2021年中国工业互联网安全大赛核能行业赛道writeup之数据库登录

原创

苦行僧(csdn) 于 2021-10-22 07:00:00 发布 44 收藏
分类专栏： 信息安全 文章标签： CTF misc 流量分析 mysql

本文链接：https://blog.csdn.net/qpeity/article/details/120895299

附件题：数据库登录（一道MISC、流量分析类型题目）

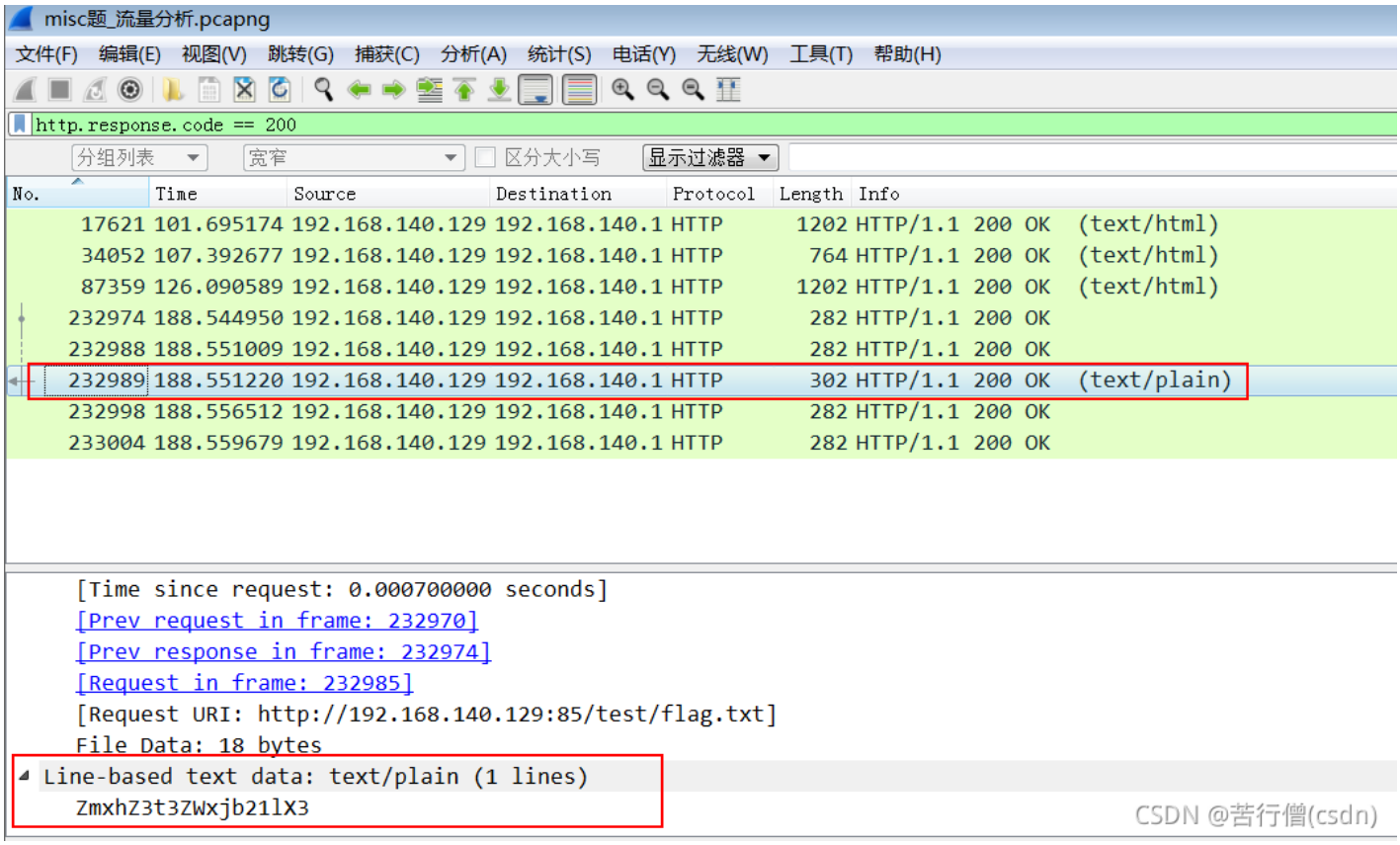
题目描述：

> 具体描述已经忘记o(╯□╰)o
>
> 大概意思就是分析附件里的.pcapng包，找到flag。流量涉及到 MySQL 数据库了。

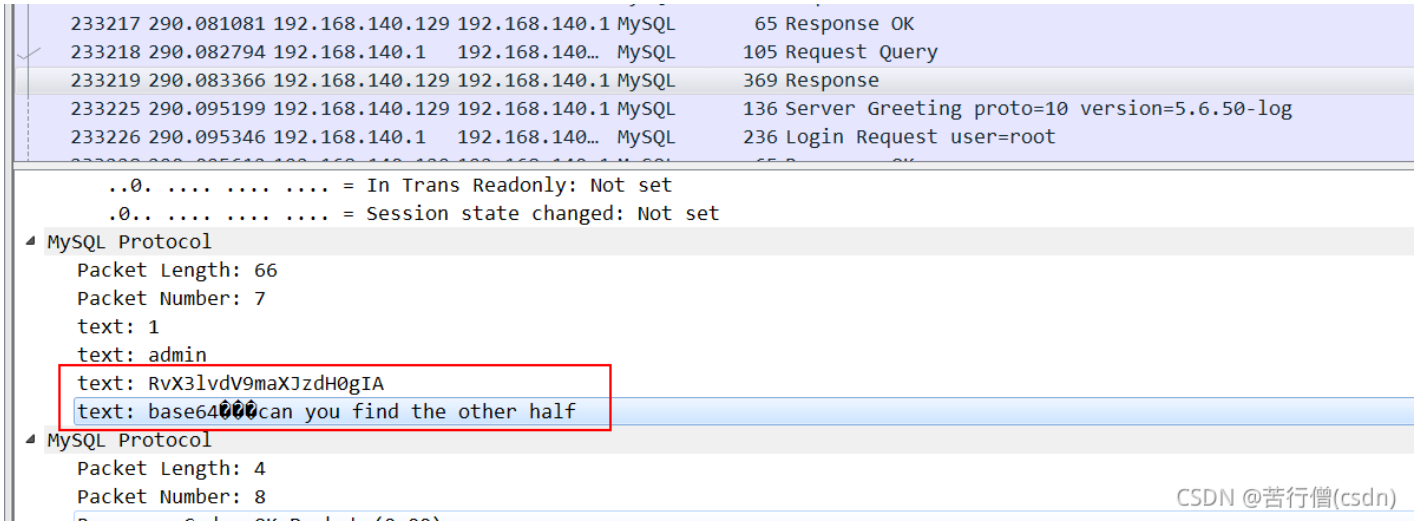
附件下载：

https://download.csdn.net/download/qpeity/33670422
https://download.csdn.net/download/qpeity/33670422用wireshark打开这个包，全局搜索一下flag，没有发现有用信息。

猜想一般黑客得手是在http访问成功的时候，所以先筛选 http.response.code == 200，发现 No.232985 包 request 请求 GET /test/flag.txt，No.232989 包 response 返回 flag.txt，里面的内容 —— ZmxhZ3t3ZWxjb21lX3



根据提示数据库登录，猜想后半段在数据库的协议中，并且流量中有MySQL协议，而且有很明显的root登录成功和select查询。筛选mysql协议，内容为Response，逐个查看MySQL Protocol的内容，发现No.233219包里面有信息，是base64编码，而且是另外半部分—— RvX3lvdV9maXJzdH0gIA



合并到一起 ZmxhZ3t3ZWxjb21lX3RvX3lvdV9maXJzdH0gIA，再base64转码得到flag —— flag{welcome_to_you_first}