




BUUCTF: wireshark

原创

末初  于 2020-09-09 09:49:50 发布  2767  收藏 2

分类专栏: [CTF_MISC_Writeup](#)

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/mochu7777777/article/details/108480193>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges#wireshark>

Challenge 1806 Solves ×

wireshark

1

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) 注意: 得到的 flag 请包上 flag{} 提交

 7fc3e8a0-69...

Flag

<https://blog.csdn.net/mochu7777777>

根据提示直接过滤出POST包

```
http.request.method==POST
```

Wireshark interface showing a network capture. The top pane displays a list of packets:

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 (application/x-www-form-urlencoded)
73	*REF*	192.168.1.102	202.101.172.47	DNS	75	Standard query 0x0274 A img.t.sinajs.cn

The bottom pane shows the details of the selected HTTP POST packet:

- [Response in frame: 26]
- [Next request in frame: 48]
- File Data: 65 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - > Form item: "email" = "flag"
 - > Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd"
 - > Form item: "captcha" = "BYUG"

The packet bytes pane shows the raw data:

```

02f0 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 /x-www-f orm-urle
0300 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e 74 2d ncoded.. Content-
0310 4c 65 6e 67 74 68 3a 20 36 35 0d 0a 0d 0a 65 6d Length: 65...em
0320 61 69 6c 3d 66 6c 61 67 26 70 61 73 73 77 6f 72 ail=flag &passwor
0330 64 3d 66 66 62 37 35 36 37 61 31 64 34 66 34 61 d=ffb756 7a1d4f4a
0340 62 64 66 66 64 62 35 34 65 30 32 32 66 38 66 61 bdfdb54 e022f8fa
0350 63 64 26 63 61 70 74 63 68 61 3d 42 59 55 47 cd&captc ha=BYUG
  
```

Text item (text), 42 bytes

Packets: 356 · Displayed: 2 / (0.6%)

flag{ffb7567a1d4f4abdfdb54e022f8facd}



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)