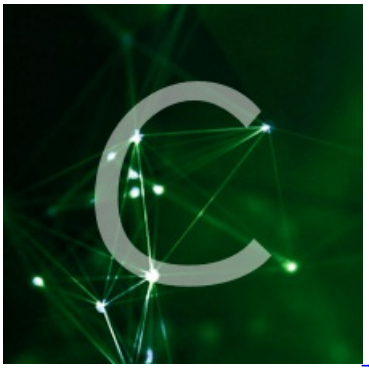
“百度杯”CTF比赛 九月场 SQL-writeup

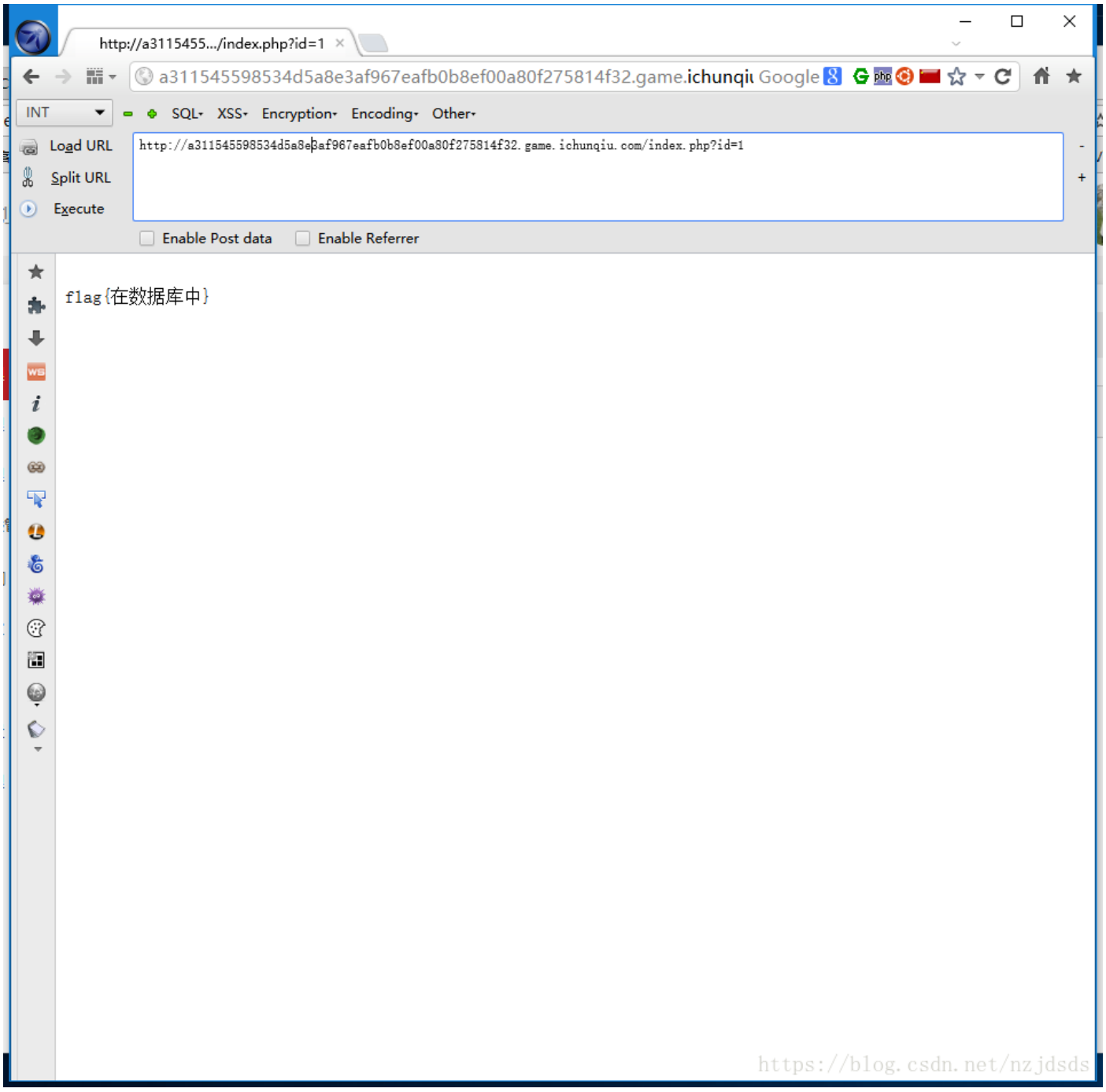
原创

大方子 于 2018-07-31 20:55:22 发布
分类专栏： CTF

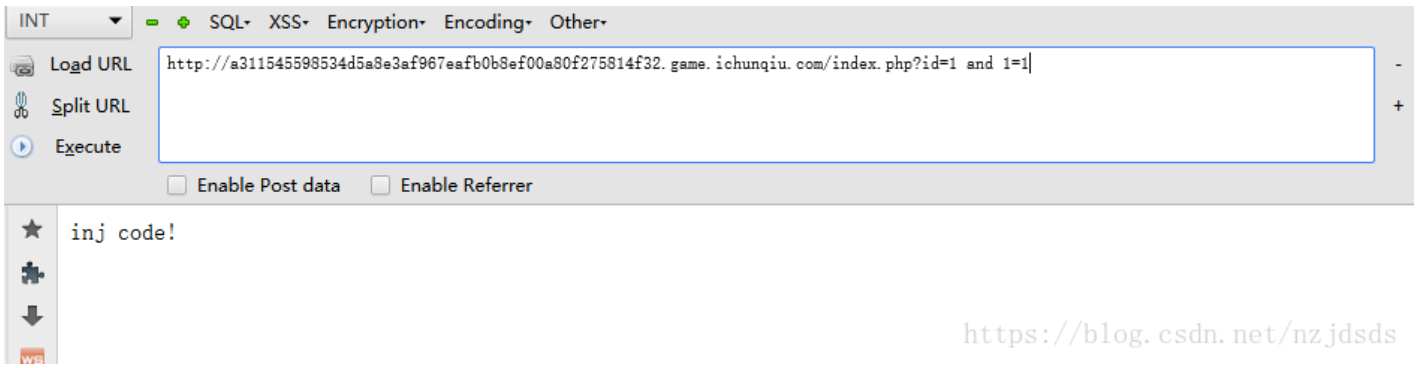


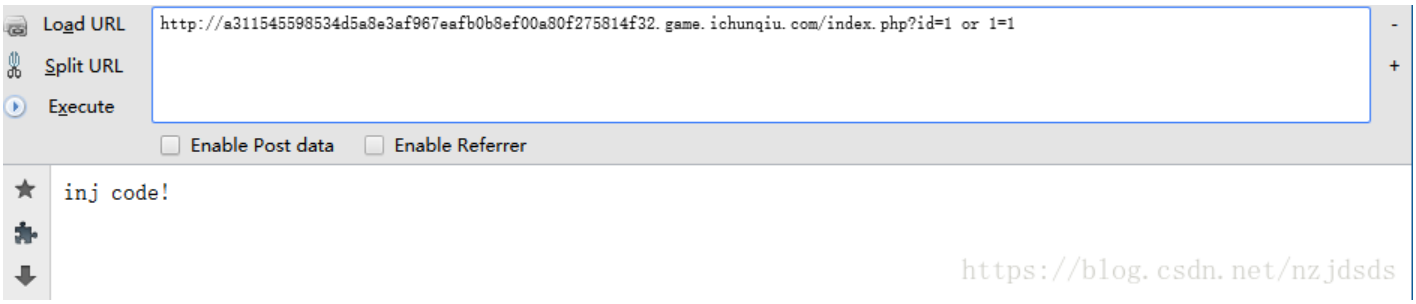
这题自己的收获：用<>隔开敏感字符，绕过防注入

题目界面:



刚开始还是老规矩输入and 1=1 发现被拦截 此外 测试了or 发现也进行了拦截

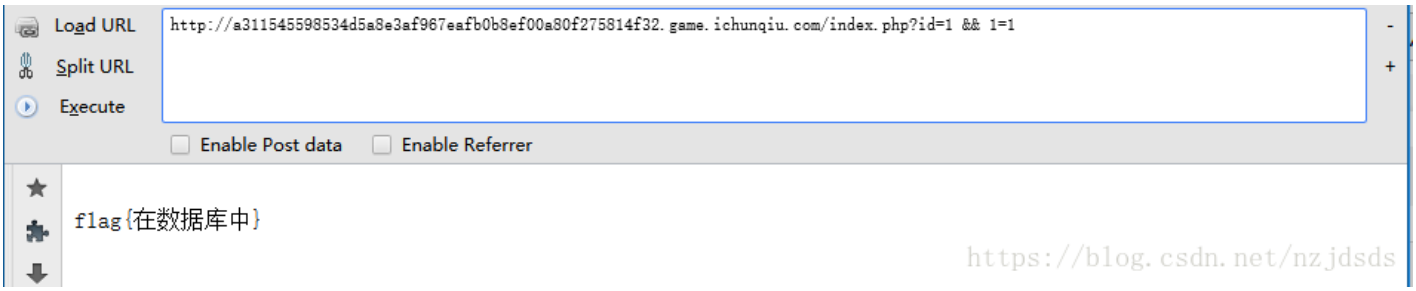




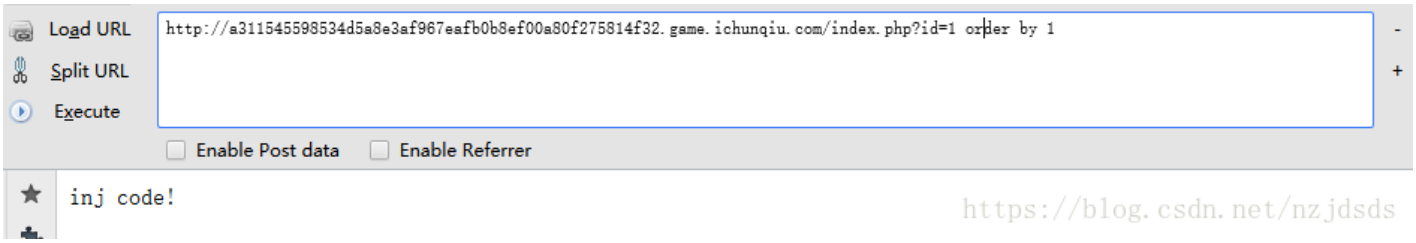
我们可以用下面的字符来替换 and 和 or

and---->&& , or-----> ||

替换后发现可以成功绕过

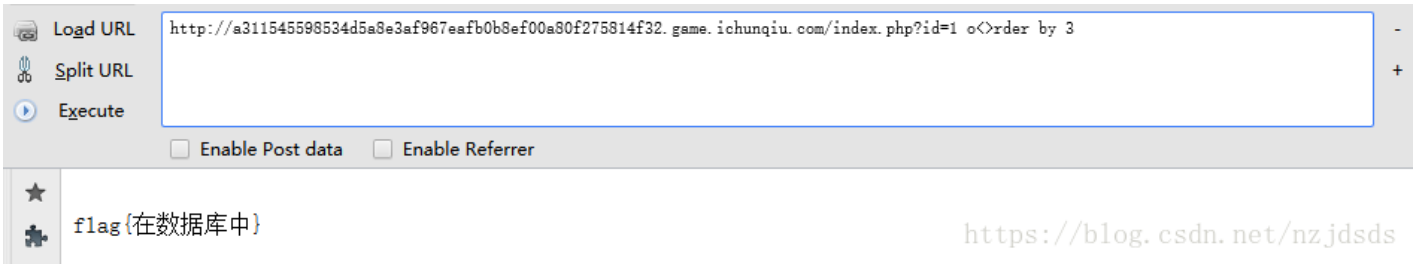


接下来进行猜字段长度 发现order by 被拦截



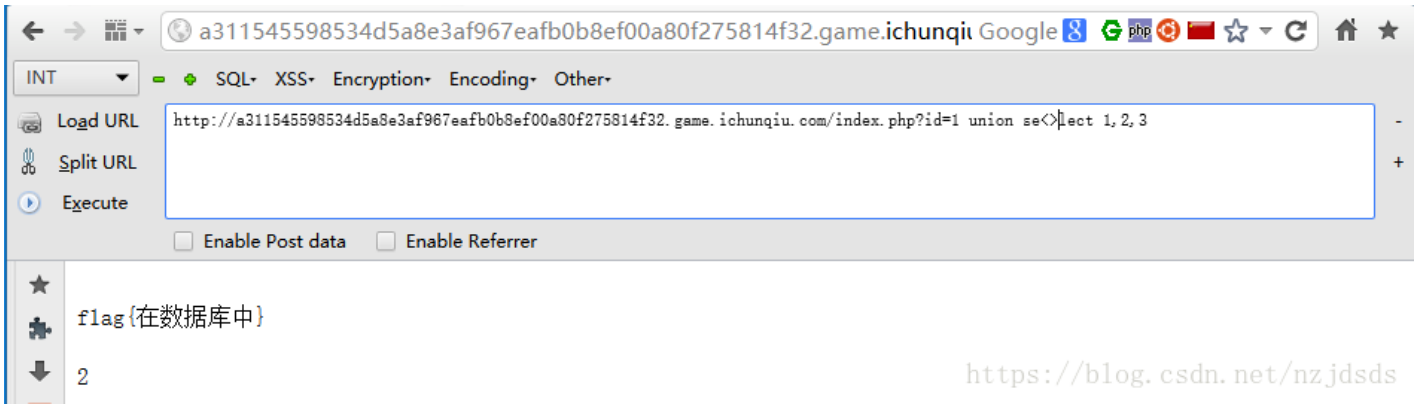
刚开始想用注释/**/来绕过 发现还是行不通，我们用<>把字符隔开，这里需要注意不要这样隔开or<>der ,这样or又是一个被拦截的字符

然后利用二分法，才接触长度为3



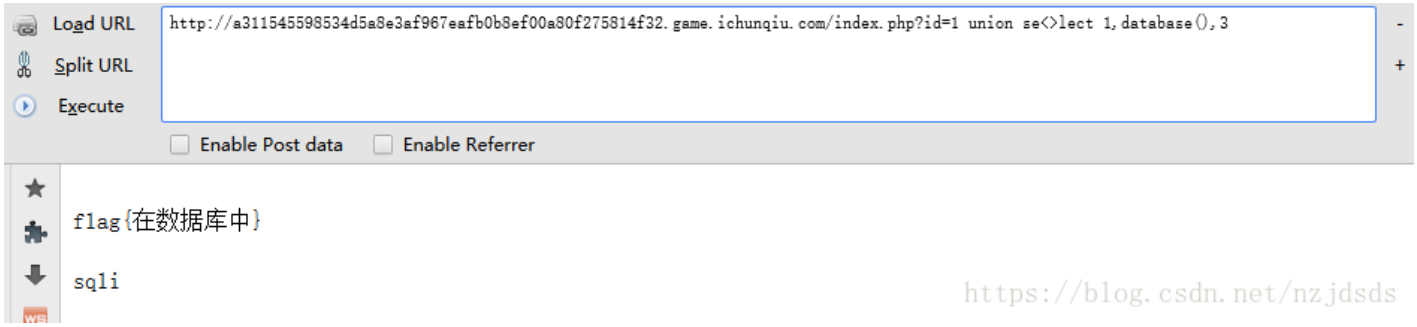
接下来就开始正式注入了

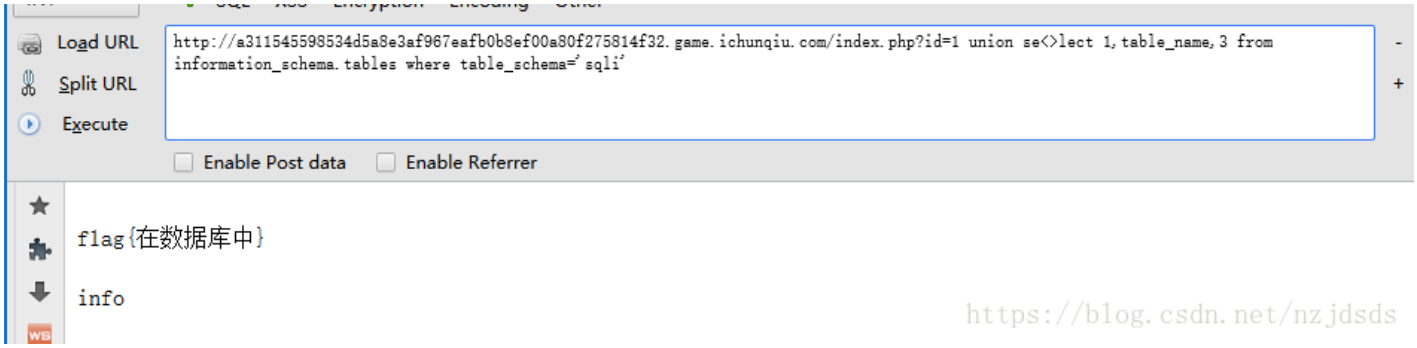
在注入的时候select会被拦截，同样我们用<>把字符分开即可



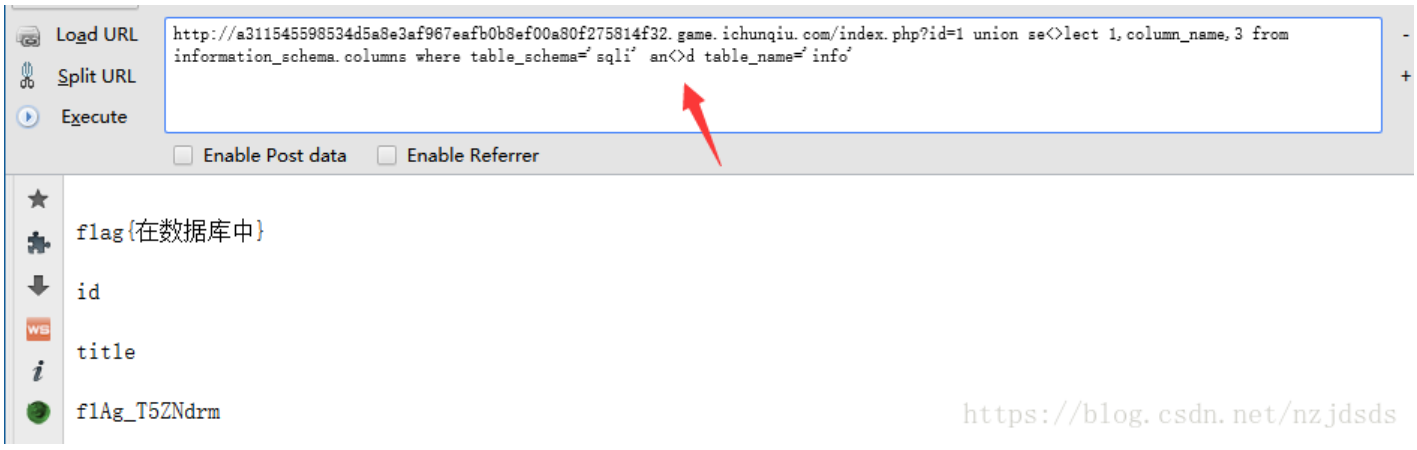
界面出现2，我们就在2的位置进行注入

接下来就是常规注入我就直接贴图了，中途遇到被拦截的字符用<>分开即可





后面出现的and记得用<>隔开



然后就出现了flag