

ctf实验吧writeup

原创

tt阿信 于 2017-08-06 15:59:49 发布 9071 收藏 1

分类专栏: [Web安全](#) 文章标签: [ctfsql注入](#) [西普实验吧](#)

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/he_and/article/details/76775445

版权



[Web安全](#) 专栏收录该内容

74 篇文章 14 订阅

订阅专栏

1.登陆一下好嘛?

不要怀疑,我已经过滤了一切,还再逼你注入,哈哈哈哈哈!

flag格式: ctf{xxxx}



根据题设,可以判断出这是一道有关sql注入的题目,拿到题的第一反应我先尝试了在url中动手脚,但是点击登录以后URL看不出有可以注入的地方,于是只好老老实实对表单动手,先用单引号试水,结果如下:

对不起,没有此用户!!

hint:

username:mask'

password:mask'

username

password

http://blog.csdn.net/he_and

额,本以为会报错的,但是貌似被处理了,但是从结果可以看到单引号没有被处理,意思是这儿可以注入。

也推测粗这里的sql语句类似是: `select ...fromwhere username = ' ' and password = ' '`;

想办法绕过: 输入 `username :mask='0` `password :mask='0`

sql语句变为: `select ...from ... where (username ='mask')='0' and (password ='mask') = '0';`

可见这是一个永真的语句, 成功绕过