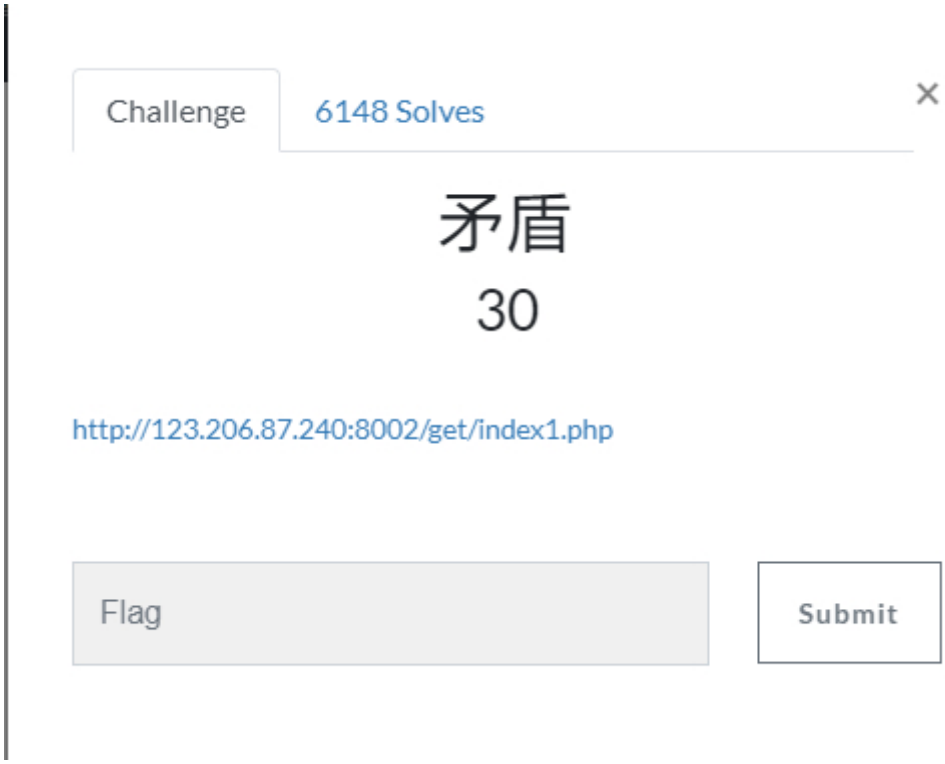
矛盾-writeup

打开题目

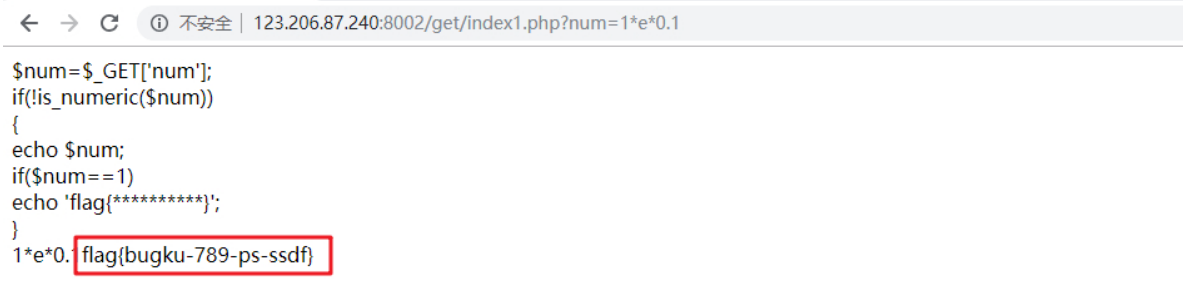


访问链接，得到一串代码，又是一道代码审计的题

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

```
//代码分析
$num=$_GET['num'];  //Get方式获取参数
if(!is_numeric($num)) //is_numeric()函数是否为数字或者数字字符串->>加个！取反,通俗点讲这里不能为数字
{
echo $num; //如果不是数字就输出
if($num==1) //矛盾吧，上面又不要数字，这里又要是1
echo 'flag{**********}'; //如果值为1则输出flag
}
```

根据提示，可以用科学计数法表示1，构造URL：?num=1e0.1 既不是纯数字，其值又等于1



其实还有很多种姿势获取到flag，授人以鱼不如授人以渔。以下讲解几个特征。

php是一个弱类型语言
==表示的是等于 ，比较两个变量的值，不比较数据类型。只要数值等于就成立了
===表示的是全等，比较的是两个变量的值和类型
== 判断时，当数字与字符串比较时，系统先将字符串转化为数字，再与数字进行比较。

is_numeric（）函数用于检测变量是否为数字或数字字符串。
is_numeric函数对于空字符%00，无论是%00放在前后都可以判断为非数值，怎么构造有思路了吗？

PHP浅谈==和===：https://blog.csdn.net/auuuuuuuu/article/details/79621635
科学计数法：https://baike.baidu.com/item/科学记数法/1612882?fr=aladdin