




writeup-web

原创

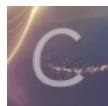
[charlie_heng](#)  于 2016-12-06 08:24:19 发布  204  收藏

分类专栏: [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/charlie_heng/article/details/53482292

版权



[web安全](#) 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

首先在地址后面加了?id=1, 但是并没有什么东西出来, 看了下源码, 要输入111

才能拿到flag, 但是要绕过他的过滤, 然后查了下intval这个函数, 发现只是转换成整数, 于是就弄了111.11来绕过, 成功拿到flag。

把过滤一注释掉, 看了下过滤二, 很明显就是sql注入, 构造语句为id=flag from ctf-就可以拿到flag了



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)