sqlmap yibasuo

这道题是一道关于sqlmap注入的流量分析的问题，类似的题目可以在网上找到。大致的原理是通过分析流量包的数据，得到sqlmap的尝试内容，由此得到flag文件的内容。

我们使用Wireshark打开这个流量包，并且筛选其中的http流。通过一番尝试，我们发现在流量包的最后部分出现了一些奇怪的内容：

```
hhh'||(SELECT 'FGtK' FROM DUAL WHERE 7118=7118 AND 9632=IF((ORD(MID((SELECT
IFNULL(CAST(flag AS CHAR),0x20) FROM test.flag ORDER BY flag LIMIT
0,1),8,1))>48),SLEEP(1),9632))||'
```

类似的内容还有很多，但是可以发现文本中'>'后面的的值在变化，直到某个值为止。可以推断，最后的那个值便是正确的该位的ASCII码值。而经过多次观察，看到如上代码中的,8,1)中的8表示的正是flag的第8位(1-base)。

所以，思路就很清晰了——通过寻找每一位最后一个出现的ASCII码值，判断出该位对应的字符。经过漫长的手动分析，最终得到正确的flag。