攻防世界 杂项 wireshark-1

原创

与日平肩以头抢地 于 2020-02-01 18:20:34 发布 2829 收藏 1

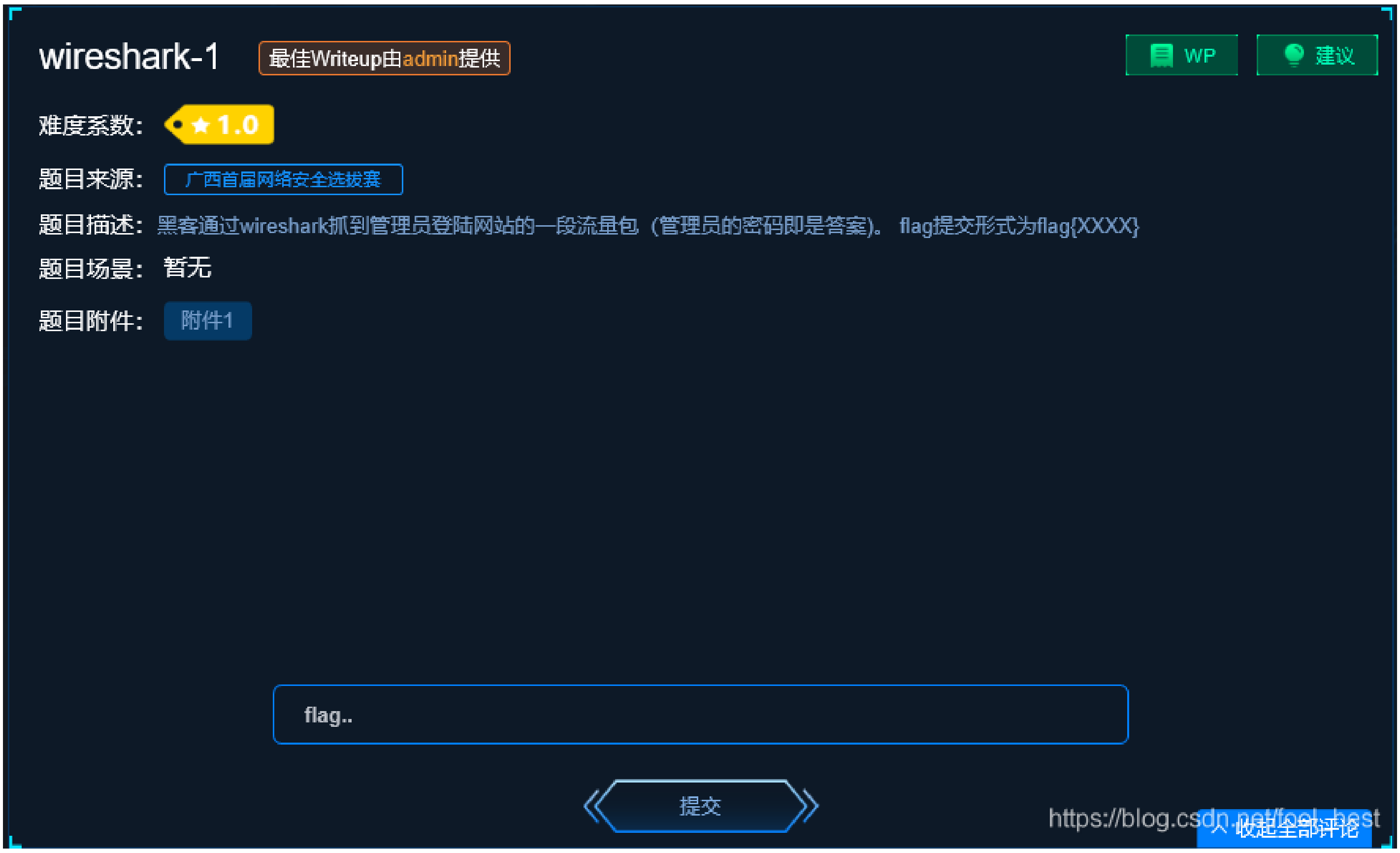
文章标签： https 安全

本文链接：https://blog.csdn.net/fool_best/article/details/104136590

版权

攻防世界 杂项 wireshark-1

原创



难度系数: ★1.0

题目来源: 广西首届网络安全选拔赛

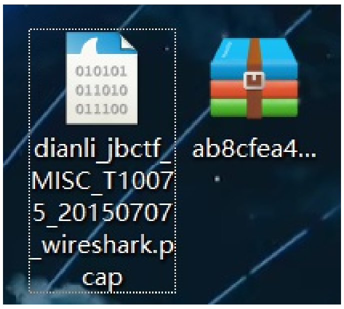
题目描述: 黑客通过wireshark抓到管理员登陆网站的一段流量包（管理员的密码即是答案)。 flag提交形式为flag{XXXX}

题目场景: 暂无

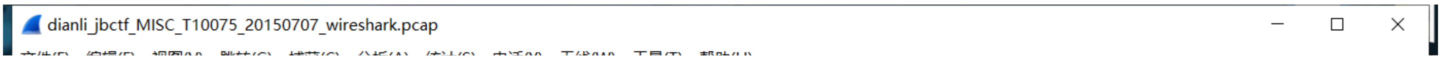
题目附件: 附件1

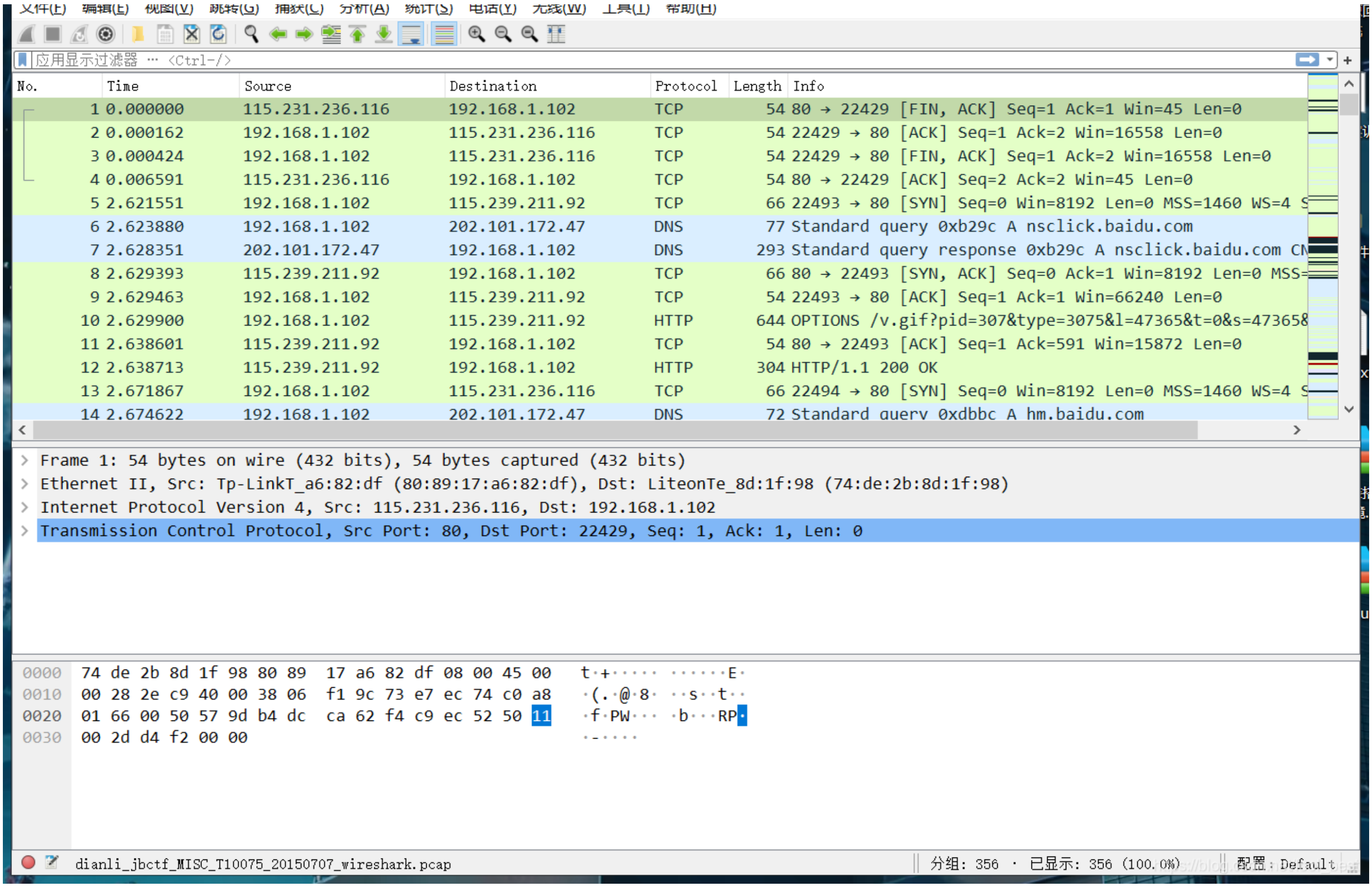
flag..

下载附件，加压一下。



使用wireshark打开解压的新文件。

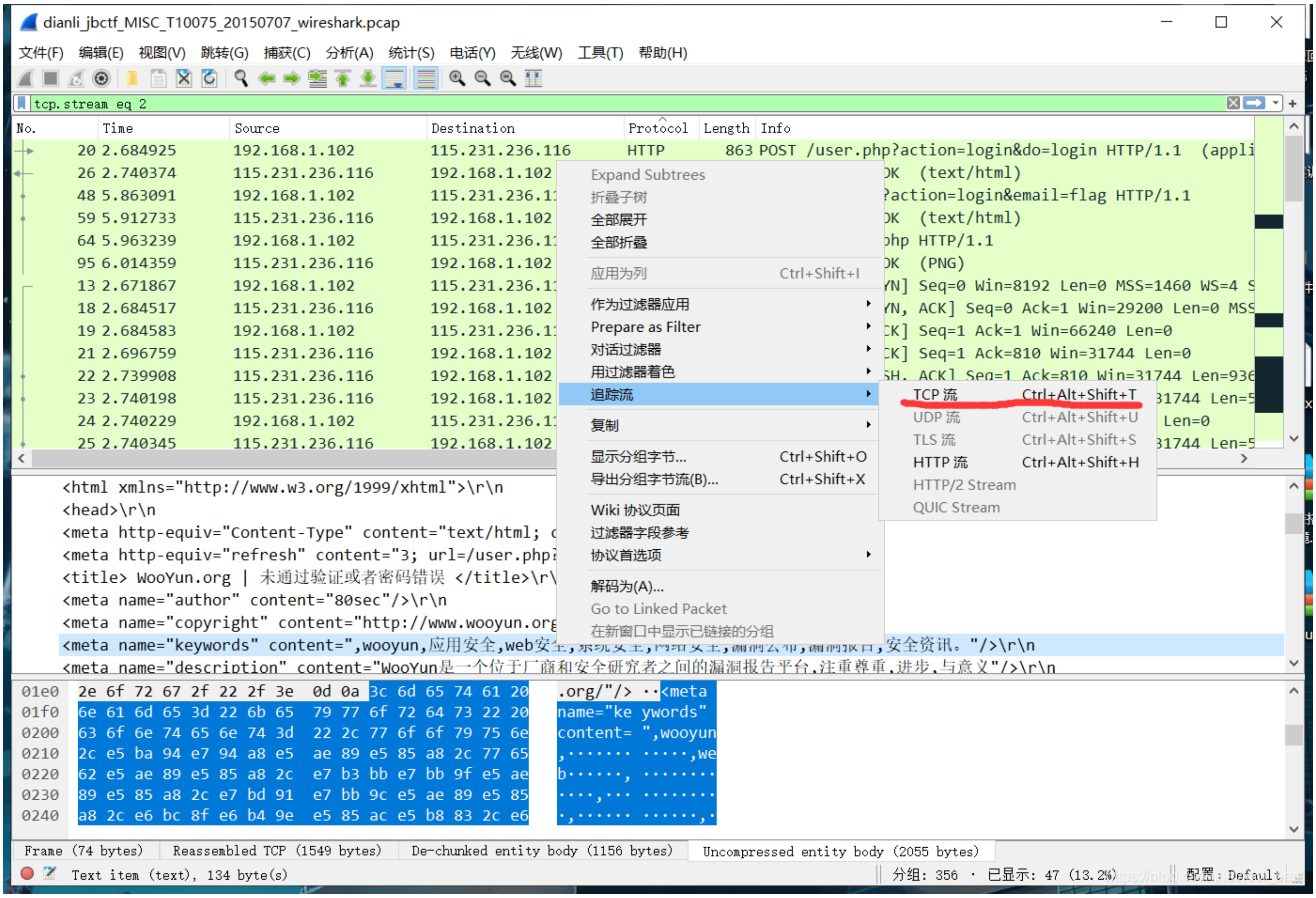



文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
    1 0.000000   115.231.236.116  192.168.1.102    TCP        54 80 → 22429 [FIN, ACK] Seq=1 Ack=1 Win=45 Len=0
    2 0.000162   192.168.1.102    115.231.236.116  TCP        54 22429 → 80 [ACK] Seq=1 Ack=2 Win=16558 Len=0
    3 0.000424   192.168.1.102    115.231.236.116  TCP        54 22429 → 80 [FIN, ACK] Seq=1 Ack=2 Win=16558 Len=0
    4 0.006591   115.231.236.116  192.168.1.102    TCP        54 80 → 22429 [ACK] Seq=2 Ack=2 Win=45 Len=0
    5 2.621551   192.168.1.102    115.239.211.92   TCP        66 22493 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
    6 2.623880   192.168.1.102    202.101.172.47   DNS        77 Standard query 0xb29c A nsclick.baidu.com
    7 2.628351   202.101.172.47   192.168.1.102    DNS       293 Standard query response 0xb29c A nsclick.baidu.com CN
    8 2.629393   115.239.211.92   192.168.1.102    TCP        66 80 → 22493 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=
    9 2.629463   192.168.1.102    115.239.211.92   TCP        54 22493 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
   10 2.629900   192.168.1.102    115.239.211.92   HTTP      644 OPTIONS /v.gif?pid=307&type=3075&l=47365&t=0&s=47365&
   11 2.638601   115.239.211.92   192.168.1.102    TCP        54 80 → 22493 [ACK] Seq=1 Ack=591 Win=15872 Len=0
   12 2.638713   115.239.211.92   192.168.1.102    HTTP      304 HTTP/1.1 200 OK
   13 2.671867   192.168.1.102    115.231.236.116  TCP        66 22494 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
   14 2.674622   192.168.1.102    202.101.172.47   DNS        72 Standard query 0xdbbc A hm.baidu.com

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: Tp-LinkT_a6:82:df (80:89:17:a6:82:df), Dst: LiteonTe_8d:1f:98 (74:de:2b:8d:1f:98)
> Internet Protocol Version 4, Src: 115.231.236.116, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 22429, Seq: 1, Ack: 1, Len: 0

0000  74 de 2b 8d 1f 98 80 89  17 a6 82 df 08 00 45 00   t·+····· ······E·
0010  00 28 2e c9 40 00 38 06  f1 9c 73 e7 ec 74 c0 a8   ·(.·@·8· ··s··t··
0020  01 66 00 50 57 9d b4 dc  ca 62 f4 c9 ec 52 50 11   ·f·PW··· ·b···RP·
0030  00 2d d4 f2 00 00                                  ·-····

dianli_jbctf_MISC_T10075_20150707_wireshark.pcap    分组: 356 · 已显示: 356 (100.0%)    配置: Default
```

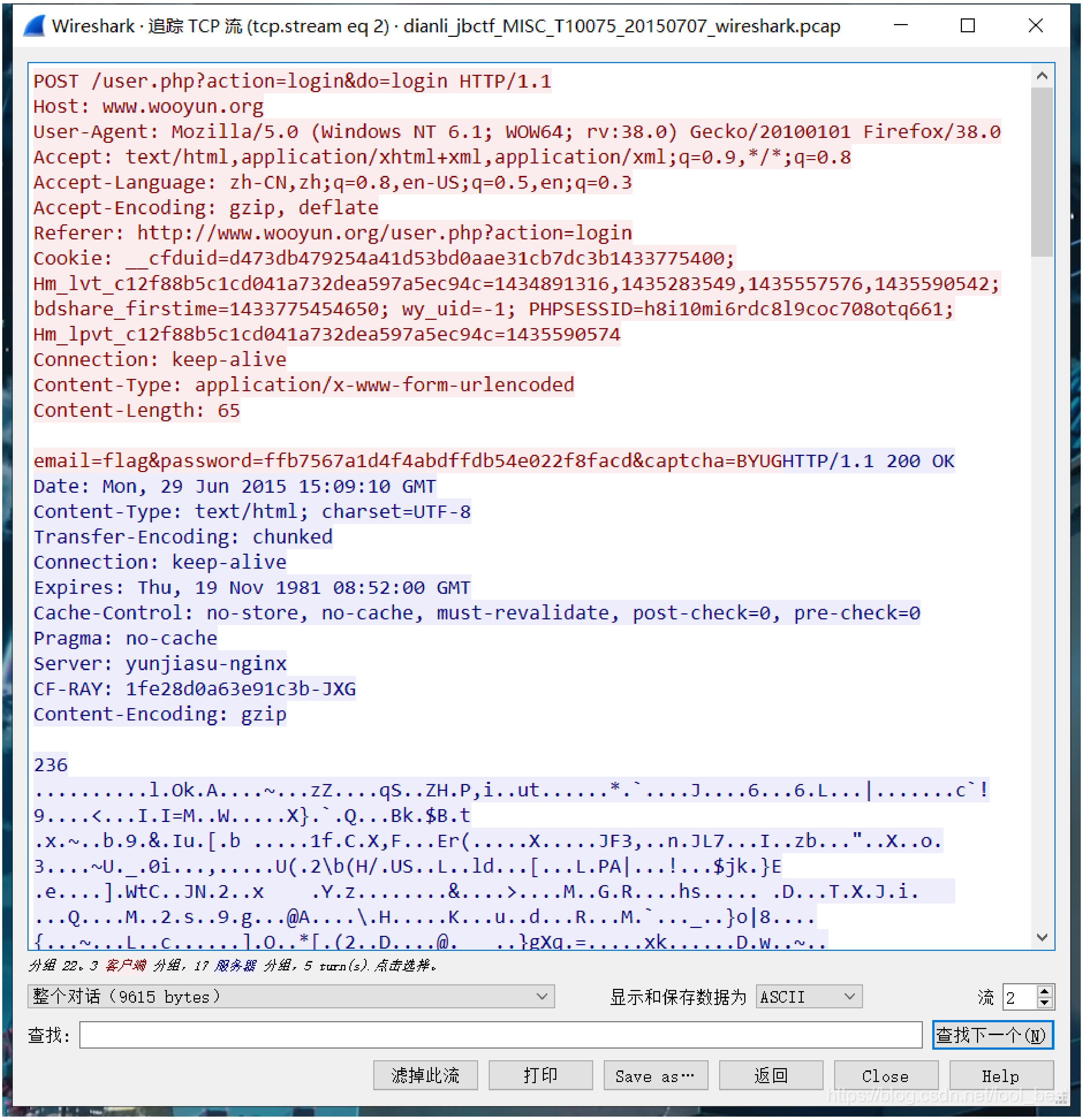
根据题目，查找的是登录网站的所抓捕的管理员信息。

所以我们直接查找Protool中的HTTP。



```
tcp.stream eq 2

No.   Time       Source           Destination      Protocol Length Info
   20 2.684925   192.168.1.102    115.231.236.116  HTTP      863 POST /user.php?action=login&do=login HTTP/1.1  (appli
   26 2.740374   115.231.236.116  192.168.1.102                  OK  (text/html)
   48 5.863091   192.168.1.102    115.231.236.11                 ?action=login&email=flag HTTP/1.1
   59 5.912733   115.231.236.116  192.168.1.102                  OK  (text/html)
   64 5.963239   192.168.1.102    115.231.236.11                 php HTTP/1.1
   95 6.014359   115.231.236.116  192.168.1.102                  OK  (PNG)
   13 2.671867   192.168.1.102    115.231.236.11                 YN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 S
   18 2.684517   115.231.236.116  192.168.1.102                  YN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS
   19 2.684583   192.168.1.102    115.231.236.11                 CK] Seq=1 Ack=1 Win=66240 Len=0
   21 2.696759   115.231.236.116  192.168.1.102                  CK] Seq=1 Ack=810 Win=31744 Len=0
   22 2.739908   115.231.236.116  192.168.1.102                  SH, ACK] Seq=1 Ack=810 Win=31744 Len=936
   23 2.740198   115.231.236.116  192.168.1.102                  31744 Len=5
   24 2.740229   192.168.1.102    115.231.236.11                  Len=0
   25 2.740345   115.231.236.116  192.168.1.102                  31744 Len=5

    <html xmlns="http://www.w3.org/1999/xhtml">\r\n
    <head>\r\n
    <meta http-equiv="Content-Type" content="text/html; c
    <meta http-equiv="refresh" content="3; url=/user.php
    <title> WooYun.org | 未通过验证或者密码错误 </title>\r\
    <meta name="author" content="80sec"/>\r\n
    <meta name="copyright" content="http://www.wooyun.org
    <meta name="keywords" content=",wooyun,应用安全,web安全,系统安全,网络安全,漏洞公布,漏洞报告,安全资讯。"/>\r\n
    <meta name="description" content="WooYun是一个位于厂商和安全研究者之间的漏洞报告平台,注重尊重,进步,与意义"/>\r\n

01e0  2e 6f 72 67 2f 22 2f 3e  0d 0a 3c 6d 65 74 61 20   .org/"/> ··<meta
01f0  6e 61 6d 65 3d 22 6b 65  79 77 6f 72 64 73 22 20   name="ke ywords"
0200  63 6f 6e 74 65 6e 74 3d  22 2c 77 6f 6f 79 75 6e   content= ",wooyun
0210  2c e5 ba 94 e7 94 a8 e5  ae 89 e5 85 a8 2c 77 65   ,······· ·····,we
0220  62 e5 ae 89 e5 85 a8 2c  e7 b3 bb e7 bb 9f e5 ae   b·····, ········
0230  89 e5 85 a8 2c e7 bd 91  e7 bb 9c e5 ae 89 e5 85   ····,··· ········
0240  a8 2c e6 bc 8f e6 b4 9e  e5 85 ac e5 b8 83 2c e6   ·,······ ······,·

Frame (74 bytes)   Reassembled TCP (1549 bytes)   De-chunked entity body (1156 bytes)   Uncompressed entity body (2055 bytes)
Text item (text), 134 byte(s)    分组: 356 · 已显示: 47 (13.2%)    配置: Default
```

在一处HTTP中找到了网站的信息，我们在keyword一行追踪TCP流。



Wireshark · 追踪 TCP 流 (tcp.stream eq 2) · dianli_jbctf_MISC_T10075_20150707_wireshark.pcap

```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
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.wooyun.org/user.php?action=login
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400;
Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,1435557576,1435590542;
bdshare_firstime=1433775454650; wy_uid=-1; PHPSESSID=h8i10mi6rdc8l9coc708otq661;
Hm_lpvt_c12f88b5c1cd041a732dea597a5ec94c=1435590574
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdffdb54e022f8facd&captcha=BYUGHTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Server: yunjiasu-nginx
CF-RAY: 1fe28d0a63e91c3b-JXG
Content-Encoding: gzip

236
..........l.Ok.A....~...zZ....qS..ZH.P,i..ut......*.`....J....6...6.L...|.......c`!
9....<...I.I=M..W.....X}.`.Q...Bk.$B.t
.x.~..b.9.&.Iu.[.b .....1f.C.X,F...Er(.....X.....JF3,..n.JL7...I..zb...."..X..o.
3....~U._.0i...,.....U(.2\b(H/.US..L..ld...[...L.PA|...!...$jk.}E
.e....].WtC..JN.2..x    .Y.z........&....>....M..G.R....hs..... .D...T.X.J.i.
...Q....M..2.s..9.g...@A....\.H.....K...u..d...R...M.`..._..}o|8....
{...~...L..c......].O..*[.(2..D....@.    ..}gXq.=.....xk......D.w..~..
```

分组 22。3 客户端 分组，17 服务器 分组，5 turn(s). 点击选择。

整个对话（9615 bytes）

显示和保存数据为 ASCII

流 2

打开之后，就找到了我们想要的flag。