

Buuctf wireshark

原创

Dexret 于 2021-11-16 15:04:11 发布 157 收藏

分类专栏: [Buuctf Misc](#) 文章标签: [wireshark](#) [网络测试工具](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Dexret/article/details/121344314>

版权



[Buuctf Misc](#) 专栏收录该内容

47 篇文章 0 订阅

订阅专栏

下载该文件, 发现该文件为wireshark的数据包

通过wireshark打开该数据包

The screenshot shows the Wireshark interface with a list of captured packets. Packet 20 is selected, showing an HTTP POST request to /user.php?action=login. The packet details pane shows the raw data and decoded content, including a truncated cookie and a line-based text data field containing email and password information.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	115.231.236.116	192.168.1.102	TCP	http > 22429 [FIN, ACK] Seq=1 Ack=1 win=45 Len=0
2	0.000162	192.168.1.102	115.231.236.116	TCP	22429 > http [ACK] Seq=1 Ack=2 win=16558 Len=0
3	0.000424	192.168.1.102	115.231.236.116	TCP	22429 > http [FIN, ACK] Seq=1 Ack=2 win=16558 Len=0
4	0.006591	115.231.236.116	192.168.1.102	TCP	http > 22429 [ACK] Seq=2 Ack=2 win=45 Len=0
5	2.621551	192.168.1.102	115.239.211.92	TCP	22493 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
6	2.623880	192.168.1.102	202.101.172.47	DNS	Standard query A nsclick.baidu.com
7	2.628351	202.101.172.47	192.168.1.102	DNS	Standard query response CNAME static.n.shifen.com A 115.239.211.92
8	2.629393	115.239.211.92	192.168.1.102	TCP	http > 22493 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1440 WS=7 SACK_PERM=1
9	2.629463	192.168.1.102	115.239.211.92	TCP	22493 > http [ACK] Seq=1 Ack=1 win=66240 Len=0
10	2.629900	192.168.1.102	115.239.211.92	HTTP	OPTIONS /v.gif?pid=307&type=3075&l=47365&t=0&s=47365&v=605&f=12000&r=http%3A%2F%2Fwww.wooyun.org%2Findex.php&u=http%3A%2F%2Fwww.wooyun.org%2Findex.php&u=http%3A%2F%2Fwww.wooyun.org%2Findex.php&u=http%3A%2F%2Fwww.wooyun.org%2Findex.php
11	2.638601	115.239.211.92	192.168.1.102	TCP	http > 22493 [ACK] Seq=1 Ack=591 win=15872 Len=0
12	2.638713	115.239.211.92	192.168.1.102	HTTP	HTTP/1.1 200 OK
13	2.671867	192.168.1.102	115.231.236.116	TCP	22494 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=2 SACK_PERM=1
14	2.674622	192.168.1.102	202.101.172.47	DNS	Standard query A hm.baidu.com
15	2.677614	192.168.1.102	202.101.172.47	DNS	Standard query A bdfmg.share.baidu.com
16	2.679829	202.101.172.47	192.168.1.102	DNS	Standard query response CNAME static.n.shifen.com A 115.239.211.92
17	2.680273	202.101.172.47	192.168.1.102	DNS	Standard query response CNAME hm.e.shifen.com A 220.181.164.39
18	2.684517	115.231.236.116	192.168.1.102	TCP	http > 22494 [SYN, ACK] Seq=0 Ack=1 win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=10
19	2.684583	192.168.1.102	115.231.236.116	TCP	22494 > http [ACK] Seq=1 Ack=1 win=66240 Len=0
20	2.684925	192.168.1.102	115.231.236.116	HTTP	POST /user.php?action=login&do=login HTTP/1.1 (application/x-www-form-urlencoded)
21	2.696759	115.231.236.116	192.168.1.102	TCP	http > 22494 [ACK] Seq=1 Ack=810 win=31744 Len=0
22	2.739908	115.231.236.116	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
23	2.740198	115.231.236.116	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
24	2.740229	192.168.1.102	115.231.236.116	TCP	22494 > http [ACK] Seq=810 Ack=994 win=65244 Len=0
25	2.740345	115.231.236.116	192.168.1.102	TCP	[TCP segment of a reassembled PDU]
26	2.740374	115.231.236.116	192.168.1.102	HTTP	HTTP/1.1 200 OK (text/html)
27	2.740390	192.168.1.102	115.231.236.116	TCP	22494 > http [ACK] Seq=810 Ack=1550 win=66240 Len=0

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.8,en;q=0.7\r\n
Referer: http://www.wooyun.org/user.php?action=login\r\n
[truncated] cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,1435557576,1435590542; bdshare_firsttime=143377545
connection: keep-alive\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 65\r\n
[Content Length: 65]
\r\n
Line-based text data: application/x-www-form-urlencoded
email=flag&password=fffb7567a1d4f4abdfdb54e022f8facd&captcha=BYUG
```

通过题意可以得到, 我们需要找到管理员提交数据的post请求

Wireshark capture showing network traffic. The packet list pane highlights a POST request (No. 20) to `/user.php?action=login&do=login` with a content type of `application/x-www-form-urlencoded`. The packet details pane shows the request body:

```

Accept-Encoding: gzip, deflate\r\n
Referer: http://www.wooyun.org/user.php?action=login\r\n
[truncated] Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,143557576,1435590542; bdshare_firsttime=143377545
connection: keep-alive\r\n
content-type: application/x-www-form-urlencoded\r\n
content-length: 65\r\n
\r\n
Line-based text data: application/x-www-form-urlencoded
email=flag&password=ffb7567a1d4f4abdfdb54e022f8facd&captcha=BYUG
  
```

The packet bytes pane shows the raw data of the request body:

```

0310 4c 65 66 67 74 68 3a 20 36 35 0d 0a 0d 0a 65 66 Length: 65...len
0320 61 69 6c 3d 66 6c 61 67 26 70 61 73 73 77 6f 72 All flag & password
0330 64 3d 66 66 62 37 35 36 37 61 31 64 34 66 34 61 d=ffb7567a1d4f4a
0340 62 64 66 66 64 62 35 34 65 30 32 32 66 38 66 61 bdfdb54e022f8fa
0350 63 64 26 63 61 70 74 63 68 61 3d 42 59 55 47 cd&captcha=BYUG
  
```

找到该post请求后，在下面可以看到该请求的具体数据

找到Line-based text data并展开

Wireshark capture showing network traffic. The packet list pane highlights the same POST request (No. 20). The packet details pane shows the request body with the `Line-based text data` section expanded to reveal the flag:

```

Accept-Encoding: gzip, deflate\r\n
Referer: http://www.wooyun.org/user.php?action=login\r\n
[truncated] Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,143557576,1435590542; bdshare_firsttime=143377545
connection: keep-alive\r\n
content-type: application/x-www-form-urlencoded\r\n
content-length: 65\r\n
\r\n
Line-based text data: application/x-www-form-urlencoded
email=flag&password=ffb7567a1d4f4abdfdb54e022f8facd&captcha=BYUG
  
```

The packet bytes pane shows the raw data of the request body:

```

0310 4c 65 66 67 74 68 3a 20 36 35 0d 0a 0d 0a 65 66 Length: 65...len
0320 61 69 6c 3d 66 6c 61 67 26 70 61 73 73 77 6f 72 All flag & password
0330 64 3d 66 66 62 37 35 36 37 61 31 64 34 66 34 61 d=ffb7567a1d4f4a
0340 62 64 66 66 64 62 35 34 65 30 32 32 66 38 66 61 bdfdb54e022f8fa
0350 63 64 26 63 61 70 74 63 68 61 3d 42 59 55 47 cd&captcha=BYUG
  
```

得到该题flag:

flag{ffb7567a1d4f4abdfdb54e022f8facd}