1、知识点

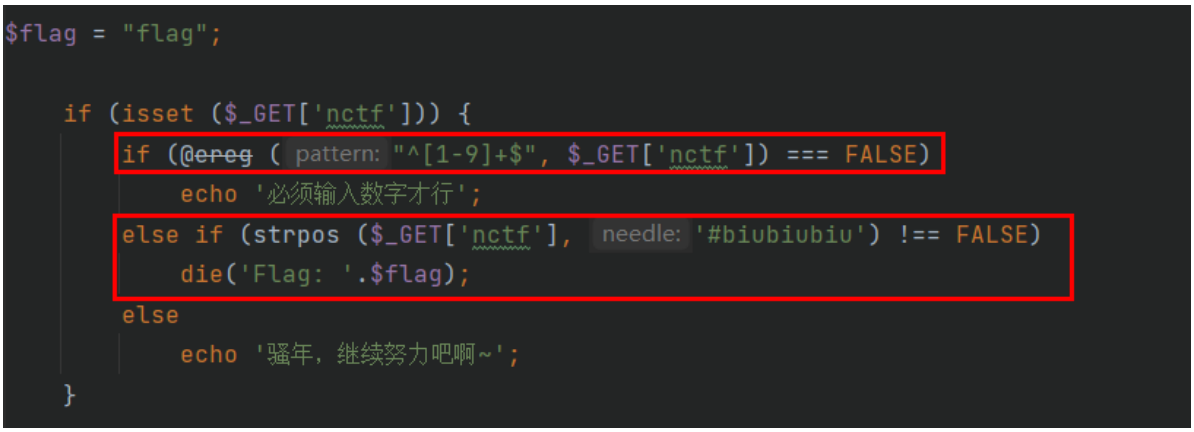
知识点	说明
strpos()	查找字符串在另一个字符串中第一次出现的位置

2、源码

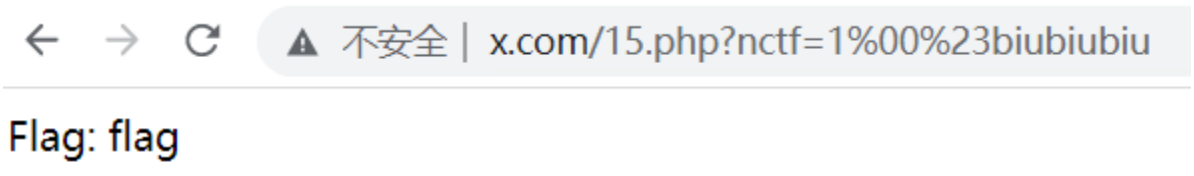
```
<?php

$flag = "flag";

    if (isset ($_GET['nctf'])) {
        if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
            echo '必须输入数字才行';
        else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
            die('Flag: '.$flag);
        else
            echo '骚年，继续努力吧啊~';
    }

 ?>
```

3、分析

1）程序通过GET方法接收参数nctf的值，并对其进行判断。nctf的值不能是纯数字，并且包含#biuibiubiu关键词，即可输出flag。

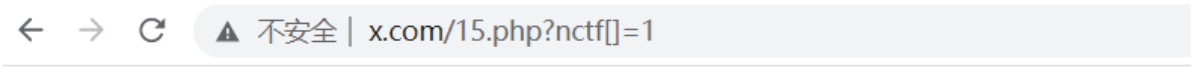


2）此时通过传入数字拼接关键词即可（需要把#换成url编码的%23），即可成功拿到flag。



Flag: flag

3）看到wp上给的另一个思路，是将nctf的值作为数组格式传入，那么此时ereg处理时就会报错，返回值为NULL，NULL是不等于FALSE的。然后在strpos中，匹配上数组格式，也会报错，返回NULL，NULL同样不等于FALSE，所以也可以绕过，拿到Flag。



(!) Warning: strpos() expects parameter 1 to be string, array given in F:\Ra

Call Stack

#	Time	Memory	Function
1	0.0009	132160	{main}( )
2	0.0010	132704	strpos ( )

Flag: flag

4、利用

```
?nctf=1%00%23biubiubiu
?nctf[]=1
```