日志分析三-SQLMAP 注入

http://www.ctf8.com/index/containers/ContainerOtherCtfDetail/57

打开日志发现大量注入流量，攻击者是通过 SQLMAP 进行注入的，全文 url 解码进行分析

找到关键注入语句：
IF%28%28ORD%28MID%28%28SELECT%20IFNULL%28CAST%28KeyIsMe%20AS%20CHAR%29%2C0x20%29%20FROM%20example.__key__%20ORDER%20BY%20ID%20LIMIT%200%2C

写脚本：

```
keystr=r'IF%28%28ORD%28MID%28%28SELECT%20IFNULL%28CAST%28KeyIsMe%20AS%20CHAR%29%2C0x20%29%20FROM%20example.__key__%20ORDER%20BY%20ID%20LIMIT%200%2C1%29%2C{0}'
l=[None]*40
try:
 with open(r'1.log','r',encoding='ISO-8859-1') as f:
     for i in f.readlines():
         for j in range(1,40,1):
             if keystr.format(j)+'%2C1%29%29%21%3D' in i:
                 tmp=i
                 l[j-1]=tmp.split("%2C1%29%29%21%3D")[-1]
 for i in l:
     tmp=i.split(r'%29%2CBENCHMARK%28')[0]
     print (chr(int(tmp)),end='')
except:
     pass
```

运行得：Key:0e1d92fbb383e1e7

写成 flag 形式：flag{0e1d92fbb383e1e7}