wireshark-1的writeup

原创

MarcusRYZ 于 2020-02-12 17:29:48 发布 726 收藏 1

分类专栏： 攻防世界MISC高手进阶区 文章标签： 安全

本文链接：https://blog.csdn.net/MarcusRYZ/article/details/104281791

攻防世界MISC高手进阶区 专栏收录该内容

13 篇文章 1 订阅

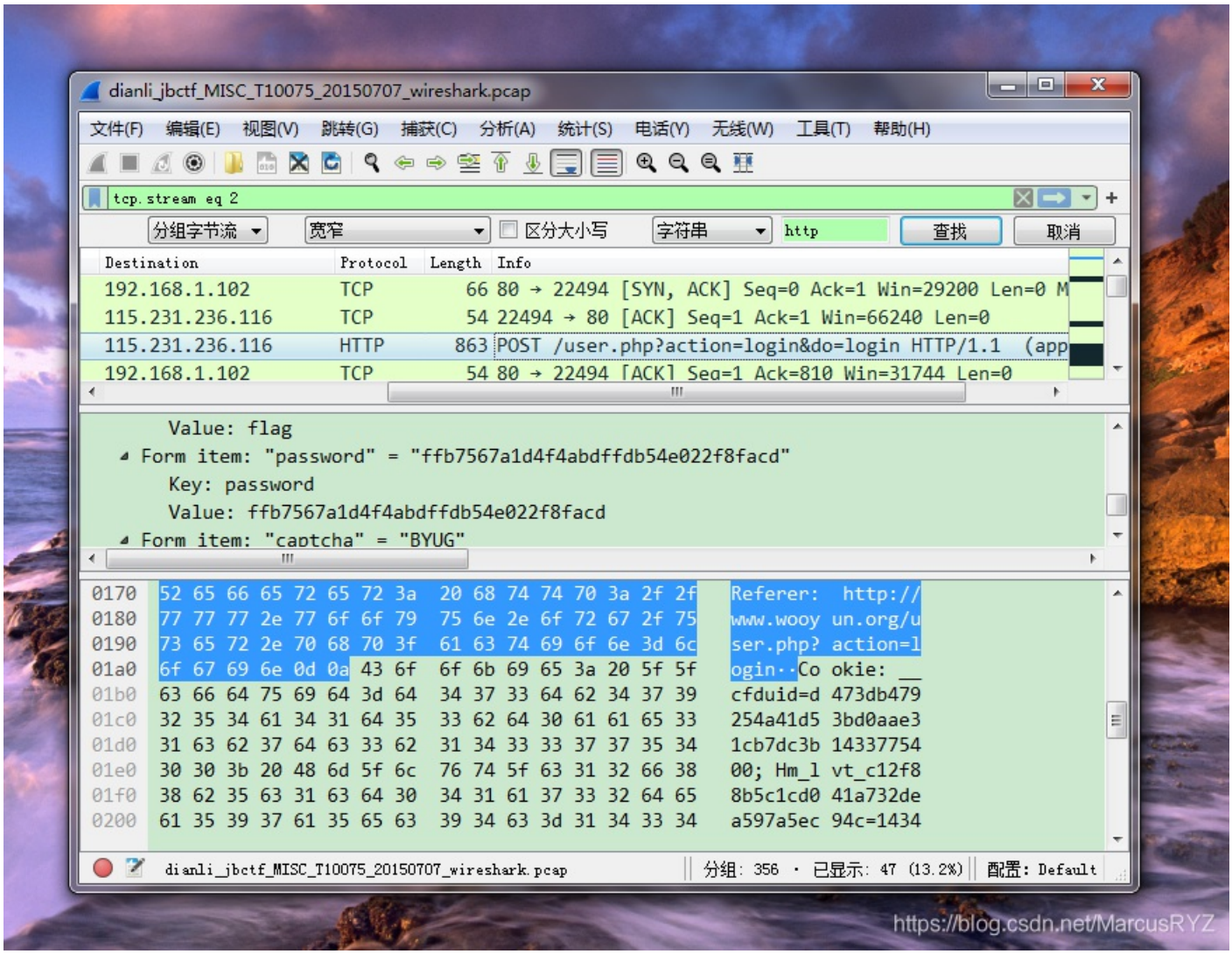
订阅专栏

大家好，我们在攻防世界misc部分新手练习区的训练已经告一段落了，相信大家在新手区的12道基础题的锤炼下，脑洞和水准已经得到了大幅提升。如果没有这种感觉，希望大家先不要着急入主高手区，可以再回顾一下做过的题目，查漏补缺。接下来，我就为大家带来攻防世界高手进阶区的writeup。

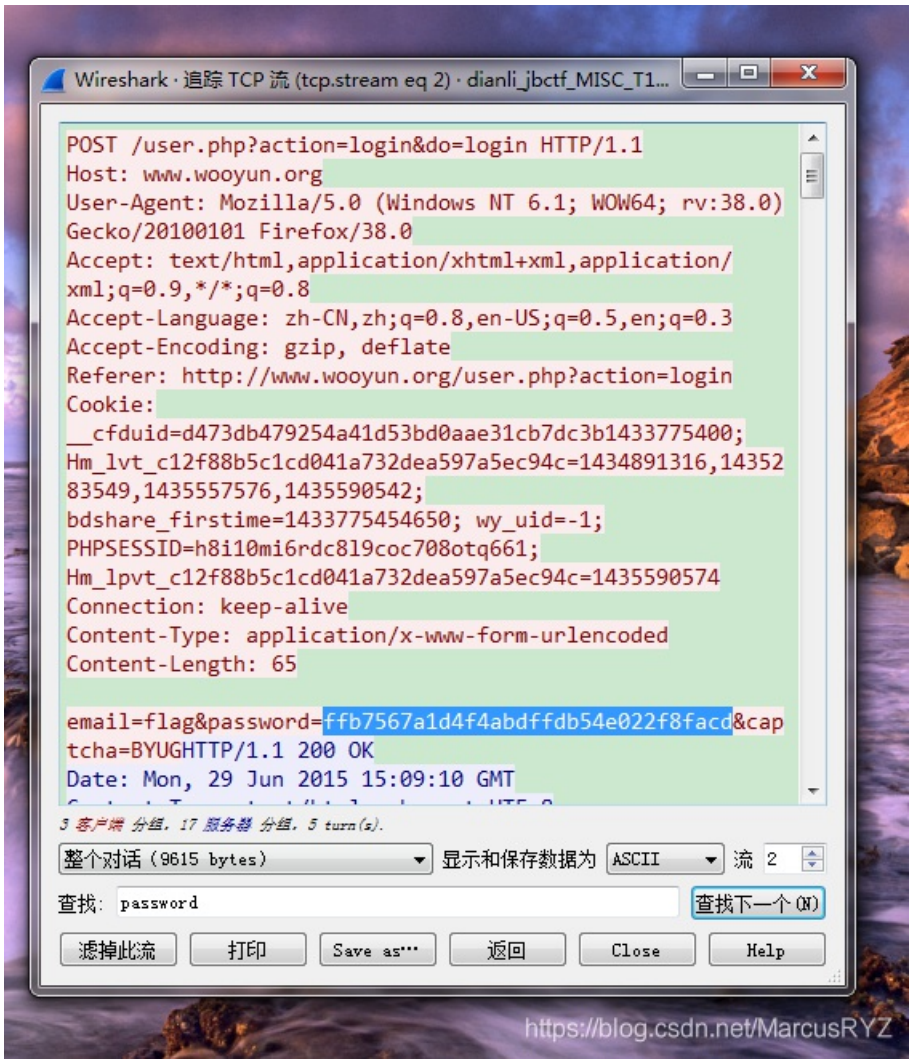
好，我们进入正题，这次我为大家带来的是攻防世界misc部分wireshark-1的writeup。

先下载附件，是一个压缩包。二话不说，立即解压。发现解压出一个流量包，于是用wireshark打开。这时我们需要关注一下题目描述：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)。其实这描述已经说得很清楚了，我们只需在这个流量包中找到登录网站的密码即可。

由于登录网站需要用到HTTP协议，且会有post、login等关键信息。故我们在wireshark的搜素框中输入HTTP并搜索，一直点查找，直到info中出现post和login。



我们追踪该项的TCP流，在查找框中输入password进行查找。就得到了flag。



flag：ffb7567a1d4f4abdffdb54e022f8facd。