流量分析五，SQL 注入

http://www.ctf8.com/index/containers/ContainerOtherCtfDetail/56

步骤一：提取关键字

文件 → 导出对象 → HTTP 导出 http 对象

```
27197 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=106%23
27211 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=107%23
27225 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=108%23
27239 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=109%23
27253 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=110%23
27267 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=111%23
27281 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=112%23
27295 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=113%23
27309 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=114%23
27323 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=115%23
27337 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=116%23
27351 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=117%23
27365 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=118%23
27379 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=119%23
27393 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=120%23
27407 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=121%23
27421 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=122%23
27435 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=123%23
27449 localhost:81 text/html 492 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=124%23
27463 localhost:81 text/html 518 bytes ?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),38,1))=125%23
```

找到注入关键字：

“%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),”

步骤二：写脚本 python3

```
# 构造一个包含 `keyid` 查询部分的模板字符串，`{0}` 是一个占位符，会在后续根据 `j` 进行替换
keystr = r'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),{0}'

# 创建一个长度为 40 的列表，用于存储匹配到的结果
l = [None] * 40

try:
    # 以 ISO-8859-1 编码打开 pcap 文件进行读取
    with open(r'F:\docker\ctf8\数据分析\enclosure\注入二\sql.pcap', 'r', encoding='ISO-8859-1') as f:
        # 按行读取文件内容
        for i in f.readlines():
            # 遍历从 1 到 39 的数字
            for j in range(1, 40, 1):
                # 判断当前行是否包含替换过的 `keystr` 模板字符串
                if keystr.format(j) + ',' in i:
                    tmp = i  # 获取当前匹配的行
                    # 提取该行 `=` 后面的部分，并保存到列表 `l` 中（保存的是可能的数字数据）
                    l[j - 1] = tmp.split("=")[-1]
```

```
    # 遍历列表 `l` 中的每一项
    for i in l:
        # 去除 `%23`（URL 编码中的 `#`），以确保只获取数字部分
        tmp = i.split(r'%23')[0]
        # 将数字字符串转换为整数，然后用 `chr` 函数转换为对应的字符
        print(chr(int(tmp)), end='')

except:
    # 如果文件操作或转换过程中出现异常，忽略错误
    pass
```

```python
# 构造一个包含 `keyid` 查询部分的模板字符串，`{0}` 是一个占位符，会在后续根据 `j` 进行替换
keystr = r'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),{0}'

# 创建一个长度为 40 的列表，用于存储匹配到的结果
l = [None] * 40

try:
    # 以 ISO-8859-1 编码打开 pcap 文件进行读取
    with open(r'F:\docker\ctf8\数据分析\enclosure\注入二\sql.pcap', 'r', encoding='ISO-8859-1') as f:
        # 按行读取文件内容
        for i in f.readlines():
            # 遍历从 1 到 39 的数字
            for j in range(1, 40, 1):
                # 判断当前行是否包含替换过的 `keystr` 模板字符串
                if keystr.format(j) + ',' in i:
                    tmp = i  # 获取当前匹配的行
                    # 提取该行 `=` 后面的部分，并保存到列表 `l` 中（保存的是可能的数字数据）
                    l[j - 1] = tmp.split("=")[-1]

    # 遍历列表 `l` 中的每一项
    for i in l:
        # 去除 `%23`（URL 编码中的 `#`），以确保只获取数字部分
        tmp = i.split(r'%23')[0]
        # 将数字字符串转换为整数，然后用 `chr` 函数转换为对应的字符
        print(chr(int(tmp)), end='')

except:
    # 如果文件操作或转换过程中出现异常，忽略错误
    pass
```

```
Run:  注入二
C:\Users\Administrator\PycharmProjects\pythonProject1\venv\Scripts\python.exe F:/docker/ctf8/数据分析/report/注入二.py
flag{c2bbf9cecdaf656cf524d014c5bf046c}
Process finished with exit code 0
```

```python
keystr=r'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),{0}'
l=[None]*40
try:
 with open(r'F:\启明星辰内部绝密资源\2023年标准化版\竞赛课程\0-CTF-Forensics\上课专用素材\附件型赛题整理
    for i in f.readlines():
        for j in range(1,40,1):
            if keystr.format(j)+',' in i:
                tmp=i
                l[j-1]=tmp.split("=")[-1]
for i in l:
    tmp=i.split(r'%23')[0]
    print (chr(int(tmp)),end='')
except:
    pass
```

Run: 注入二

```
D:\PathTools\Python37\python.exe F:/docker/ctf8/上课提交/report/注入二.py
flag{c2bbf9cecdaf656cf524d014c5bf046c}
Process finished with exit code 0
```