# CTF中php语言之is_numeric()和sleep()函数的绕过

原创

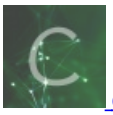
д一点红ж 于 2019-09-27 18:10:16 发布 4384 收藏 4

分类专栏： ctf 文章标签： ctf



本文链接：https://blog.csdn.net/qq_41814777/article/details/84069392







```
 ` <?php
include 'flag.php';
isset($_GET['time'])?$time = $_GET['time']:$time = 0;
isset($_GET['num'])?$num = $_GET['num']:$num = 0;
$c=is_numeric($time) and is_numeric($num);
if ($num == 0) {
    if($num){
        if($c){
            if(!is_numeric($time))
                echo 'Time time must be number';
            else if ($time < 60 * 60 * 24 * 30 * 1)
                echo 'This time is too short';
            else if ($time > 60 * 60 * 24 * 30 * 2)
                echo 'This time is too long';
            else{
                sleep((int)$time);
                echo $flag;
            }
        }
        else
            echo 'Try again';
    }
    else
        echo 'Try again';
}
else
    echo 'Try again';
echo '<hr>';
highlight_file(__FILE__);
?>
```

is_numeric() 函数用于检测变量是否为数字或数字字符串。若是则为true,否则为false

很明显该题用了两个比较关键的函数is_numeric()和sleep（）这也是问题解决得关键。

要拿flag首先要绕过这两个函数，对于这题的sleep(),要延缓其下面程序执行的时间。但是我们又不能等太久，可以构造php中的科学计数法绕过，就构造一个time=0.3e07（等价于0.3乘10的7次方）的参数吧！当它强制转化为零的时候就会变成零，这样可以满足条件。

对于is_numeric();题目要求弱等于零，又要为一个不为零的数，我们可以构造一个0e1abc的数绕过，“0e1abc”=”0"。进行比较运算时，如果遇到了0e\d+这种字符串，就会将这种字符串解析为科学计数法。所以上面例子中2个数的值都是0因而就相等了。如果不满足0e\d+这种模式就不会相等。