

攻防世界之wireshark-1

原创

金帛 于 2022-03-03 22:55:39 发布 38 收藏

分类专栏: [攻防世界Misc](#) 文章标签: [wireshark](#)

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/l2872253606/article/details/123266084>

版权



[攻防世界Misc](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

解压文件, 是个流量包, 用wireshark打开

根据提示

The screenshot shows a challenge page with the following details:

- Title: wireshark-1
- Best Writeup by: 系统战队 • admin (23 likes)
- Difficulty: 1.0 (1 star)
- Source: 广西首届网络安全选拔赛
- Description: 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}
- Scenario: 暂无
- Attachments: 附件1

At the bottom, there is a text input field containing the text "flag..".

答案就是管理员的密码, 在最上栏搜索一下protocol为http的包,

然后再搜索`http.request.method=="POST"`, 找出是以POST为请求的流量包

发现只有一个符合条件, 接着看一下包的内容

The image shows a Wireshark capture of an HTTP POST request. The packet list pane shows a POST request to `/user.php?action=login&do=login` with a length of 863 bytes. The packet details pane shows the request body is HTML Form URL Encoded with the following data:

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

The packet bytes pane shows the raw data of the request body, with the flag value highlighted in blue: `4c-14355-90574`.

滑下即可发现flag，最终转化一下得到

flag{ffb7567a1d4f4abdfdb54e022f8facd}