



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Student Note: Complete all sections highlighted in yellow.

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	Natasha pentestingcorp
Contact Name	Natasha Harris
Contact Title	pentesters

Document History

Version	Date	Author(s)	Comments
001	06/31/2023	Natasha H.	

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.

- The website looks pretty
- Some system services required user authentication

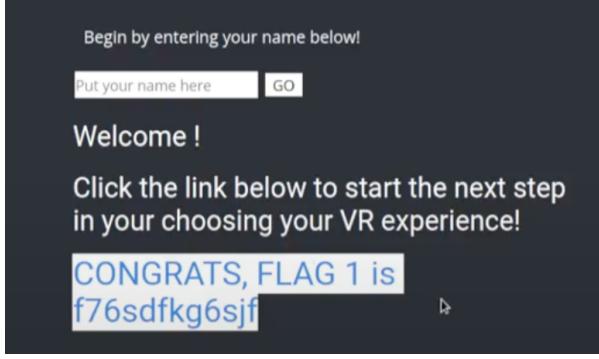
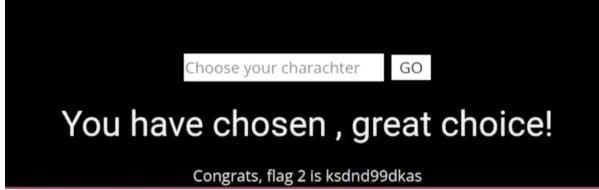
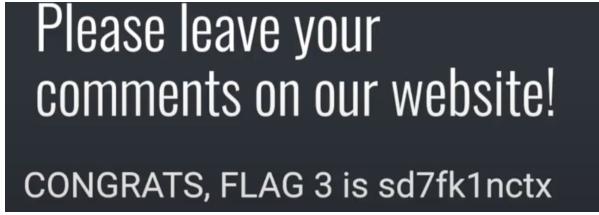
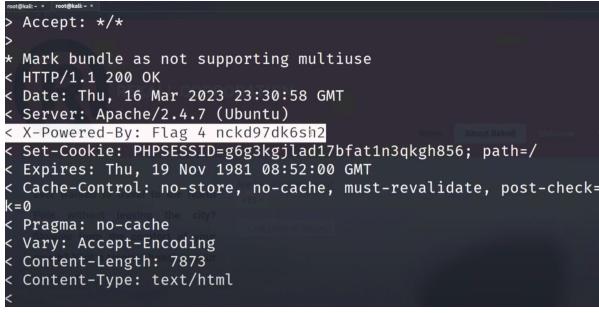
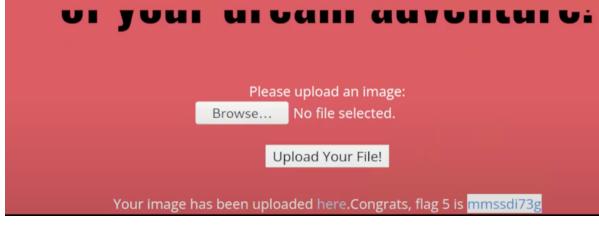
Summary of Weaknesses

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.

- XSS Reflected
- XSS Stored
- Sensitive Data Exposure
- Local File Inclusion
- Advanced Local File Inclusion
- SQL Injection
- Sensitive Data Exposure
- Command Injection
- Advanced Command Injection
- Weak User Credentials
- PHP Injection
- Session Management
- Directory Traversal

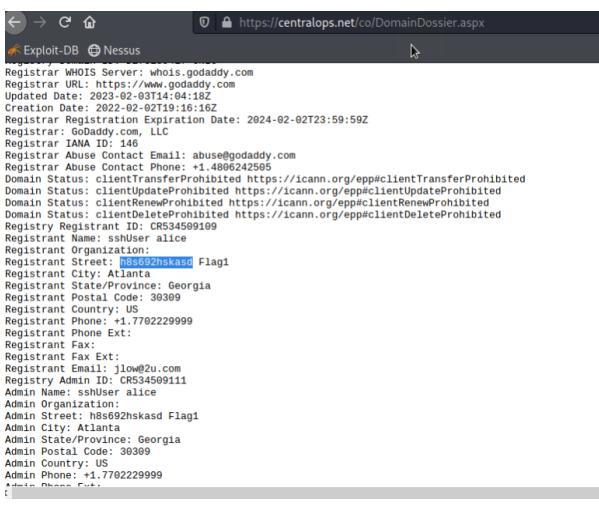
Executive Summary

[Provide a narrative summary of your steps and findings, including screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A-Z summary of your assessment.]

Day 1	Images
Flag 1 Vulnerability: XSS Reflected	 <p>Begin by entering your name below!</p> <p>Put your name here <input type="text"/> GO</p> <p>Welcome !</p> <p>Click the link below to start the next step in your choosing your VR experience!</p> <p>CONGRATS, FLAG 1 is f76sdfkg6sjf</p>
Flag 2 Vulnerability: Advanced XSS Reflected	 <p>Choose your character <input type="text"/> GO</p> <p>You have chosen , great choice!</p> <p>Congrats, flag 2 is ksdnd99dkas</p>
Flag 3 Vulnerability: XSS Stored	 <p>Please leave your comments on our website!</p> <p>CONGRATS, FLAG 3 is sd7fk1nctx</p>
Flag 4 Vulnerability: Sensitive Data Exposure	 <pre> > Accept: */* > * Mark bundle as not supporting multiuse < HTTP/1.1 200 OK < Date: Thu, 16 Mar 2023 23:30:58 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: Flag_4_nckd97dk6sh2 < Set-Cookie: PHPSESSID=g6g3kgjlad17bfat1n3qkgh856; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check= k=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html <</pre>
Flag 5 Vulnerability: Local File Inclusion	 <p>Please upload an Image:</p> <p><input type="button"/> Browse... No file selected.</p> <p><input type="button"/> Upload Your File!</p> <p>Your image has been uploaded here.Congrats, flag 5 is mmssdi73g</p>

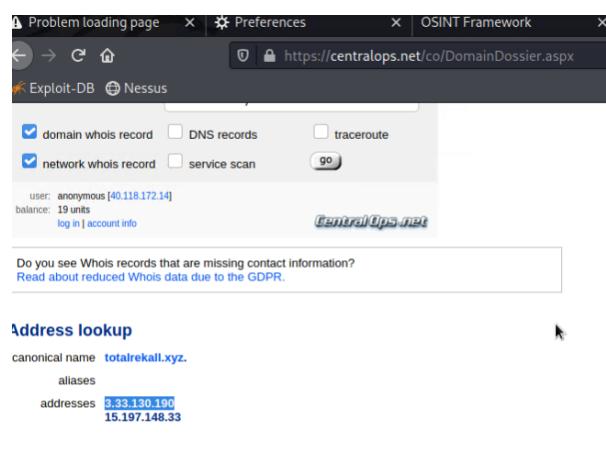
<h2>Flag 6</h2> <p>Vulnerability: Local File Inclusion</p>	<p>Please upload an Image:</p> <p><input type="button" value="Browse..."/> No file selected.</p> <p><input type="button" value="Upload Your File!"/></p> <p>Your Image has been uploaded here. Congrats, flag 6 is <code>id8skd62hdd</code></p>
<h2>Flag 7</h2> <p>Vulnerability: SQL Injection</p>	<p>Login:</p> <p>[REDACTED]</p> <p>Password:</p> <p>[REDACTED]</p> <p>Login</p> <p>Congrats, flag 7 is <code>bcs92jsk233</code></p>
<h2>Flag 8</h2> <p>Vulnerability: Sensitive Data Exposure</p>	<p>Login:</p> <p>[REDACTED]</p> <p>Password:</p> <p>[REDACTED]</p> <p>Login</p> <p>Successful login! flag 8 is <code>87fsdkf6djf</code>, also check out the admin only networking tools HERE</p>
<h2>Flag 9</h2> <p>Vulnerability: Sensitive Data Exposure</p>	<pre>User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:<code>dkkdudfkdy23</code></pre>
<h2>Flag 10</h2> <p>Vulnerability: Command Injection / Session Management vulnerability</p>	<p>Congrats, flag 10 is <code>ksdnnd99dkas</code></p> <h3>MX Record Checker</h3> <p><input type="text" value="www.example.com"/> <input type="button" value="Check your MX"/></p>
<h2>Flag 11</h2> <p>Vulnerability: Command Injection</p>	<p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is <code>opshdkasy78s</code></p>
<h2>Flag 12</h2> <p>Vulnerability: Weak User Credentials</p>	<p>Successful login! flag 12 is <code>hsk23oncsd</code>, also the top secret legal data located here: HERE</p>

<h2>Flag 13</h2> <p>Vulnerability: PHP Injection</p>	<p>Souvenirs for your VR experience</p> <p>Dont come back from your empty handed!</p> <p>Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options...</p> <p><i>hello/app</i></p> <p>Congrats, flag 13 is jdka7sk23dd</p>
<h2>Flag 14</h2> <p>Vulnerability: Session Management</p>	<p>Admin Legal Documents - Restricted Area</p> <p>Welcome Admin...</p> <p>You have unlocked the secret area, flag 14 is dks93jlsd7d</p>
<h2>Flag 15</h2> <p>Vulnerability: Directory Traversal</p>	<p>"New" Rekall Disclaimer</p> <p>Going to Rekall may introduce risk:</p> <p>Please seek medical assistance if you experience:</p> <ul style="list-style-type: none"> - Headache - Vertigo - Swelling - Nausea <p>Congrats, flag 15 is dk sdf7sjd5sg</p>

Day 2	Images
<h2>Flag 1</h2> <p>Vulnerability: Open Sourced Data</p>	 <p>Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registry ID: CR534569109 Registrar: GoDaddy.com, LLC Registrar IANA ID: 146 Registrar Abuse Contact Email: abuse@godaddy.com Registrar Abuse Contact Phone: +1.4886242585 Domain Status: clientTransferProhibited https://icann.org/eppclientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/eppclientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/eppclientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/eppclientDeleteProhibited Registry Registrant ID: CR534569109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: 123 Main St, Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534569111 Admin Name: sshUser alice Admin Organization: Admin Street: 123 Main St, Flag1 Admin City: Atlanta Admin State/Province: Georgia Admin Postal Code: 30309 Admin Country: US Admin Phone: +1.7702229999</p>

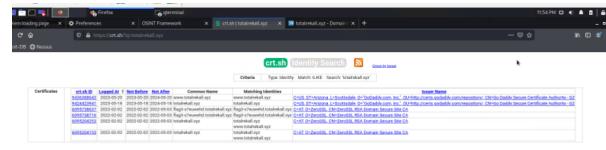
Flag 2

Vulnerability: Open sourced data



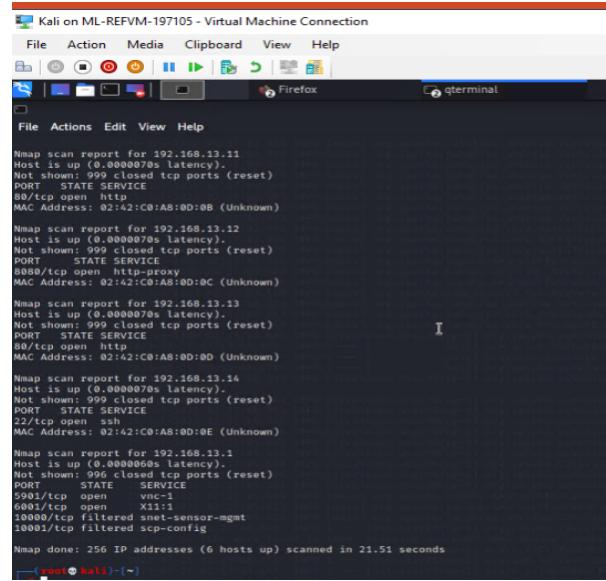
Flag 3

Vulnerability: Open sourced data



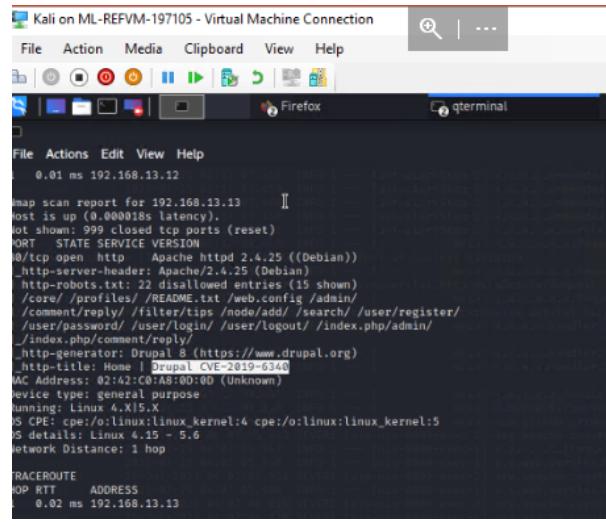
Flag 4

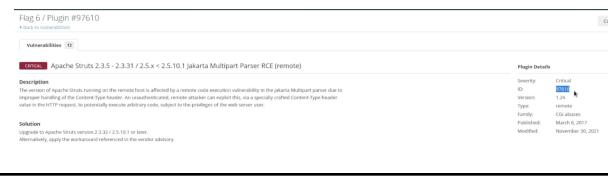
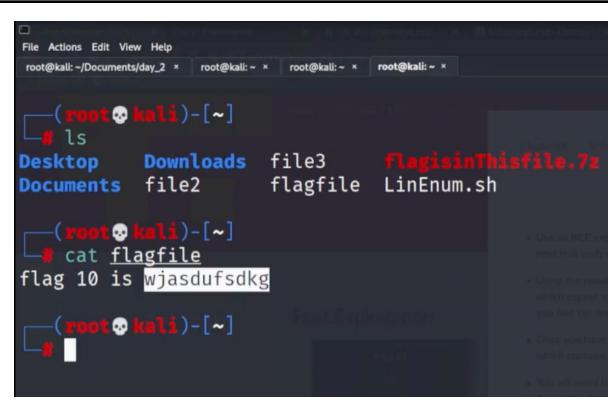
Vulnerability: Total hosts within local network



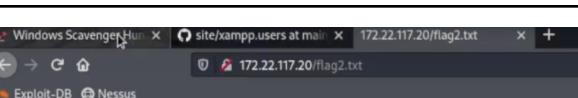
Flag 5

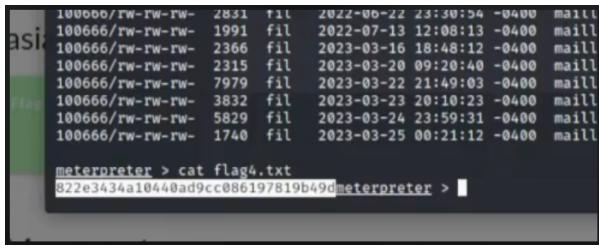
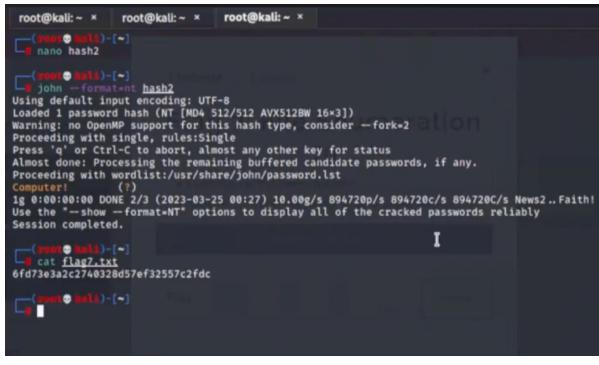
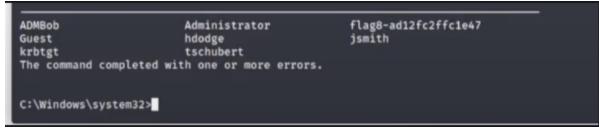
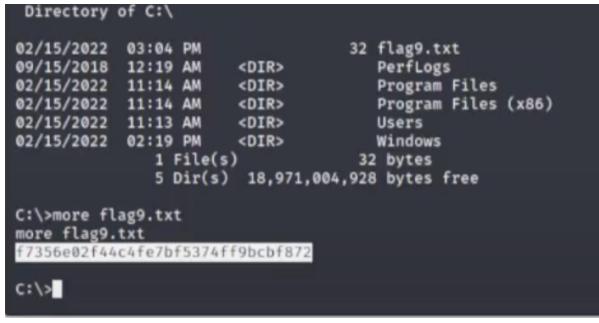
Vulnerability: Drupal, Returned Scan Results



<h2>Flag 6</h2> <p>Vulnerability: Apache Struts</p>	
<h2>Flag 7</h2> <p>Vulnerability: Apache Tomcat Remote Code Execution</p>	<pre>find / -type f -iname "*flag*" /root/.flag7.txt /sys/devices/platform/serial8250/ /sys/devices/platform/serial8250/ /sys/devices/platform/serial8250/ /sys/devices/platform/serial8250/ /sys/devices/virtual/net/eth0/flags /sys/module/scsi_mod/parameters/c /proc/sys/kernel/acpi_video_flags /proc/sys/kernel/sched_domain/cpu /proc/sys/kernel/sched_domain/cpu /proc/kpageflags cat /root/.flag7.txt 8ks 6sbhss</pre>
<h2>Flag 8</h2> <p>Vulnerability: Shellshock</p>	<pre># 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/ # 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 flag8-9dnx5shdf5</pre>
<h2>Flag 9</h2>	<pre>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 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>
<h2>Flag 10</h2> <p>Vulnerability: Struts exploitation</p>	

Flag 11	<pre>[+] The target is vulnerable. [*] Sending POST to /node with link http://192.168.13.100 [*] Sending stage (39282 bytes) to 192.168.13.100 [*] Meterpreter session 4 opened (172.28.151.100 meterpreter > getuid Server username: www-data meterpreter > </pre>
Flag 12	<pre>File Actions Edit View Help root@kali: ~/Documents/day_2 * root@kali: ~ * root@kali: ~ * root@kali: ~ * \$ 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 d7sdfksdf384</pre>

Days 3	Images																				
<h2 data-bbox="445 1129 572 1172">Flag 1</h2> <p>Vulnerability: Open Source Exposed Information</p>	 <pre data-bbox="843 1129 1421 1322"> File Actions Edit View Help └── hashcat [hash](-) └── name hash └── hashcat [hash](-) └── name hash └── hashcat [hash](-) └── name hash Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long" Hashcat will attempt to automatically force loading these as that type instead Hashcat v5.2.0-dev (2022-03-25) Official Build - SHA256-Derived Loaded 1 password hash (md5crypt, crypt(3) \$1\$ (and variants) [MD5 512/512 AVX512BW 16x=1]) Total 1 unique password hash(s) found Proceeding with single, rules:single Press q or Ctrl-C to abort, almost any other key for status Almost done... Processed 1 password, 0 rejected, 0 buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Status: 1 password hash(s) cracked ig 0:00:00:00 DONE 2/3 (2022-03-25 00:10) 7.142g/s 9957c/s 8957c/s 123456...JAKE Use the --show option to display all of the cracked passwords reliably Session completed: └── hashcat [hash](-) └── crackon [hash](-) </pre>																				
<h2 data-bbox="445 1372 572 1415">Flag 2</h2>																					
<h2 data-bbox="445 1552 572 1594">Flag 3</h2>	 <table border="1" data-bbox="843 1550 1421 1674"> <tr> <td>ls</td> <td>Desktop</td> <td>Downloads</td> <td>File2</td> <td>Flagfile</td> <td>hash</td> <td>Music</td> <td>Public</td> <td>shell.php</td> <td>Templates</td> </tr> <tr> <td></td> <td>Documents</td> <td>file2</td> <td>flag1.txt</td> <td>flagfile.php</td> <td>LinEnum.sh</td> <td>Pictures</td> <td>Scripts</td> <td>shell.php.jpg</td> <td>Videos</td> </tr> </table>	ls	Desktop	Downloads	File2	Flagfile	hash	Music	Public	shell.php	Templates		Documents	file2	flag1.txt	flagfile.php	LinEnum.sh	Pictures	Scripts	shell.php.jpg	Videos
ls	Desktop	Downloads	File2	Flagfile	hash	Music	Public	shell.php	Templates												
	Documents	file2	flag1.txt	flagfile.php	LinEnum.sh	Pictures	Scripts	shell.php.jpg	Videos												

Flag 4	
Flag 5	
Flag 6	
Flag 7	
Flag 8	
Flag 9	
Flag 10	

Summary Vulnerability Overview

Vulnerability	Severity
---------------	----------

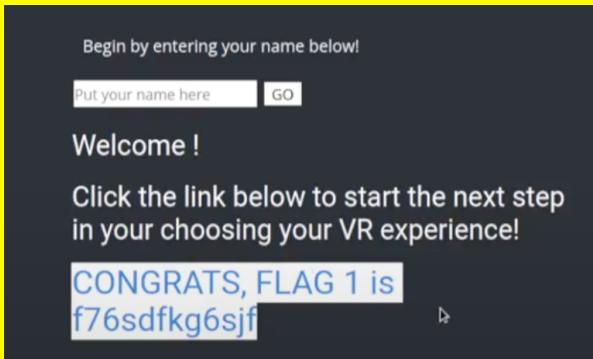
Vulnerability Type	Severity
XSS Reflected	Low
XSS Stored	Medium
Sensitive Data Exposure	Medium
Local File Inclusion	Critical
Advanced Local File Inclusion	Critical
SQL Injection	Critical
Sensitive Data Exposure	High
Command Injection	Critical
Advanced Command Injection	Critical
Weak User Credentials	Medium
PHP Injection	High
Session Management	Critical
Directory Traversal	Medium

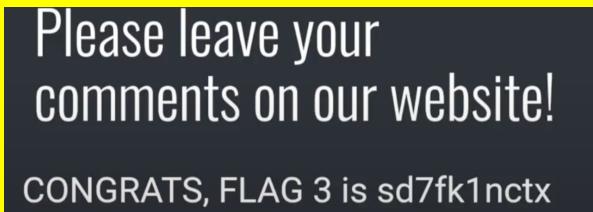
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.0/24
Ports	80, 22, 5901, 6001, 10000, 10001

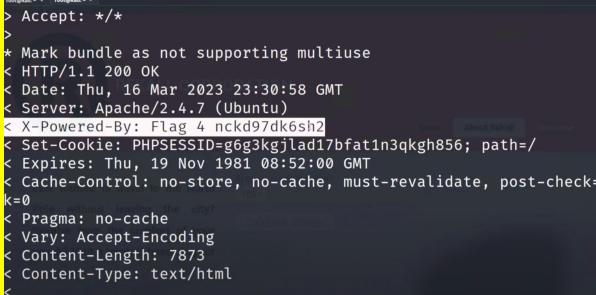
Exploitation Risk	Total
Critical	6
High	2
Medium	4
Low	1

Vulnerability Findings

Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Low
Description	The website has a lack of input validation allowing for users to push across html scripting tags to cause the page to return information about their session or to display a notification to users.
Images	
Affected Hosts	192.168.14.35
Remediation	Implement input validation on all user input boxes

Vulnerability 2	Findings
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	Users can inject html scripting tags into the page to modify how the page reacts to other users. This can allow for malicious users to force others to be redirected to other pages.
Images	
Affected Hosts	totalrekall.com

Remediation	Store all user submitted data into a database to be called on and remove directly appending them to the page so they will not be executed on load for the client. Implement input validation to watch for any html script tags as they are not found natively in english.
--------------------	--

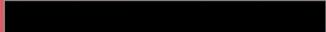
Vulnerability 3	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Medium
Description	Due to a misconfiguration on the machine standard request cause for the machine to return information about the services it is running.
Images	 A terminal window showing an Apache log entry. The log entry details a standard HTTP request for a file named 'index.html'. The response header includes various metadata such as 'Accept: */*', 'Content-Type: text/html', and 'Content-Length: 7873'. It also shows session management information like 'Set-Cookie: PHPSESSID=g6g3kgjlad17bfat1n3qkgh856; path=/', a timestamp ('Date: Thu, 16 Mar 2023 23:30:58 GMT'), and server details ('Server: Apache/2.4.7 (Ubuntu)').
Affected Hosts	192.168.13.14
Remediation	

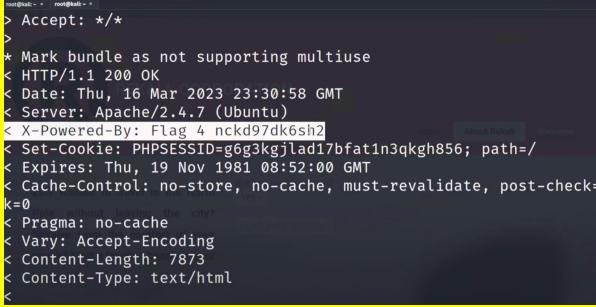
Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A user can upload a malicious shell script to the website that calls on the server to execute commands pushed across the url
Images	 A screenshot of a web browser displaying a URL that includes a local file inclusion vulnerability. The URL is '192.168.14.35/souvenirs.php?message=helloooooo'; system('ls')'. The page content shows the result of the command execution, likely listing files on the server.
Affected Hosts	192.168.14.35
Remediation	Implement input validation on all user submitted files, Upload all user

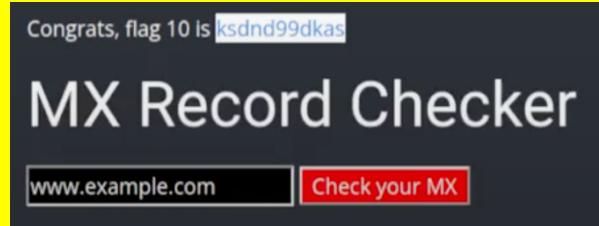
	submitted content to a database to be called on to review direct server execution potential.
--	--

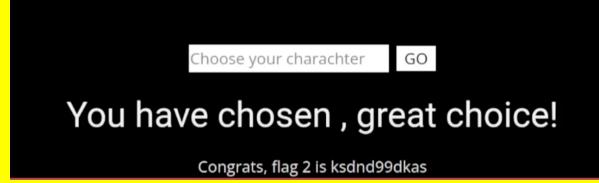
Vulnerability 5	Findings
Title	Advanced Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	Even though the server now limits the type of file that a user can upload, A user can still upload a shell file under a different type. Since the server still executes the file it will still allow for remote code execution
Images	
Affected Hosts	192.168.13.14
Remediation	Upload all user submitted files into a backend database that can be called and displayed without directly executing the file being loaded

Vulnerability 6	Findings
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	A user can submit the payload ok' '1'='1' –, to cause the sql database to return true validating the user to log in even though they did not provide a valid password

Images	<p>Login:</p>  <p>Password:</p>  <p>Login</p> <p>Successful login! flag 8 is 87fsdkf6djf, also check out the admin only networking tools HERE</p>
Affected Hosts	192.168.13.14
Remediation	Implement input validation on all logins to catch for sql syntax, Normalize the server input to look for valid logins and drop anything defined outside normal password syntax

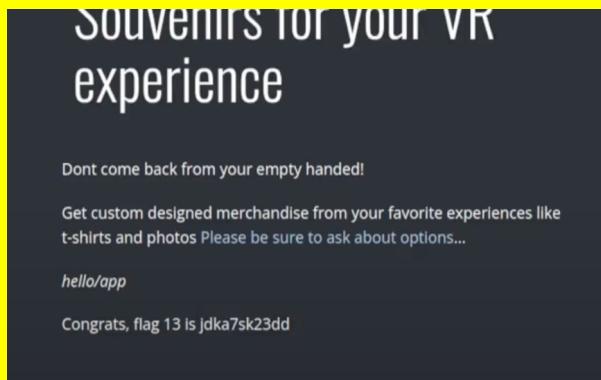
Vulnerability 7	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	High
Description	When a user submits a request for the welcome page the server is mis configured and sends the user excess information, including the direct service running the server.
Images	 <pre> root@kali: ~# curl http://192.168.13.14/ > Accept: */* > < HTTP/1.1 200 OK < Date: Thu, 16 Mar 2023 23:30:58 GMT < Server: Apache/2.4.7 (Ubuntu) < X-Powered-By: PHP/8.1.12 < Set-Cookie: PHPSESSID=g6g3kgjlad17bfat1n3qkgh856; path=/ < Expires: Thu, 19 Nov 1981 08:52:00 GMT < Cache-Control: no-store, no-cache, must-revalidate, post-check= k=0 < Pragma: no-cache < Vary: Accept-Encoding < Content-Length: 7873 < Content-Type: text/html < </pre>
Affected Hosts	192.168.13.14
Remediation	Reconfigure the server's settings when responding to a request at this page.

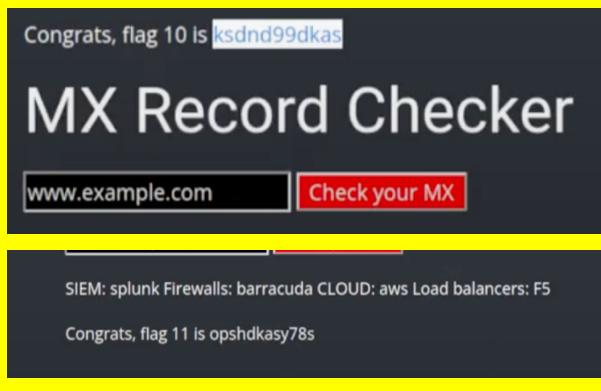
Vulnerability 8	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Users are able to submit commands through the websites mx record checker
Images	 <p>Congrats, flag 10 is ksdnd99dkas</p> <h1>MX Record Checker</h1> <p>www.example.com Check your MX</p>
Affected Hosts	192.168.13.14
Remediation	Implement input validation on all user submitted information, Remove the ability to submit symbols into the web form as they are not found in the standard english language when speaking.

Vulnerability 9	Findings
Title	Advanced Command Injection
Type (Web app / Linux OS / Windows OS)	web app
Risk Rating	critical
Description	In this input field the website has input validation to catch for ampersand characters but the website does not catch the pipe operator .
Images	 <p>Choose your characterter GO</p> <p>You have chosen , great choice!</p> <p>Congrats, flag 2 is ksdnd99dkas</p>
Affected Hosts	192.168.13.14
Remediation	Redefine the characters that are usable within the input box to strictly those found within standard english language.

Vulnerability 10	Findings
Title	Weak User Credentials
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	Medium
Description	Due to a previous vulnerability allowing users to request the /etc/passwd file, we discover all users available within the environment, with this they are able to use a brute force attack to discover the user malina's password is malina.
Images	Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE
Affected Hosts	192.168.13.14
Remediation	Change user credentials and fix the previous mentioned vulnerabilities to remove attackers ability to determine users found within the environment.

Vulnerability 11	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	web app
Risk Rating	High
Description	An attacker is able to submit malicious php queries through the url when requesting a page from the server.

Images	 <p>Dont come back from your empty handed!</p> <p>Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options...</p> <p><i>hello/app</i></p> <p>Congrats, flag 13 is jdk7sk23dd</p>	
Affected Hosts	192.168.13.14	
Remediation	Disable the ability for the server to execute arbitrary requests, specify the list of pages a user is able to access with user role management dependent on the submitted cookie associated with their user.	

Vulnerability 12	Findings	
Title	Session Management	
Type (Web app / Linux OS / Windows OS)	web app	
Risk Rating	critical	
Description	An individual is able to notice an ID declaration in the url bar for the admin page. Using a brute forcing tool they are able to increment through as many id's as they may need, to find the correct id for the administrator.	
Images	 <p>Congrats, flag 10 is <code>ksdnd99dkas</code></p> <h2>MX Record Checker</h2> <p><code>www.example.com</code> <input type="button" value="Check your MX"/></p> <hr/> <p>SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5</p> <p>Congrats, flag 11 is <code>opshdkasy78s</code></p>	
Affected Hosts	192.168.13.14	
Remediation	Implement session management through user cookies rather than the url bar. and randomize the users id through random number generation.	

Vulnerability 13		Findings
Title	Directory Traversal	
Type (Web app / Linux OS / Windows OS)	web app	
Risk Rating	medium	
Description	A user is able to request different subpages within the website to be displayed through the URL bar. With the previous vulnerability of command injection the user can	
Images	 <p>"New" Rekall Disclaimer</p> <p>Going to Rekall may introduce risk:</p> <p>Please seek medical assistance if you experience:</p> <ul style="list-style-type: none"> - Headache - Vertigo - Swelling - Nausea <p>Congrats, flag 15 is dksdf7sjd5sg</p>	
Affected Hosts	192.168.13.14	
Remediation	Disable the ability for the server to execute arbitrary requests, specify the list of pages a user is able to access with user role management dependent on the submitted cookie associated with their user.	