

BUUCTF之wireshark

原创

金鼎 于 2022-04-15 22:12:44 发布 174 收藏

分类专栏: [BUUCTF之Misc](#) 文章标签: [CTF](#)

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/I2872253606/article/details/124205163>

版权



[BUUCTF之Misc 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

下载解压文件, 用wireshark打开, 然后Ctrl+F, 搜索password

The screenshot shows the Wireshark interface with a search filter set to 'password'. The packet list pane shows a POST request to 'http://www.wooyun.org/user.php?action=login&do=login'. The packet details pane shows the 'Form Data' section with the following items:

- Form item: "email" = "flag"
- Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd"
- Form item: "captcha" = "BYUG"

The packet bytes pane shows the raw data of the request, with the password field highlighted in blue:

```
02d0 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 alive: Content-T
02e0 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e e: application
02f0 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 /x-www-form-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 &password
0330 64 3d 66 66 62 37 35 36 67 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
```

password那串字符就是flag, 裹上flag的格式就好了

```
flag{ffb7567a1d4f4abdfdb54e022f8facd}
```