities. Using metasploit allowed us to gain access through different open ports too.

Summary Vulnerability Overview

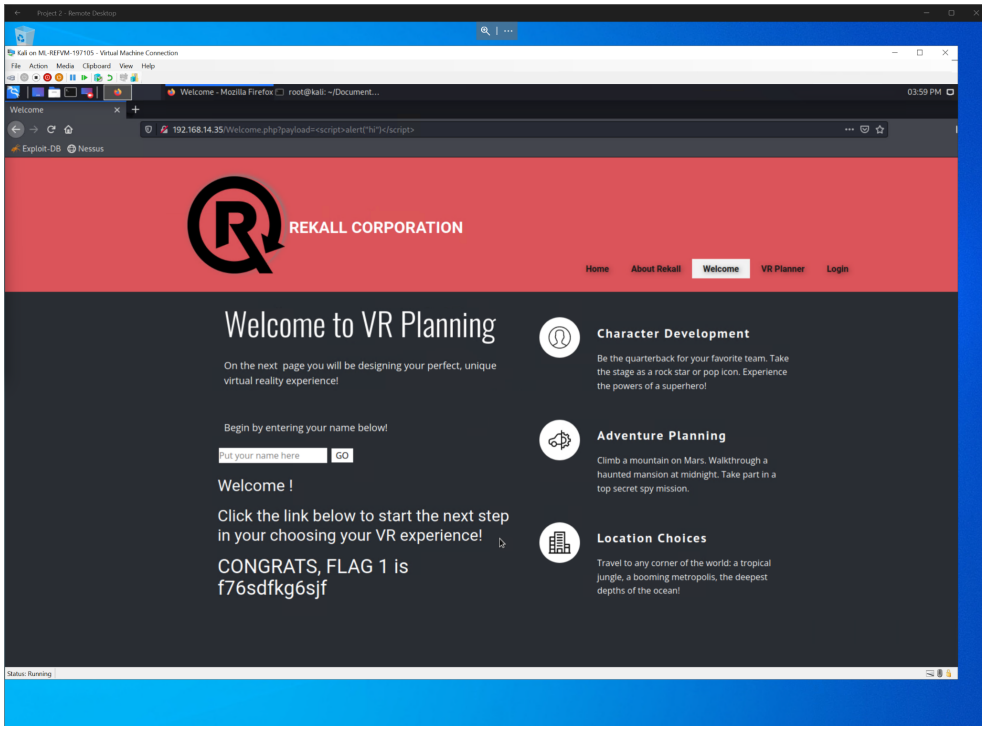
Vulnerability	Severity
XSS reflected	Medium
XSS reflected (advanced)	Medium
Sensitive Data Exposure	Critical
Local File Inclusion	Critical
Local File Inclusion (advanced)	Critical
Sensitive Data Exposure HTML	Critical
Sensitive Data Exposure Files	Critical
Command Injection	Critical
Command Injection (advanced)	Critical
Brute Force Attack	Critical
Open Source Exposed Data	Medium
Nmap Scan Results	Critical
Aggressive Nmap Scan	Critical
XSS Stored	Critical
PHP injection	Critical
Session Management	Critical
Directory Traversal	Critical
ping totalrekall.xyz	Critical
Nessus Scan Results	Critical
Sensitive Data Exposure (Tanya4life)	Critical
Password Guessing	Critical
Vulnerable FTP port 21	Critical
Vulnerable Port	Critical

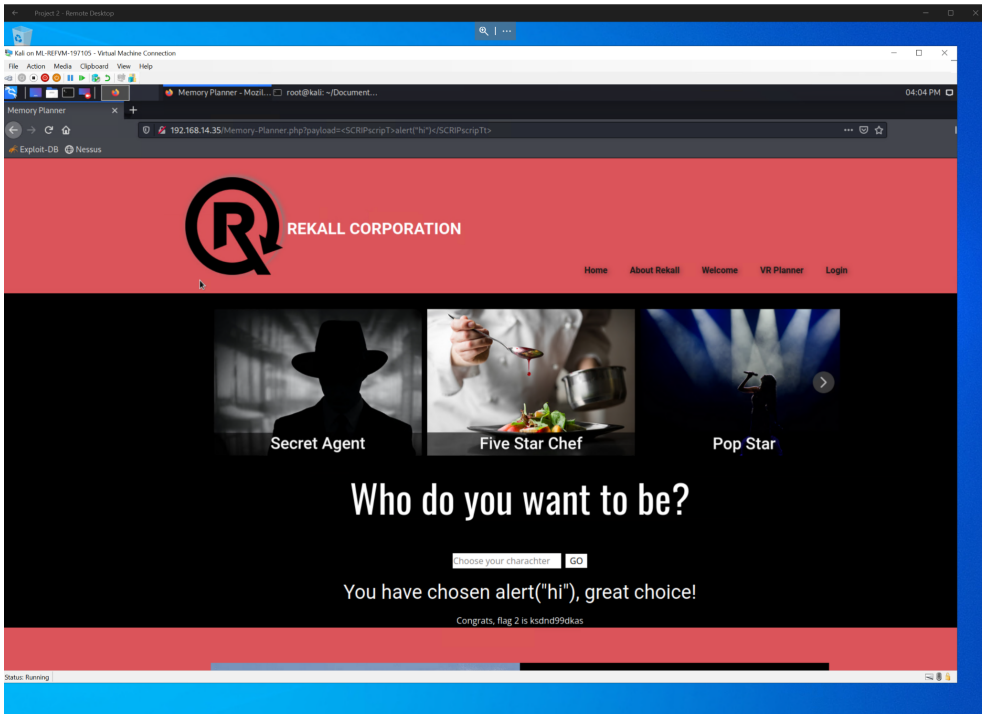
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35 192.168.13.13 192.168.13.12 192.168.13.14 192.168.13.10 192.168.13.1 172.22.117.20 172.22.117.10
Ports	80 21 110

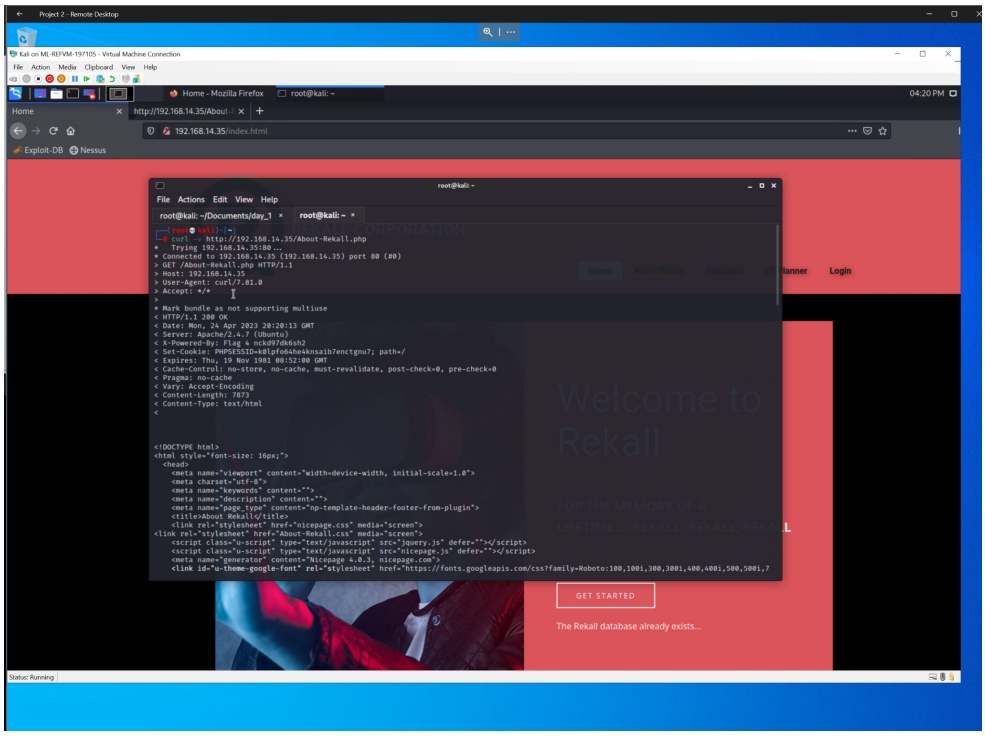
Exploitation Risk	Total
Critical	20
High	0
Medium	3
Low	0

Vulnerability Findings

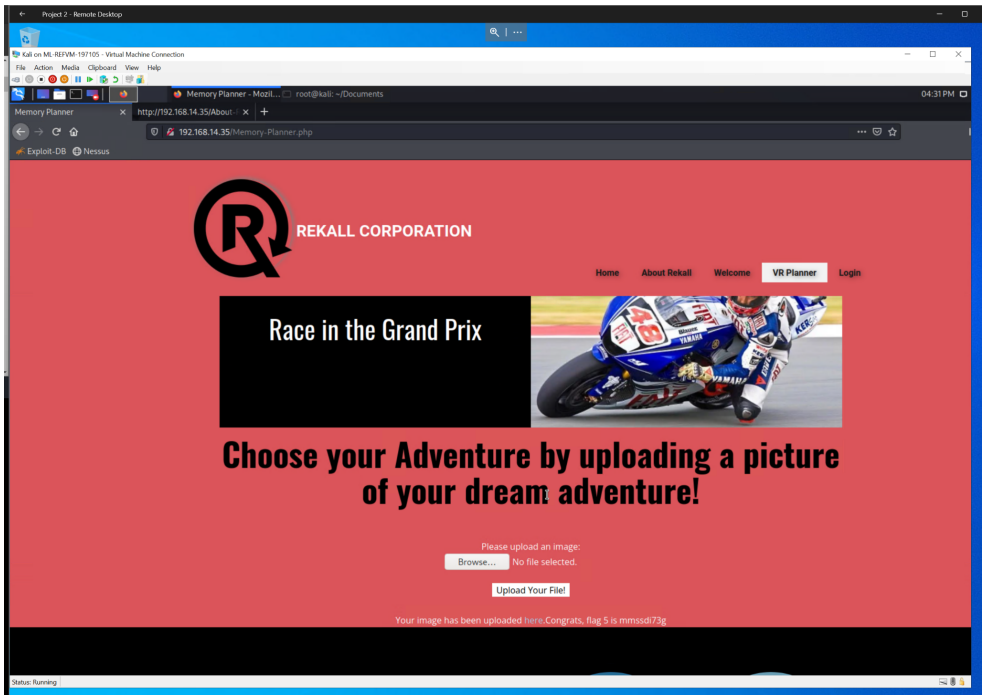
Vulnerability 1	Findings
Title	XSS reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	In Welcome.php a malicious script of <script>alert(“hi”)</script> was successful
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

Vulnerability 2	Findings
Title	XSS Reflected (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	In Memory-Planner.php input validation removes to word “script” in an attempt to stop cross-site scripting, but in the payload you split it up to avoid it. <SCRIPscripT>alert(“hi”)</SCRIPscripTt>
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger Input Validation so no script can be entered

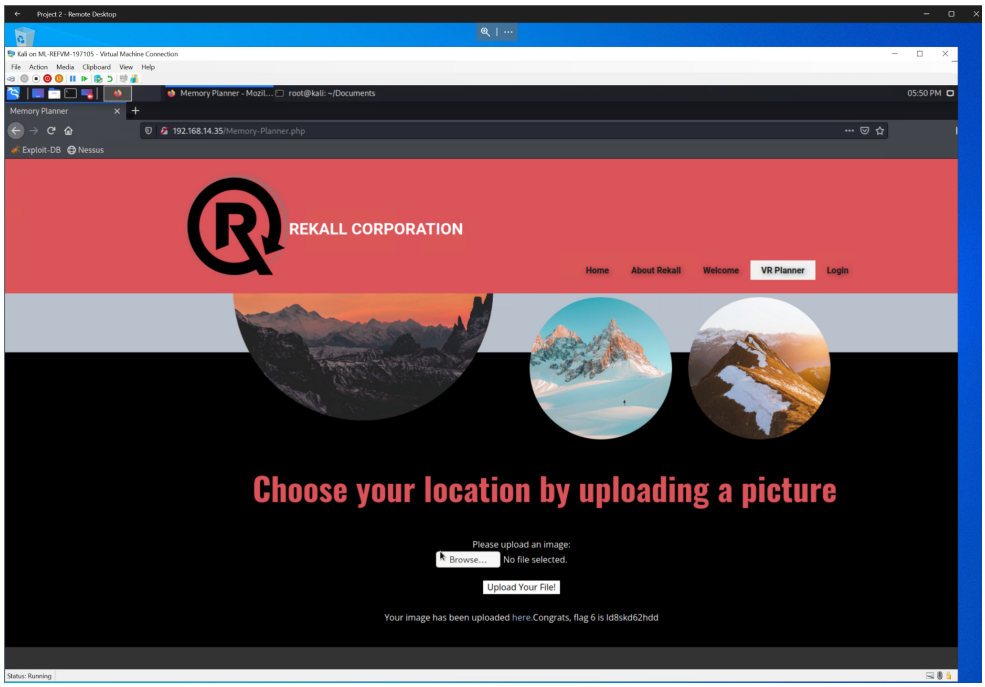
Vulnerability 3	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using a cURL request on http://192.168.14.35/About-Rekall.php all the data is exposed.

Images	
Affected Hosts	192.168.14.35
Remediation	close port 80

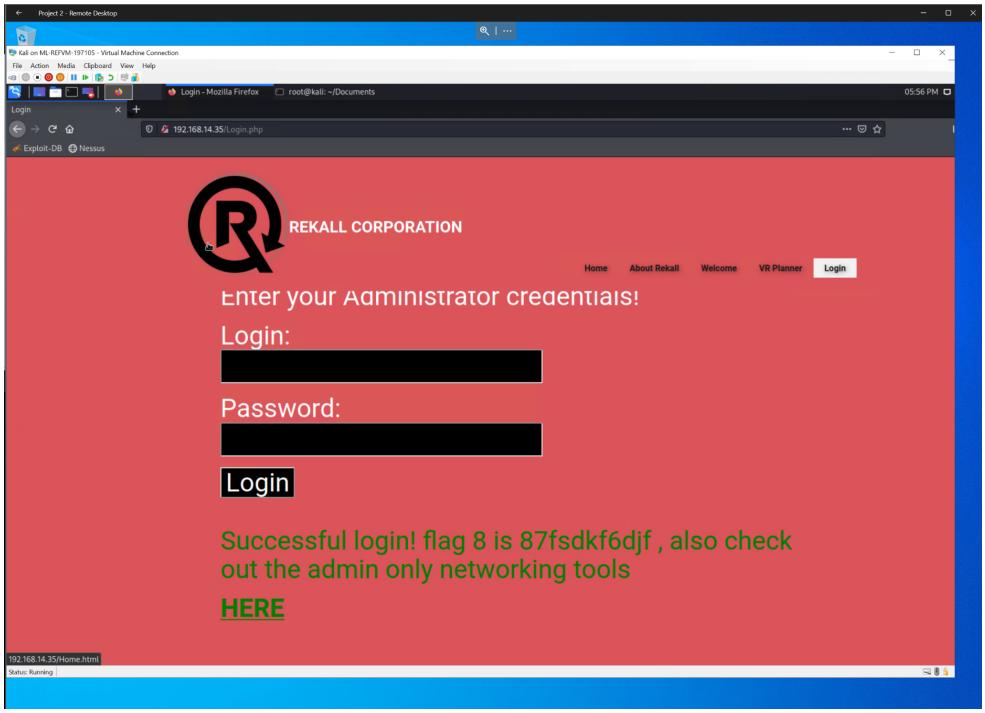
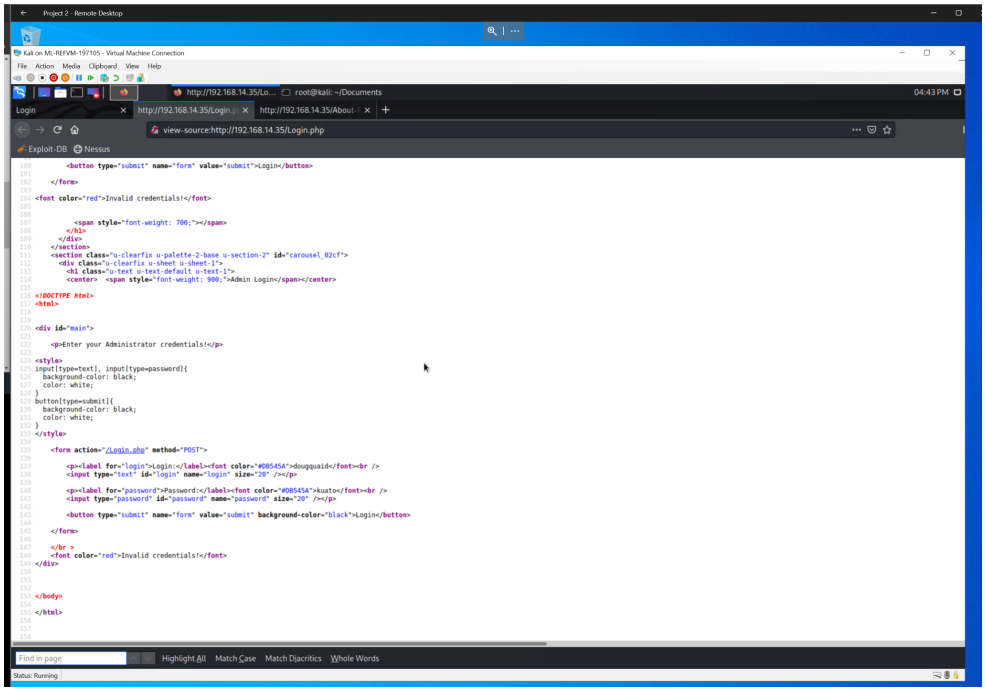
Vulnerability 4	Findings
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In Memory-Planner.php on the second field uploading any .php file is successful

Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

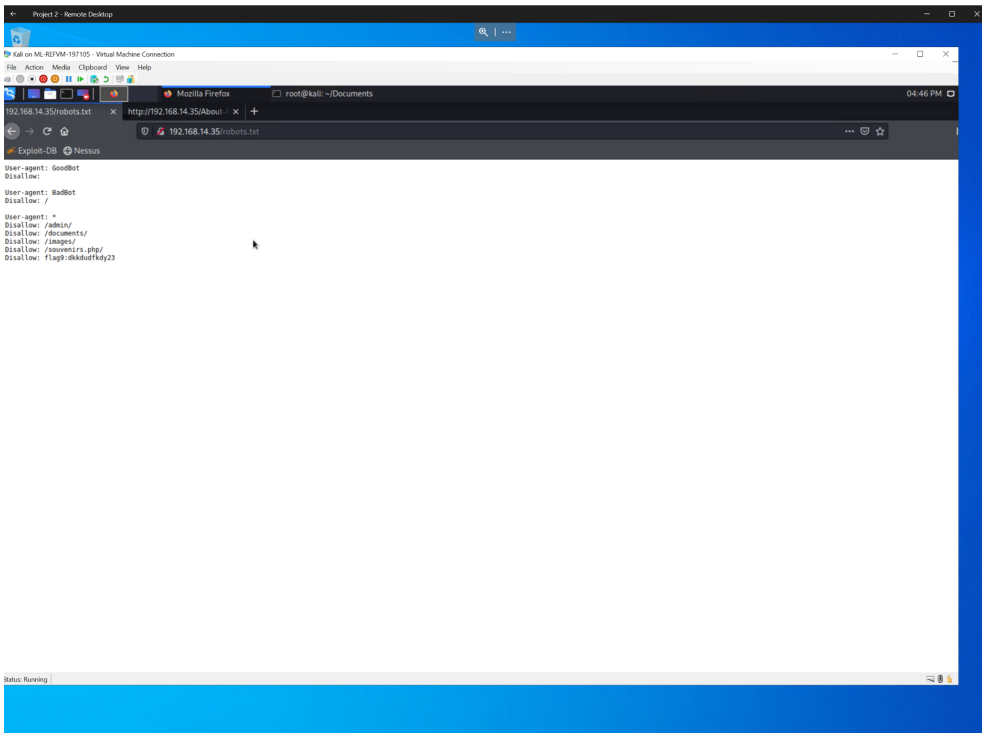
Vulnerability 5	Findings
Title	Local file inclusion (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In Memory-Planner.php on the third field where there is some input validation for “.jpg”. To avoid this the file name was trevsscript.jpg.php which was successfully uploaded.

Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation

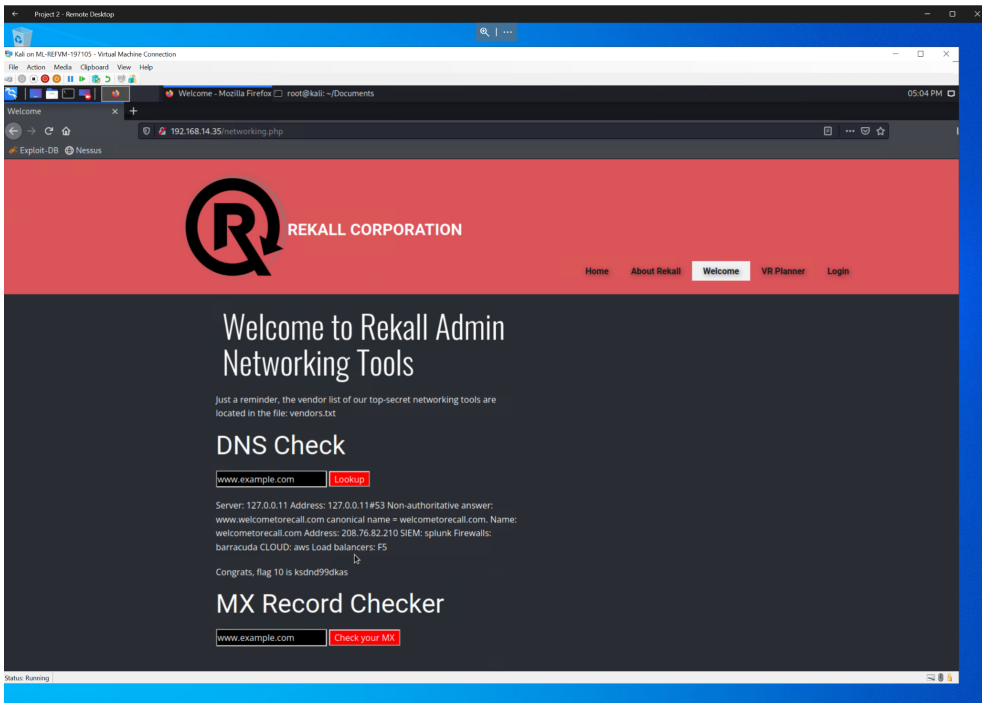
Vulnerability 6	Findings
Title	Sensitive Data Exposure HTML
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Login credentials can be found in the HTML of the Login.php

Images	 
Affected Hosts	192.168.14.35
Remediation	Add extra security to the Login.php HTML so that login credentials can not be seen.

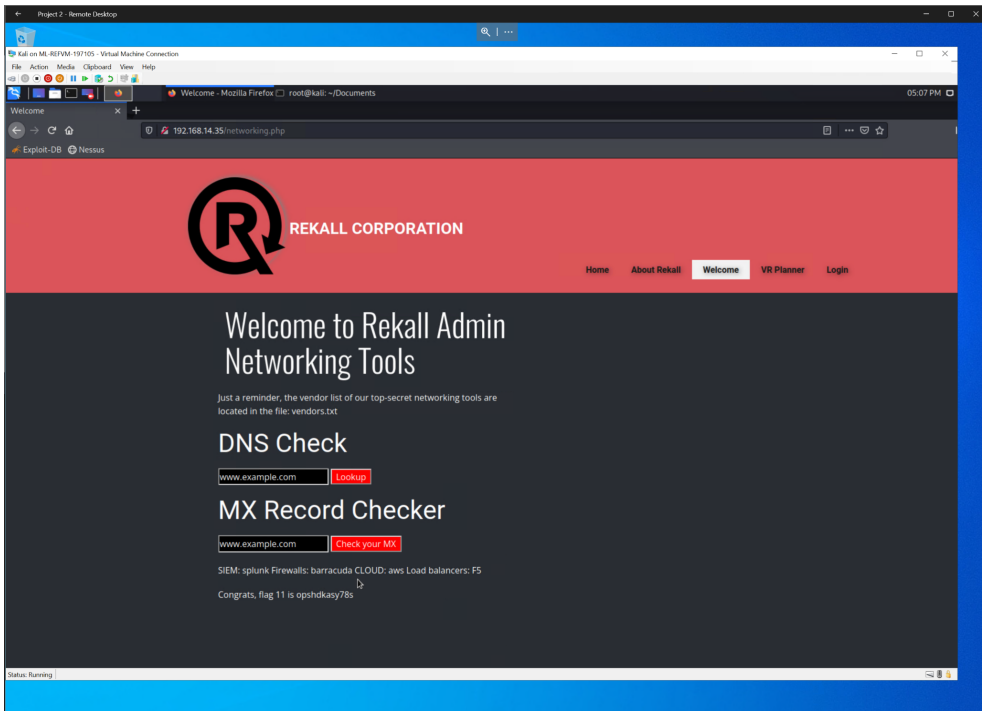
Vulnerability 7	Findings
Title	Sensitive Data Exposure Files

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	By accessing robots.txt data about the system is vulnerable.
Images	
Affected Hosts	192.168.14.35
Remediation	Add extra protection to sensitive files

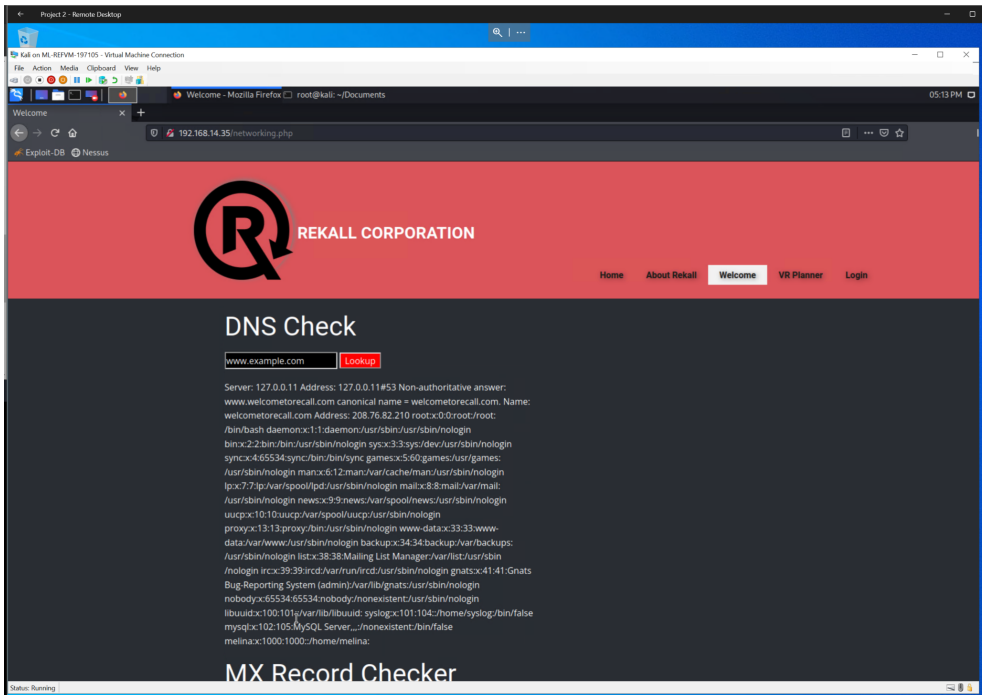
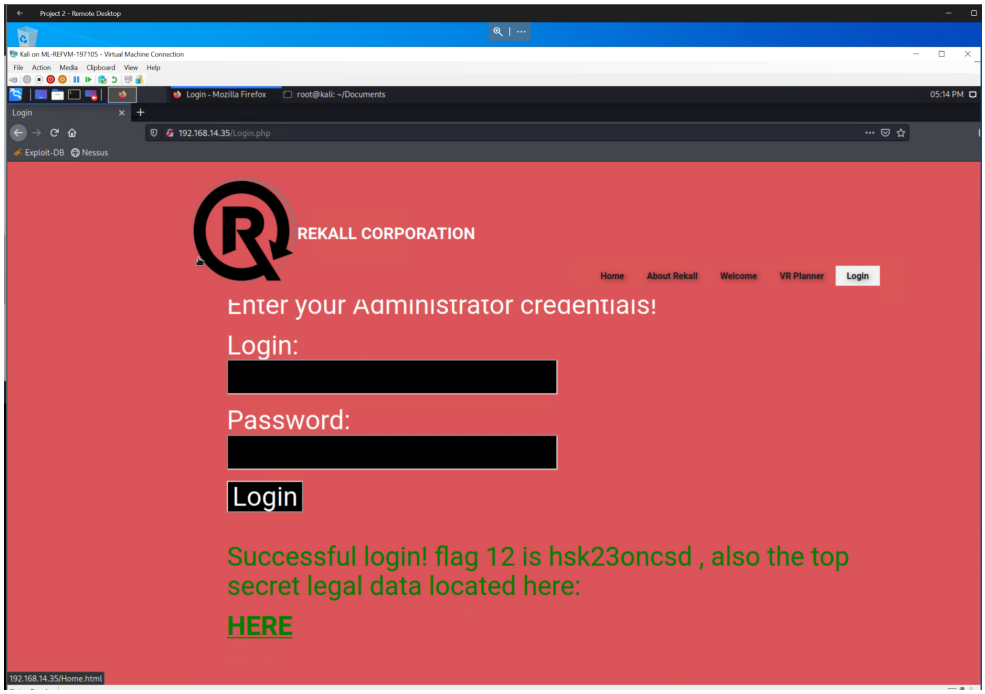
Vulnerability 8	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In networking.php on the first field by using the injection www.welcometorecall.com && cat vendors.txt, the file vendors.txt can be viewed.

Images	
Affected Hosts	192.168.14.35
Remediation	Input validation

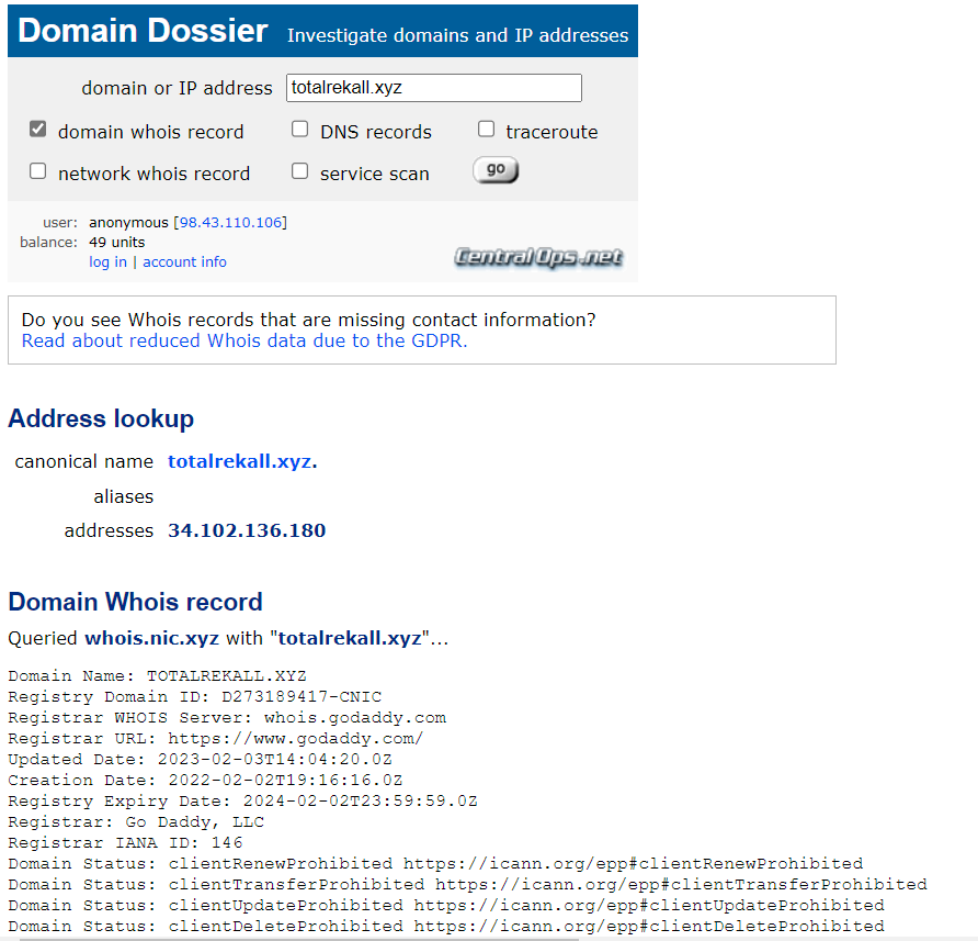
Vulnerability 9	Findings
Title	Command Injection (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	In networking.php on the second field there is input validation that gets rid of “&” and “;”. Though you can still pipe the commands like this payload www.welcometorecall.com | cat vendors.txt.

Images	
Affected Hosts	192.168.14.35
Remediation	Add an input validation that also does not allow piping

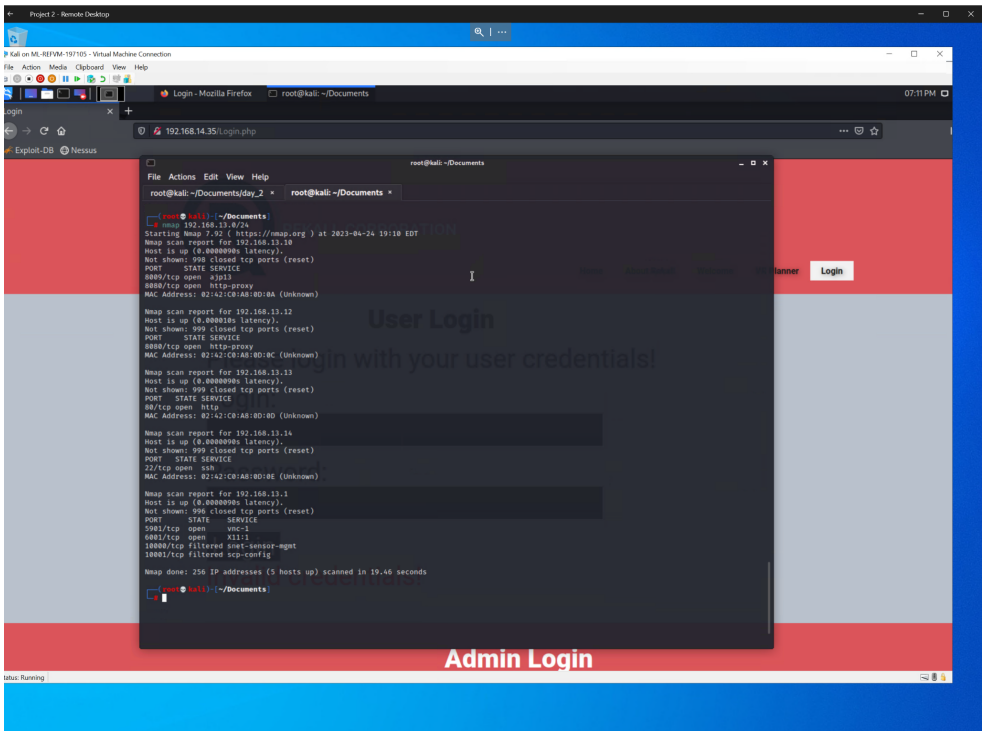
Vulnerability 10	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using the command injection www.welcometorecall.com && cat /etc/passwd the users can be seen. One user was melina and with some guessing it is easy to discover that melina's password is melina.

Images	 
Affected Hosts	192.168.14.35
Remediation	Require strong passwords for users

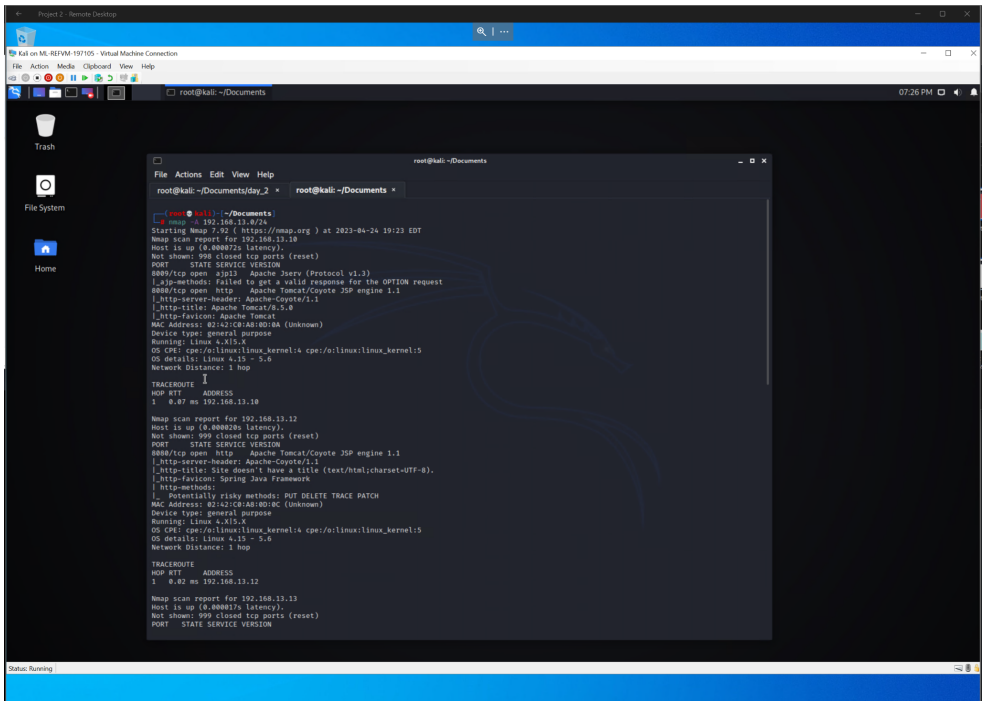
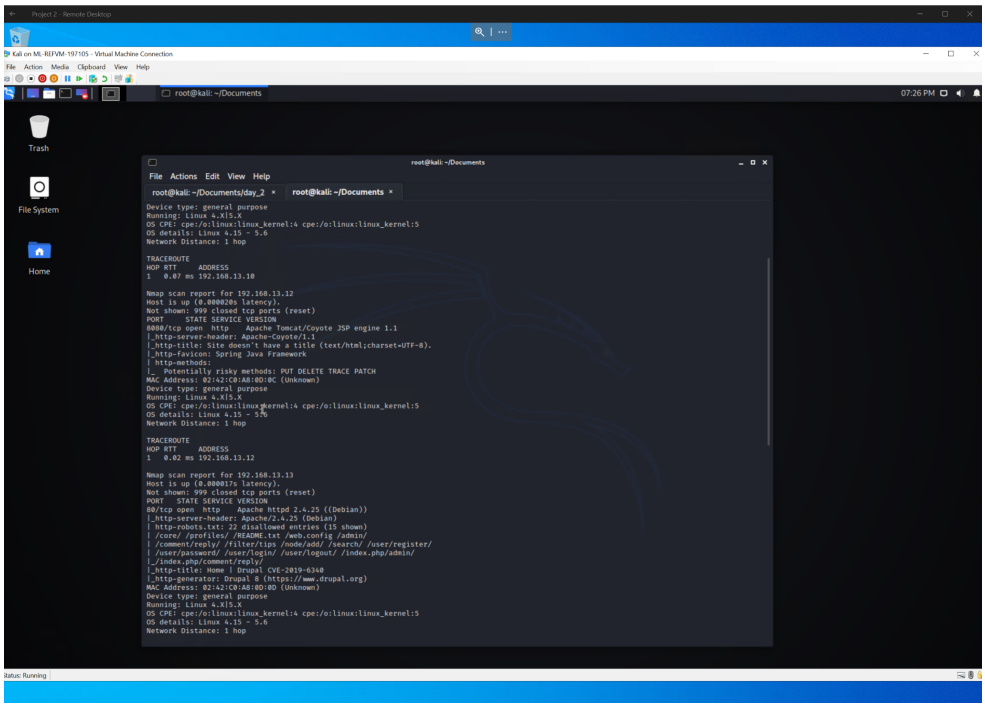
Vulnerability 11	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web app

Risk Rating	Medium
Description	On the Domain Dossier webpage, viewing the WHOIS data for totalrekall.xyz gives access to sensitive data.
Images	
Affected Hosts	34.102.136.180
Remediation	Do not allow sensitive data to be shared publicly through this webpage.

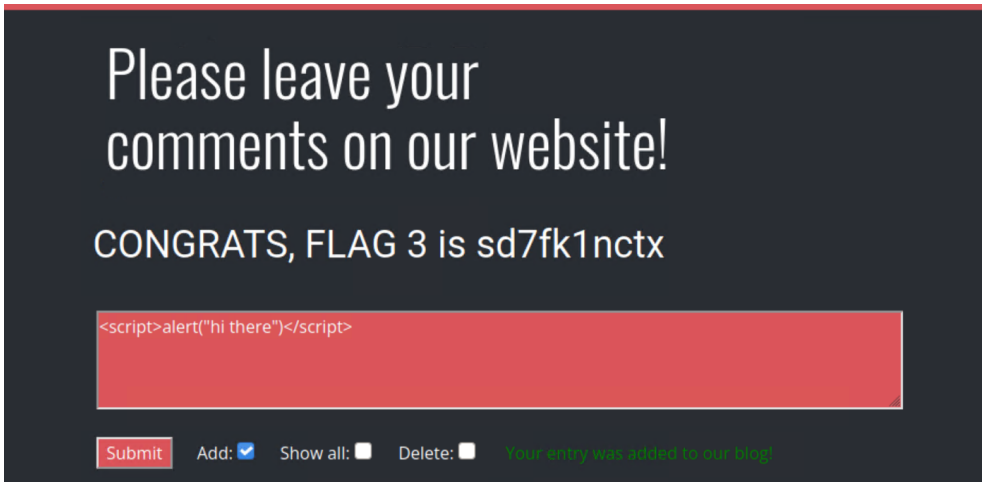
Vulnerability 12	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An Nmap scan on 192.168.13.0/24 showed that there are 5 hosts up

Images	
Affected Hosts	192.168.13.1 192.168.13.10 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Block these IPs to be viewed for unauthorized users

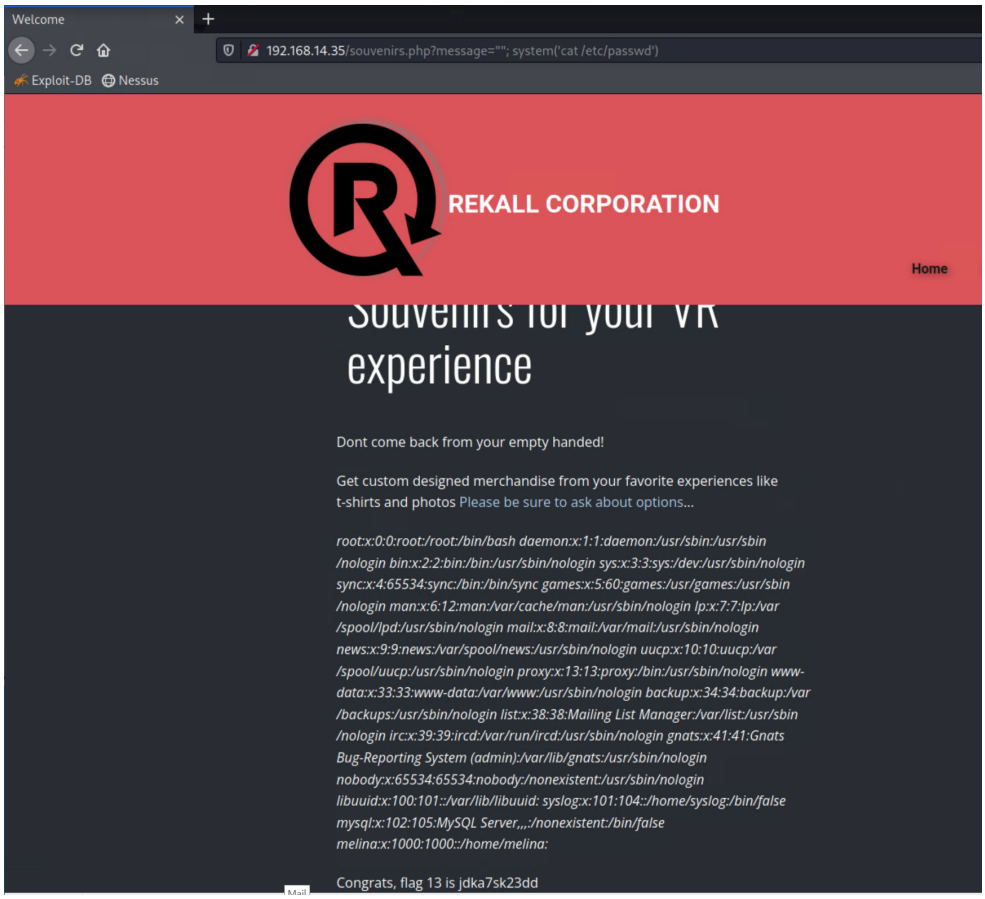
Vulnerability 13	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An aggressive Nmap scan nmap -A 192.168.13.0/24 to discover the host that runs Drupal

Images	 
Affected Hosts	192.168.13.12
Remediation	Keep this information hidden from unauthorized users

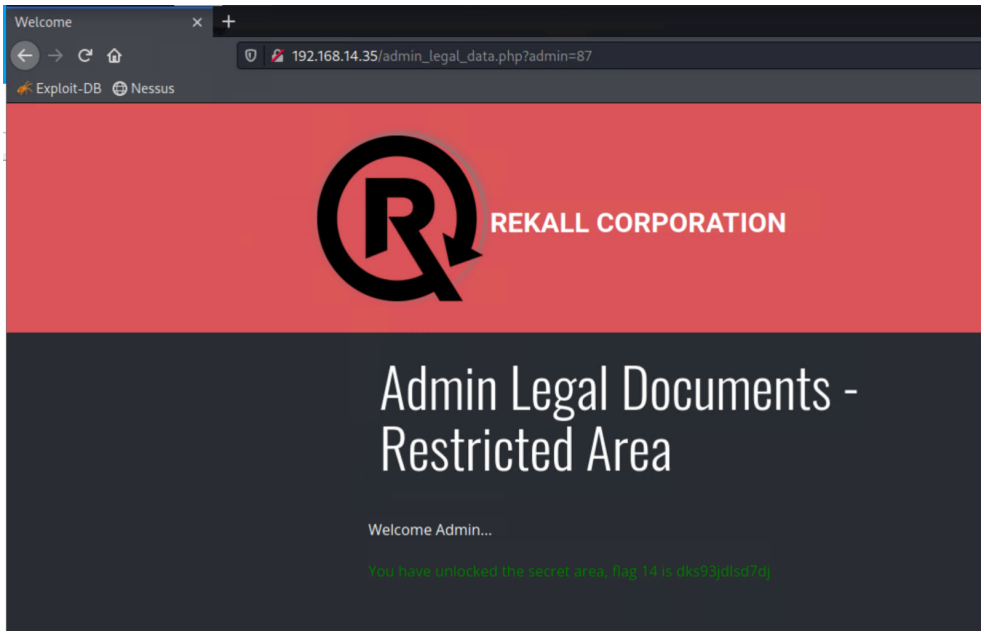
Vulnerability 14	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App

Risk Rating	Critical
Description	Entered <script>alert(“hi there”)</script> into the comment section, and this will then alert every user to click on the post.
Images	
Affected Hosts	192.168.14.35
Remediation	I would recommend implementing a strong content security policy. This would help block any abnormal request and limit cross site scripting. You can also add input validation.

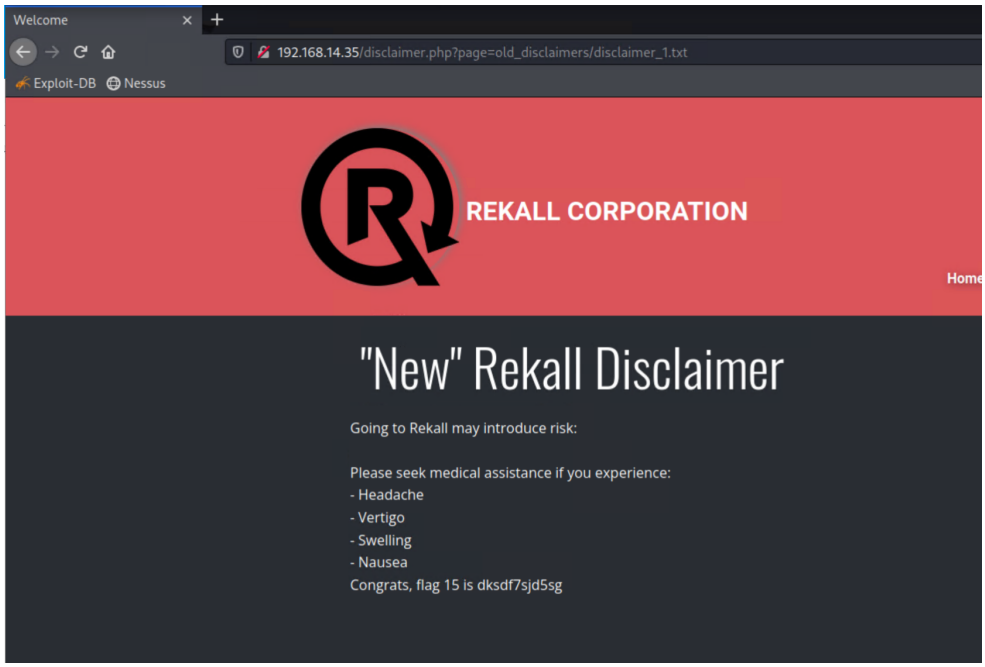
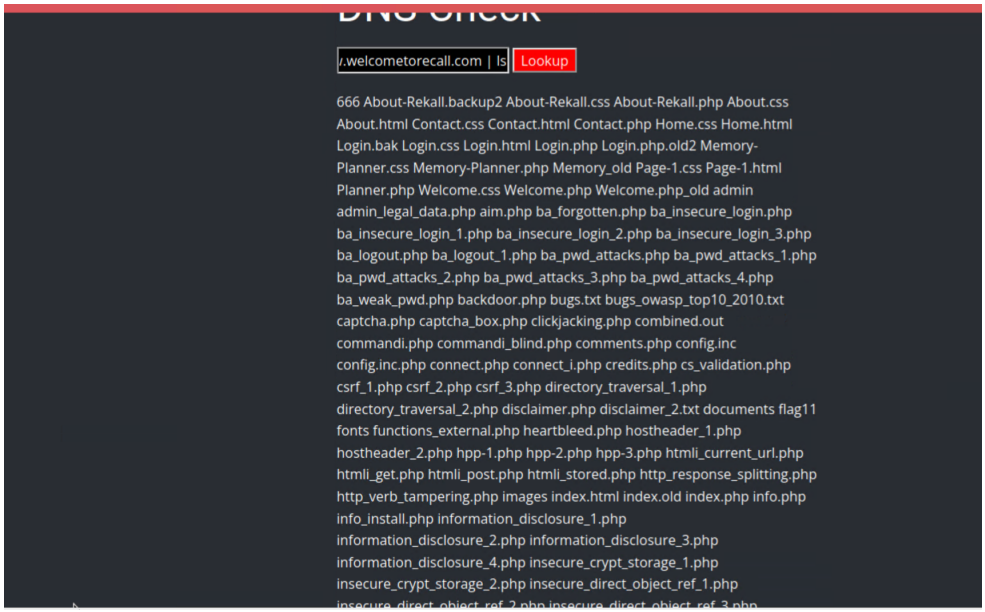
Vulnerability 15	Findings
Title	PHP injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	The hidden webpage was identified in the robots.txt file found in Flag 9. The payload was entered into the URL to exploit the vulnerability.

Images	
Affected Hosts	192.168.14.35
Remediation	Input validation will help with this exploit. This will help ensure that actors do not have the opportunity to attack against the web application.

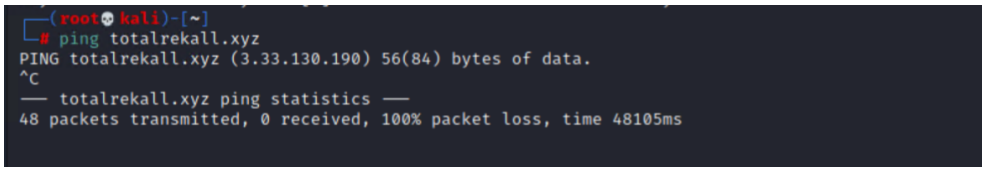
Vulnerability 16	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	The link to this page was found in flag 12. Needed to test out different session IDs in the URL, and with session 87 the flag was found.

Images	
Affected Hosts	192.168.14.35
Remediation	The cookie session must be more protected to avoid this vulnerability. Rekall must add stronger encryption to protect confidential sessions, so that the browser does not return to certain sessions.

Vulnerability 17	Findings
Title	Directory traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using the vulnerability from flags 10 and 11 were able to discover the old_disclaimer directory. Then using directory traversal we were able to find the new exploit.

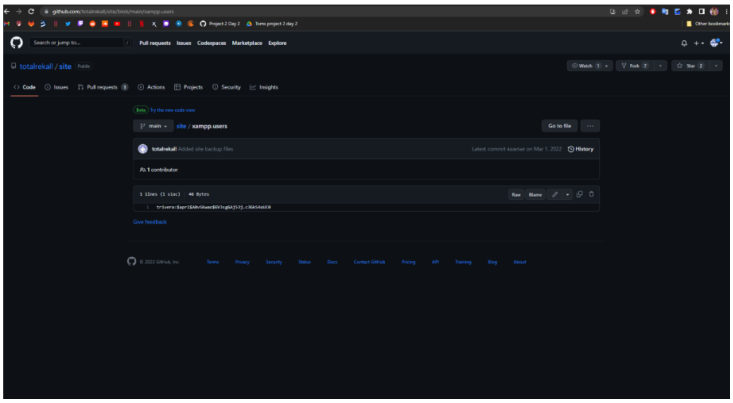
Images	 
Affected Hosts	192.168.14.35
Remediation	Same remediation from flags 10 and 11 to avoid actors finding certain directories that actors can get into by using directory traversal. To avoid directory traversal I would recommend limiting the web server access to certain confidential directories.

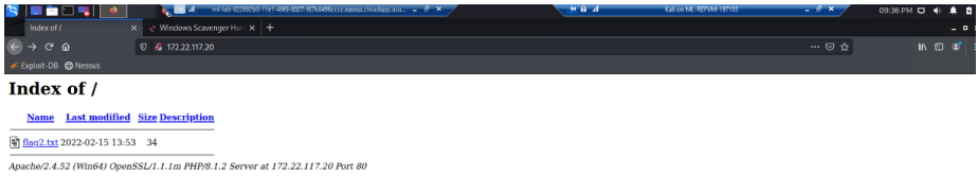
Vulnerability 18	Findings
Title	ping totalrekall.xyz
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical

Description	In Kali terminal ran the command ping totalrekall.xyz
Images	
Affected Hosts	totalrekall.xyz
Remediation	Ping request gives actors to detect network subnets to find potential hosts. I would block ping requests to any server to not allow actors to gain useful information to attack the network.

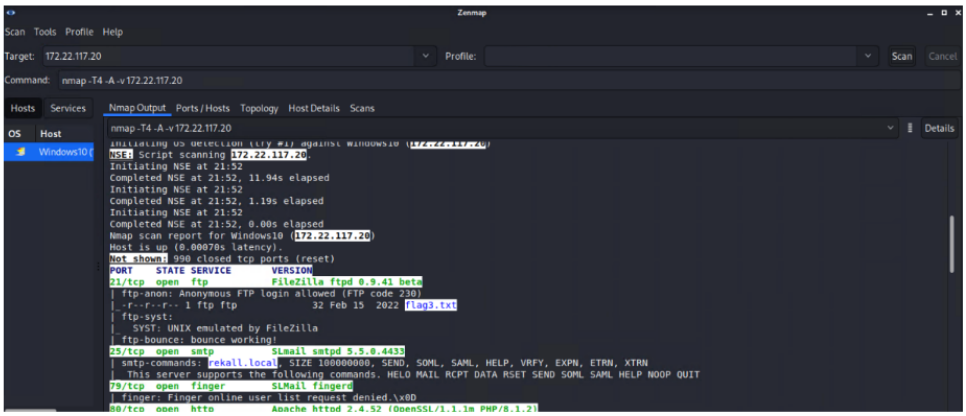
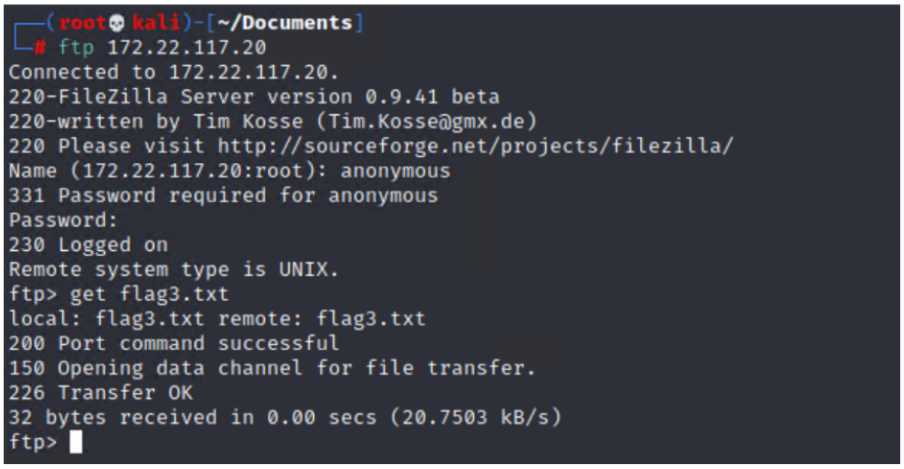
Vulnerability 19	Findings
Title	Nessus scan results
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Ran a Nessus scan on 192.167.13.12 to find the vulnerability.
Images	
Affected Hosts	192.168.13.12
Remediation	Using Nessus on IP addresses allows actors to find potential vulnerabilities, and with this scan we did find on which was Apache Struts. I would recommend doing their research to know more about vulnerabilities in their own system, and to mitigate the damage. Add tools to constantly monitor the network in order to find if actors are attacking these exploits.

Vulnerability 20	Findings
Title	Tanya4life
Type (Web app / Linux OS / WIndows OS)	Windows OS

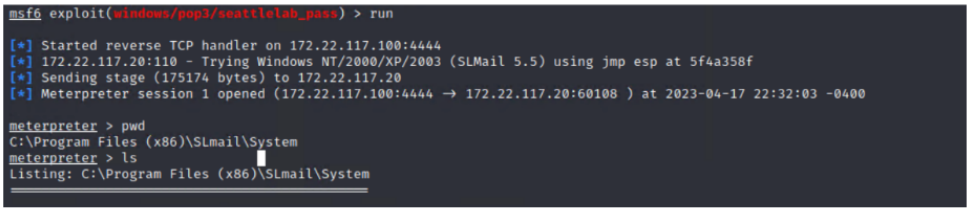
Risk Rating	Critical
Description	Sensitive data exposure by using the password that was found in the totalrekall gitHub repository. Using John the Ripper on the password hash that was found we were able to discover that the password was Tanya4life.
Images	
Affected Hosts	github.com/totalrekall
Remediation	Do not allow certain information that actors can find and use to attack the network. Also to secure user credentials with strong encryption.

Vulnerability 21	Findings
Title	Password guessing
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the credentials from the previous flag and knowing that 172.22.117.20 has an open port 80.
Images	
Affected Hosts	172.22.117.0/24 172.22.117.20 172.22.117.10
Remediation	First change the trivera credentials. Add a strong firewall to prevent access to the network because it controls ports. Knowing if a port scan is happening will allow you time to protect the network.

Vulnerability 22	Findings
Title	Vulnerable FTP port 21

Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using NMAP scan on 172.22.117.20 reveals an open port.
Images	 
Affected Hosts	172.22.117.20
Remediation	In port 21 anything that is sent through this is in plain text. This is why they need to close port 21 to avoid this exploitation.

Vulnerability 23	**Findings**
Title	Vulnerable Port
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using metasploit console to get a meterpreter session by setting RHOSTS to 172.22.117.20.

Images	
Affected Hosts	172.22.117.20
Remediation	Recommend to patch your email servers to avoid this vulnerability.