实验吧web之简单的sql注入1

原创

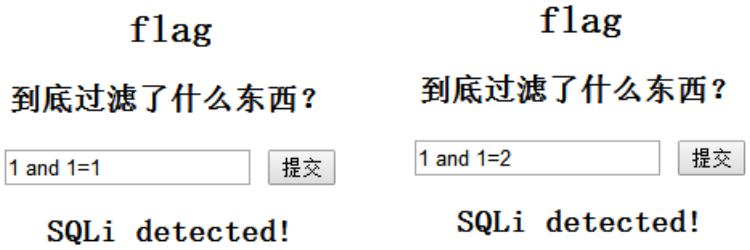
Flemington、 于 2017-05-06 19:56:24 发布 8236 收藏 1

本文链接：https://blog.csdn.net/Everywhere_wwx/article/details/71289107

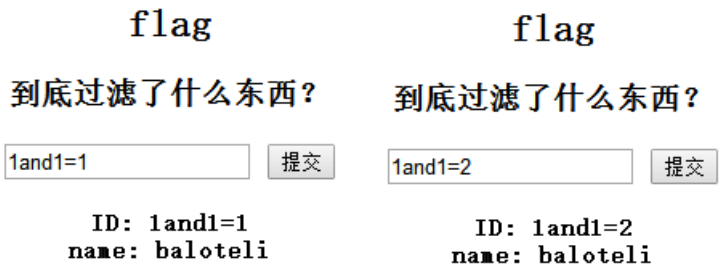
0x.部分题解

一、通过加英文单引号1‘，检测到存在注入： php?id=1

二、按常规步骤输入1 and 1=1和1 and 1=2的时候，发现报了“SQLi deteced!”而无法查询：php?1 and 1=1 php?1 and 1=2



那么，去掉空格输入1and1=1和1and1=2呢？



确定是过滤了空格！

三、绕过过滤空格的进行手工注入，常用一对英文括号()或者程序中常用的一对注释符/**/来替代空格。

四、输入1/**/union/**/select/**/flag/**/from/**/flag/**/where/**/1=1，顺利输出预期结果：

【至于字段flag和表flag就是纯粹猜测的】

五、加单引号闭合，执行：

1'/**/union/**/select/**/flag/**/from/**/flag/**/where/**/'1'='1