MMS协议分析

发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge ， 2020 ， 工业信息安全技能大赛 ， 湖州站
Challenge | 2020 | 工业信息安全技能大赛 | 湖州站 | MMS协议分析

点击此处获得更好的阅读体验

WriteUp来源

转自https://www.hyluz.cn/?id=98

题目描述

> *某地市自动化网络安全专工对某变电站进行渗透测试，截获通信数据包，发现该场站某主机通过MMS协议进行数据通信。请尝试对截获数据包解析并找出隐藏flag信息，其中flag提交格式为:flag{}。Hint：请先进行凯撒再Hex解密。*

题目考点

- *MMS协议*

解题思路

打开流量发现MMS协议

不懂协议，也看不懂它在做什么，过滤mms流量粗略地看一看有类似flag的东西

解密完发现部分有意义，最后把所有字母的ascii值-3即可

```
import string

flag_enc = "666f61677e494353667h756h7d646173617g"
flag_dec = ""
for c in flag_enc:
    if c in string.digits:
        flag_dec += c
    else:
        flag_dec += chr(ord(c)-3)
# 666c61677b494353667e756e7a646173617d
```

之后转ascii即可

Flag

```
flag{ICSf~unzdasa}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/工业信息安全技能大赛/湖州站/iCMxuomrXK8oEjun8SxScj.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # 工业信息安全技能大赛 # 湖州站
S7comm
隐藏的木马文件