## 1、知识点

| 知识点 | 说明 |
| --- | --- |
| strcmp() | 比较两个字符串是否相等，并返回整数；str1 > str2返回正数，str1 < str2返回负数，str1 = str2返回0 |

## 2、源码

```
<?php
$flag = "flag";
if (isset($_GET['a'])) {
    if (strcmp($_GET['a'], $flag) == 0) //如果 str1 小于 str2 返回 < 0； 如果 str1大于 str2返回 > 0；如果两者相等，返回 0。

    //比较两个字符串（区分大小写）
        die('Flag: '.$flag);
    else
        print 'No';
}

?>
```

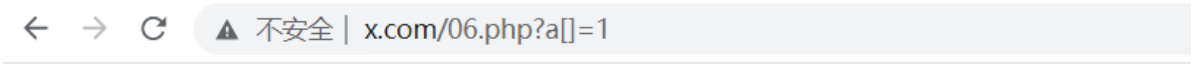
## 3、分析

1）程序对用户传入的参数a，使用strcmp函数进行判断是否等于$flag的值，等于即输出$flag的值。


2）这里我们可以使用两种方法：

- ?a=flag
- ?a[]=1

第一种就是传入和$flag值相等的值，即可成功读取；但现实情况中我们如果知道这个值了就没必要去读取这个值，所以第二种方法是利用了strcmp函数的缺陷，strcmp是用于比较字符串的值是否相等，当其中一个参数的值不是字符串能处理的类型（如数组），就会报错，但报错之后还是会继续执行后面的程序。




**Warning: strcmp() expects parameter 1 to be string, array given in F:\Rang**

**Call Stack**

| # | Time | Memory | Function |
|---|---|---|---|
| 1 | 0.0009 | 130912 | {main}( ) |
| 2 | 0.0009 | 131032 | strcmp ( ) |

Flag: flag

## 4、利用

```
?a=flag
?a[]=1
```