

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](#)

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/qpeity/article/details/120895299>

版权



[信息安全 专栏收录该内容](#)

12 篇文章 0 订阅

订阅专栏

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`

misc题_流量分析.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http.response.code == 200

No.	Time	Source	Destination	Protocol	Length	Info
17621	101.695174	192.168.140.129	192.168.140.1	HTTP	1202	HTTP/1.1 200 OK (text/html)
34052	107.392677	192.168.140.129	192.168.140.1	HTTP	764	HTTP/1.1 200 OK (text/html)
87359	126.090589	192.168.140.129	192.168.140.1	HTTP	1202	HTTP/1.1 200 OK (text/html)
232974	188.544950	192.168.140.129	192.168.140.1	HTTP	282	HTTP/1.1 200 OK
232988	188.551009	192.168.140.129	192.168.140.1	HTTP	282	HTTP/1.1 200 OK
232989	188.551220	192.168.140.129	192.168.140.1	HTTP	302	HTTP/1.1 200 OK (text/plain)
232998	188.556512	192.168.140.129	192.168.140.1	HTTP	282	HTTP/1.1 200 OK
233004	188.559679	192.168.140.129	192.168.140.1	HTTP	282	HTTP/1.1 200 OK

[Time since request: 0.000700000 seconds]
 [Prev request in frame: 232970]
 [Prev response in frame: 232974]
 [Request in frame: 232985]
 [Request URI: http://192.168.140.129:85/test/flag.txt]
 File Data: 18 bytes

Line-based text data: text/plain (1 lines)
 ZmxhZ3t3ZWxjb21lX3

CSDN @苦行僧(csdn)

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

233217	290.081081	192.168.140.129	192.168.140.1	MySQL	65	Response OK
233218	290.082794	192.168.140.1	192.168.140...	MySQL	105	Request Query
233219	290.083366	192.168.140.129	192.168.140.1	MySQL	369	Response
233225	290.095199	192.168.140.129	192.168.140.1	MySQL	136	Server Greeting proto=10 version=5.6.50-log
233226	290.095346	192.168.140.1	192.168.140...	MySQL	236	Login Request user=root

..0. = In Trans Readonly: Not set
 .0.. = Session state changed: Not set

MySQL Protocol
 Packet Length: 66
 Packet Number: 7
 text: 1
 text: admin
 text: RvX3lvdV9maXJzdH0gIA
 text: base64000can you find the other half

MySQL Protocol
 Packet Length: 4
 Packet Number: 8

CSDN @苦行僧(csdn)

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