

bugku WEB 矛盾 writeup

原创

T0mrwi1b3t 于 2020-12-03 11:14:39 发布 39 收藏

分类专栏: [bugku web](#)

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_50597969/article/details/110523493

版权



[bugku](#) 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏



[web](#)

19 篇文章 0 订阅

订阅专栏

bugku WEB 矛盾

矛盾

小结

绕过is_numeric() //判断参数是否为数字

矛盾

Challenge 20459 Solves

矛盾

30

<http://123.206.87.240:8002/get/index1.php>

https://blog.csdn.net/weixin_50597969

```
$num=$_GET['num'];  
if(!is_numeric($num))  
{  
echo $num;  
if($num==1)  
echo 'flag{*****}';  
}
```

https://blog.csdn.net/weixin_50597969

函数is_numeric() 判断变量是否为数字

is_numeric

(PHP 4, PHP 5, PHP 7)

is_numeric — 检测变量是否为数字或数字字符串

描述

```
bool is_numeric ( mixed $var )
```

https://blog.csdn.net/weixin_50597969

如果var是数字和数字字符串返回TRUE否则返回FALSE
即num既不能是数字字符，但是要等于1
因此，构造payload num=1a（开头为1，字母随意）提交上去

```
$num=$_GET['num'];  
if(!is_numeric($num))  
{  
echo $num;  
if($num==1)  
echo 'flag{*****}';  
}  
1aflag{bugku-789-ps-ssdf}
```

https://blog.csdn.net/weixin_50597969

得到flag

小结

考察绕过