BuuCTF 数据包中的线索

原创

Kevin_xiao~ 于 2021-08-06 19:12:02 发布 172 收藏
分类专栏： CTF题目(misc) 文章标签： 密码学 misc
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/qq_52907838/article/details/119461856
版权

CTF题目(misc) 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

下载附件，得到一个pcappng的文件：

看到这个后缀加上题目中有流量，就想到用wireshark打开，如果还不知道wireshark如何安装和使用可以看一下这篇文章：wireshark抓包新手使用教程 - 锅边糊 - 博客园 (cnblogs.com)

打开后看到TCP的包，直接过滤http的包，查看HTTP包，看到第二个HTTP包中有类似于base64加密的东西：

```
    File Data: 86332 bytes
- Line-based text data: text/html (1107 lines)
    /9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAIBAQIBAQICAgICAgICAwUDAwMDAwYEBAMFBwYHBwcG\r\n
    BwcICQsJCAgKCAcHCg0KCgsMDAwMBwkODw0MDgsMDAz/2wBDAQICAgMDAwYDAwYMCAcIDAwMDAwM\r\n
    DAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAz/wAARCAHgAkQDASIA\r\n
    AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA\r\n
    AAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3\r\n
    ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5ZmqKjpKWm\r\n
    p6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA\r\n
    AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSEx\r\n
    BhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElK\r\n
    U1RVV1dYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3\r\n
    uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD9/KKK\r\n
    KACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo\r\n
    AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigA\r\n
    oooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACi\r\n
    iigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKK\r\n
    KACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo\r\n
    AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigAoooo AKKKKACiiigA\r\n
```

https://blog.csdn.net/qq_52907838

拿去解密：https://the-x.cn/base64

发现是图片，另存为图片：

flag{209acebf6324a09671abc31c869de72c}

得到答案。