

# XCTF-wireshark-1

原创

米兔的猴子 于 2021-12-22 15:54:19 发布 28 收藏

文章标签: [wireshark](#) [测试工具](#) [网络](#)

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/one\\_redhant/article/details/122087660](https://blog.csdn.net/one_redhant/article/details/122087660)

版权

The image shows a CSDN article preview for 'wireshark-1'. It features a dark blue background with white and yellow text. The title 'wireshark-1' is at the top left. To its right is a badge indicating '22' likes and '最佳Writeup由系统战队·admin提供'. Below the title, the '难度系数' (Difficulty Coefficient) is shown as '1.0' with a star icon. The '题目来源' (Source) is '广西首届网络安全选拔赛'. The '题目描述' (Description) states: '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}' (A hacker captured a network traffic packet of an administrator logging into a website using Wireshark (the administrator's password is the answer). The flag submission format is flag{XXXX}). The '题目场景' (Scenario) is '暂无' (None). The '题目附件' (Attachments) section has a '附件1' (Attachment 1) button. The CSDN logo and the author's name 'CSDN @米兔的猴子' are at the bottom right.

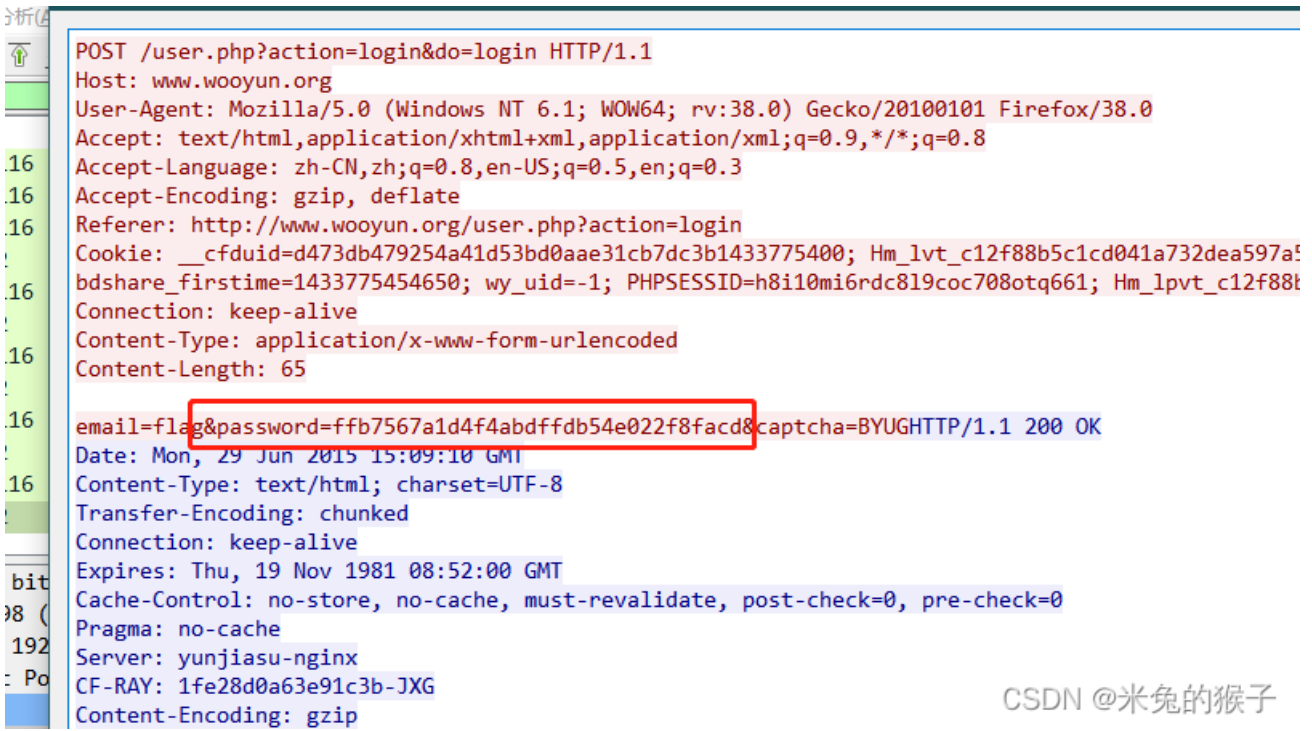
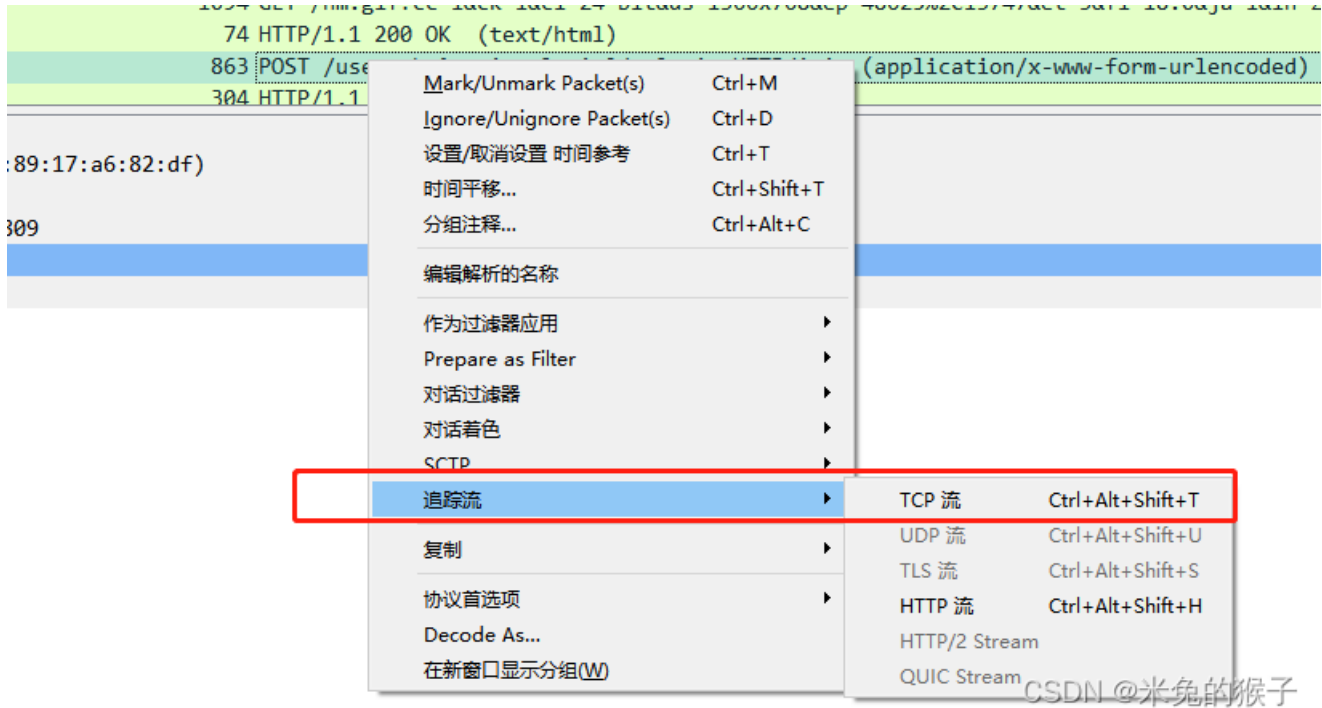
把附件下载之后, .pcap包使用wireshark 打开, 题目中的意思是管理员的密码就是答案。

既然是找密码, 那么应该是post方式上传的密码。

在下图中的协议栏中查找http协议, 里面就直接能看到post数据包了。

The image is a screenshot of the Wireshark network traffic analysis tool. The main pane shows a list of captured packets. The selected packet is number 863, which is an HTTP POST request. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. Under the Hypertext Transfer Protocol section, the 'HTML Form URL Encoded' data is shown as 'application/x-www-form-urlencoded', and the 'Form item: "email" = "flag"' is visible. The packet bytes pane at the bottom shows the raw data of the packet. The CSDN logo and the author's name 'CSDN @米兔的猴子' are at the bottom right.

我们进行TCP流跟踪，就是可以看到post请求的内容了



很容易就找到了flag{ffb7567a1d4f4abdffdb54e022f8facd}

CSDN @米兔的猴子

CSDN @米兔的猴子