buuctf—wireshark 1

原创

小常吃不下了 于 2021-10-17 13:02:00 发布 67 收藏

分类专栏： CTF BUUCTF 文章标签： wireshark html python

本文链接：https://blog.csdn.net/weixin_52620919/article/details/120809791


CTF 同时被 2 个专栏收录

32 篇文章 1 订阅

订阅专栏


BUUCTF

37 篇文章 0 订阅

订阅专栏

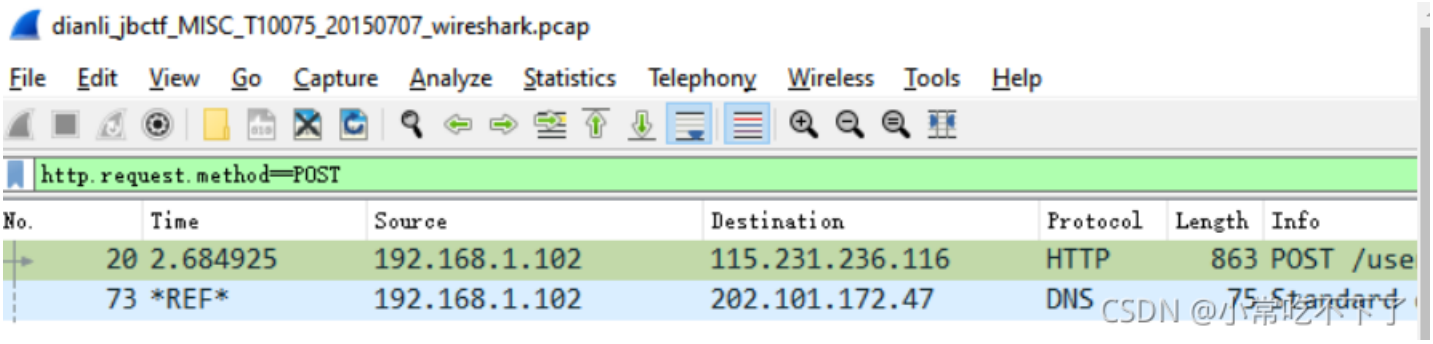
题目　解题快手榜

wireshark

1

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) 注意：得到的 flag 请包上 flag{} 提交

用wireshak进行post过滤



追踪流

Wireshark · 追踪 HTTP 流 (tcp.stream eq 2) · dianli_jbctf_MISC_T10075_20150707_wireshark.pcap

```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.wooyun.org/user.php?action=login
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400;
Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,1435283549,1435557576,1435590542; bdshare_firs
wy_uid=-1; PHPSESSID=h8i10mi6rdc8l9coc708otq661; Hm_lpvt_c12f88b5c1cd041a732dea597a5ec94c=1435590
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdffdb54e022f8facd&captcha=BYUGHTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:10 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```


得到答案

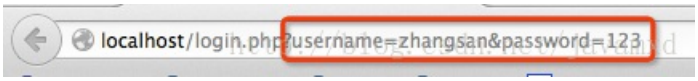
补充知识：

利用POST进行用户登录的安全问题剖析

应用实例：登录

用户登录操作常用的有两种方式，GET和POST

GET登录后，我们会在url地址栏中看到登录的用户名和密码，如此一来便毫无安全可言



使用GET方法所有参数都包含在URL中，所有访问网站的URL都会记录在服务器的访问日志中
相比于GET而言，POST就安全得多。

POST是通过携带数据体传递用户登录信息，登录的数据并不会出现在URL和服务器访问日志中。

但这也并不十分安全，只要拦截到了传递的数据体，用户名和密码就能轻松获取。