实验吧 你真的会PHP吗 writeup

原创

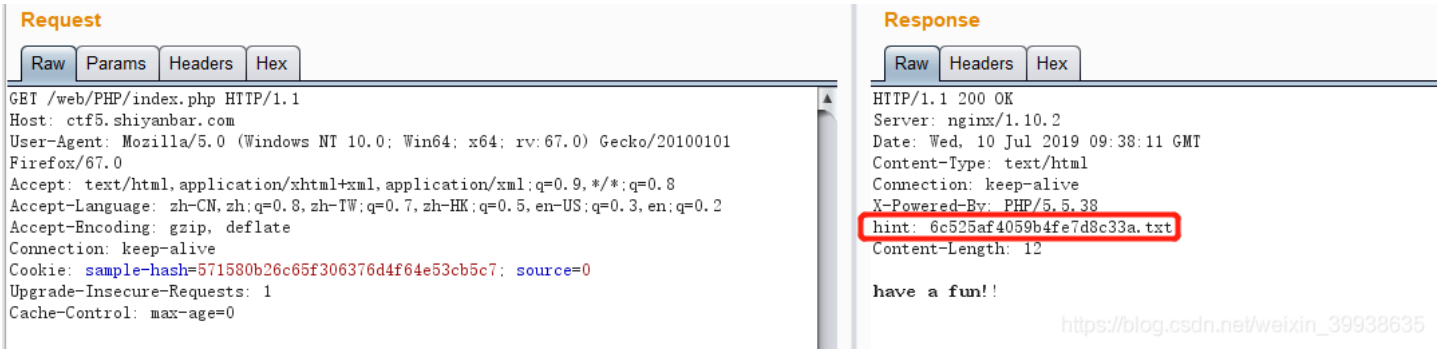
zero-L 于 2019-07-10 09:48:06 发布 146 收藏

分类专栏： ctf 实验吧 文章标签： ctf 实验吧 writeup 你真的会php吗

本文链接：https://blog.csdn.net/weixin_39938635/article/details/95307355

题目传送门 http://ctf5.shiyanbar.com/web/PHP/index.php

抓个包先，发现hint



访问得到源码

```php
<?php


$info = "";
$req = [];
$flag="xxxxxxxxxx";

ini_set("display_error", false);
error_reporting(0);


if(!isset($_POST['number'])){
   header("hint:6c525af4059b4fe7d8c33a.txt");

   die("have a fun!!");
}

foreach([$_POST] as $global_var) {
```

```
    foreach($global_var as $key => $value) {
        $value = trim($value);
        is_string($value) && $req[$key] = addslashes($value);
    }
}


function is_palindrome_number($number) {
    $number = strval($number);
    $i = 0;
    $j = strlen($number) - 1;
    while($i < $j) {
        if($number[$i] !== $number[$j]) {
            return false;
        }
        $i++;
        $j--;
    }
    return true;
}


if(is_numeric($_REQUEST['number'])){

   $info="sorry, you cann't input a number!";

}elseif($req['number']!=strval(intval($req['number']))){

     $info = "number must be equal to it's integer!! ";

}else{

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

     if($value1!=$value2){
          $info="no, this is not a palindrome number!";
     }else{

          if(is_palindrome_number($req["number"])){
              $info = "nice! {$value1} is a palindrome number!";
          }else{
             $info=$flag;
          }
     }

}

echo $info;
```

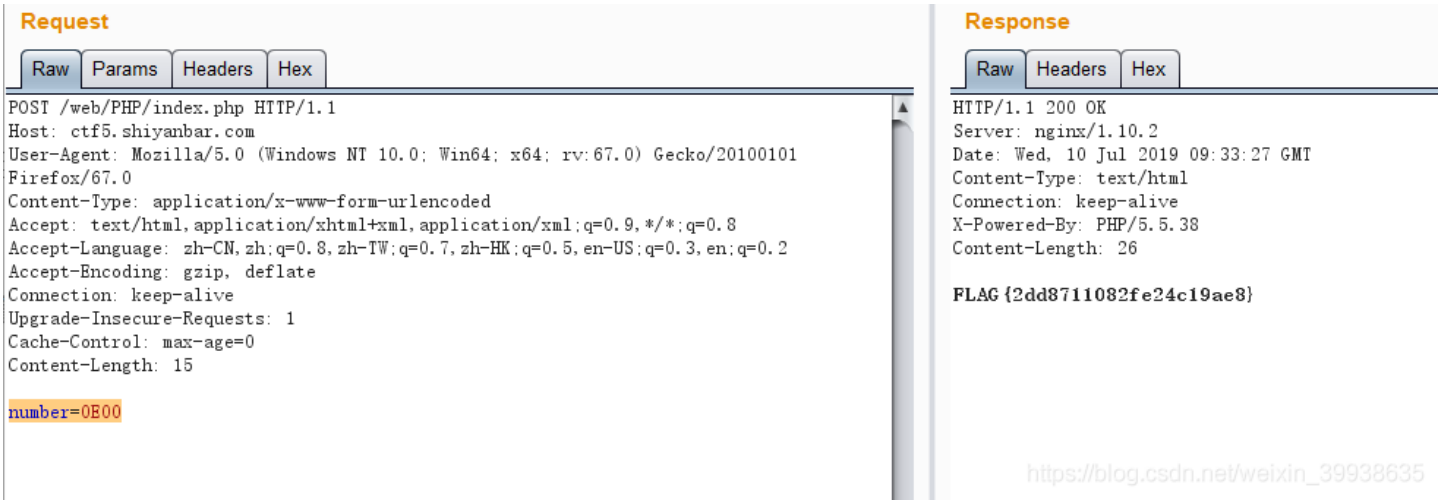
可以看到，需要提交一个number字段，经过**is_numeric**函数判断，number反转后的值与number相同，但number不是回文数字，才可以得到flag。

百度is_numeric的源码，看下它的判断标准
放一个参考链接
http://www.vuln.cn/8198

> 经过查找，找到真正的处理函数_is_numeric_string_ex,省略一些代码，我们只用知道哪些字符能够出现在is_numeric的参数中，很明显可以看出，
> **空格、\t、\n、\r、\v、\f、+、-能够出现在参数开头，“点”能够在参数任何位置，E、e只能出现在参数中间。**

于是我们构造一个
number=0E00，满足上述条件（0==0E00）

得到flag



补充：看了下大家的writeup发现还有使用溢出绕过的
参考链接
https://blog.csdn.net/qq_30464257/article/details/85014654