**数据包取证总结**

1. 先观察题目，如果题目有明确指示某端口，或某协议。然后根据提示的端口和协议构造过滤表达式，否则话一般都是考http协议的那种 （wireshark打开数据包后，使用了过滤表达式后先搜索一下关键字flag，如果简单的题话会有flag）

题目：BUUCTF-Misc-sqltestfl

1. 如果题目有类似于BUUCTF-Misc-sqltest这种类型的，二话不说wireshark打开数据包后，直接导出全部为html，根据题目来获取flag

参考文档：第一届HappyCTF大赛WriteUp.pdf

