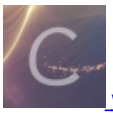
writeup-web

原创

charlie_heng 于 2016-12-06 08:24:19 发布 204 收藏

分类专栏： web安全

本文链接：https://blog.csdn.net/charlie_heng/article/details/53482292



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