BUUCTF Misc wireshark 1

原创

m0_55842055 于 2021-10-13 22:41:09 发布 51 收藏
文章标签： wireshark

本文链接：https://blog.csdn.net/m0_55842055/article/details/120753777

题目很明显的提示就是用分析wireshark网络流量包的阅读

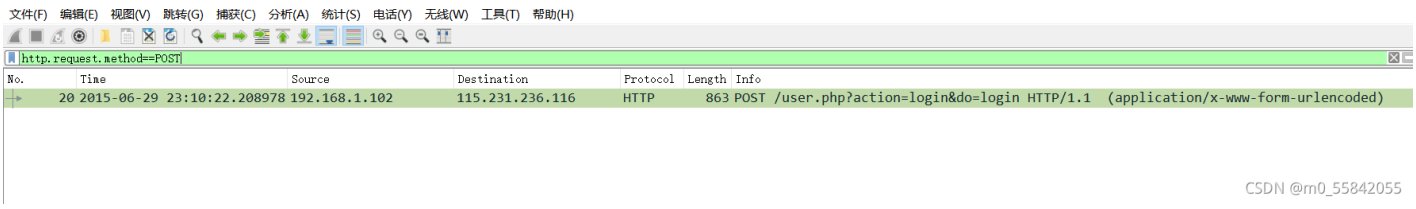
打开流量包，

第一个想法就是，浏览一下从大部分中找小部分，发现http比较特殊。

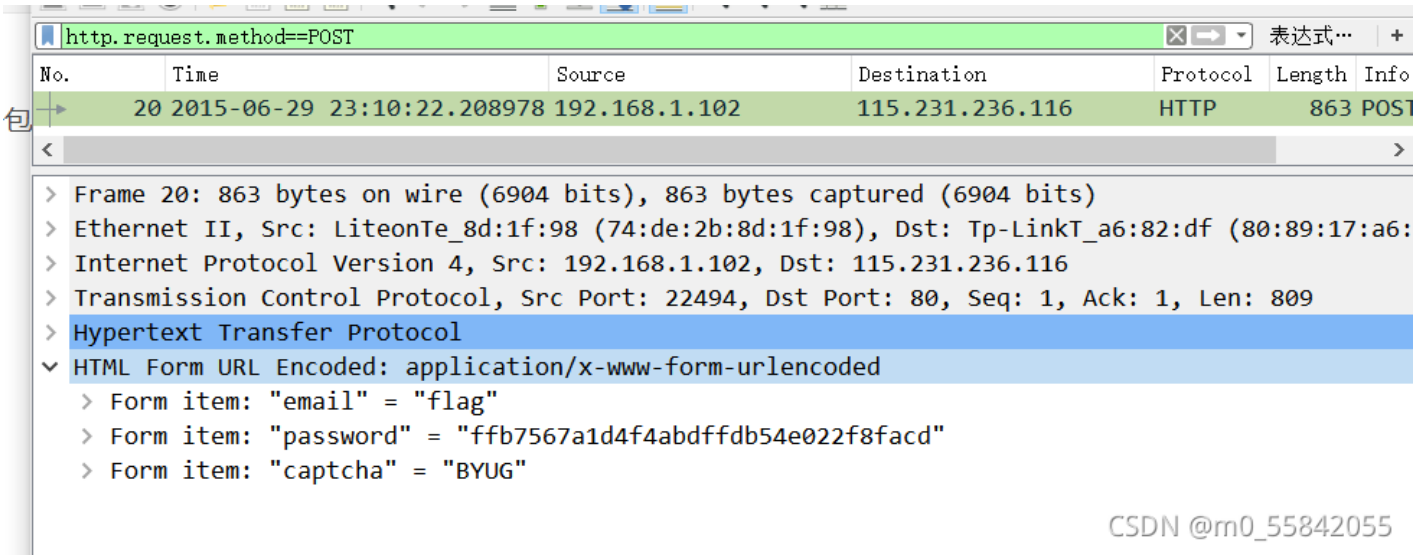
4	2015-06-29 23:10:19.530644	115.231.236.116	192.168.1.102	TCP	54	80 → 22429 [ACK]
5	2015-06-29 23:10:22.145604	192.168.1.102	115.239.211.92	TCP	66	22493 → 80 [SYN]
6	2015-06-29 23:10:22.147933	192.168.1.102	202.101.172.47	DNS	77	Standard query 0
7	2015-06-29 23:10:22.152404	202.101.172.47	192.168.1.102	DNS	293	Standard query r
8	2015-06-29 23:10:22.153446	115.239.211.92	192.168.1.102	TCP	66	80 → 22493 [SYN,
9	2015-06-29 23:10:22.153516	192.168.1.102	115.239.211.92	TCP	54	22493 → 80 [ACK]
10	2015-06-29 23:10:22.153953	192.168.1.102	115.239.211.92	HTTP	644	OPTIONS /v.gif?p
11	2015-06-29 23:10:22.162654	115.239.211.92	192.168.1.102	TCP	54	80 → 22493 [ACK]
12	2015-06-29 23:10:22.162766	115.239.211.92	192.168.1.102	HTTP	304	HTTP/1.1 200 OK
13	2015-06-29 23:10:22.195920	192.168.1.102	115.231.236.116	TCP	66	22494 → 80 [SYN]
14	2015-06-29 23:10:22.198675	192.168.1.102	202.101.172.47	DNS	72	Standard query 0
15	2015-06-29 23:10:22.201667	192.168.1.102	202.101.172.47	DNS	81	Standard query 0
16	2015-06-29 23:10:22.203882	202.101.172.47	192.168.1.102	DNS	297	Standard query r
17	2015-06-29 23:10:22.204326	202.101.172.47	192.168.1.102	DNS	284	Standard query r

第二个想法是：从题目出发，既然是上传登录信息，就直接搜索 http.request.method==post

因为上传用户登录信息使用的一定是http里的post方法。



找到这个上传数据包后就可以在其中找登录的密码信息。



在HTML FROM URL RNCODED 中可以找到管理员用post上传的password