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	UTA Cybersecurity Bootcamp Report, LLC
Contact Name	Harshal Shekatkar
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	05/22/2023	Harshal Shekatkar	

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.

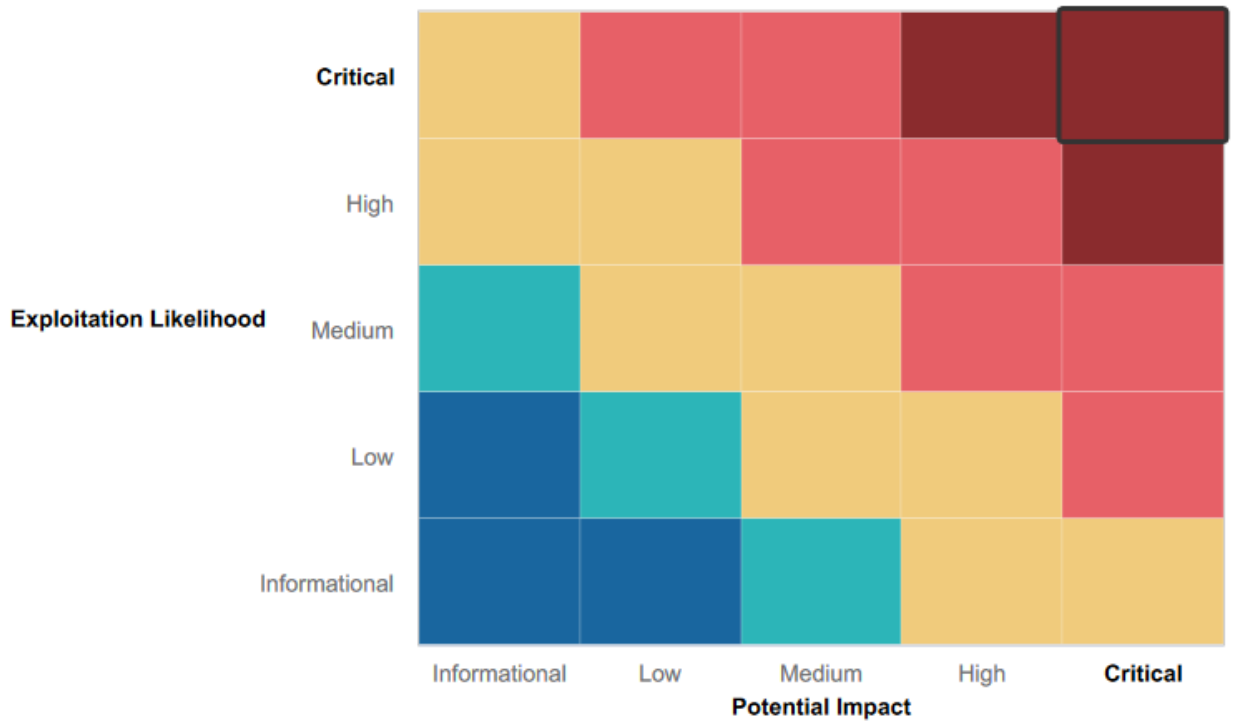
Executive Summary of Findings

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 is committed to strengthen its system defense and data integrity which is evident from ordering penetration testing. This will give them solutions to mitigate system vulnerabilities.

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.

- XSS vulnerability
- Sensitive data exposure
- Local file inclusion
- SQL injection
- Command injection
- PHP injection
- Session management
- Directory traversal
- Open source exposed data
- Apache Tomcat Remote Code Execution
- Shellshock exploit
- Struts Exploit
- Drupal exploit
- CVE-2019-14287 – SSH login
- Anonymous File Transfer Protocol (FTP)
- SLmail exploit
- Scheduled task exploit
- Kiwi exploit
- Privilege Escalation
- Lateral Movement – Root Access

Executive Summary

Penetration Testing was done to simulate how an external attacker might try to gain access to Rekall's systems and data. Goal was to identify ways in which an external attacker can penetrate Rekalls's systems and to determine what impact it might have on company's confidential data and infrastructure.

Exploitation was done using various techniques.

- XSS & SQL injection
- Command & PHP injection
- Apache Tomcat Remote Code Execution
- Session management
- Directory traversal
- Search of exposed data
- Shellshock, Struts, Drupal exploits
- CVE-2019-14287 – SSH login
- Anonymous File Transfer Protocol (FTP) exploit
- SLmail, Scheduled task exploits
- Kiwi, Privilege Escalation, Lateral Movement – Root Access exploit

Summary Vulnerability Overview

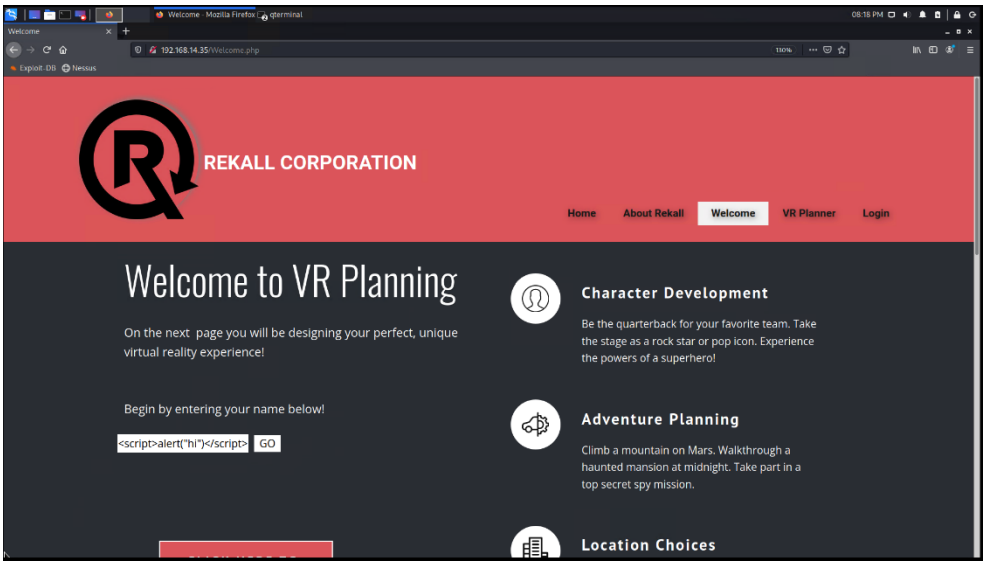
Vulnerability	No of instances	Severity
XSS vulnerability	3	Critical
Sensitive data exposure	5	Critical
Local file inclusion	2	High
SQL injection	1	Critical
Command injection	1	High
Brute force attack	2	Critical
PHP injection	1	Critical
Session management	1	Critical
Directory traversal	1	Critical
Open source exposed data	2	Critical
Visibility of IP hosts	1	Medium
Apache Tomcat Remote Code Execution	2	Critical
Shellshock exploit	1	Critical
Struts Exploit	1	Critical
Drupal exploit	1	High
CVE-2019-14287 – SSH login	1	Critical
Anonymous File Transfer Protocol (FTP)	1	High
SLmail exploit	1	Critical
Scheduled task exploit	1	High
Kiwi exploit	3	Critical
Privilege Escalation	1	Critical
Lateral Movement – Root Access	1	Critical

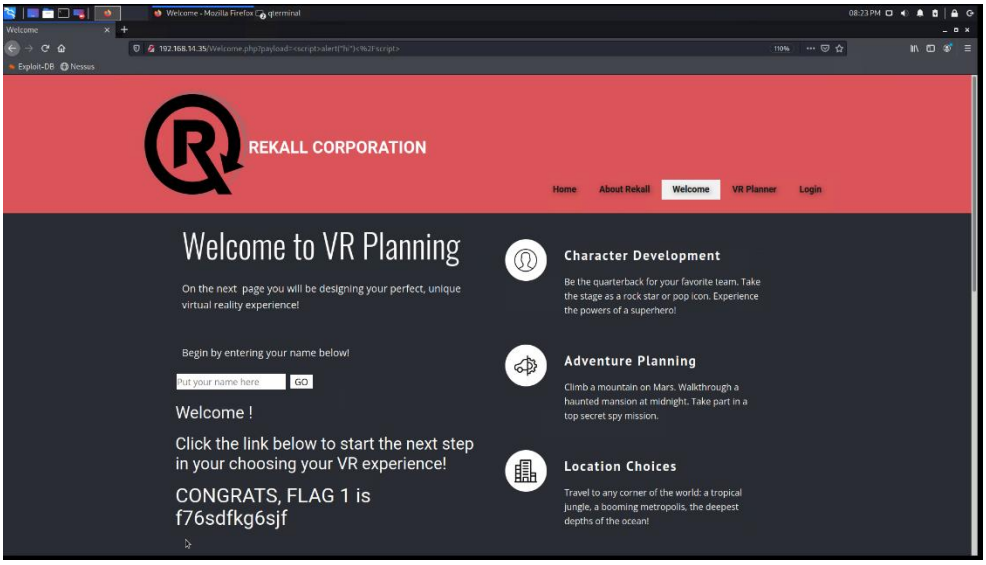
The following summary tables represent an overview of the assessment findings for this penetration test:

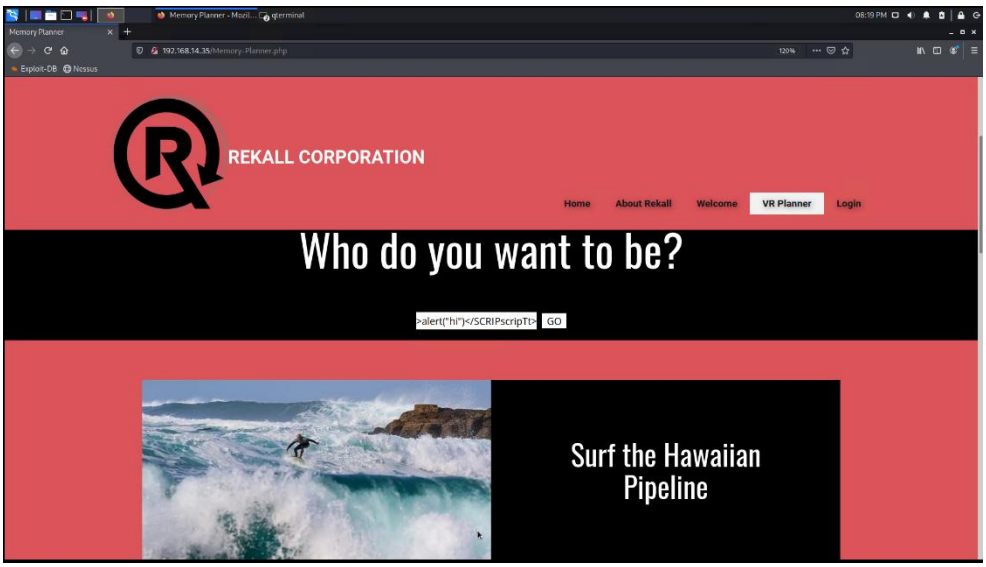
Scan Type	Total
Hosts	192.168.14.35 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.100 172.22.117.20 172.22.117.10
Ports	80, 110, 22, 21

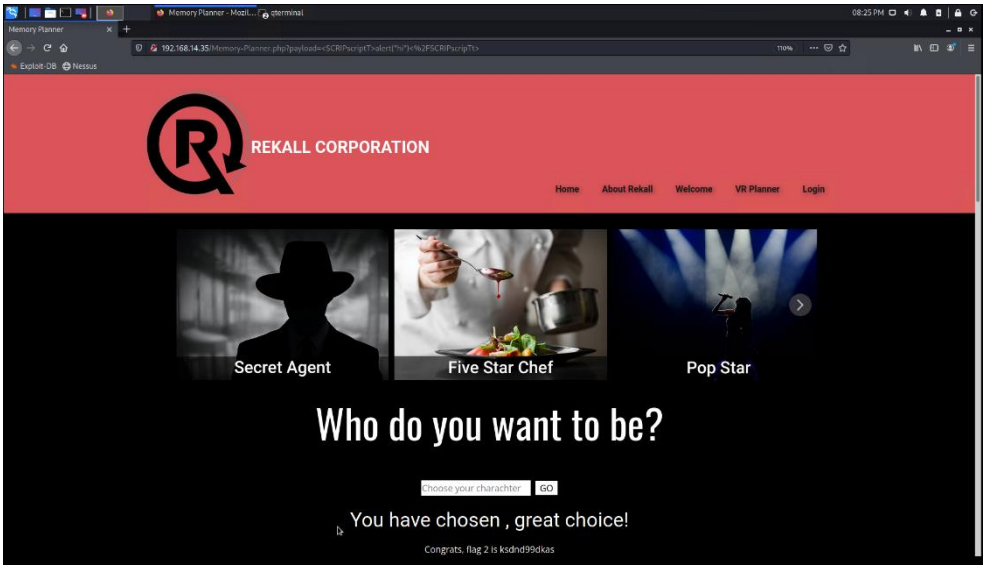
Exploitation Risk	Total
Critical	27
High	6
Medium	1
Low	0

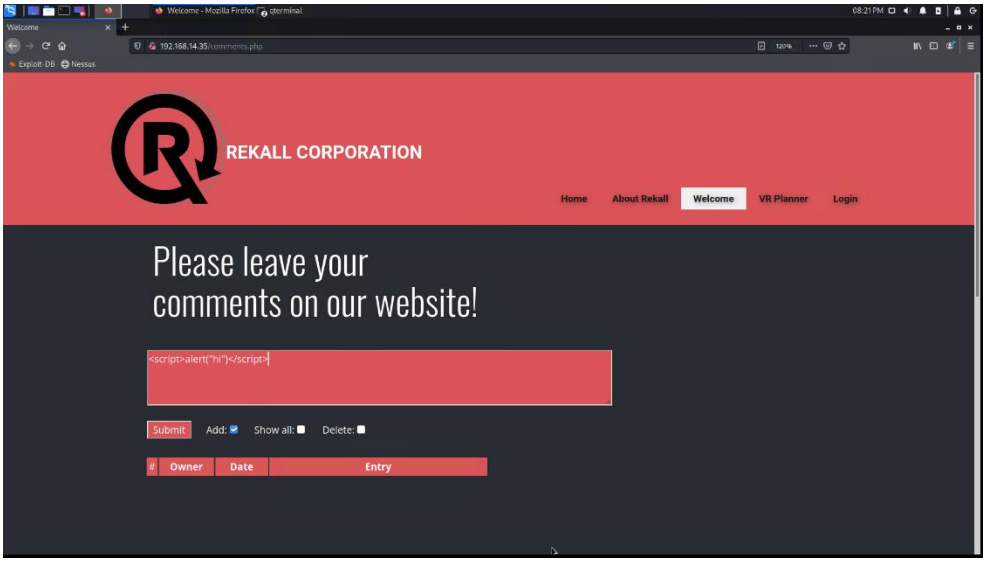
Vulnerability Findings

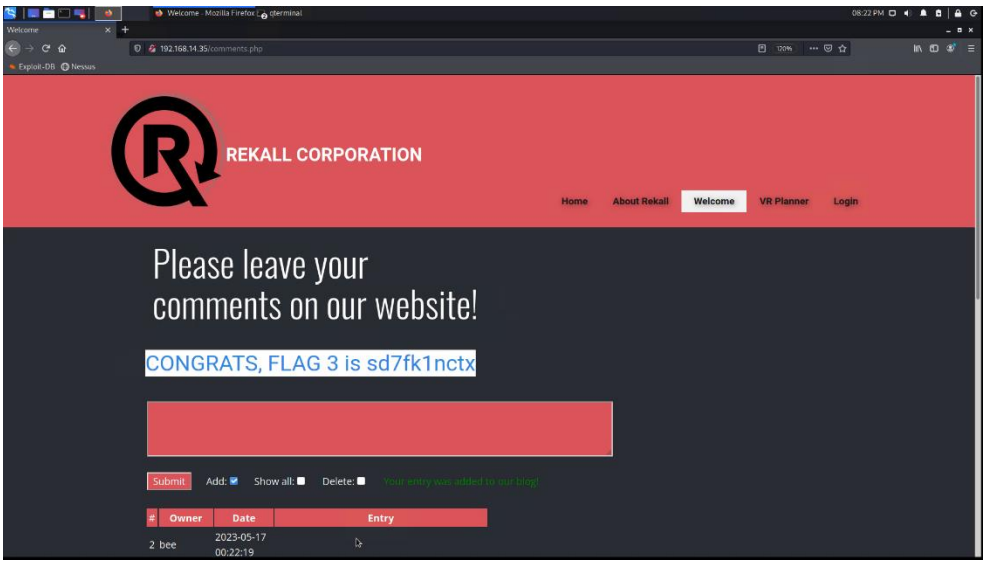
Vulnerability 1	Findings
Title	XSS reflected vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Web app is vulnerable to malicious script
Images	

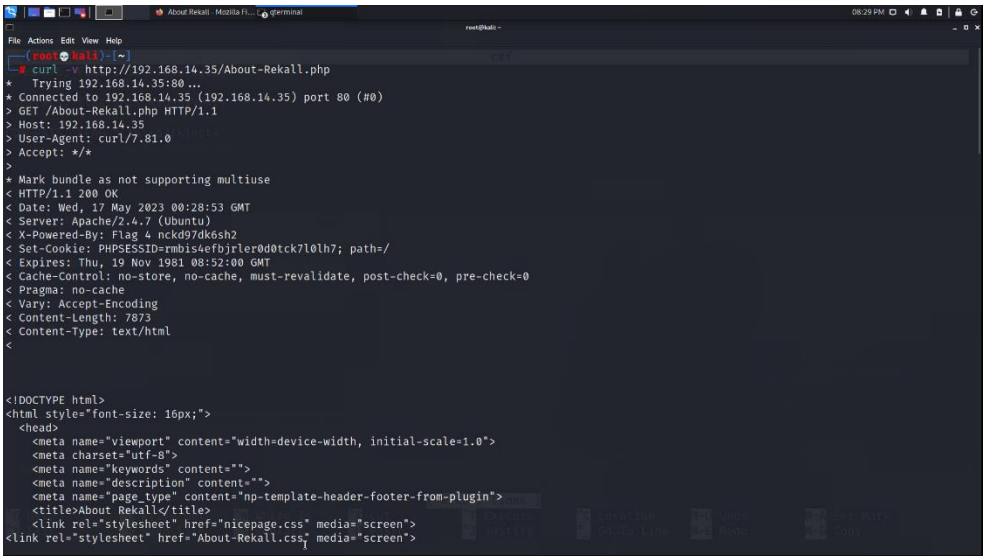
	
Affected Hosts	192.168.14.35
Remediation	Validate all input data, make sure that only the allow listed data is allowed, and ensure that all variable output in a page is encoded before it is returned to the user.

Vulnerability 2	**Findings**
Title	XSS reflected (advanced) vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Web app is vulnerable to malicious script
Images	

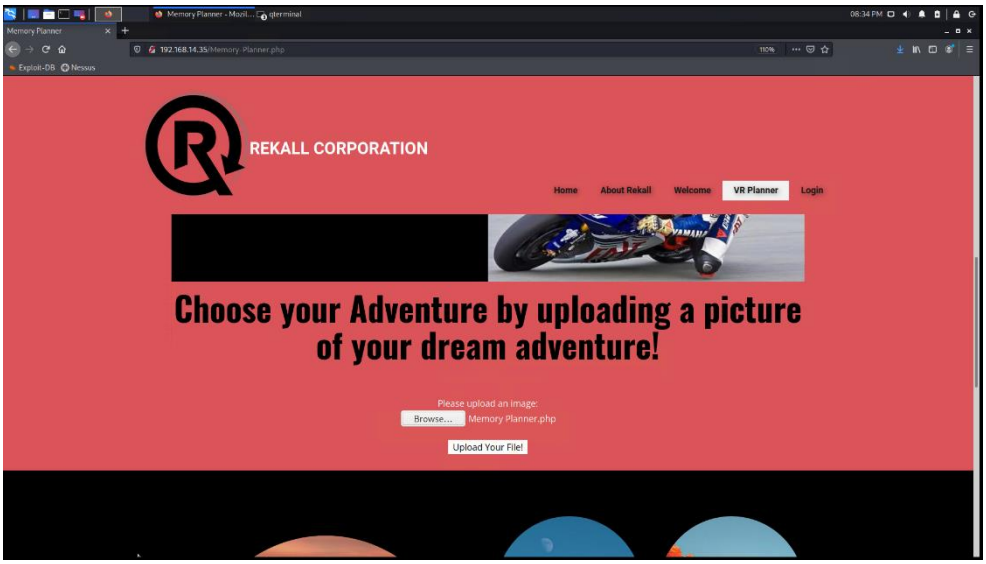
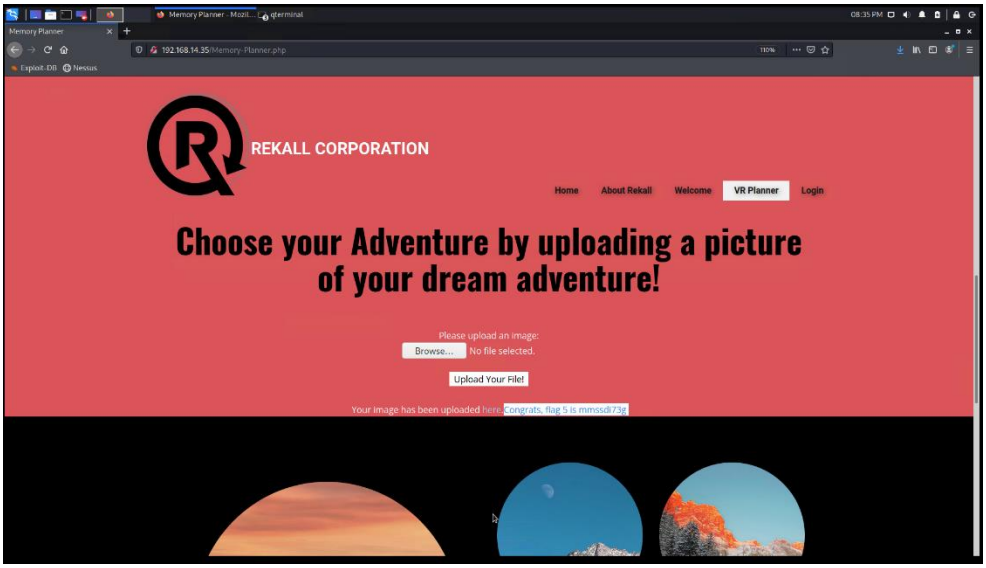
	
Affected Hosts	192.168.14.35
Remediation	Validate all input data, make sure that only the allow listed data is allowed, and ensure that all variable output in a page is encoded before it is returned to the user.

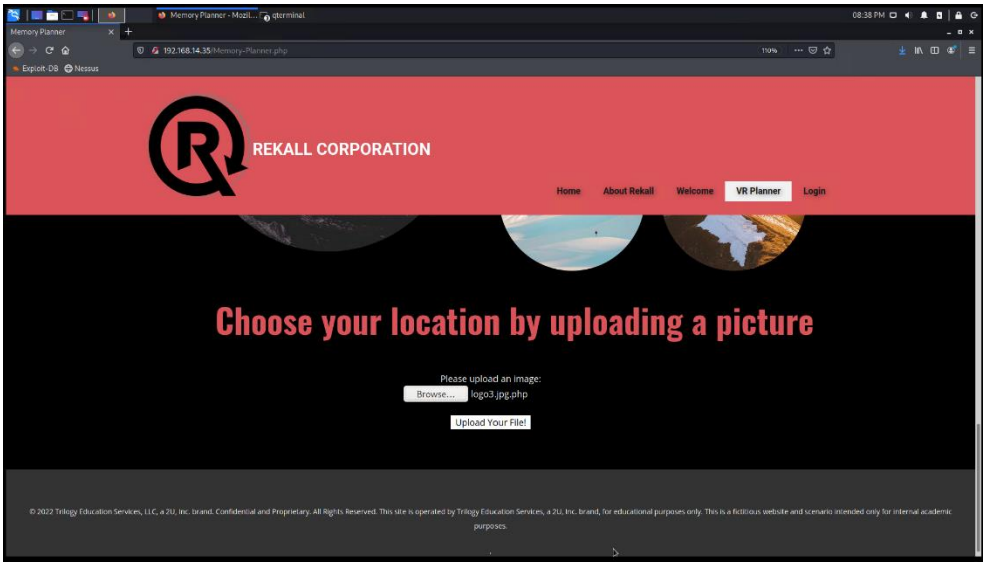
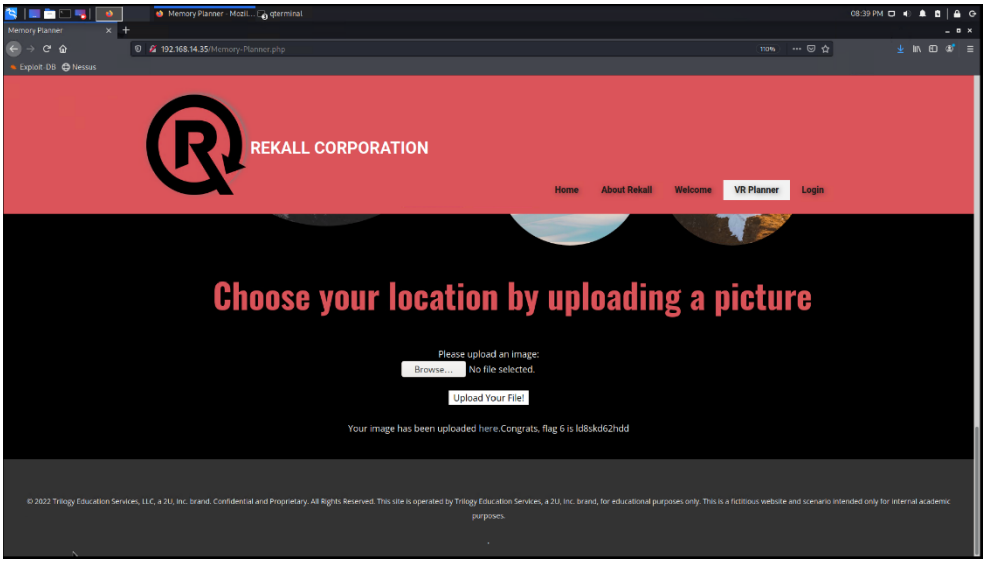
Vulnerability 3	Findings
Title	XSS stored vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Web app is vulnerable to malicious script
Images	

	
Affected Hosts	192.168.14.35
Remediation	Validate all input data, make sure that only the allow listed data is allowed, and ensure that all variable output in a page is encoded before it is returned to the user.

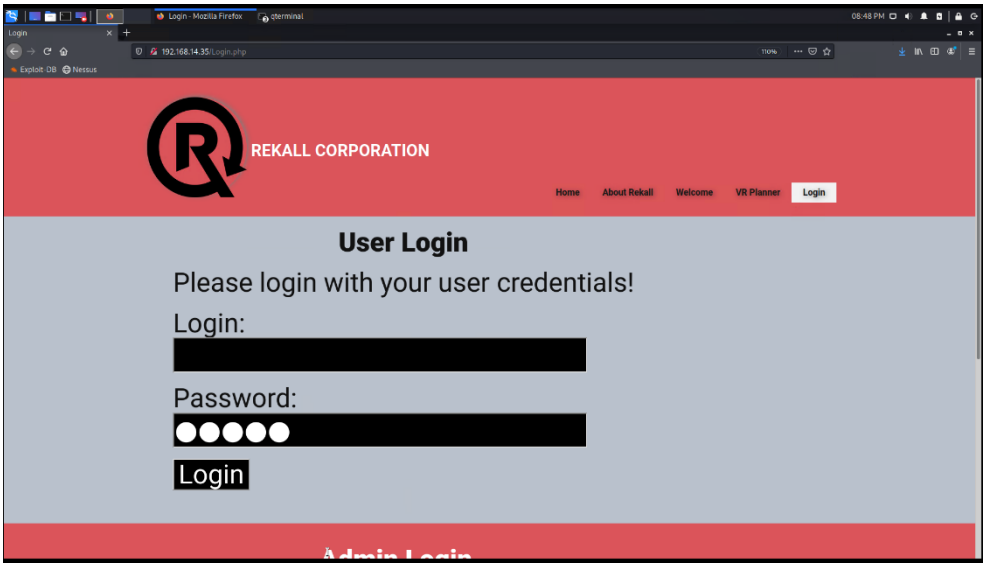
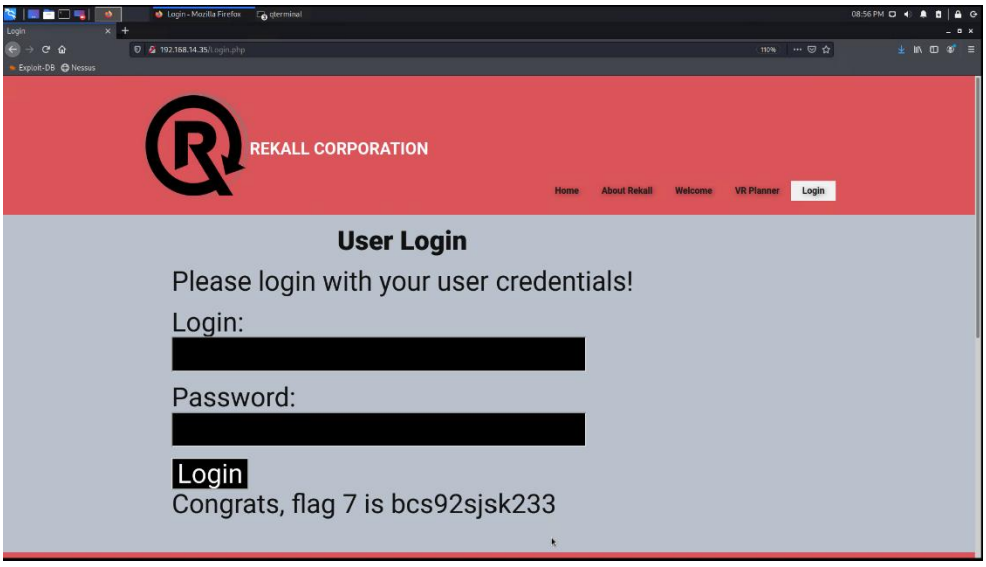
Vulnerability 4	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Used Curl to list HTTP response headers
Images	

Affected Hosts	192.168.14.35
Remediation	Ensure sensitive data is not listed in HTTP headers

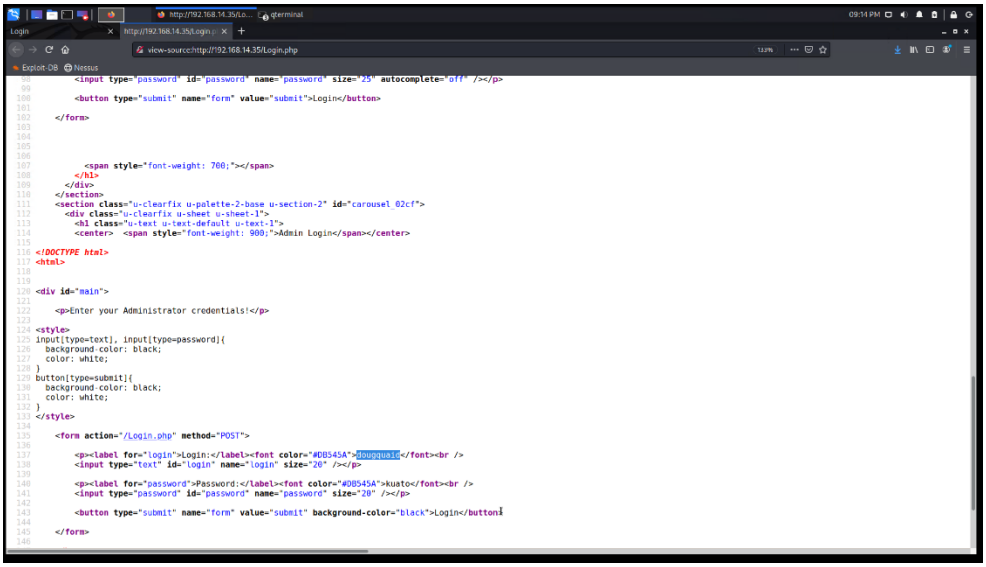
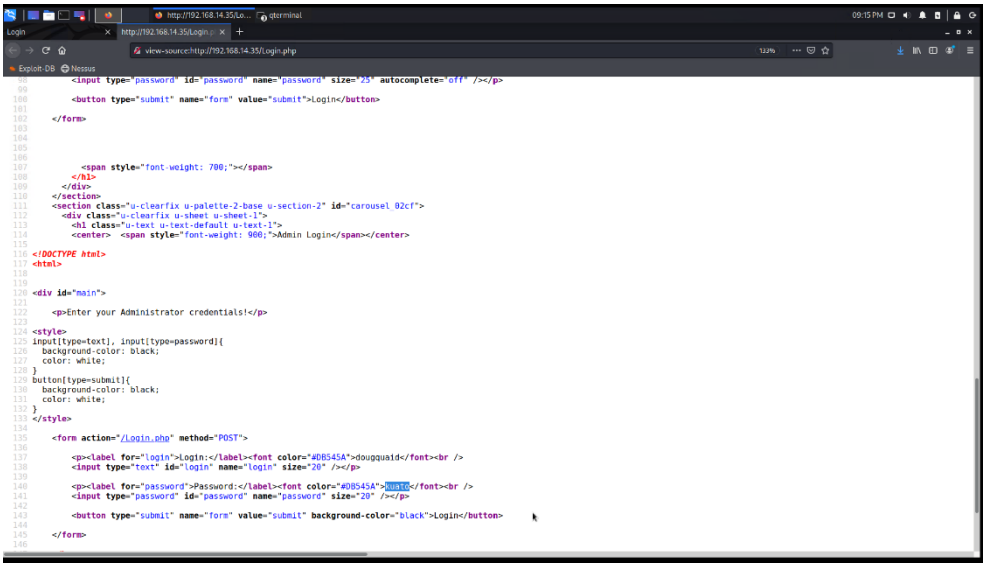
Vulnerability 5	**Findings**
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	Uploading a PHP file was successful
Images	 
Affected Hosts	192.168.14.35
Remediation	Restrict types of files allowed to upload

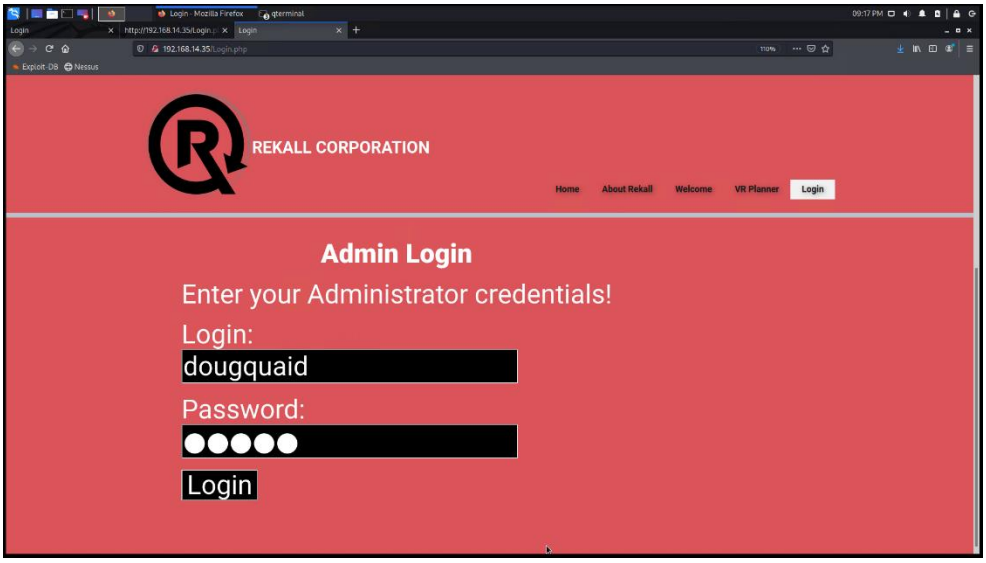
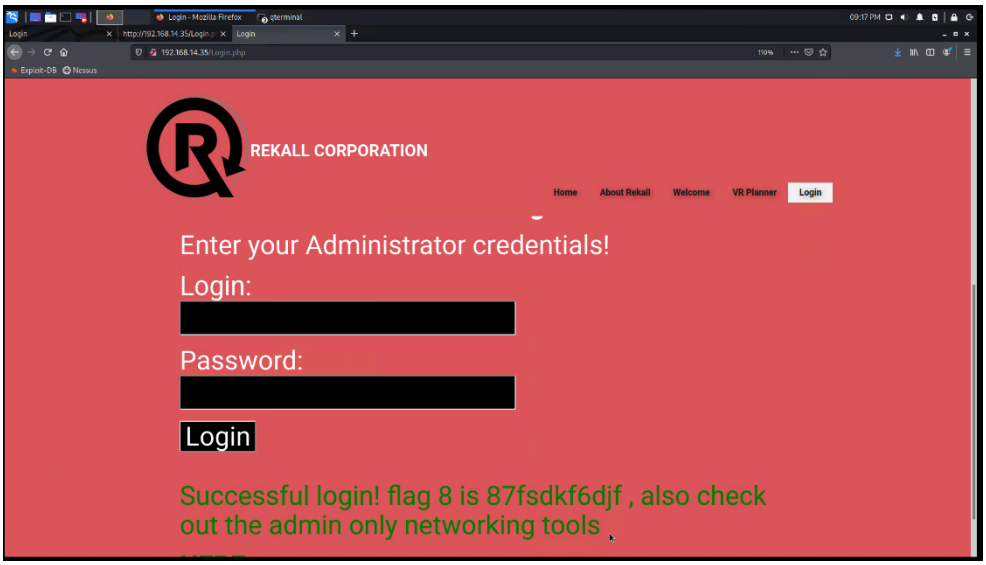
Vulnerability 6	Findings
Title	Local file inclusion (advanced)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	The input validation checks for the presence of .jpg, so to bypass this upload, jpg word was used in name of malicious script: script.jpg.php
Images	 
Affected Hosts	192.168.14.35
Remediation	Use validation to check if file extension is correct

Vulnerability 7	Findings

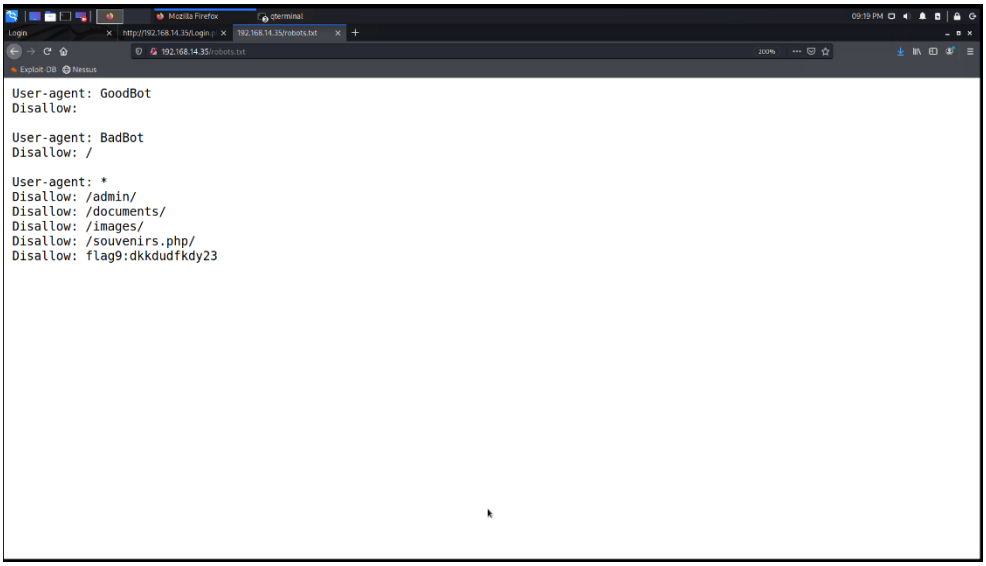
Title	SQL injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Executed SQL statement in password field on login page
Images	 
Affected Hosts	192.168.14.35
Remediation	API with Parameterized Statements: Switching from taking direct input in a web app to using a safe API is probably the safest way to deal with SQL injection. Character Escaping: If an API is not available, web application should be able to escape special characters.

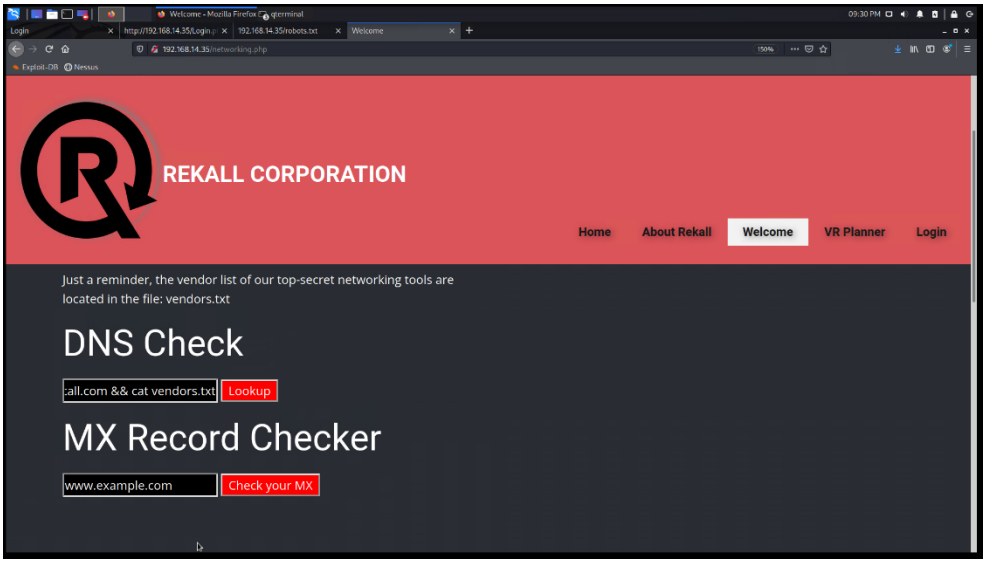
Vulnerability 8	**Findings**
Title	Sensitive data exposure

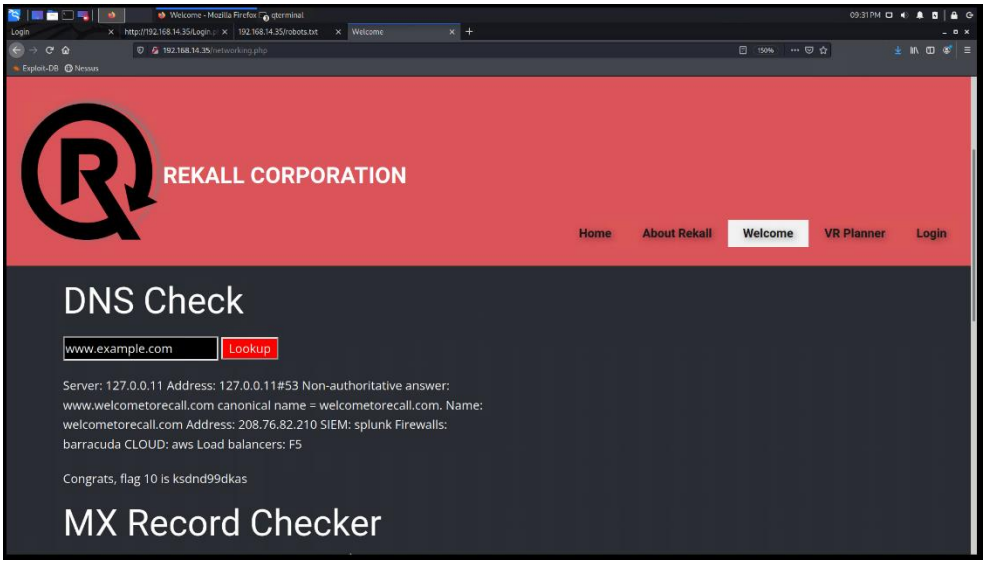
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Login credential of user are in the HTML
Images	 

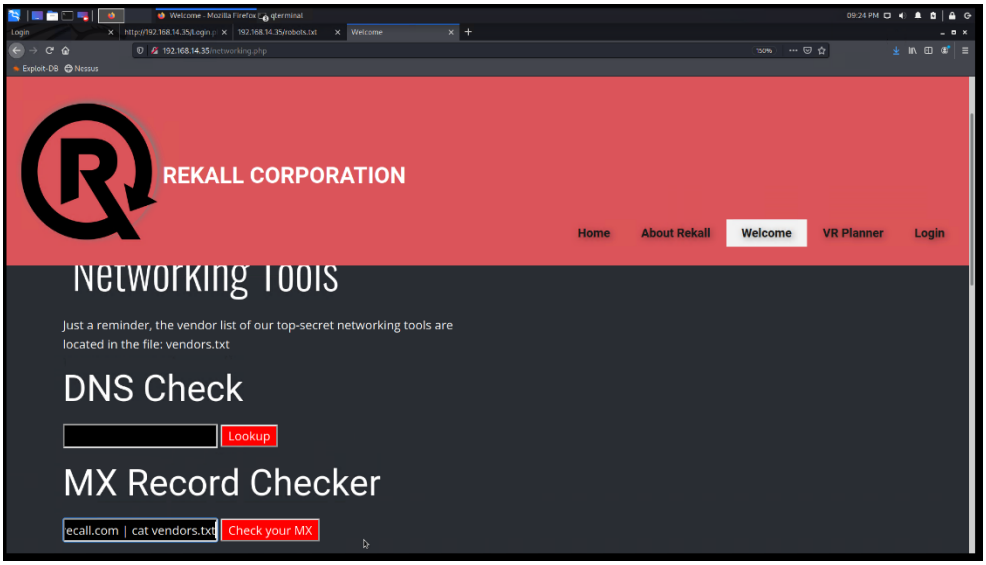
	 
Affected Hosts	192.168.14.35
Remediation	General login policy should be multi factor authentication. Remove login credential from HTML

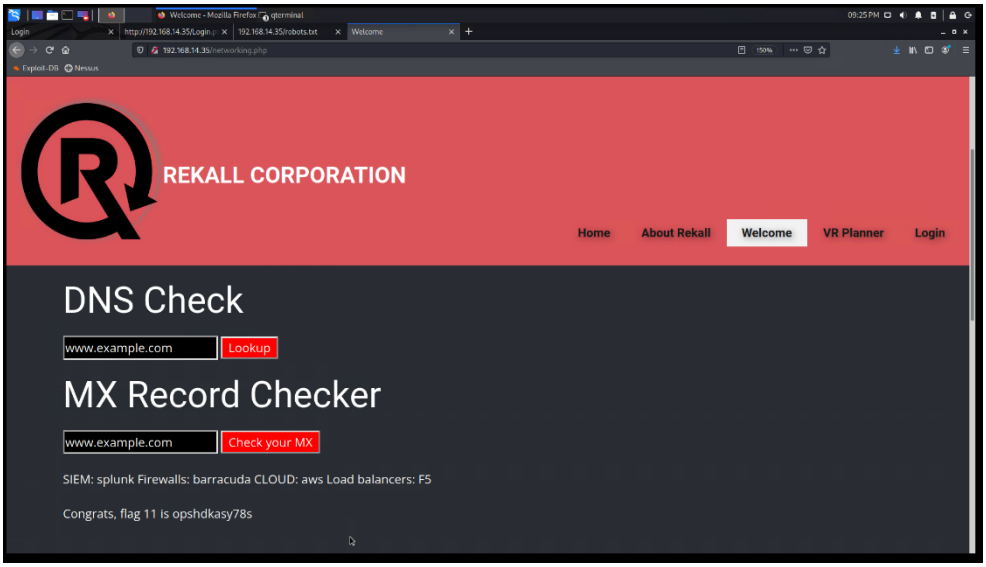
Vulnerability 9	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Accessing 192.168.14.35/robots.txt exposes sensitive data

Images	
Affected Hosts	192.168.14.35
Remediation	Check file privileges. Only authorized users must be given access to sensitive data/files.

Vulnerability 10	Findings
Title	Command injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Using command injection gave access to vendors.txt file
Images	

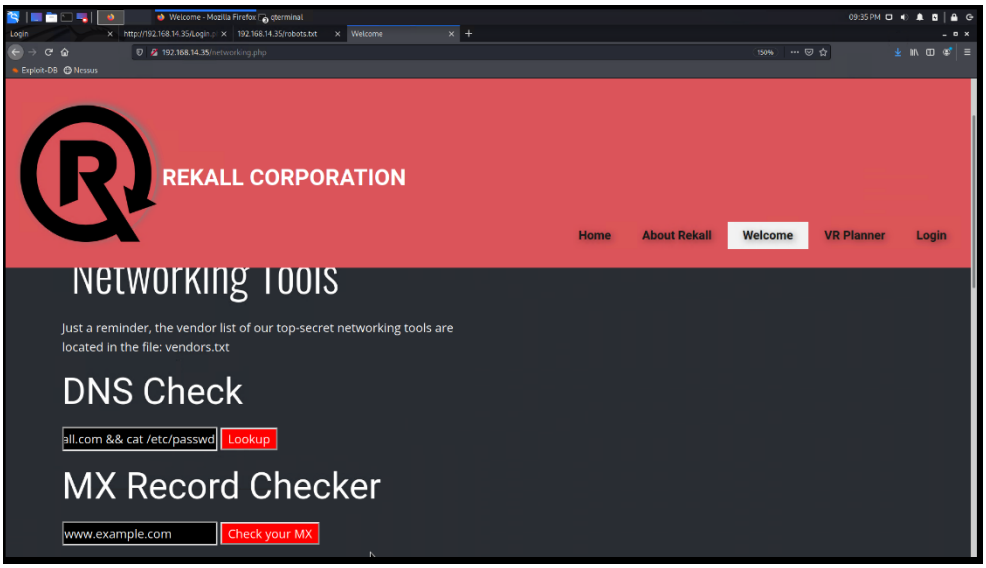
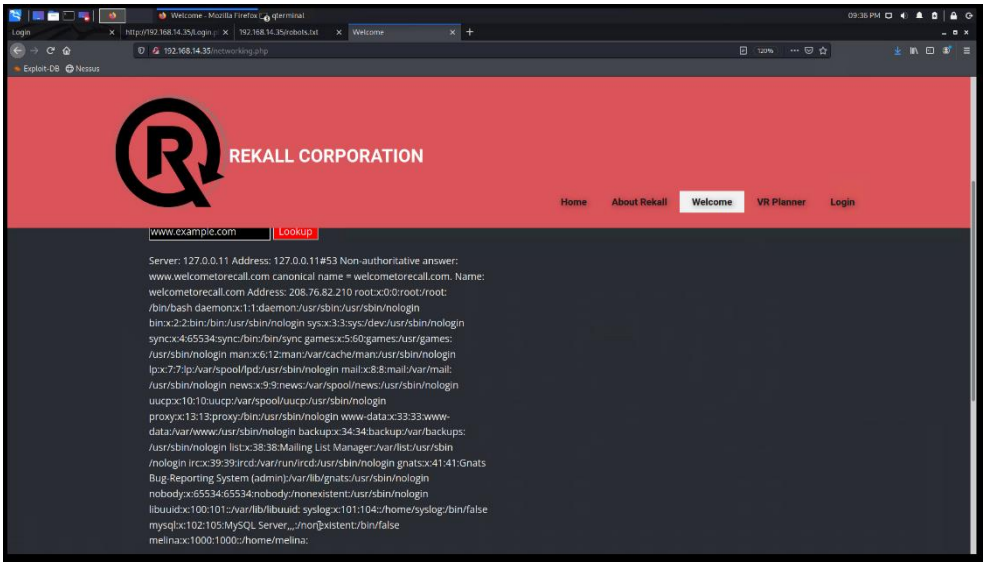


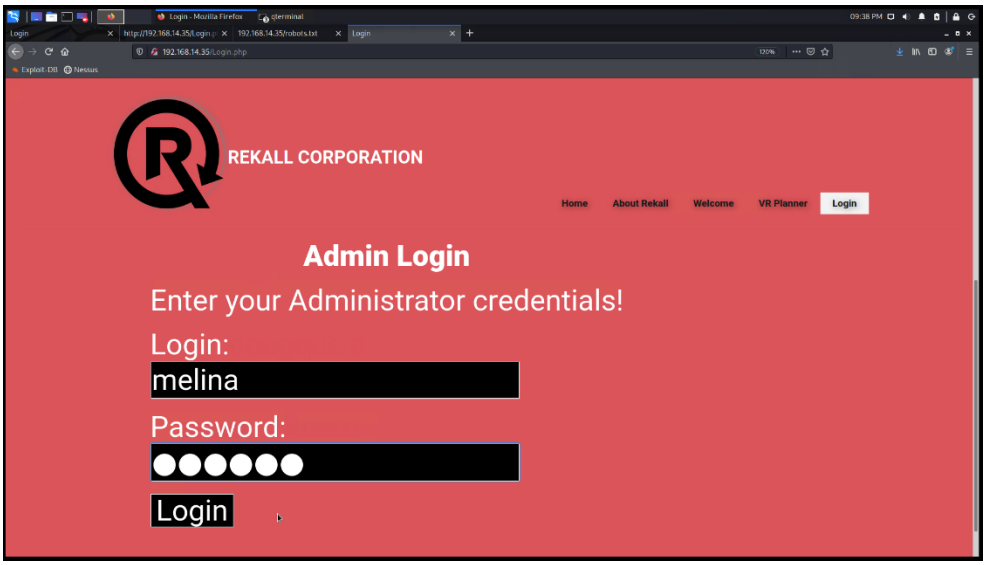
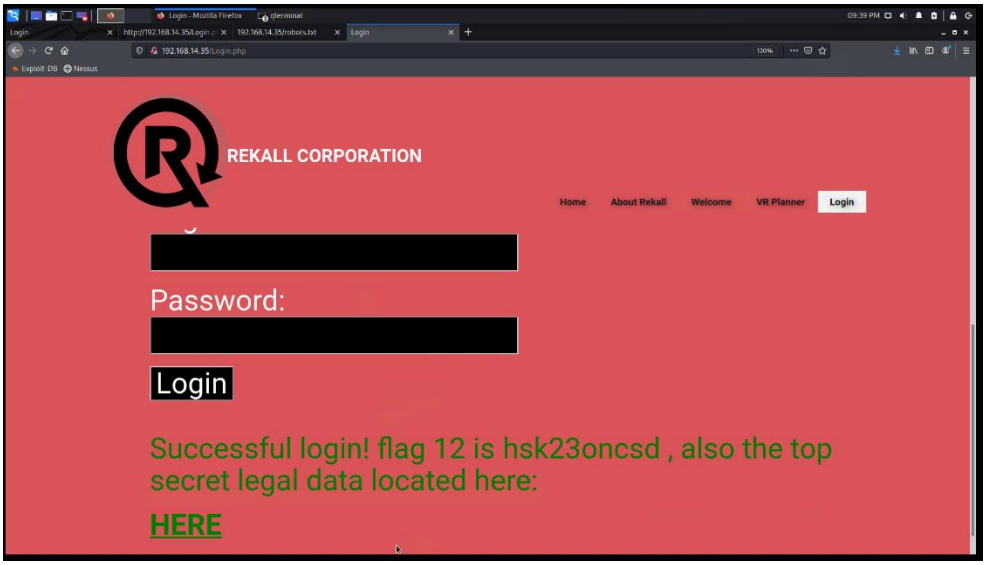




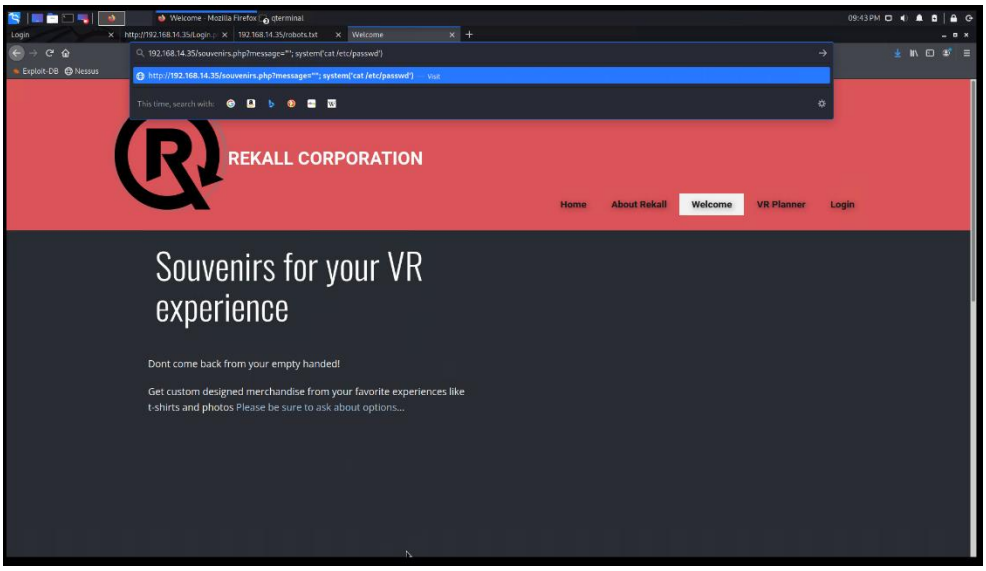
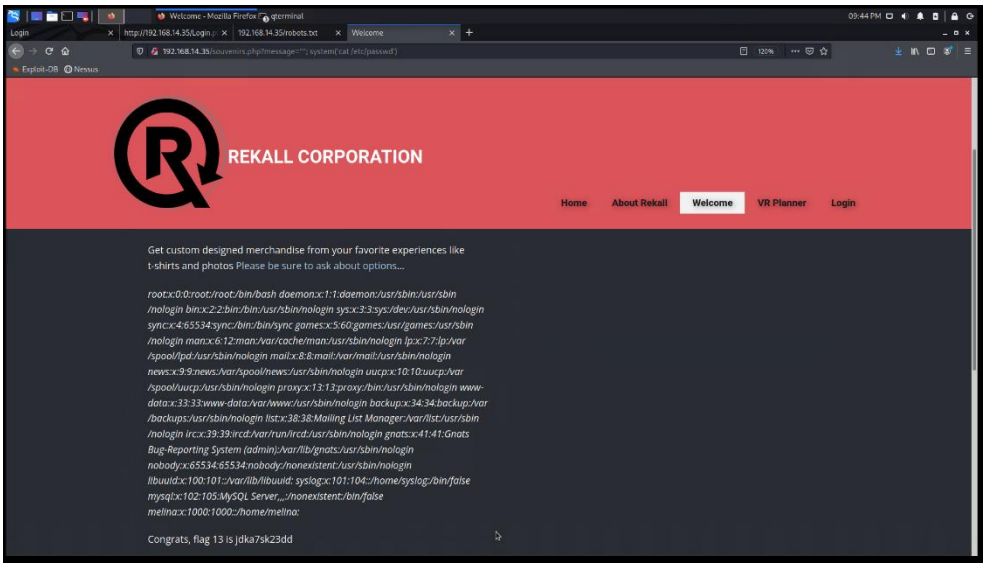
Affected Hosts	192.168.14.35
Remediation	Use Strong Input Validation

	Check file privileges. Only authorized users need to have access to sensitive files.

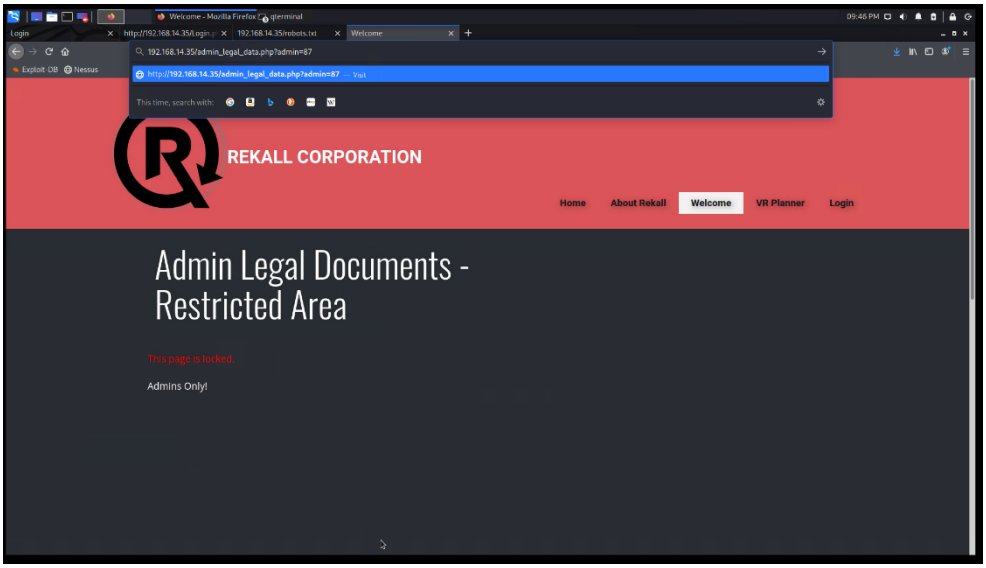
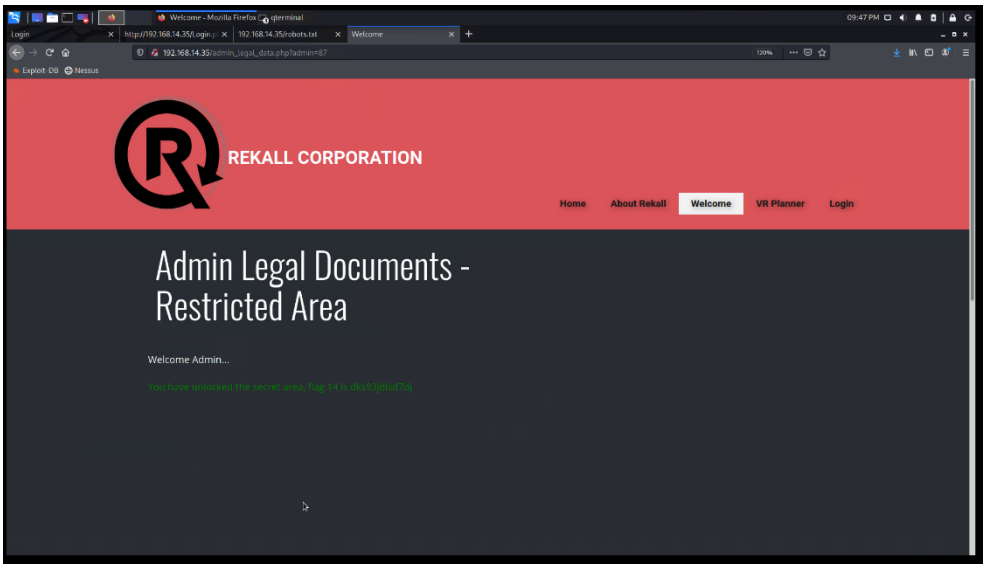
Vulnerability 11	Findings
Title	Brute force attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Using command injection gave access to passwd file. Used brute force attack to login.
Images	 

	 
Affected Hosts	192.168.14.35
Remediation	Use Strong Input Validation. Check file privileges. Only authorized users need to have access to sensitive files. Password policy must be complex.

Vulnerability 12	Findings
Title	PHP injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	`souvenirs.php was identified in robots.txt. Changing URL to include payload gave access to passwd file`

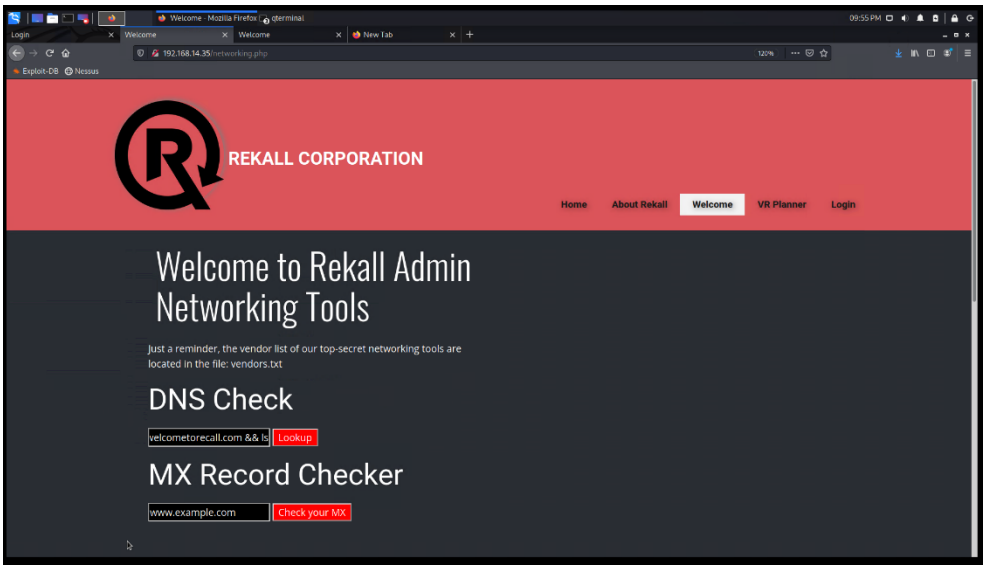
Images	 
Affected Hosts	192.168.14.35
Remediation	Use Strong Input Validation. Check file privileges. Only authorized users need to have access to sensitive files.

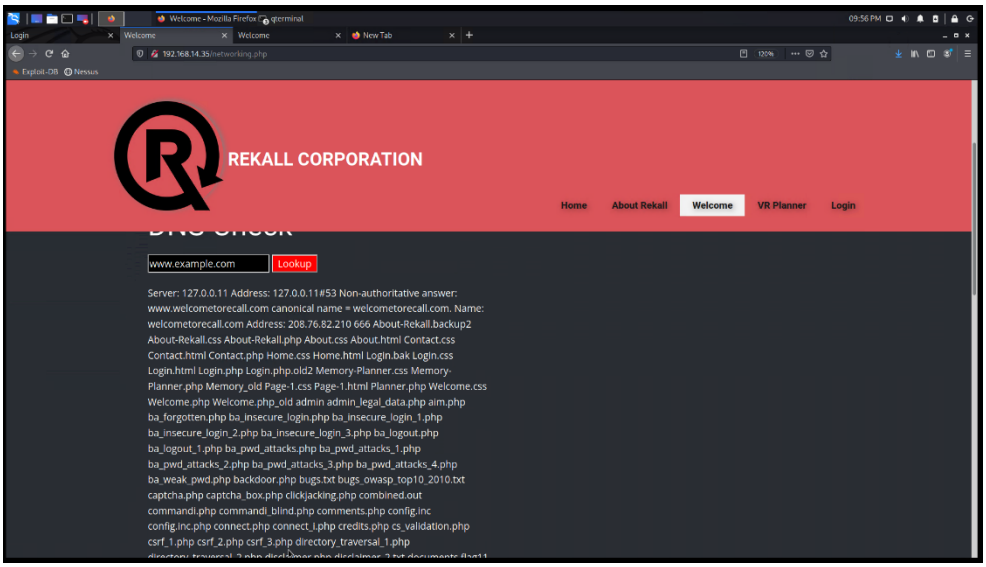
Vulnerability 13	Findings
Title	Session management
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Using Burp tested different session IDs

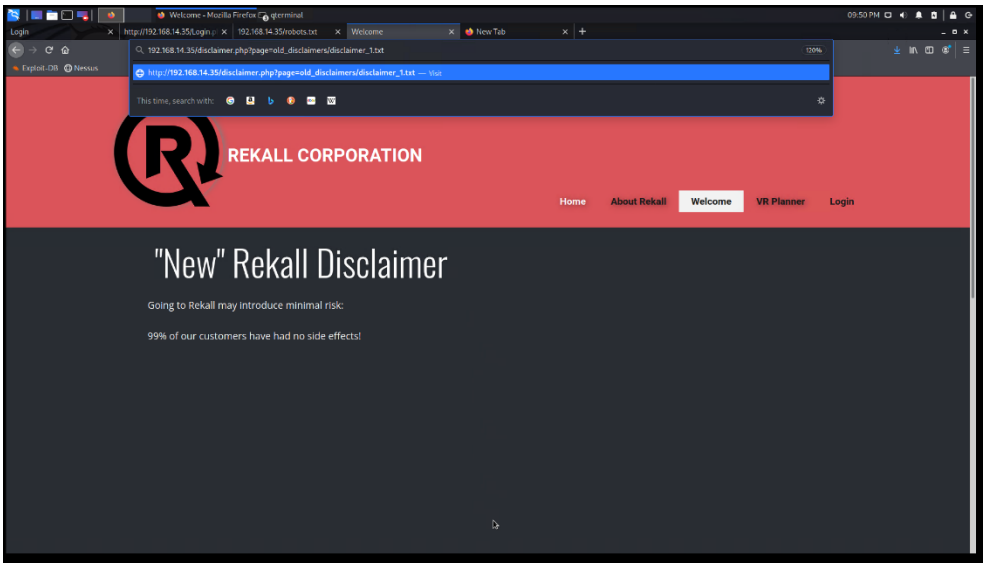
Images	 
Affected Hosts	192.168.14.35
Remediation	Inactivity timeout for every session

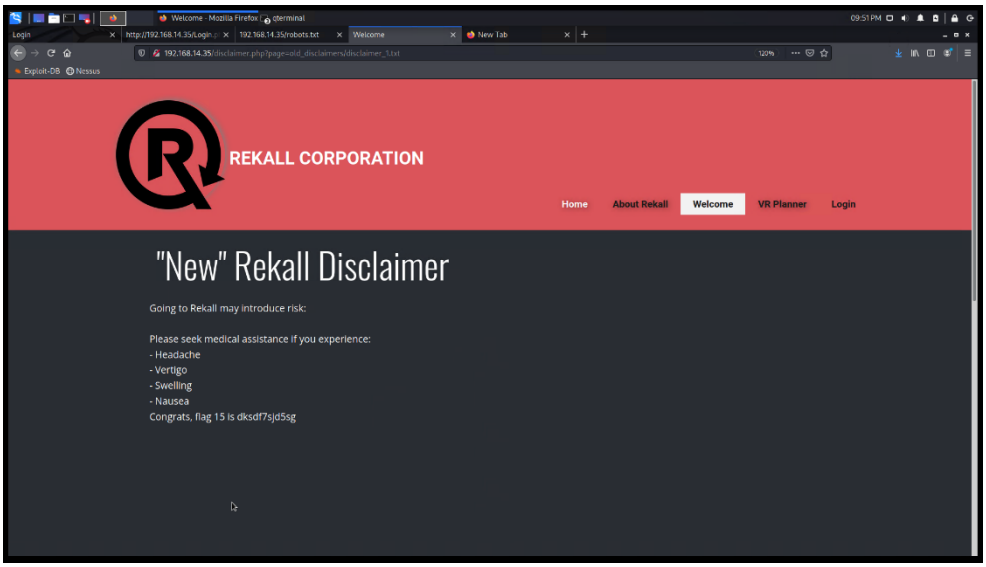
Vulnerability 14	Findings
Title	Directory traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Was able to get access old directories / files using command injection

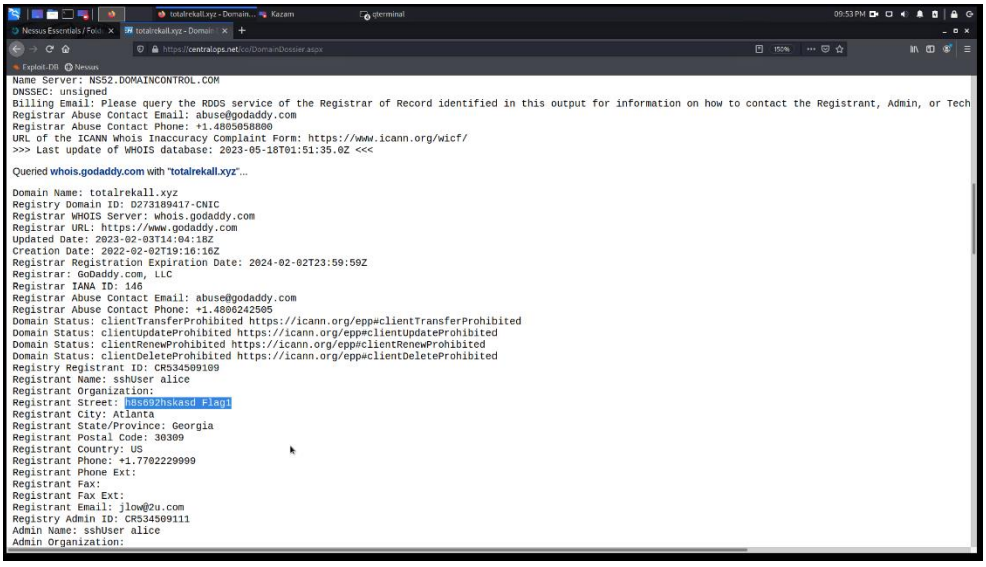
Images



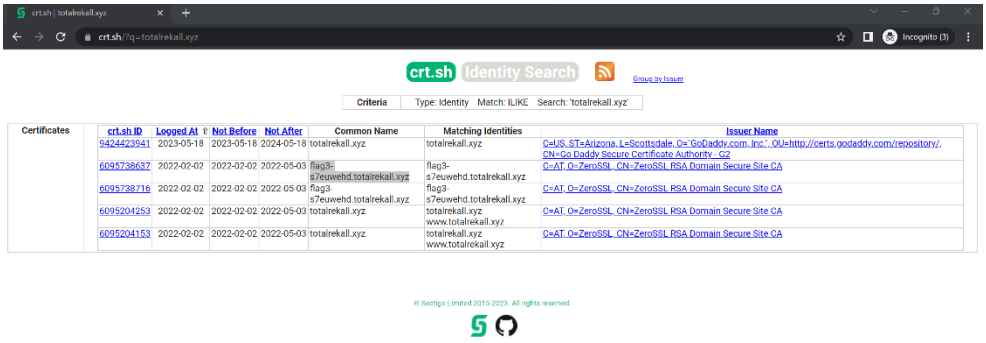




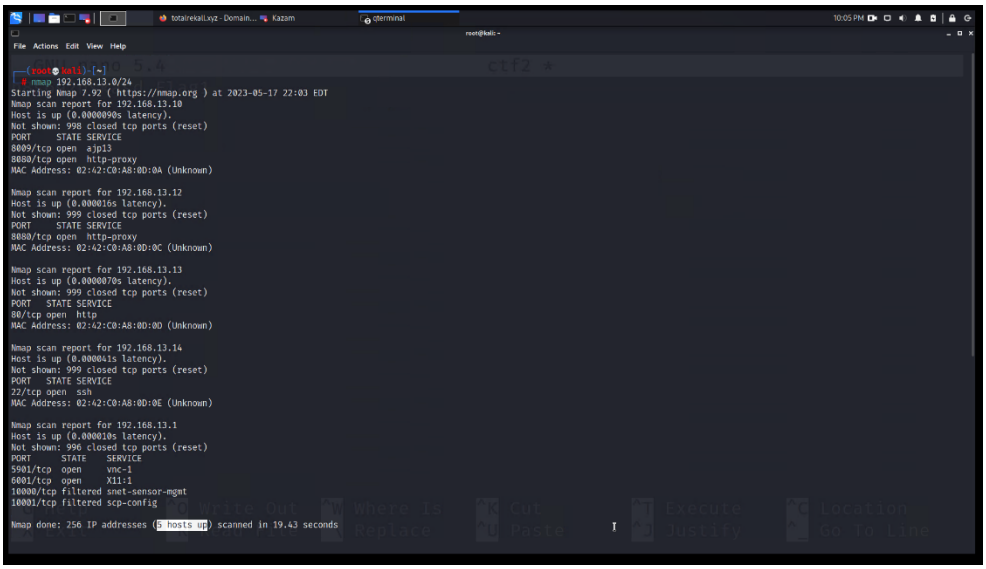
	
Affected Hosts	192.168.14.35
Remediation	Use Strong Input Validation. Check file privileges. Only authorized users need to have access to sensitive files.

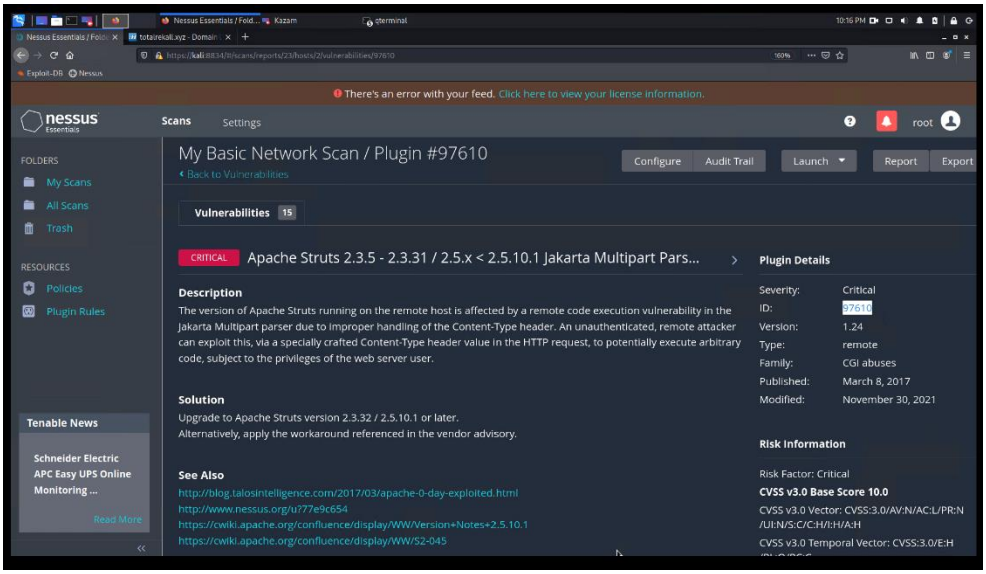
Vulnerability 15	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Viewing data from WHOIS data for totalrekall.xyz on Domain Dossier webpage. SSH user data is exposed.
Images	
Affected Hosts	totalrekall.xyz

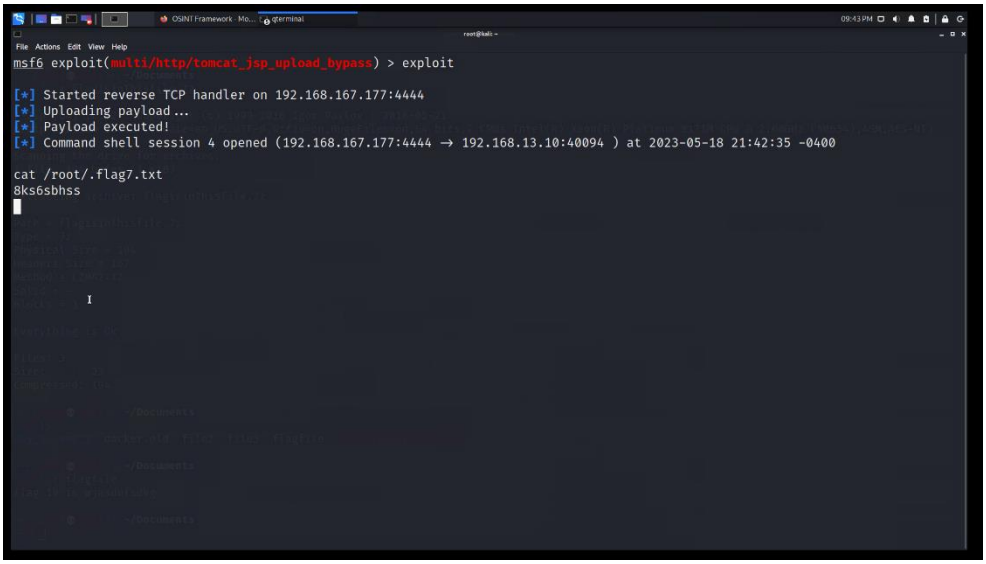
Remediation	Remove any sensitive data from publicly available resources like whois data.

Vulnerability 16	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Search for totalrekall.xyz on crt.sh
Images	
Affected Hosts	totalrekall.xyz
Remediation	Remove any sensitive data from publicly available resources like crt.sh

Vulnerability 17	**Findings**
Title	Visibility of IP hosts
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Nmap scan for the network (192.168.13.0/24) shows there are 5 hosts excluding the host scanning from.

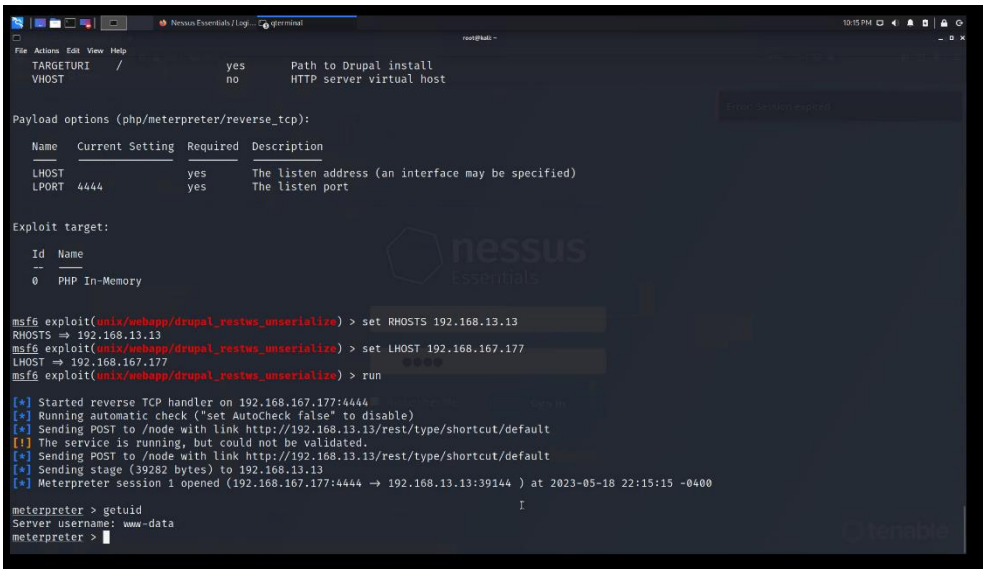
Images	
Affected Hosts	192.168.13.0, 192.168.13.10, 192.168.13.12, 192.168.13.13, 192.168.13.11, 192.168.13.14
Remediation	Use IP hiding technique

Vulnerability 18	Findings
Title	Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Nessus scan shows Apache struts vulnerability
Images	
Affected Hosts	192.168.13.12
Remediation	Update Apache

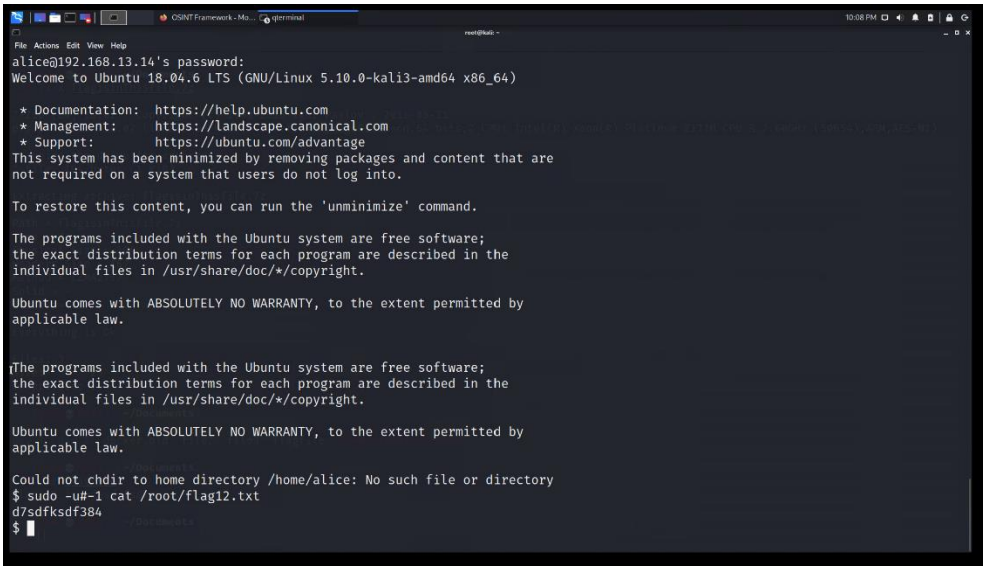
Vulnerability 19	Findings
Title	Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Use exploit multi/http/tomcat_jsp_upload_bypass
Images	
Affected Hosts	192.168.13.10
Remediation	Update Apache

Vulnerability 20	Findings
Title	Shellshock Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Use exploit to get a Meterpreter shell MSF: exploit/multi/http/apache_mod_cgi_bash_env_exec Able to list contents of sudoers and passwd file
Images	Didn't take screenshot exploit/multi/http/apache_mod_cgi_bash_env_exec cat /etc/sudoers (in shell) cat /etc/passwd (in shell)
Affected Hosts	192.168.13.11
Remediation	Use shellshock scanner. Monitor logs.

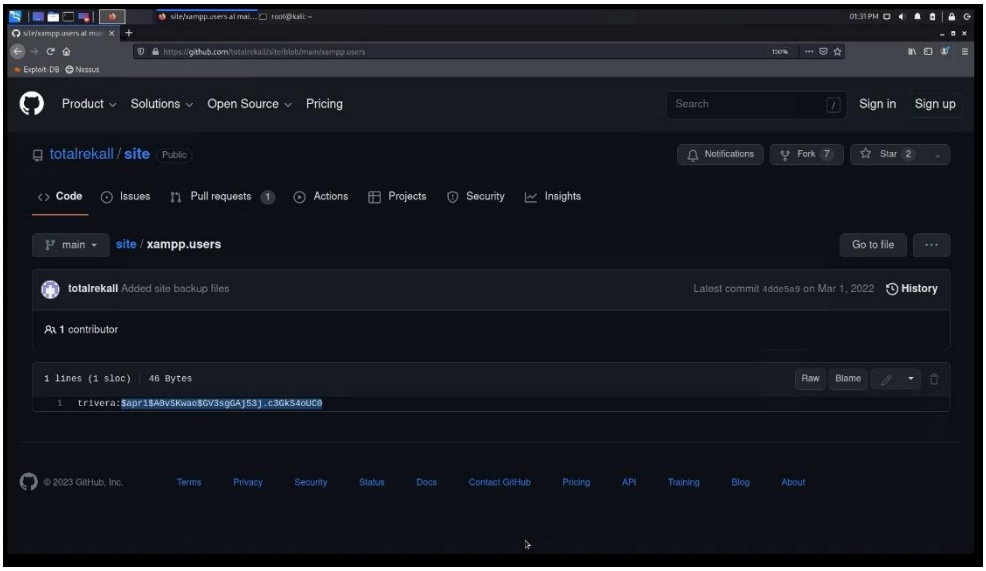
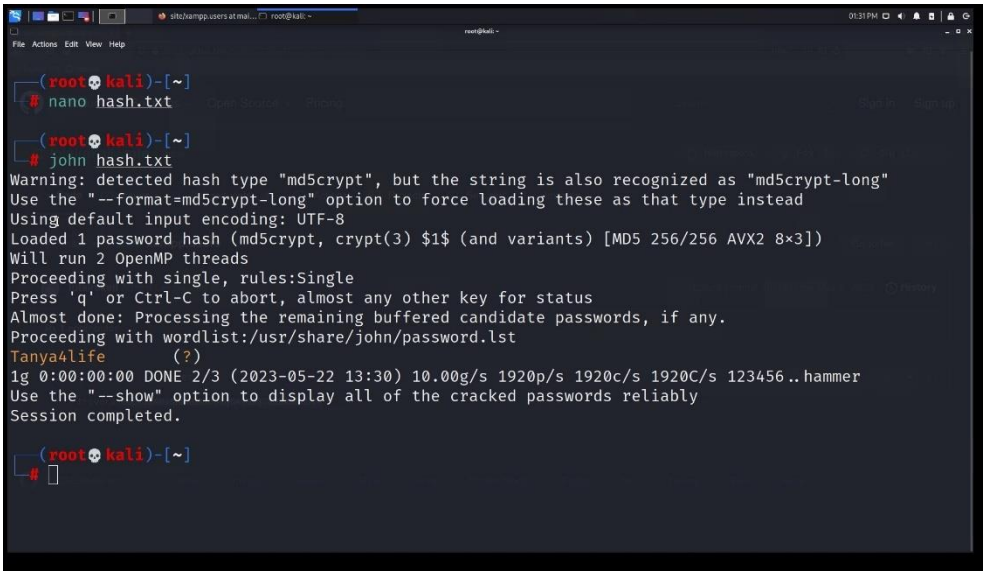
Vulnerability 21	Findings
Title	Struts Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Use exploit to get a Meterpreter shell MSF: multi/http/struts2_content_type_ognl Able to download file from root folder
Images	Didn't take screenshot multi/http/struts2_content_type_ognl downloaded /root/flagisinThisfile.7z extracted 7z x flagisinThisfile.7z used cat to view contents
Affected Hosts	192.168.13.11
Remediation	Use shellshock scanner. Monitor logs.

Vulnerability 22	Findings
Title	Drupal exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Use exploit to get a Meterpreter shell MSF: unix/webapp/drupal_restws_unserialize
Images	
Affected Hosts	192.168.13.13

Remediation	Upgrade Drupal installation

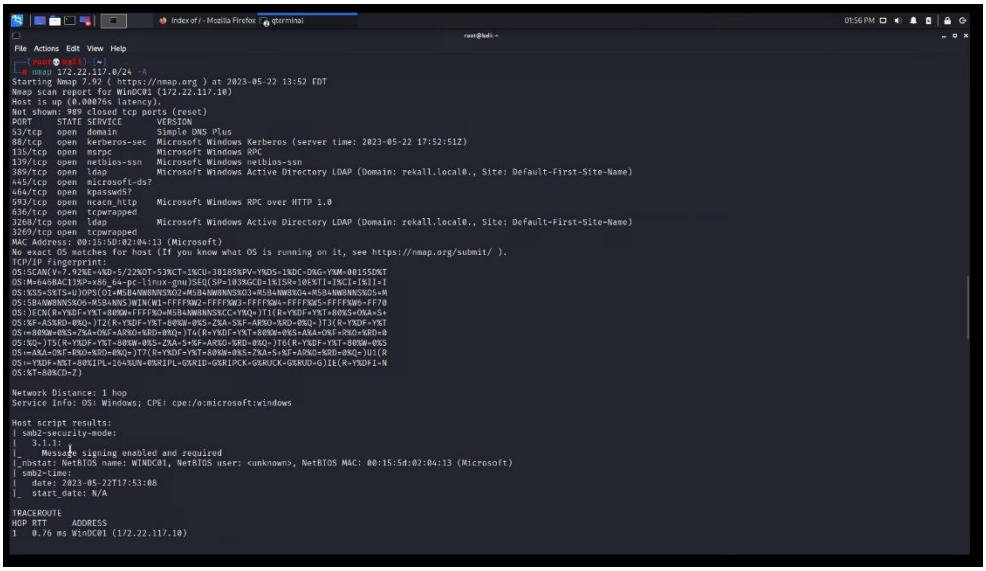
Vulnerability 23	Findings
Title	CVE-2019-14287 – SSH login
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	SSH data exposed on whois data is used to login
Images	
Affected Hosts	192.168.13.14
Remediation	Change login details. Remove any sensitive data from publicly available resources like whois data.

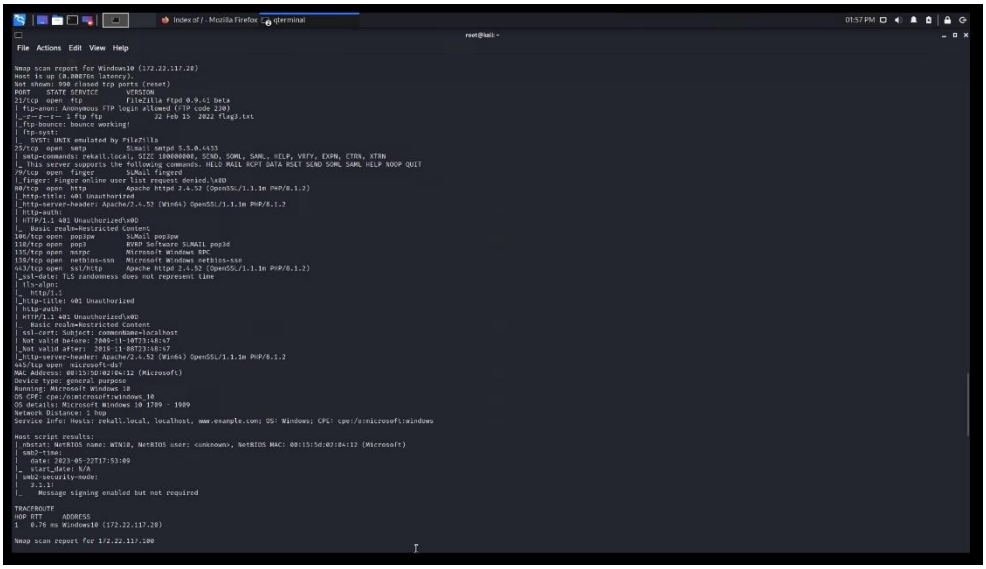
Vulnerability 24	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Login credentials and password hash publicly available on github.

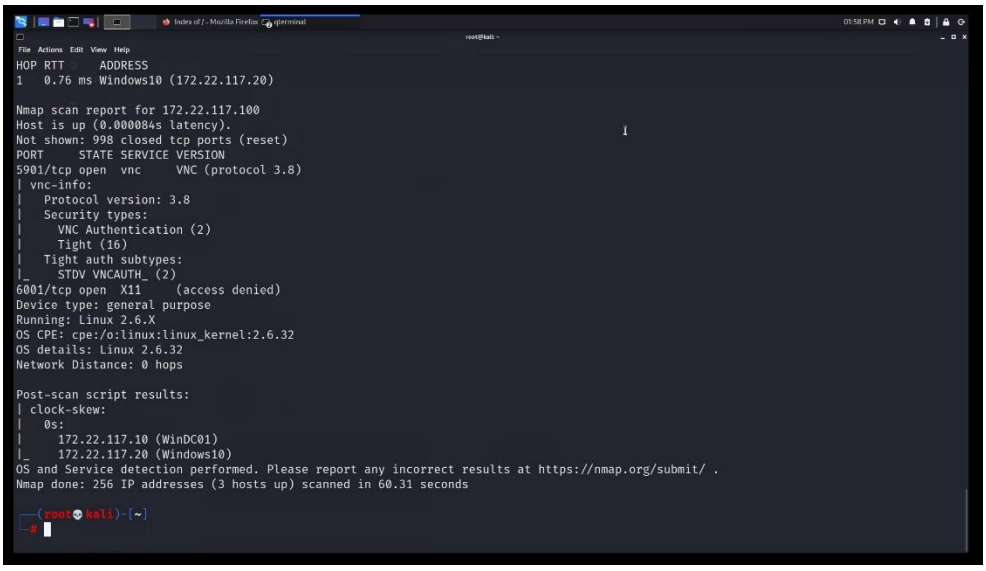
Images	 
Affected Hosts	totalrekall.xyz
Remediation	Scan for company data on public websites. Remove sensitive data from public domains. Change login credentials for trivera

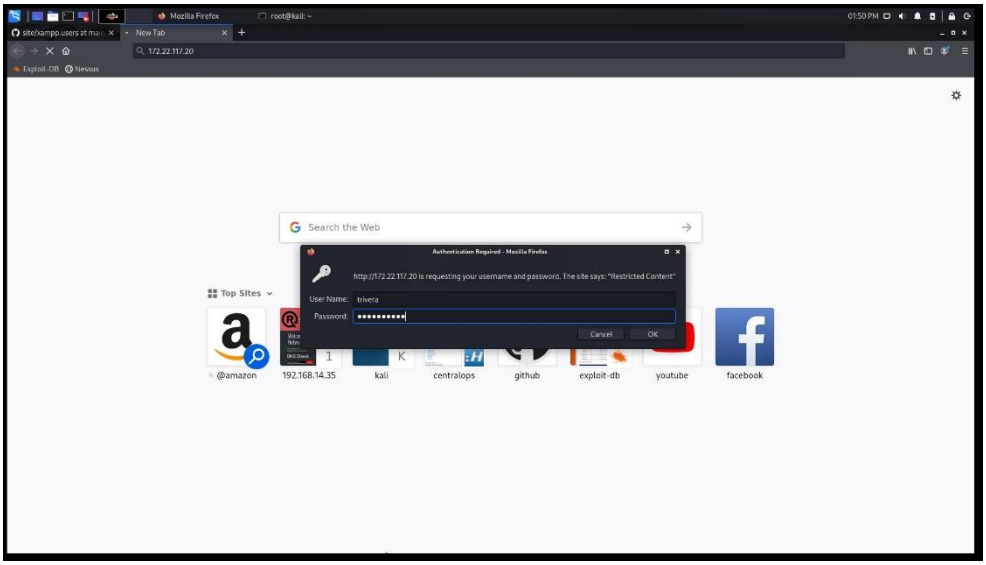
Vulnerability 25	Findings
Title	Brute force attack
Type (Web app / Linux OS / WIndows OS)	Web app / Windows OS
Risk Rating	**Critical**
Description	Scan of the subnet (172.22.117.0/24) reveals three hosts: 172.22.117.100 172.22.117.20 172.22.117.10 Login was enabled through HTTP on 172.22.117.20 using trivera credentials

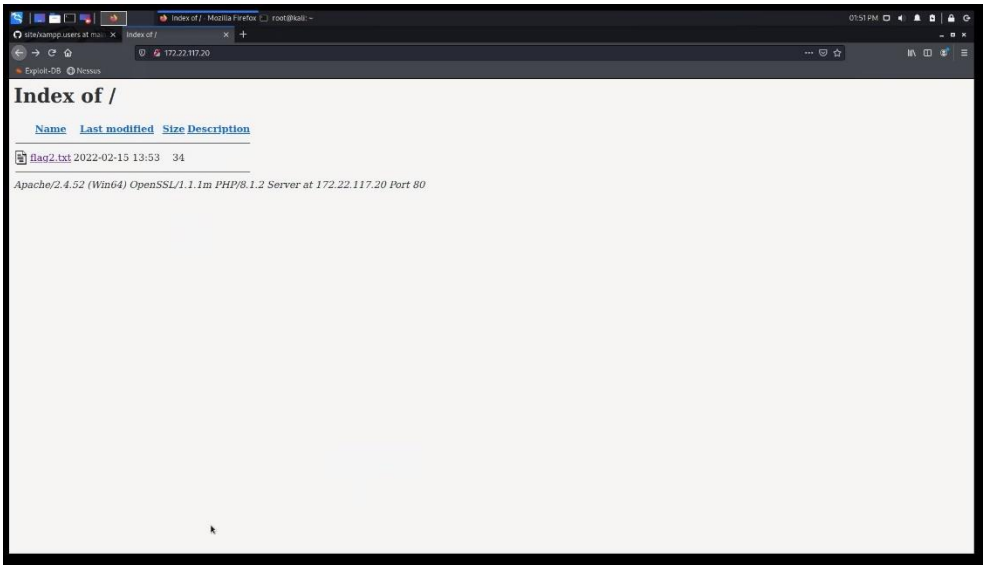
Images

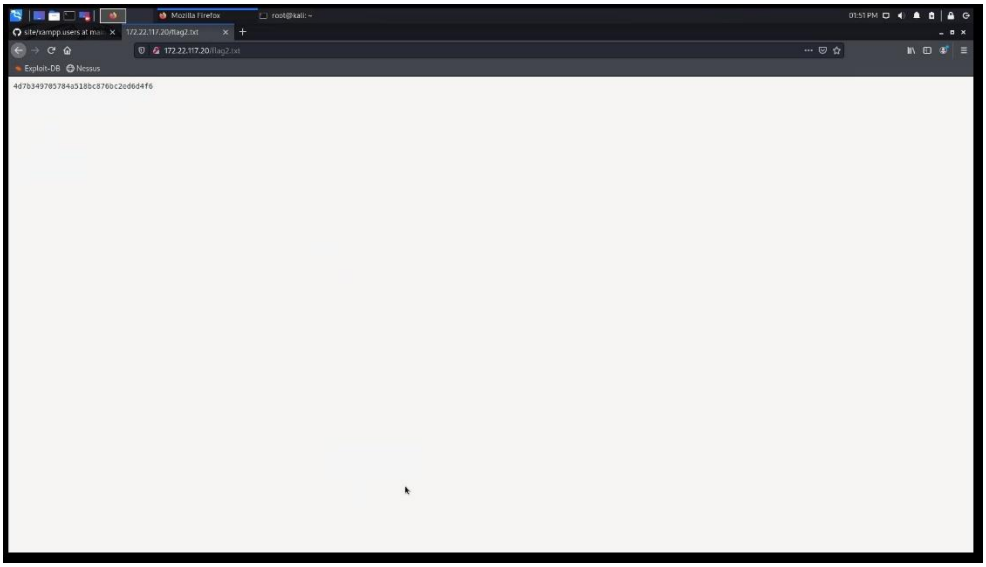






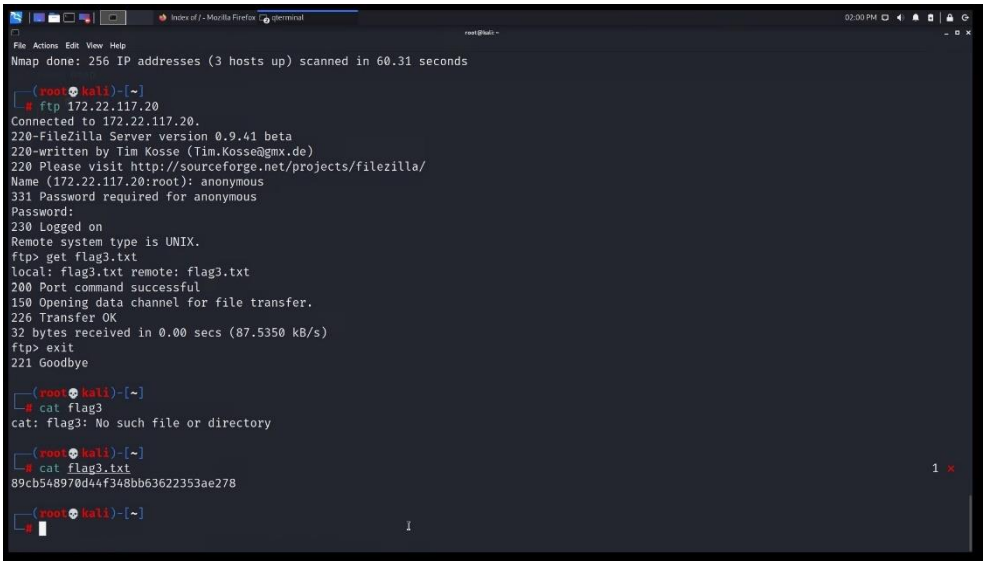




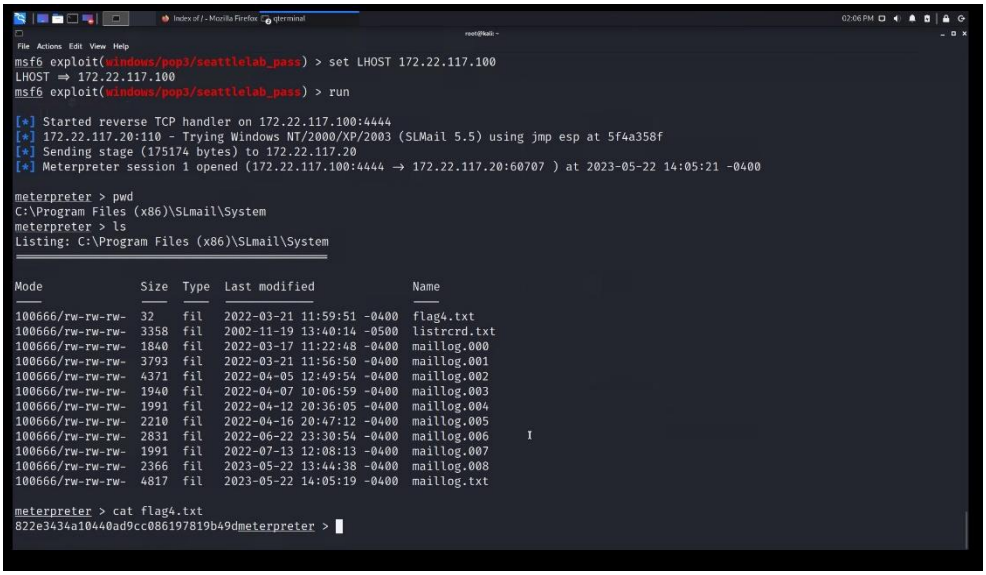


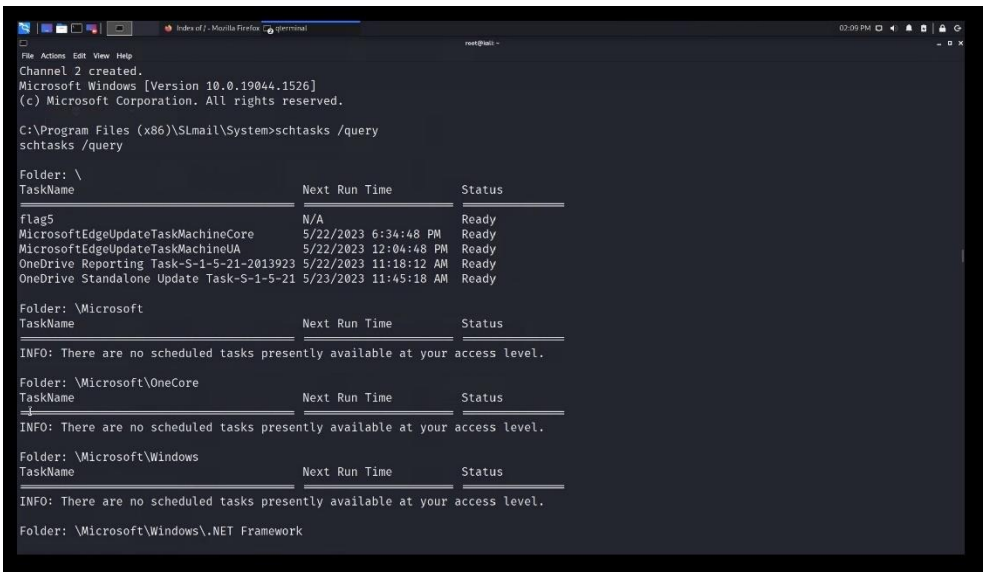
Affected Hosts	172.22.117.20
Remediation	Scan for company data on public websites.

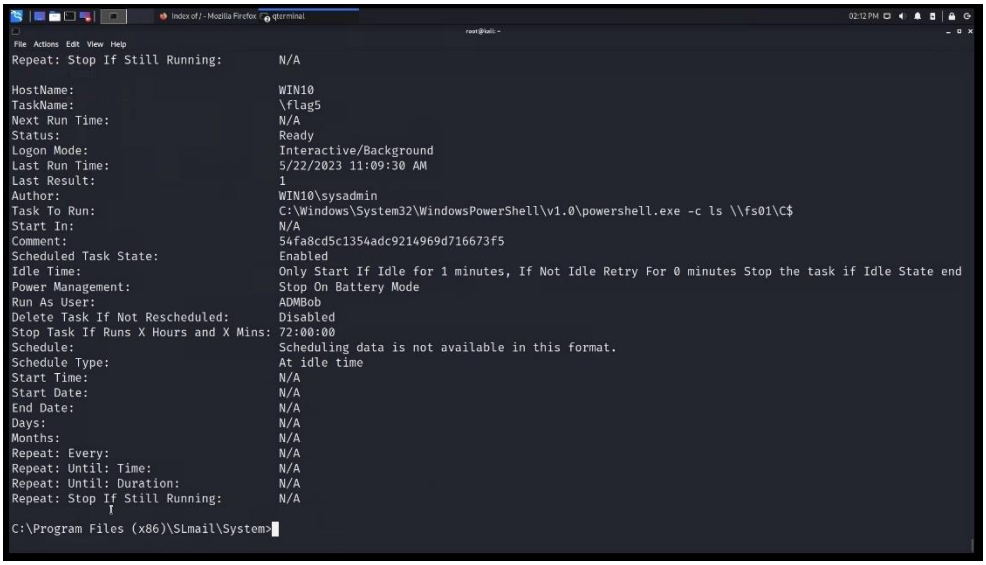
	Remove sensitive data from public domains. Change login credentials for trivera Monitor HTTP traffic

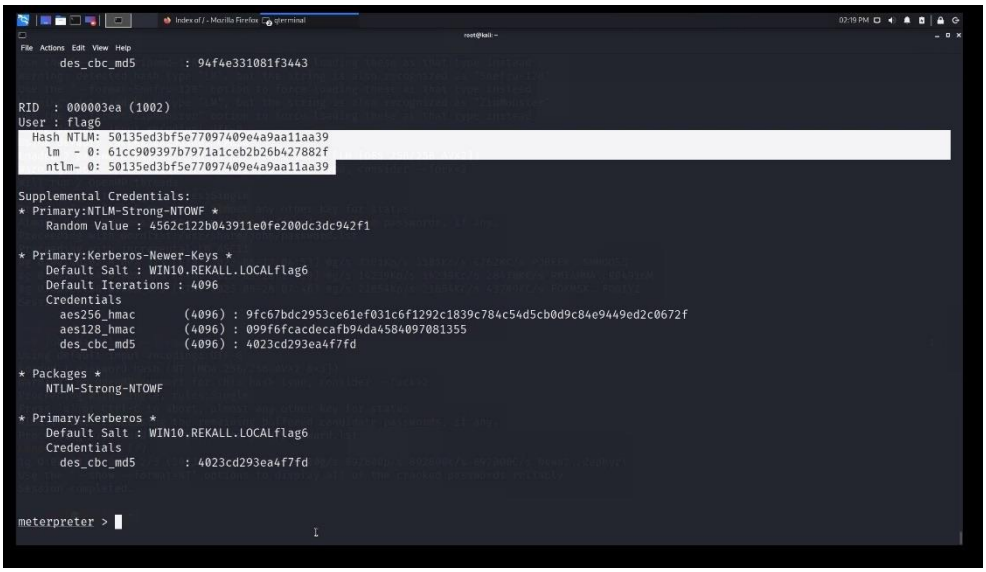
Vulnerability 26	Findings
Title	Anonymous File Transfer Protocol (FTP)
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	Port scan revealed FTP port 21 was open on 172.22.117.20. Used ‘anonymous’ as user ID to FTP and gain access to file
Images	
Affected Hosts	172.22.117.20
Remediation	Disable FTP if not needed. If FTP is needed, then adjust the account and directory access to make it more secure. Disable Anonymous authentication in FTP.

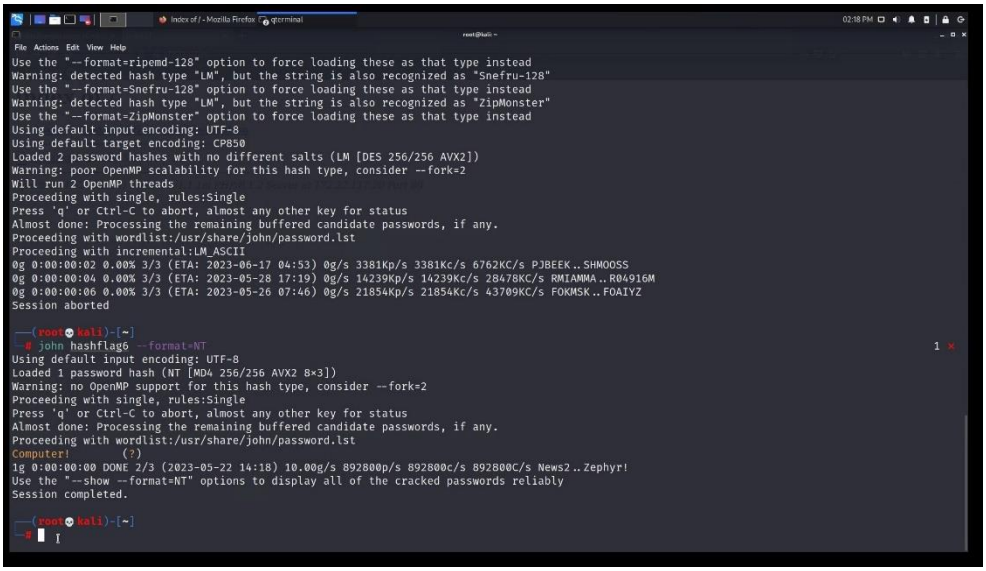
Vulnerability 27	Findings
Title	SLmail exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Port scan revealed SLMail service running on SMTP port 25 AND on POP3 port 110. Using exploit (windows/pop3/seattlelab_pass) got meterpreter access.

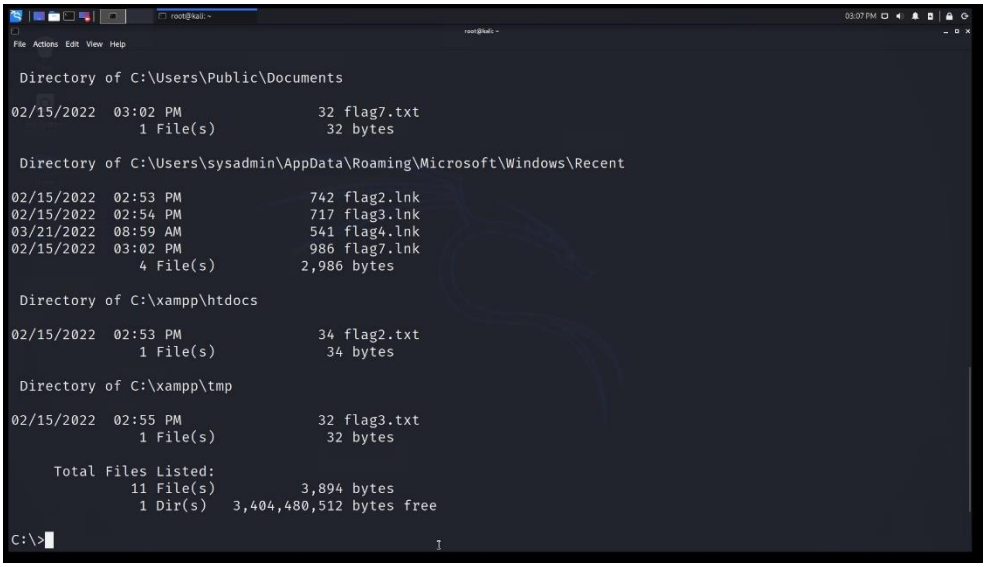
Images	
Affected Hosts	172.22.117.20
Remediation	Upgrade to SLMail to newer version

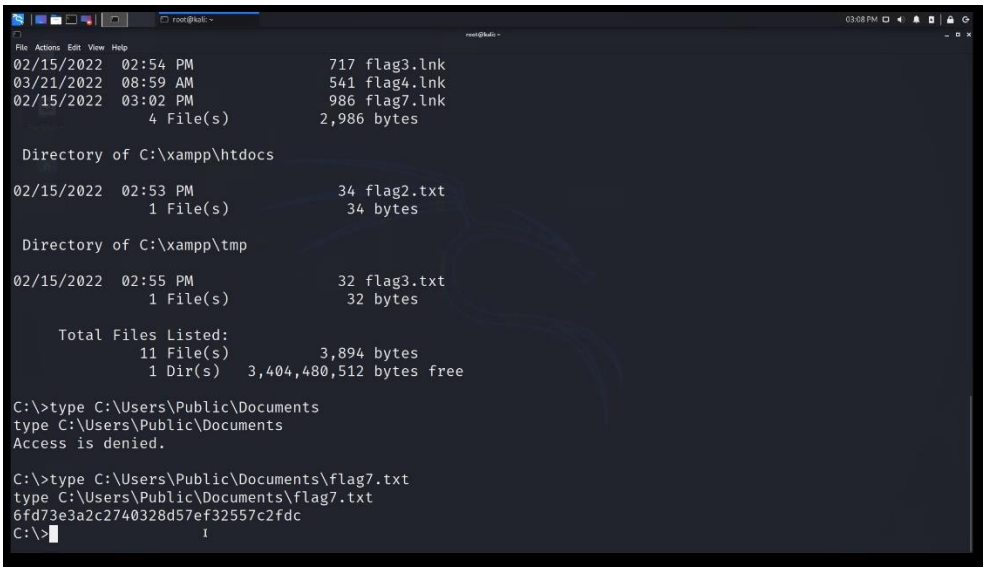
Vulnerability 28	Findings
Title	Scheduled task exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**High**
Description	Able to list scheduled task after gaining access to meterpreter. Can be used to schedule recurring execution of malicious code.
Images	

	
Affected Hosts	172.22.117.20
Remediation	Create an alert for whenever any new scheduled tasks are created

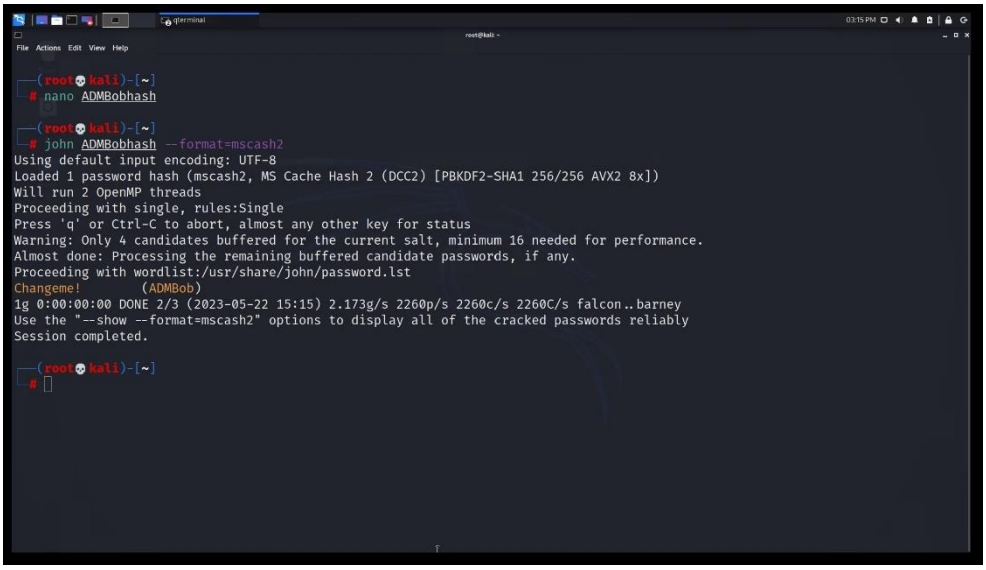
Vulnerability 29	Findings
Title	Kiwi exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Used Kiwi for LSA dump. Got access to password hash
Images	

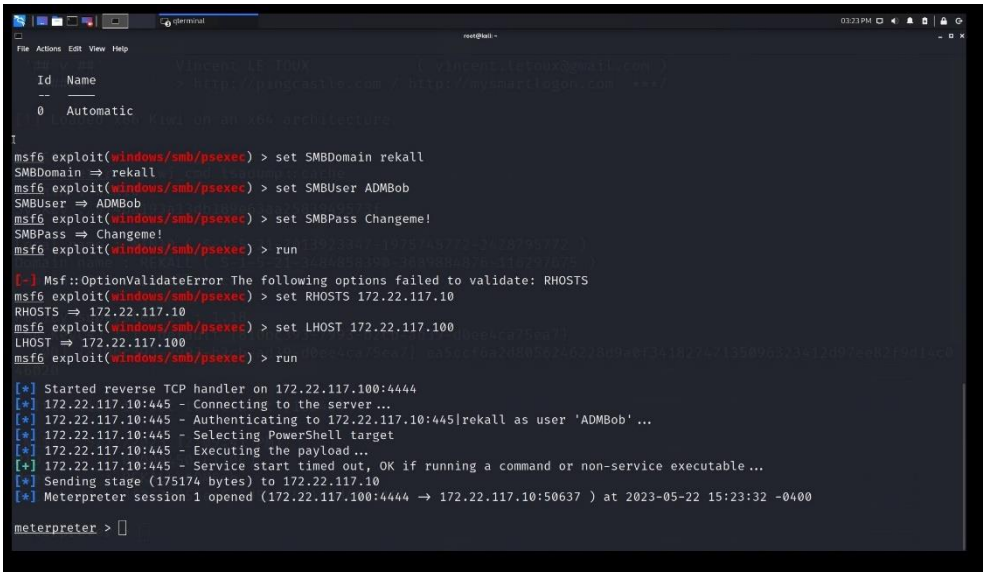
	
Affected Hosts	172.22.117.20
Remediation	Use software to disable Kiwi.

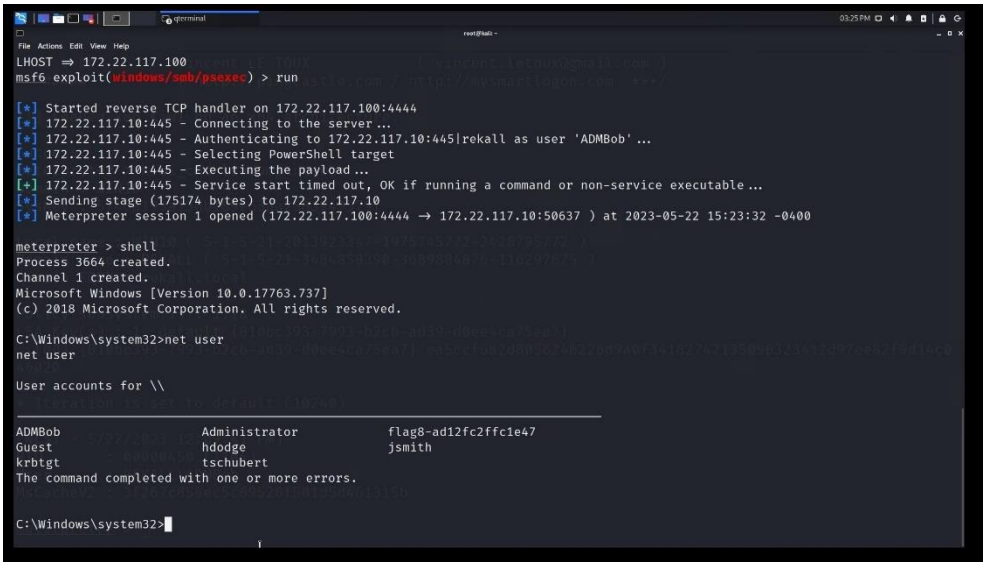
Vulnerability 30	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Used search command in meterpreter to search documents
Images	

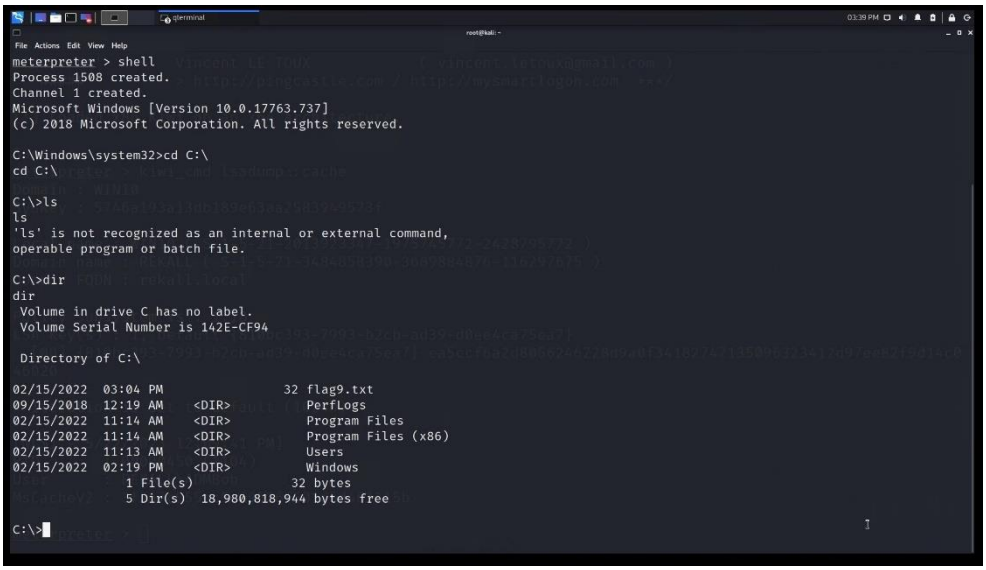
	
Affected Hosts	172.22.117.20
Remediation	Check user authorization for file access. Restrict access to files for all user and only authenticate access to authorized users.

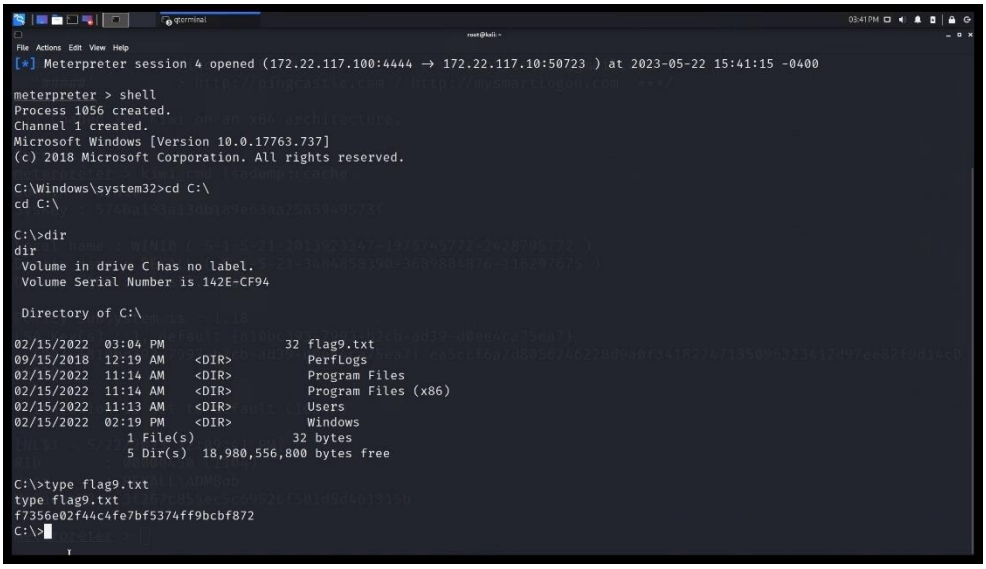
Vulnerability 31	**Findings**
Title	Kiwi exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Used Kiwi to get access to password hash. Used john to get password.
Images	

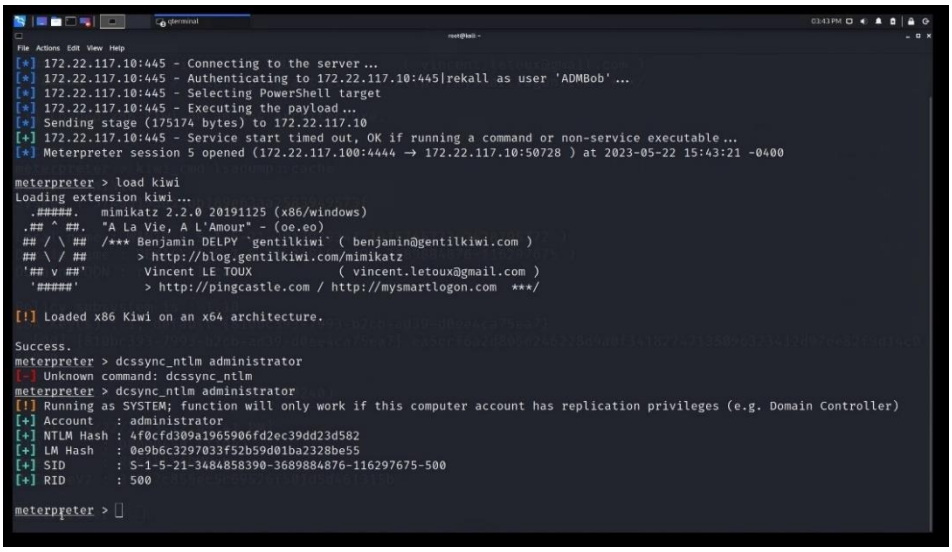
	
Affected Hosts	172.22.117.20
Remediation	Change admin ADMBob credentials and password. Remove any unknown / unused users. Check if the right users have admin access.

Vulnerability 32	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Used PsExec module in Metasploit to get access to system shell on server. Once shell was open, listed user accounts
Images	

	
Affected Hosts	172.22.117.10
Remediation	Change admin ADMBob credentials and password. Remove any unknown / unused users. Check if the right users have admin access. Check file privileges.

Vulnerability 33	Findings
Title	Lateral Movement – Root Access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Got root access and listed files
Images	

	
Affected Hosts	172.22.117.10
Remediation	Change admin ADMBob credentials and password. Remove any unknown / unused users. Check if the right users have admin access. Check file privileges.

Vulnerability 34	**Findings**
Title	Kiwi exploit (Domain controller)
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Used DCSync to get access to password data
Images	
Affected Hosts	172.22.117.20
Remediation	Block privilege escalation. Disable user account. Change password.