你真的会php,PHP语言学习之你真的会PHP吗？

转载

飞蝉智投 于 2021-03-24 01:52:31 发布 12 收藏
文章标签： 你真的会php
本文主要向大家介绍了PHP语言学习之你真的会PHP吗？通过具体的内容向大家展示，希望对大家学习php语言有所帮助。

刚刚做了实验吧的题目，现在整理一下

写出解题思路，希望能够帮助到那些需要帮助的人

所有的wp都是以一题一篇的形式写出

主要是为了能够让读者更好的阅读以及查找，

希望你们不要责怪！！共勉！！！

你真的会PHP吗？分值：30

来源： 实验吧

难度：中

参与人数：4163人

Get Flag：714人

答题人数：888人

解题通过率：80%

你真的会PHP吗？

会？还是不会？

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

解题思路：这一题可以get需要知识点，也可以回忆一下关于以前的知识

点击链接，进行抓包处理就会得到：

进入这个链接就会得到：http://ctf5.shiyanbar.com/web/PHP/6c525af4059b4fe7d8c33a.txt

```
<?php
$info = ""; $req = [];$flag="xxxxxxxxxx";ini_set("display_error", false); error_reporting(0); if(!isset($_POST[‘numbe
{   header("hint:6c525af4059b4fe7d8c33a.txt");   die("have a fun!!"); }foreach([$_POST] as $global_var) {     fore
```

接下来进行代码审计：

```
if(is_numeric($_REQUEST[‘number‘])){       $info="sorry, you cann‘t input a number!";//条件1：输入的不能只是数字 }elseif($req[‘number‘]!=strval(intval($req[‘number‘])))
{           $info = "number must be equal to it‘s integer!! ";  //条件2：输入的值经过变整型又变成字符型后应该与原来一
样 }else{      $value1 = intval($req["number"]);     $value2 = intval(strrev($req["number"]));       if($value1!=$valu
{//条件3：输入的值直接变成整型应该和其颠倒之后再变成整型一
样          $info="no, this is not a palindrome number!";     }else{                  if(is_palindrome_number($req["numb
{//条件4：输入的不能是回文，就是颠倒和原来不能一
样             $info = "nice! {$value1} is a palindrome number!";          }else{             $info=$flag;          }     } } echo
```

我看writeup看到有两种解法：

利用intval溢出

intval最大的值取决于操作系统。 32 位系统最大带符号的 integer 范围是 -2147483648 到 2147483647。举例，在这样的系统上， intval(‘1000000000000’) 会返回 2147483647。

64 位系统上，最大带符号的 integer 值是 9223372036854775807。

通过上面我们知道服务器的操作系统是32位的，所以我们构造2147483647就可以同时满足2，3条件。

通过把空字符可以绕过is_numeric的判断(如%00,%20),所以我们构造以下poc，

number=2147483647%00 和number=2147483647%20都可。 我们来看上面的payload是怎么绕过上面的条件的，

首先因为我们post的number中包含%00或者%20这样的空字符，

所以在is_numeric判断时，会返回false,接下来 $req[‘number‘]!=strval(intval($req[‘number‘])) intval会忽略掉我们的空字符%00与%20，所以这里也就绕过了，然后：

```
$value1 = intval($req["number"]);$value2 = intval(strrev($req["number"]));
```

这两个值要相等，由于我们输入的number已经达到了intval的最大值，

所以当执行strrev后，得到7463847412这个值，这个值经过intval转换为2147483647，所以这两个值相等了。 但是2147483647又不是回文数，所以得到flag。

注：strval会忽略掉%00与%20 注：如果你输入number=’1’这样的字符，后台存储的字符串时’\’1\”，意思就是会把引号作为你输入的字符串的一部分。

这是个很奇怪的特性，大家可以测试一下 注：其中很多细节，我是通过把源码拷贝到本地执行得到的结果，大家也可以测试一下自己的想法。

0x02科学记数法绕过

因为要求不能为回文数，但又要满足
intval(req["number"])=intval(strrev(req["number"])=intval(strrev(req[“number”]))，

所以我们采用科学计数法构造poc为number=0e-0%00，这样的话我们就可以绕过。 一定要时-0，才不会被判定为回文数

本文由职坐标整理并发布，希望对同学们有所帮助。了解更多详情请关注职坐标编程语言PHP频道！