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	Spark LLC
Contact Name	Jaylan Howden
Contact Title	Chief Information Security officer

Document History

Version	Date	Author(s)	Comments
001	April, 29 2024	Jaylan Howden	Day 1
002	April, 30 2024	Jaylan Howden	Day 2
003	May, 1 2024	Jaylan Howden	Day 3

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.

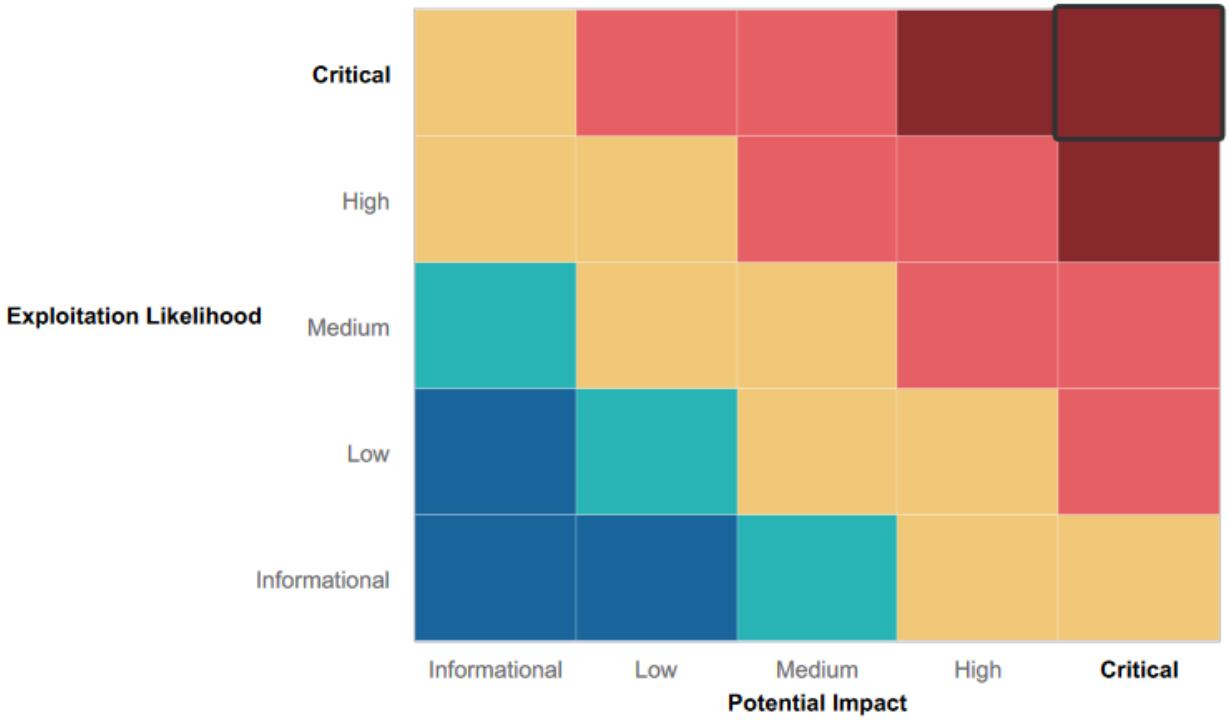
Executive Summary of Findings

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.

- Input validation being used to reduce risk of SQL Injection, Cross site scripting, Directory Traversal and Command Injection
- Great offensive and defensive security plan
- Network is up and running

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.

- The web application is vulnerable to SQL injection and Cross-site scripting (XSS).
- SSH open to login from outside of network
- Old Apache server susceptible to attack
- Privilege Escalation.
- 5 IP addresses open to being scanned
- Numerous open ports on both Linux and Windows Servers
- Old Drupal Service susceptible to attack
- Sensitive login credentials and company data available on open github repository

Executive Summary

Spark LLC successfully achieved all objectives outlined in the scope of work for this penetration test. Our team precisely executed each phase of the test, including Reconnaissance, Identification of Vulnerabilities and Services, Vulnerability Exploitation, and Reporting. During this process, we located credentials, used them to access Rekall's local network, escalated our privileges to administrator, and compromised critical servers such as the Apache and SLMail servers, as well as two additional machines on the network.

In the first stage of our attack on Rekall's web application, our team found and tested numerous known attacks and exploits on the web application. Spark LLC found that the web application was vulnerable to cross-site scripting attacks on the webpage. The webpage was susceptible to reflected and stored cross-site scripting attacks on numerous pages throughout the web application allowing for scripts to be carried out on the web application. Next, our team was able to find that the web app was also vulnerable to local file inclusion attacks which allowed our team to upload files onto the VR Planner web page. Furthermore, Spark LLC was able to successfully input malicious SQL commands onto the login.php toolbar on the web application. Another attack we found while searching through the web application was that it is susceptible to command injection attacks on the networking.php web page while revealing sensitive data.

In addition to further investigation our team through reconnaissance using OSINT we found using a search on crt.sh exposed stored certificates showing data. Furthermore, our team found user credentials openly exposed in the HTML source code on the login.php web page in plain view. Additionally, the robots.txt file was found through our reconnaissance and provided confidential information that is available to the general public. Further research by Spark LLC uncovered another user's credentials on an open GitHub repository which led our team to gain unauthorized access to the web host files and directories from the GitHub repository. Furthermore, the information gained from GitHub, should not be open to the public internet as it can have catastrophic effects due to what is contained on GitHub.

Next Spark LLC started to deploy our test into the Linux network. Through a port and network scan using Mmap our team discovered 5 open public IP addresses. Using the results from the Nmap scan we found a host running and using an old version of Drupal. Using the stolen credentials gained during reconnaissance our team was able to gain access using SSH Port 22 and escalate our privileges to root-level users. Also using Metasploit in Kali Linux our team was able to run a reverse code execution attack using Metasploit interpreter which gave our team admin access.

Subsequently, Spark LLC continued our testing into the Windows OS domain. Our team first started the test on the Windows OS domain by conducting a port scan using Nmap. The port scan results indicated that numerous ports were open and susceptible to exploits such as Port 21(FTP), and Port 21(SLMailService). Using Metasploit again using previous credentials found earlier in the test we conducted an exploit using a reverse shell which gave our team access where we then scheduled tasks in the Windows Machine Scheduler as root-level users. Furthermore using Kiwi a module in Metasploit we were able to dump usernames and password hashes. Using John the Ripper on Kali Linux we were able to crack the passwords and gain more user credentials.

In conclusion, Spark LLC would like to thank Rekall Corporation for letting our team conduct this penetration test on your network and systems. Throughout the penetration test, our team was able to find numerous CVE vulnerabilities and old outdated vulnerable Applications and Operating systems. These vulnerabilities should be resolved ASAP as if not they can have financial repercussions and great damage to day-to-day operations for Rekall and damage to Rekall's reputation. Our team has shown each exploitation that we completed successfully and notes on recommendations to resolve the exploitations that were found. Thank you again Rekall Corporation and we hope to continue our partnership in business in the future.

Summary Vulnerability Overview

Vulnerability	Severity
XSS reflected	Critical
Local File Inclusion	Critical
XSS Stored	Critical
Open source exposed data	Medium
SQL Injection	Critical
Command Injection	Critical
Open source exposed data	Medium
Certificate Search using crt.sh	Medium
User Credentials Exposure	Critical
Sensitive Data Exposure	Medium
Unsecured HTML	High
Using User Credentials	Critical
Local file inclusion	Critical
Directory traversal	Critical
Data exposed on crt.sh	Medium
Aggressive Nmap Scan	Critical
Nmap Scan Results	Critical
Data on Dossier	Medium
Nessus Scan Results	Critical
Privilege Escalation	Critical
Exposed data on totalrekall Public GitHub site	Critical
FTP Login	High
SLMAIL Metasploit Exploit	High
LSA Dump	Critical

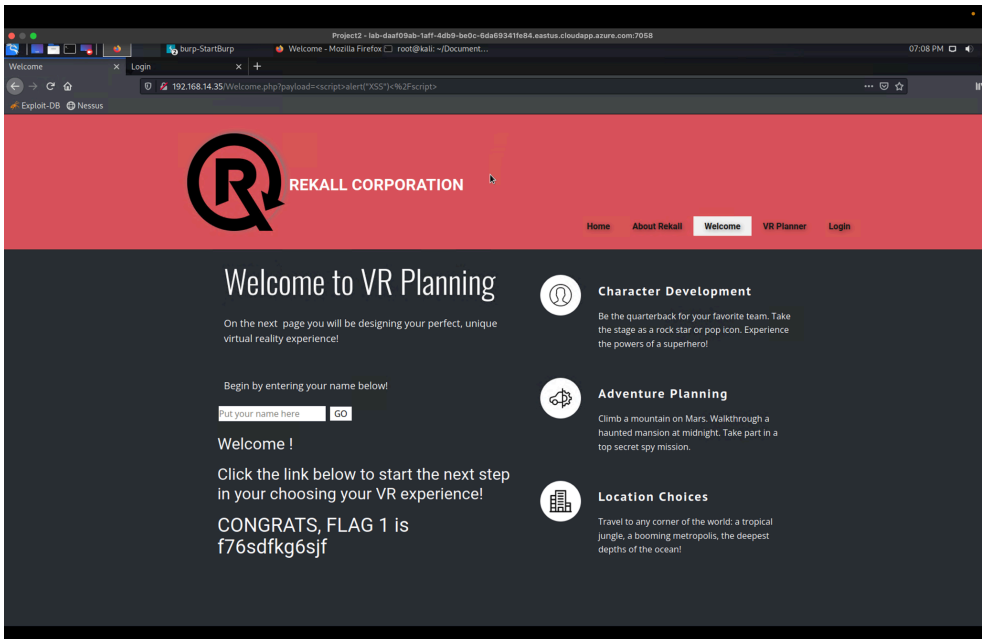
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	34.102.136.180 : totalrekall.xyz 192.168.13.10 : Linux 192.168.13.11 : Linux 192.168.13.12 : Linux 192.168.13.13 : Linux 192.168.13.14 : Linux 192.168.13.1 : Linux 172.22.117.20 : Windows 10 172.22.117.10 : Windows Domain Controller 172.22.117.100 : Windows host
Ports	21(FTP) 22(SSH) 80(HTTP) 106(TCP) 110(POP3) 587(SMTP)

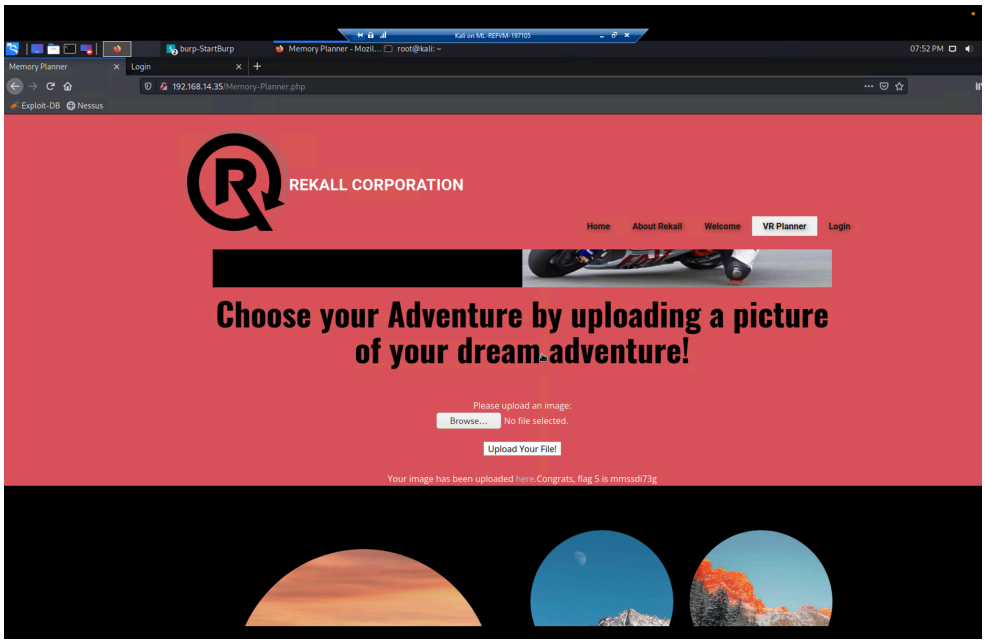
Exploitation Risk	Total
Critical	16
High	3
Medium	6
Low	0

Vulnerability Findings

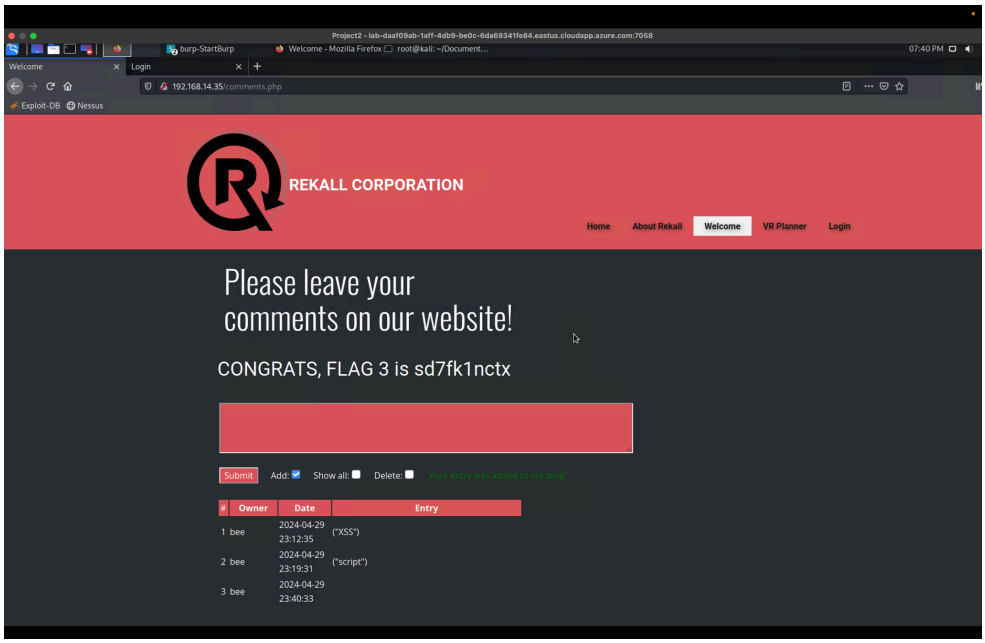
Vulnerability 1	Findings
Title	XSS reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Malicious script successfully reflected on host home page <script>alert(Document.cookie)</script>

Images	
Affected Hosts	192.168.14.35
Remediation	Require input validation throughout the web app

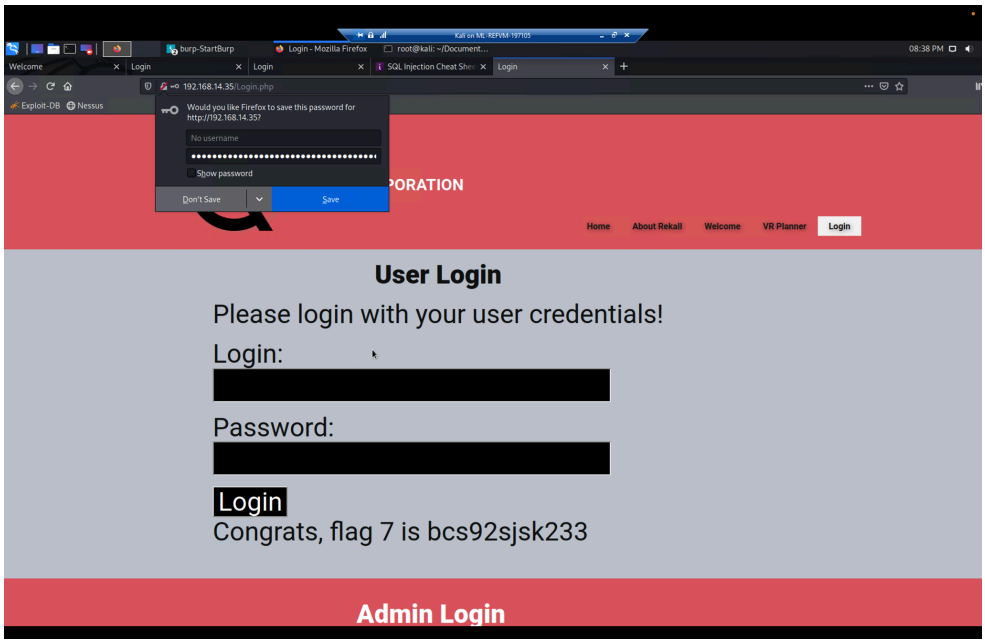
Vulnerability 2	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	LFI was successfully completed, and a.php file was submitted using the VR Planner page's toolbar.

Images	
Affected Hosts	192.168.14.35
Remediation	Prevent file paths from being able to be appended directly; if possible, restrict API to allow inclusion only from a directory and the directories below it

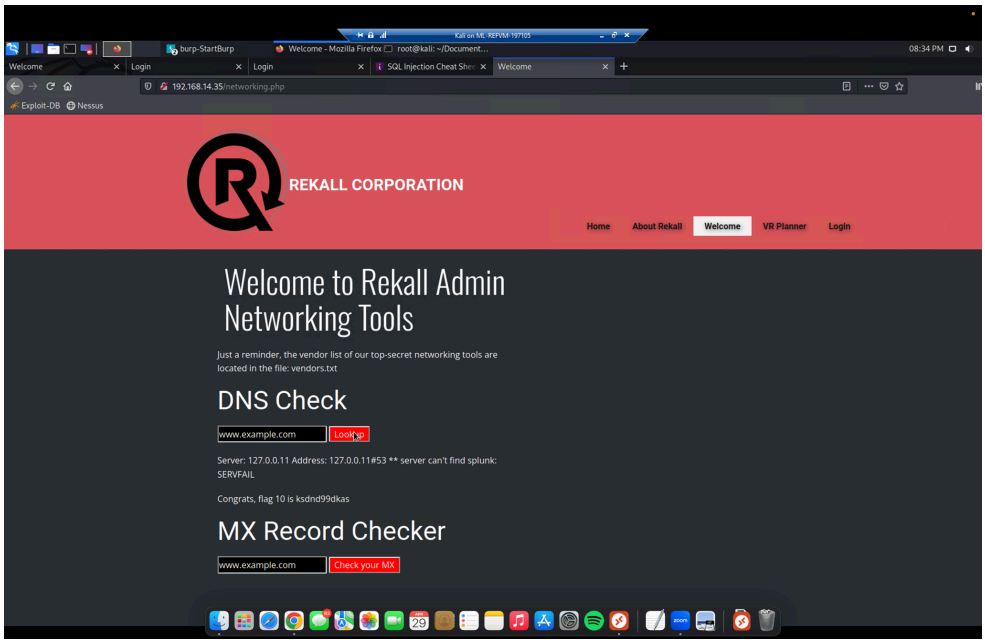
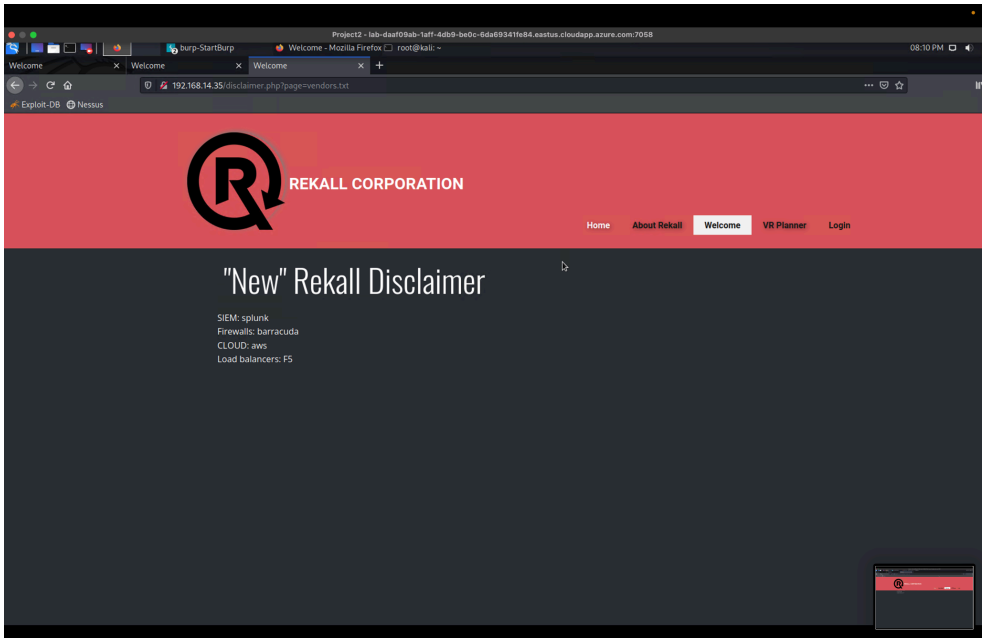
Vulnerability 3	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	While accessing /Comments page, entered <script>alert(“Hi”)</script> to reveal Flag 3

Images	
Affected Hosts	192.168.14.35
Remediation	Implement XSS protection to disallow injection of script code

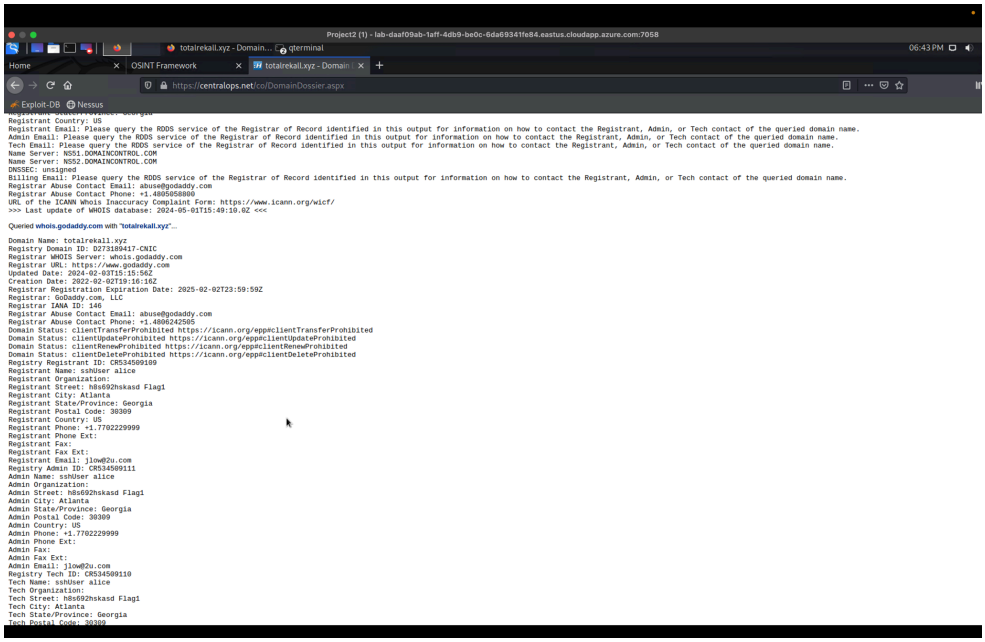
Vulnerability 4	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	While accessing /Login.php page, payload (Name or “1=1”) was entered in toolbar intended for password successfully resulting in exploit

Images	
Affected Hosts	192.168.14.35
Remediation	Disallow web app to accept direct input and/or implement character escaping

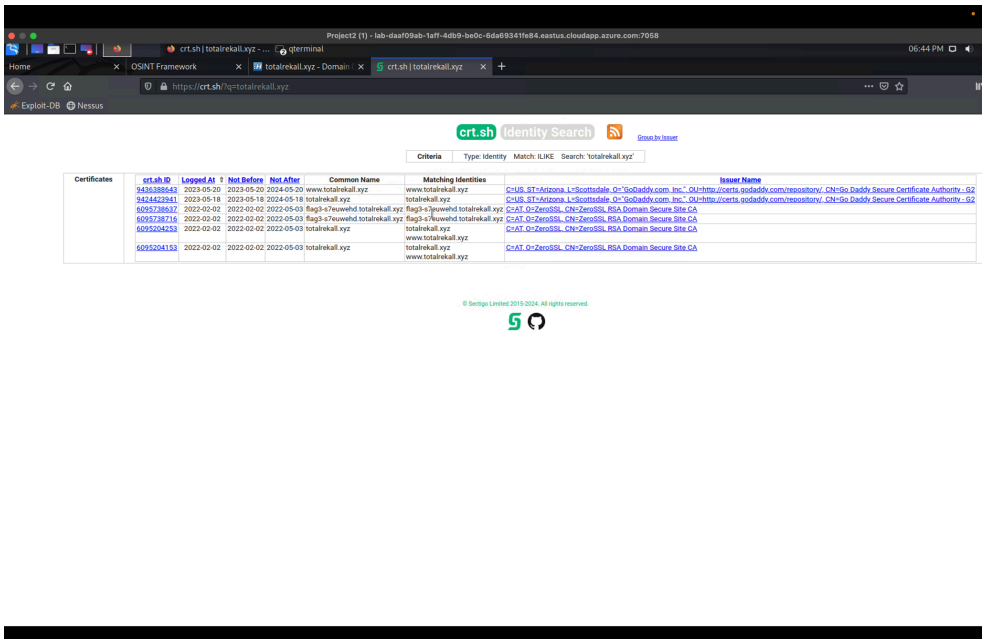
Vulnerability 5	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Navigation allowed from /Networking.php to 192.168.14.35/disclaimer.php?page=vendors.txt via 192.168.14.35/networking.php Able to input “splunk” inside of toolbar intended for DNS Check

Images	 
Affected Hosts	192.168.14.35
Remediation	Implement input validation that does not leak important data

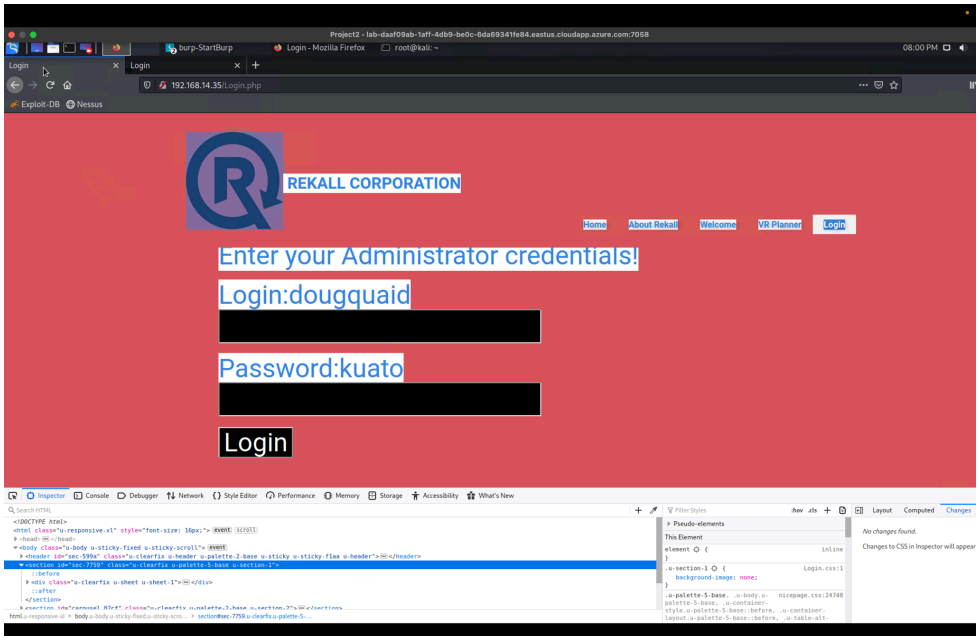
Vulnerability 6	Findings
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	On the Domain Dossier webpage, viewed the WHOIS data with OSINT for

	Total rekall.xyz to access sensitive information
Images	
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Ensure no sensitive data is being shared publicly, clean up WHOIS records

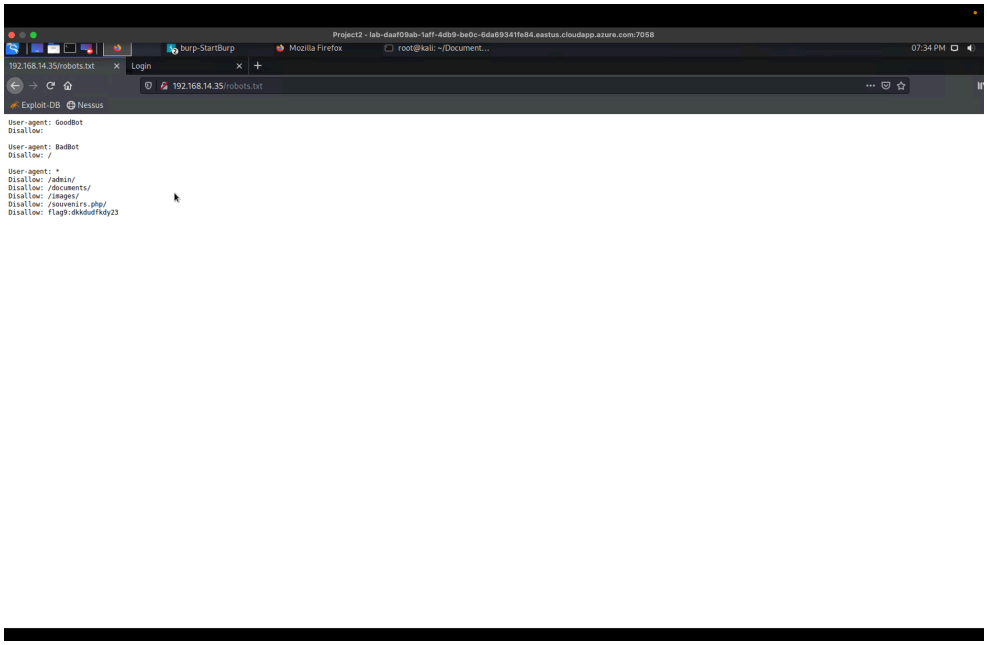
Vulnerability 7	Findings
Title	Certificate Search using crt.sh
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Searched for totalrekall.xyz on crt.sh, found stored certificate

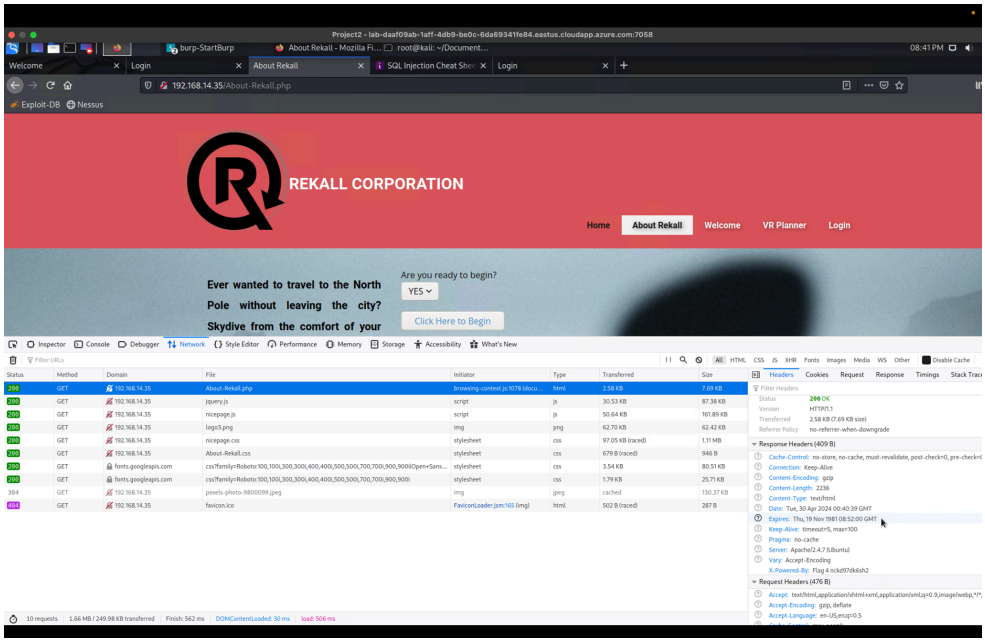
Images	
Affected Hosts	34.102.136.180
Remediation	Protect information from being exposed by the crt.sh site

Vulnerability 8	Findings
Title	User Credentials Exposure
Type (Web App / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	User credentials are visible within HTML of the Login.php and when highlighting page in a web browser

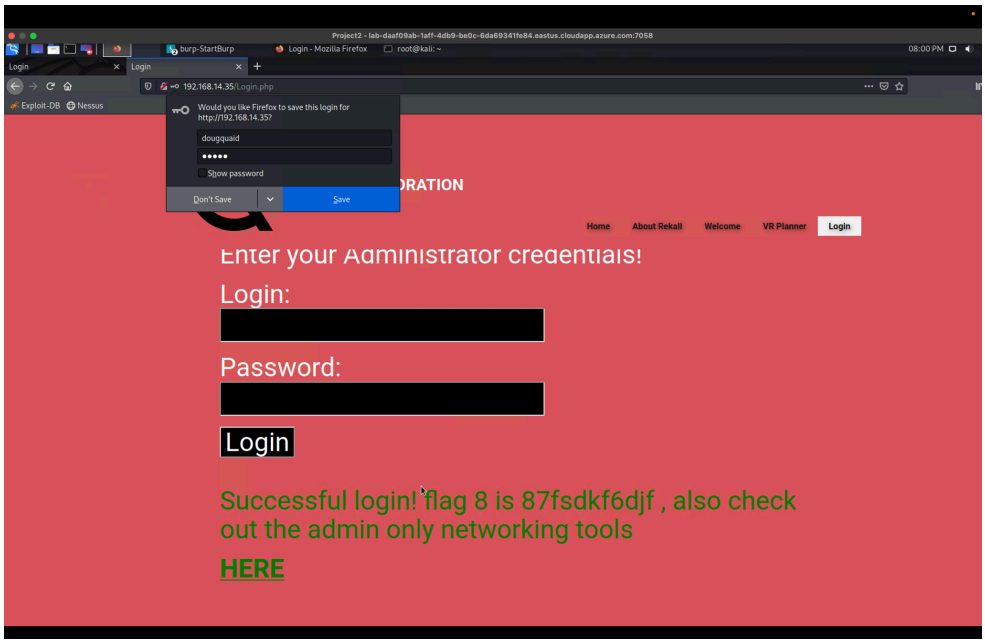
Images	
Affected Hosts	192.168.14.35
Remediation	Delete this information from the HTML, implement 2-factor authentication for enhanced security-

Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Unrestricted access to robots.txt page

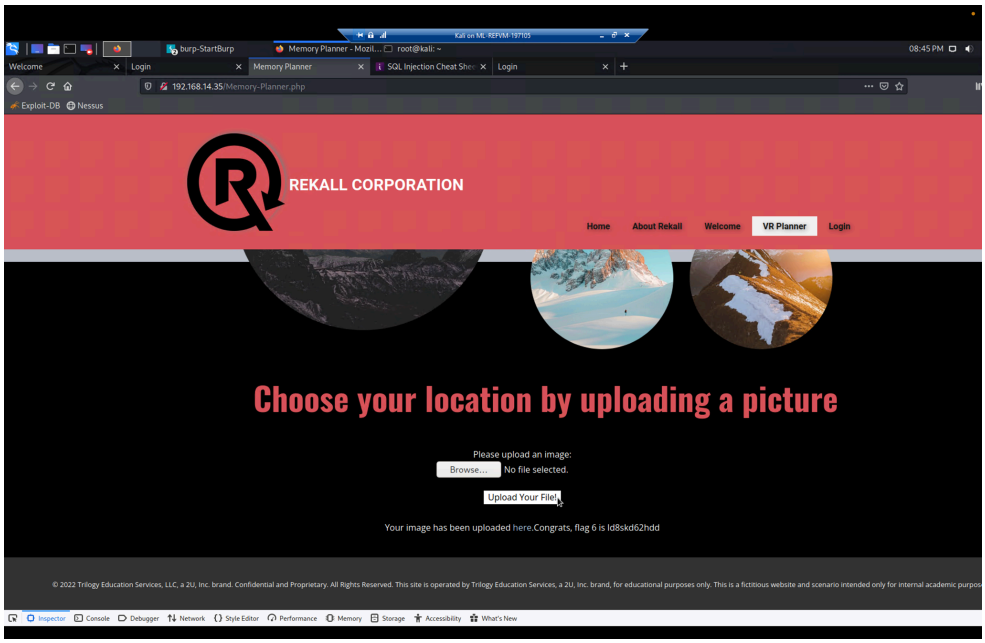
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to robots.txt to authorized users only

Vulnerability 10	Findings
Title	Unsecured HTML
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	The flag appears in the HTTP response headers. These headers can be seen using BURP or via a cURL request, such as: curl -v http://192.168.14.35/About-Rekall.php
Images	
Affected Hosts	192.168.13.14
Remediation	Restrict what information is shown on headers

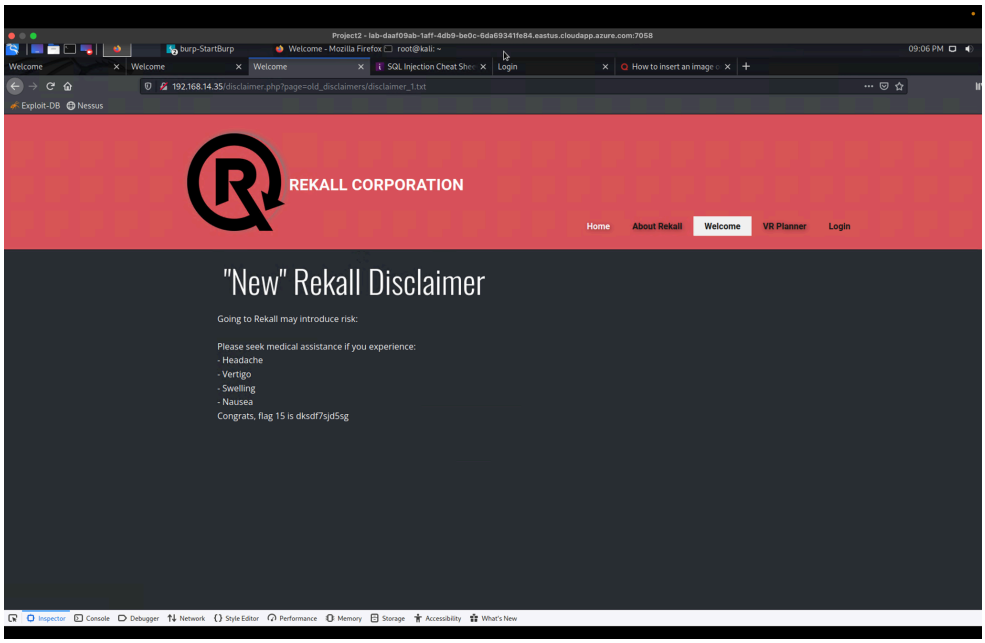
Vulnerability 11	Findings
Title	Using User Credentials
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using the user credentials found in the html we were able to login

Images	
Affected Hosts	192.168.13.14
Remediation	Clean up html files so that user credentials are not seen by unwanted users.

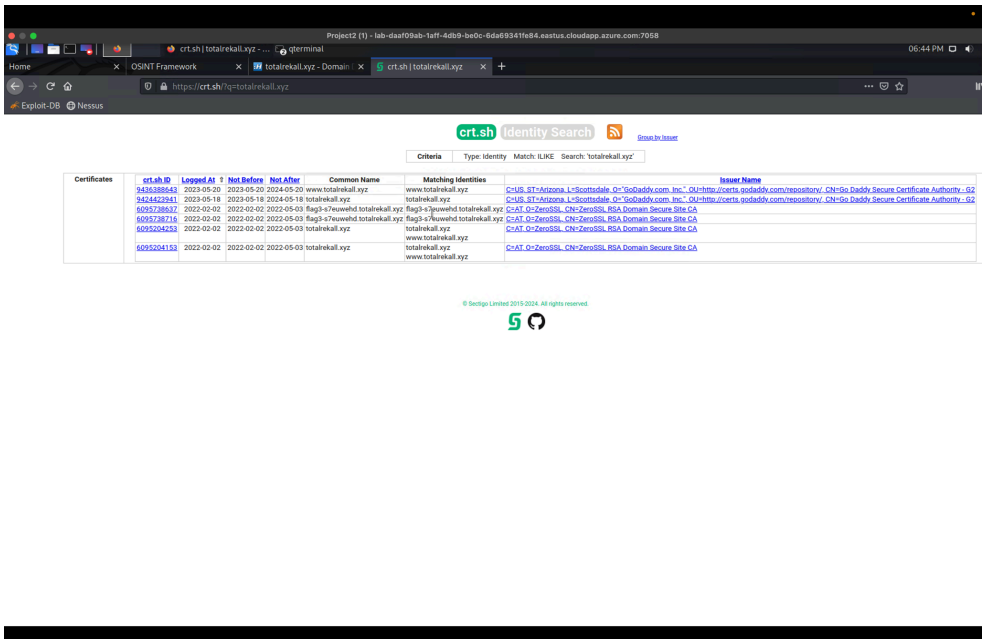
Vulnerability 12	Findings
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	The input validation checks for the presence of .jpg, so to bypass this upload, we named our malicious script: script.jpg.php

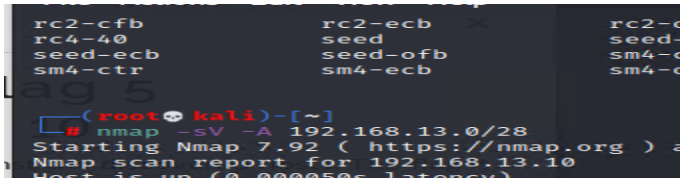
Images	
Affected Hosts	192.168.13.14
Remediation	Make sure that the files being uploaded are actual jpg files and not other files with jpg added to the end of them

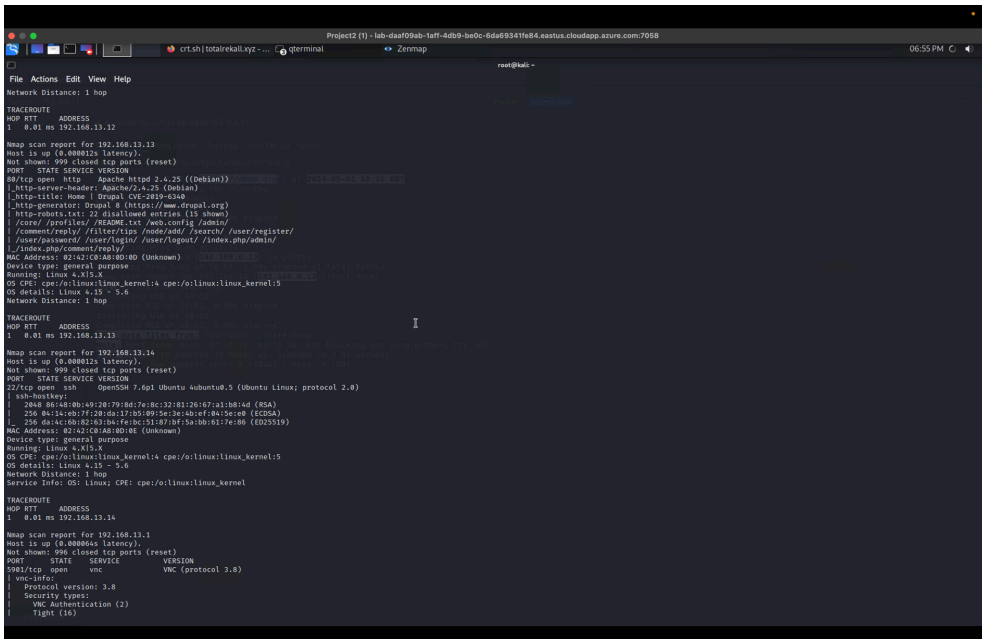
Vulnerability 13	Findings
Title	Directory traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Using directory traversal we changed the url to http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt to find this web page that houses the “new” disclaimer for rekall

Images	
Affected Hosts	192.168.13.14
Remediation	Remove old files from the web app so they cannot be accessed through directory traversal.

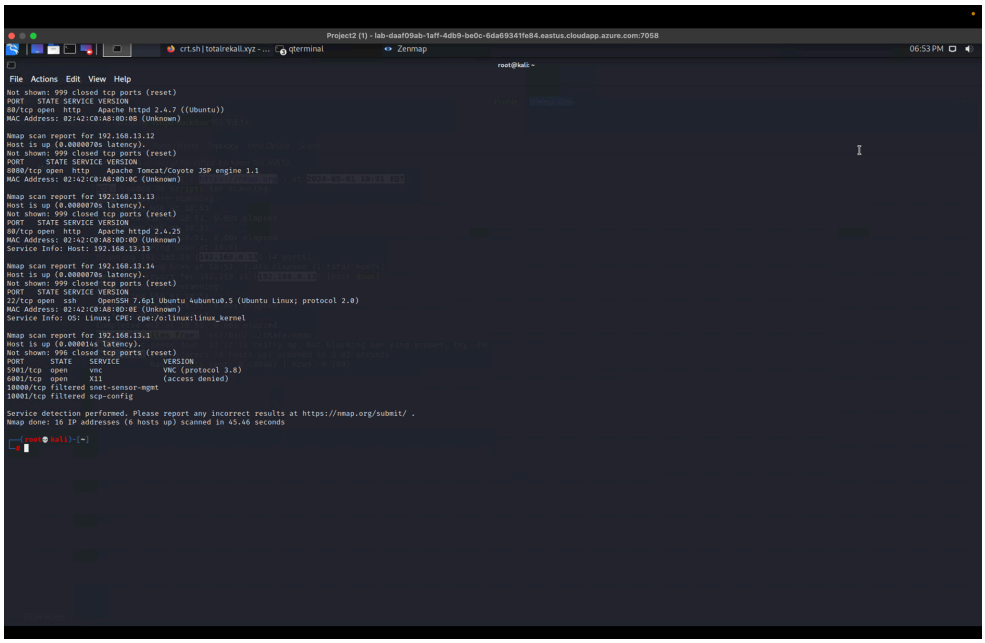
Vulnerability 14	Findings
Title	Data exposed on crt.sh
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Medium
Description	Certificate information on crt.sh

Images	
Affected Hosts	
Remediation	

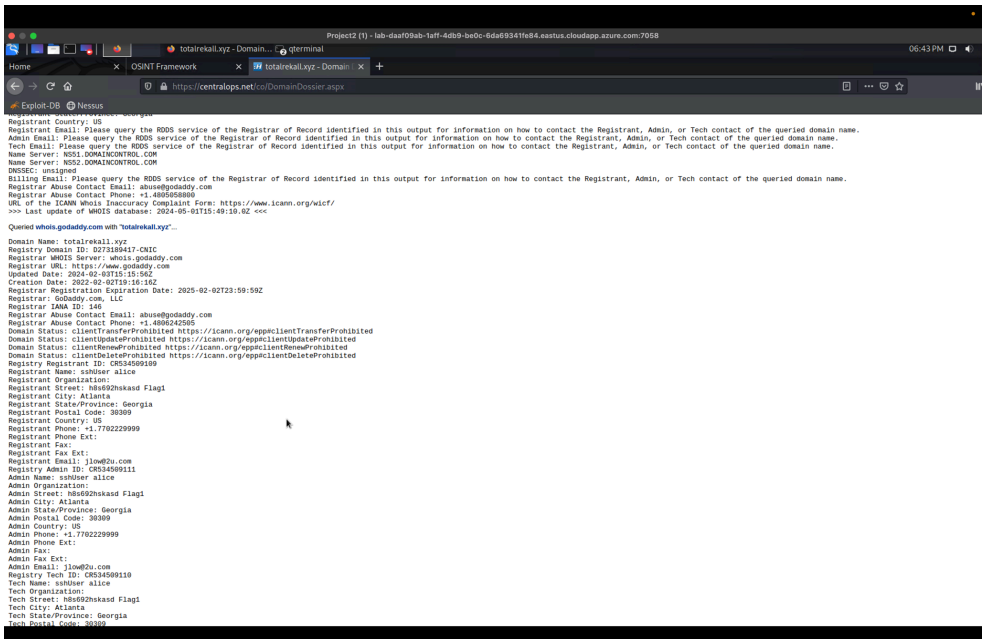
Vulnerability 15	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Ran aggressive Nmap scan (Nmap -A 192.168.13.0/28) to discover host running Drupal
Images	

	
Affected Hosts	192.178.13.12
Remediation	Block probes, restrict information returned, slow down the aggressive Nmap scan, and/or return misleading information

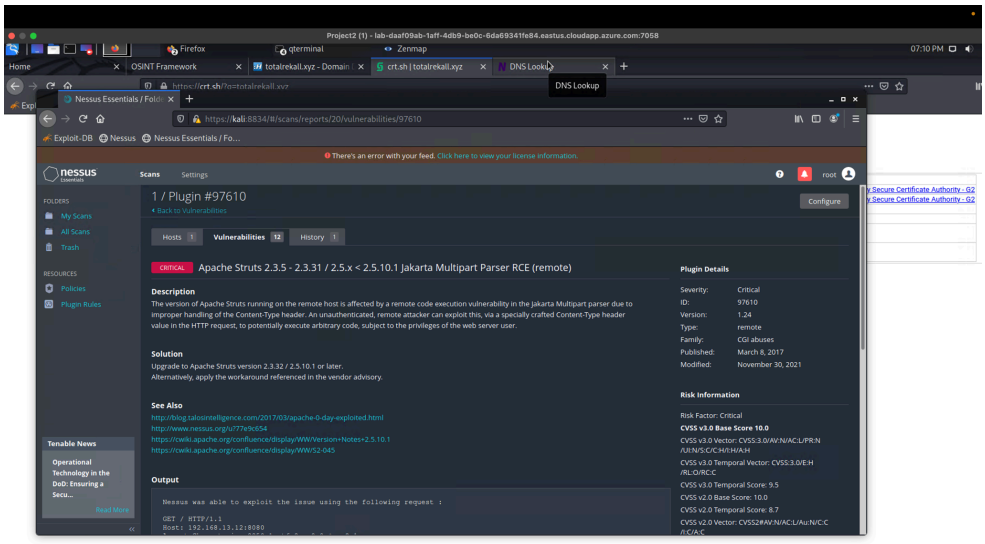
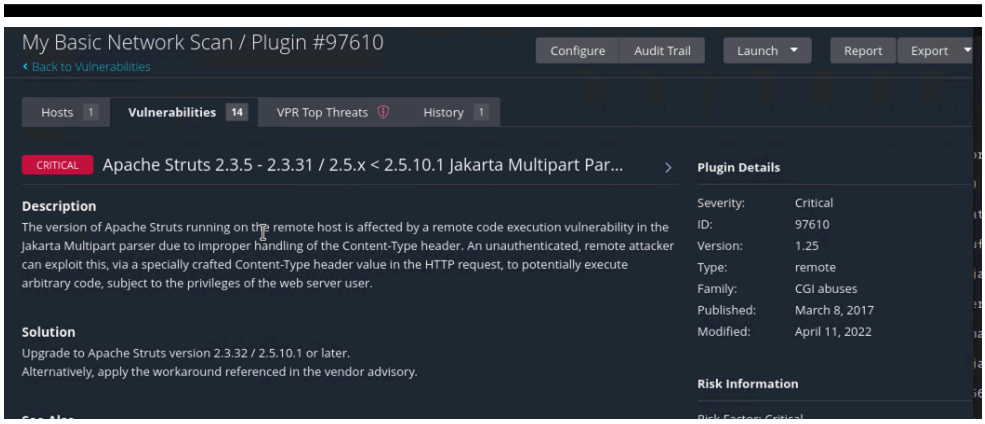
Vulnerability 16	Findings
Title	Nmap Scan Results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	An Nmap scan on 192.168.13.0/24 revealed 5 hosts are visible with exposed IP's

Images	
Affected Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
Remediation	Implement IP blocking for unauthorized users

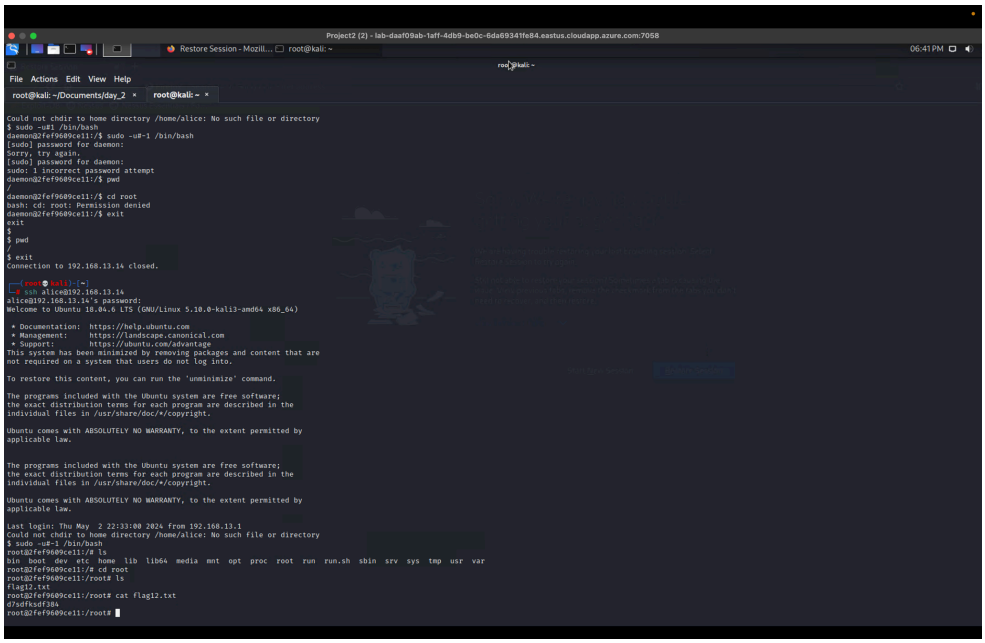
Vulnerability 17	Findings
Title	Data on Dossier
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Medium
Description	On the Domain Dossier webpage, we viewed the WHOIS data for totalrekall.xyz.

Images	
Affected Hosts	192.168.13.14
Remediation	Make sure that the data on domain dossier does not contain sensitive information

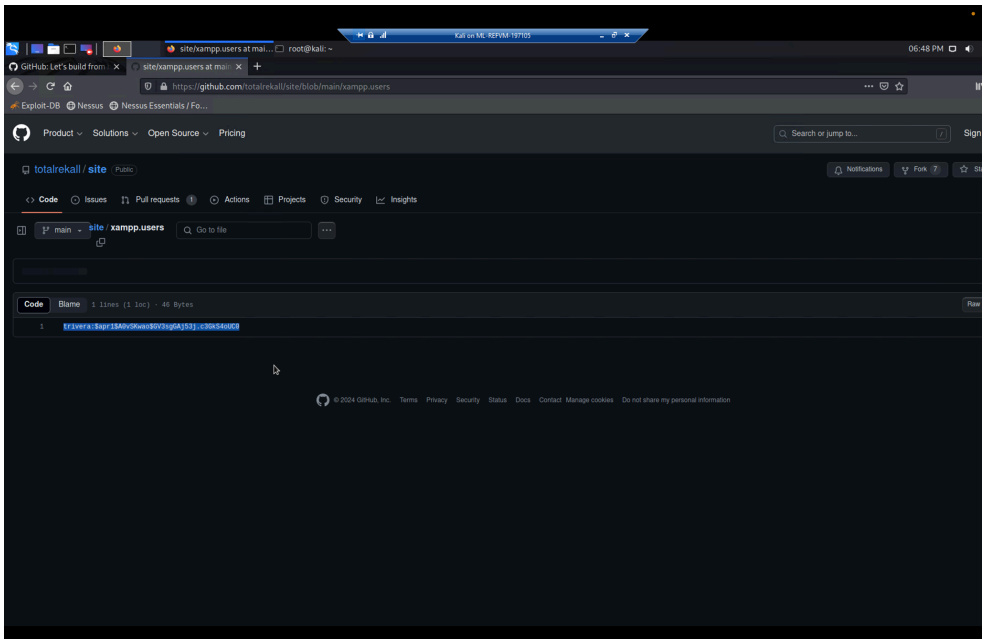
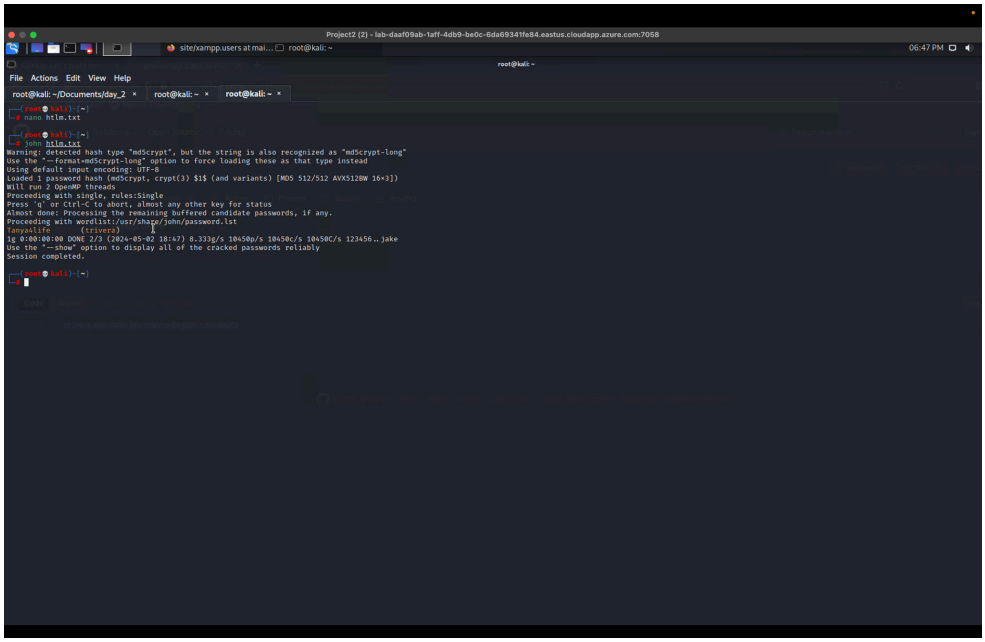
Vulnerability 18	Findings
Title	Nessus scan results
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Running a nessus scan we found that the system had many a vulnerability on the apache server

Images	 
Affected Hosts	192.168.13.12
Remediation	Perform and conduct regular updates on apache and other server so they are not susceptible to exploits

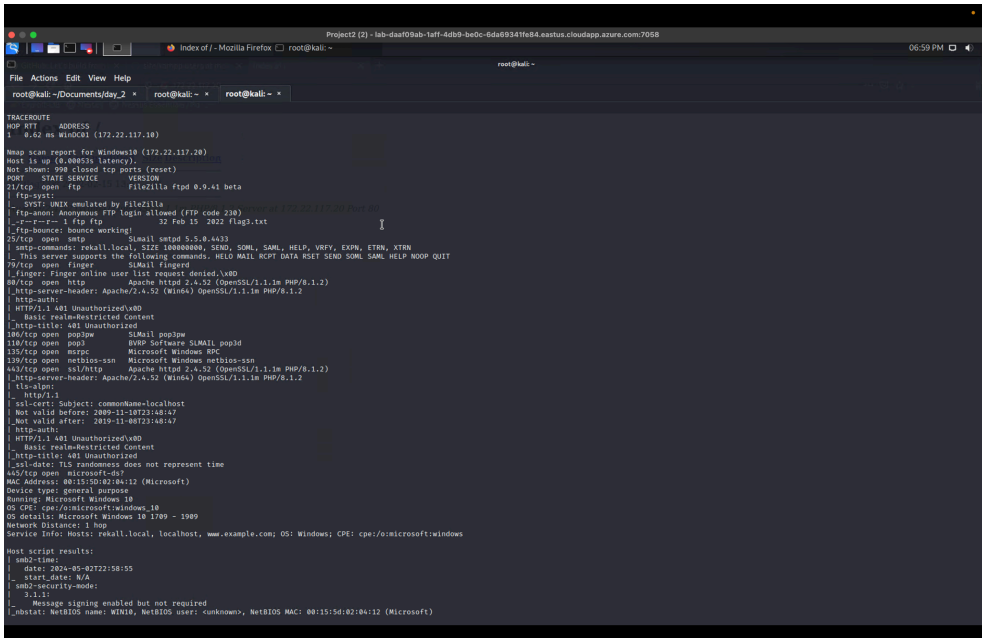
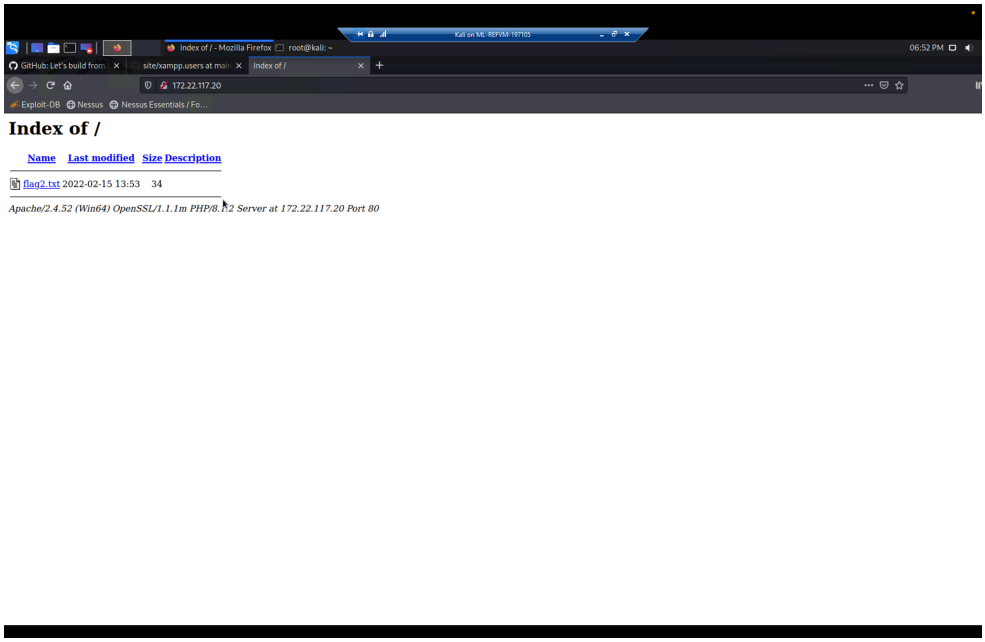
Vulnerability 19	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	Using stolen credentials, our team was able to ssh and escalate our privileges to root

Images	
Affected Hosts	192.168.13.14
Remediation	Close port 22, enforce stronger credentials, and/or implement 2-factor authentication

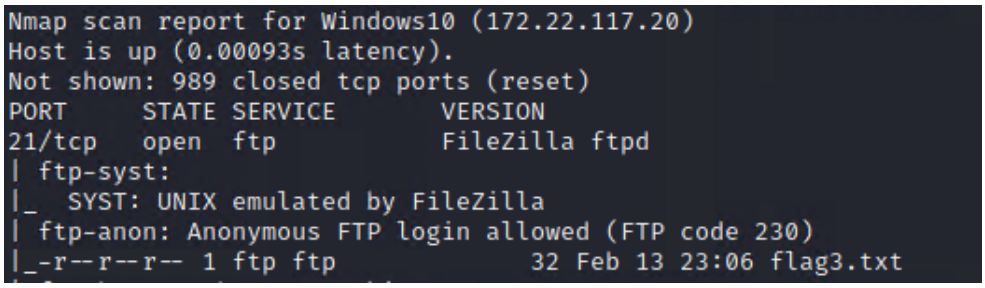
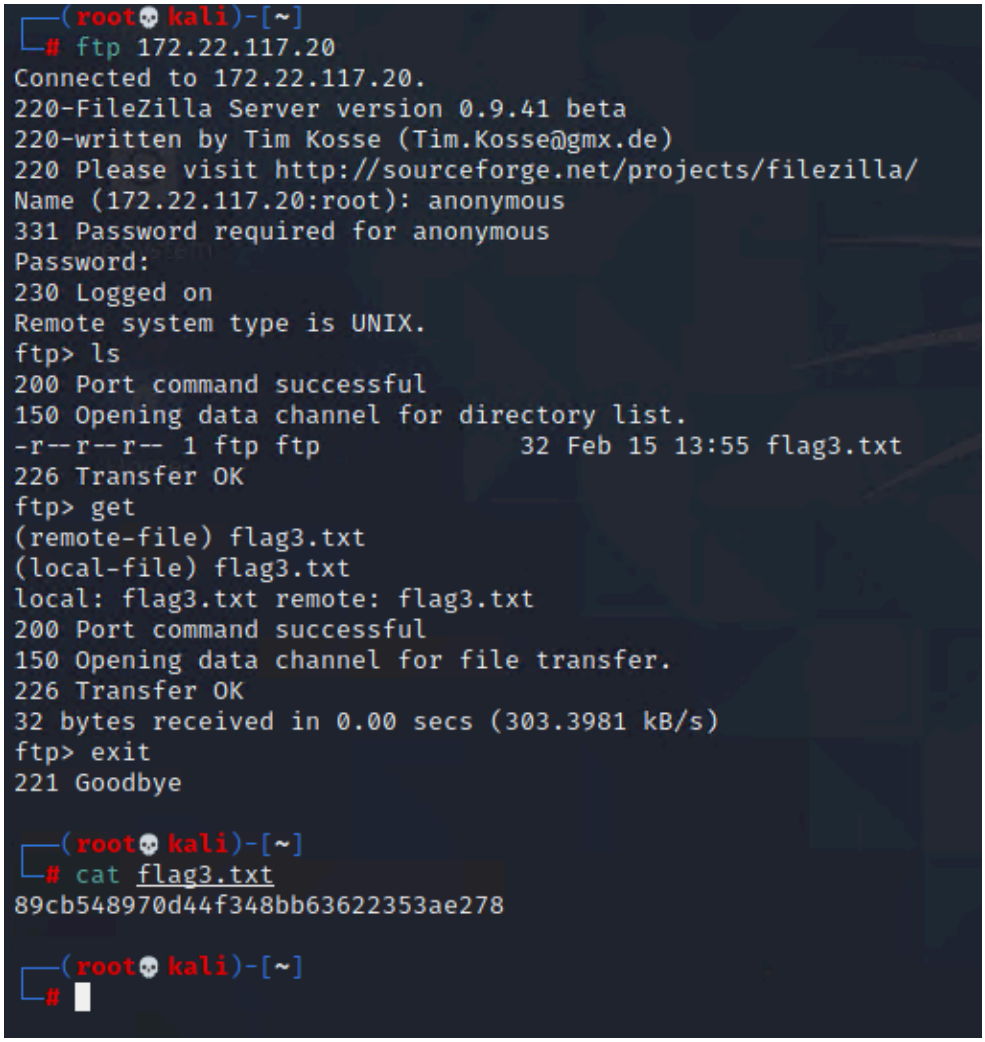
Vulnerability 20	Findings
Title	Exposed data on totalrekall Public GitHub site
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	We discovered that the public GitHub site for totalrekall had an exposed hash for a user. We were able to crack the hash using john the ripper.

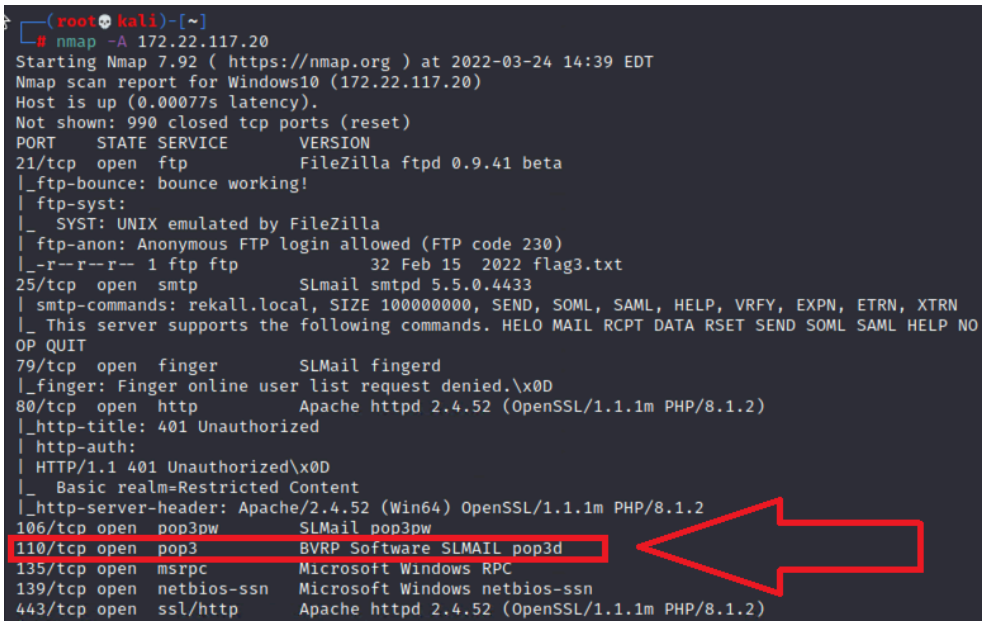
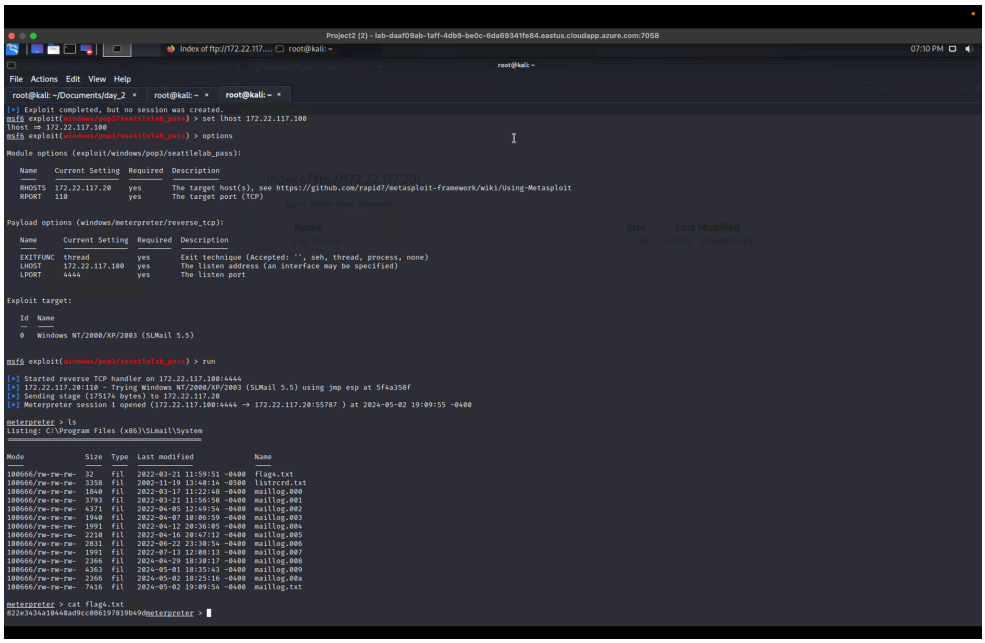
Images	 
Affected Hosts	172.22.117.20:Windows10 172.22.117.10:Windows Domain Controller 172.22.117.100:Windows host
Remediation	Remove hashes from the Github site, Salt hashes to make them more difficult to crack, Require complex passwords that are regularly updated.

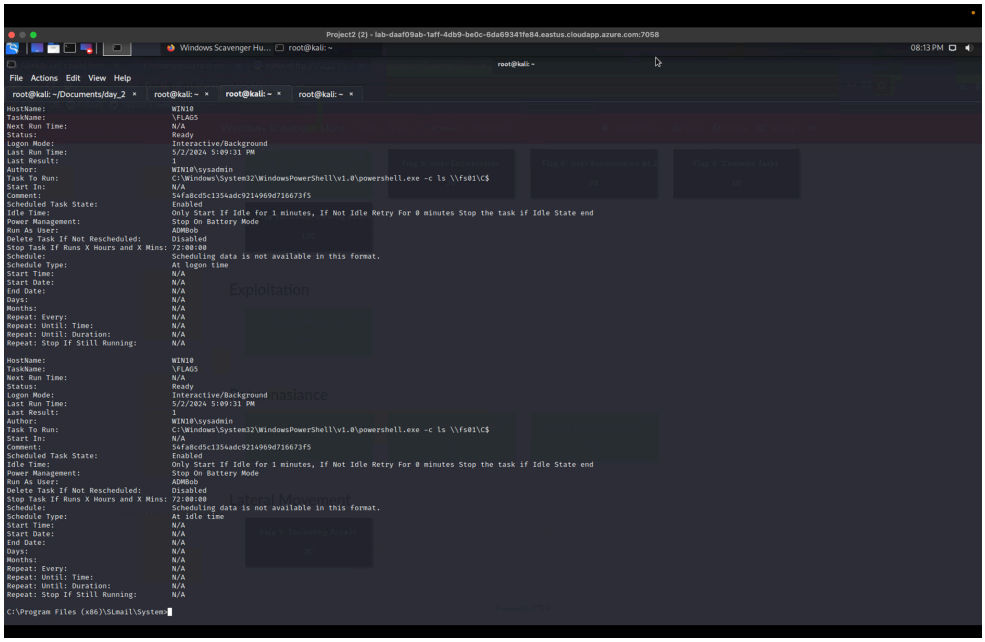
Vulnerability 21	Findings
Title	Windows Port Scan
Type (Web app / Linux OS / WIndows OS)	Windows OS

Risk Rating	High
Description	Conducted a port scan on the ip address subnet 172.22.117.0/24 which revealed numerous open ports such as port 80 (HTTP) which we then used to login and used the previous cracked password to login and get access to the network.
Images	 
Affected Hosts	172.22.117.20
Remediation	Require 2 factor authentication, Require stronger passwords

Vulnerability 22	Findings
Title	FTP Login

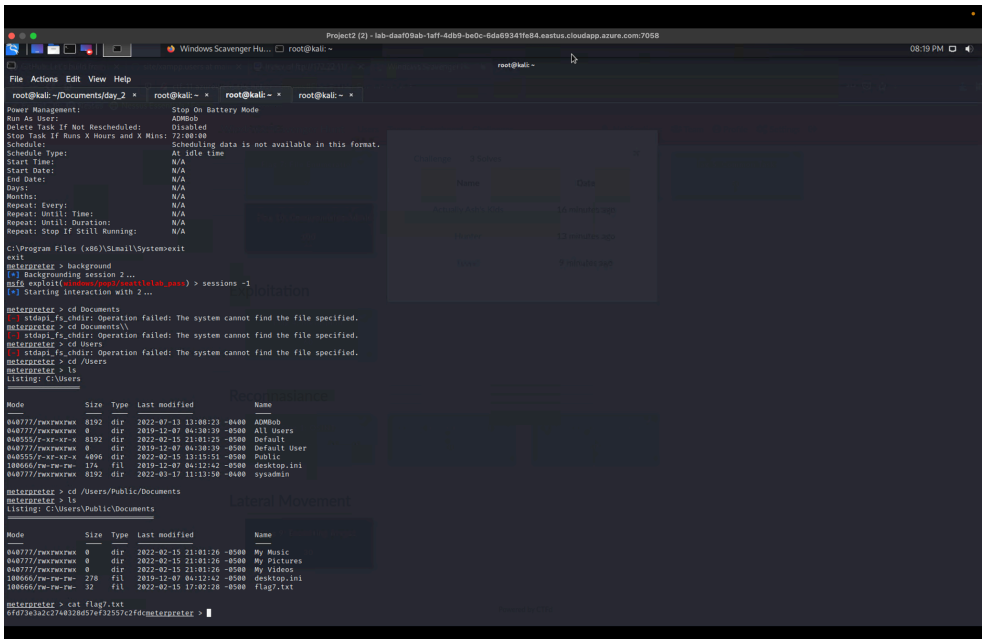
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	From the port scan our team was able to see that Port 21 (FTP) was open and anonymous access was enabled which led us to logging using FTP to access the network.
Images	 
Affected Hosts	172.22.117.20
Remediation	Switch to FTPS or SFTP which are more secure than standard FTP which is vulnerable to sniffing, spoofing and brute force attacks.

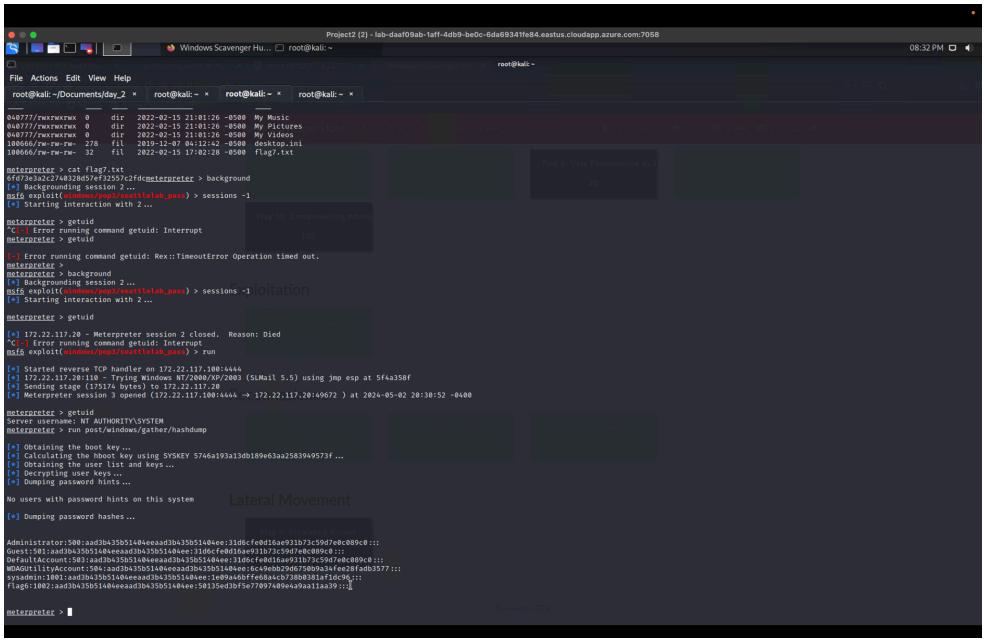
Vulnerability 23	Findings
Title	SLMAIL Metasploit Exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	The port scan also revealed that the SLMail service is running on SMTP port 25 AND on POP3 port 110. This led us to using metasploit to find an exploit that can be leveraged and used to gain access to the network.
Images	 
Affected Hosts	172.22.117.20
Remediation	Remove the slmail/pop3 service running on port 110.

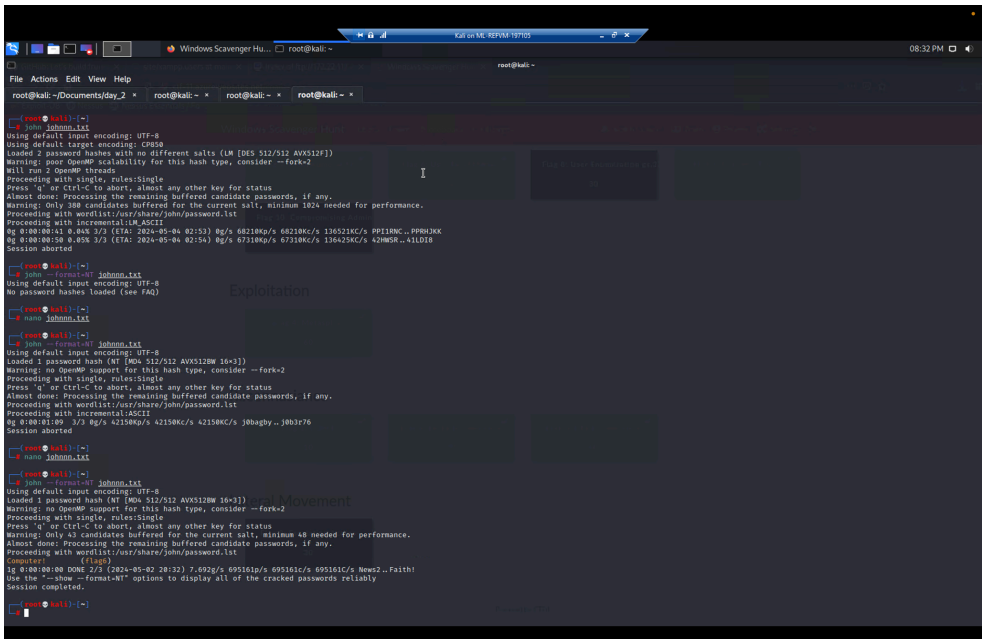
Vulnerability 24	Findings
Title	Windows Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using the same shell we were able to access the windows task scheduler.
Images	
Affected Hosts	172.22.117.20
Remediation	Require 2 factor authentication, require password changes every 6 months.

Vulnerability 25	Findings
Title	LSA Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Using the kiwi on the metasploit interface, we use the command “lsa_dump_sam” which reveals a password hash with a username. Using John the ripper we cracked the ntlm hash which revealed credentials.

Images





	
Affected Hosts	172.22.117.20
Remediation	Require 2 factor authentication, require password changes every 6 months.