whaleCTF-30days-web【第二期】-登录无效-writeup

原创

sec小玖 于 2018-07-23 17:17:27 发布 579 收藏
分类专栏： CTF web 文章标签： CTF web

题目：

> 为什么后台无法登录了？好像增加了cookie也不能登录··
> 答案格式是：whaleCTF{xxxx}。
> 答题地址：http://ctf.whaledu.com:10802/23h72gdsi8/

访问网页，发现输入什么点击按钮都无效，查看网页源代码，发现是个假的表单：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
  <form method="POST" action="#">
    <p><input name="user" type="text" placeholder="Username"></p>
    <p><input name="password" type="password" placeholder="Password"></p>
    <p><input value="Login" type="button"/></p>
  </form>
<!--hint:paramenter:hint-->
</div>
</body>
</html>
```

发现有一个hint提示，尝试各种get、post、cookie等方式提交参数hint，发现get方式提交显示了网页源代码：

```php
<?php
error_reporting(0);

include_once("flag.php");

$cookie = $_COOKIE['Whale'];

if(isset($_GET['hint'])){
    show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
else {
?>

<?php
}
$KEY='Whale:www.whalectf.com';
?>
```

发现这里包含了flag.php，当满足条件时，输出flag！

首先获取了cookie中Whale的值，并进行了反序列化，然后跟"$KEY"进行===比较。

先来了解几个用到的概念：

什么是序列化（serialize）：

将任意一个对象（字符串、数组、类等）转变为一个静态的字符串，这样对象就可以作为一个简单的变量传入任何需要该对象的php中了。

什么是反序列化（unserialize）：

相反，反序列化就是将这段静态的字符串还原为一个php对象原本的样子。但反序列化的根源在于unserialize()函数的参数是可控的，如果反序列化对象中存在魔术方法，而魔术方法中的代码能够被我们控制就产生了漏洞。魔术方法通俗来讲就是当碰到对应的情况的时候自动运行的方法。比如__construct（）调用构造函数、__distruct（）调用析构函数等。

举个栗子：

```
<?php
$str = "whaleCTF";
$arr = array("name"=>"whale","id"=>1);

class A{
 public $a = 10;
}

class B{
 public $b = 123;
 public function setb(){
  $b = 222;
 }
}

$a = new A();
$b = new B();

echo 'str-'.serialize($str).'<br>';
echo 'array-'.serialize($arr).'<br>';
echo 'classA-'.serialize($a).'<br>';
echo 'classB-'.serialize($b).'<br>';

?>
```

我们分别对字符串、数组、只有变量的类、包含变量和方法的类4类对象进行序列化：

```
str-s:8:"whaleCTF";
array-a:2:{s:4:"name";s:5:"whale";s:2:"id";i:1;}
classA-O:1:"A":1:{s:1:"a";i:10;}
classB-O:1:"B":1:{s:1:"b";i:123;}
```

其中s代表字符串string、a代表数组array、O代表类object；数字代表长度；""中的为具体内容。

如果是一个数组，先列出数组和其中元素，接着把每个元素枚举。

每个子对象包含三个值：类型，长度以及值。

通过类A和类B可发现，序列化只会保存变量，不会保存方法。

学习了php的反序列化，继续来看这道题~~

我们需要提交一个cookie，并且反序列化后和“$KEY”相等。

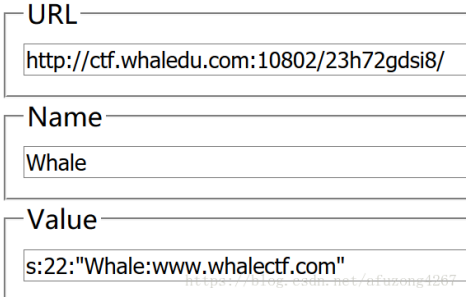
我们发现页面最底部：$KEY='Whale:www.chalectf.com'，但是这是一个坑（ㄟ(ﾟ▽ﾟ)ㄏ）。

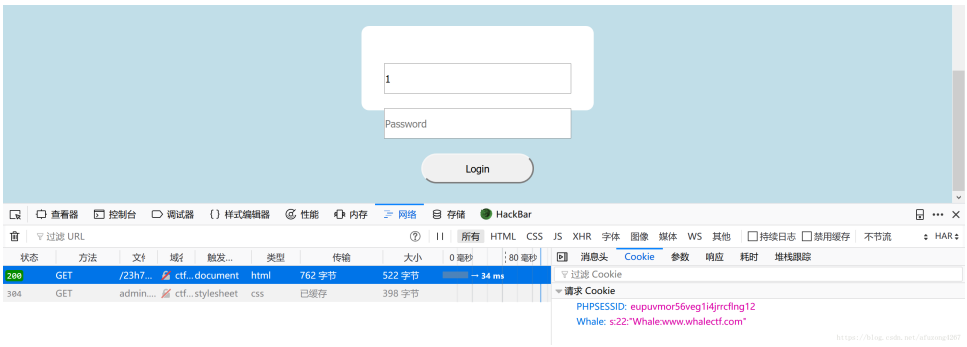
我们首先通过php代码对$KEY='Whale:www.chalectf.com'进行序列化操作：

```
<?php
$KEY='Whale:www.whalectf.com';
echo serialize($KEY)
?>
```

得到一串字符：s:22:"Whale:www.whalectf.com"

重新请求网站，并添加cookie->Whale:s:22:"Whale:www.whalectf.com"





但是提交仍然不正确，仔细观察发现是对“$KEY”进行了比较：

```
elseif (unserialize($cookie) === "$KEY")
{
    echo "$flag";
}
```

重新对“$KEY”进行序列化操作得到：s:0:""

再次提交得到flag！

whaleCTF{unserialize_by_ph5}