

云演CTF Web题型 021 php黑魔法

原创

静默开水 于 2022-01-20 10:27:01 发布 1620 收藏

分类专栏: [web题解题思路](#) [CTF PHP基础知识点](#) 文章标签: [php](#) [安全](#) [经验分享](#) [unctf](#)

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/cadandme/article/details/122595886>

版权



[web题解题思路](#) 同时被 3 个专栏收录

7 篇文章 0 订阅

订阅专栏



[CTF](#)

14 篇文章 0 订阅

订阅专栏



[PHP基础知识点](#)

2 篇文章 0 订阅

订阅专栏

php黑魔法

```
<?php
highlight_file('2.php');
function noother_says_correct($number)
{
    $one = ord('1');
    $nine = ord('9');
    for ($i = 0; $i < strlen($number); $i++)
    {
        $digit = ord($number[$i]);
        if ( ($digit >= $one) && ($digit <= $nine) )
        {
            return false;
        }
    }
    return $number == '54975581388';
}

$flag='{*****}';
if(nother_says_correct($_GET['key']))
    echo "flag is ".$flag;
else
    echo 'access denied';
?> access denied
```

CSDN @静默开水

- 代码审计题型
- ord() 函数返回字符串的首个字符的 ASCII 值。

知道以上函数的使用方法, 就可以知道这道题应该怎么解

```
<?php
highlight_file('2.php');
function noother_says_correct($number)
{
    $one = ord('1');
    $nine = ord('9');
    for ($i = 0; $i < strlen($number); $i++)
    {
        $digit = ord($number[$i]);
        if ( ($digit >= $one) && ($digit <= $nine) )
        {
            return false;
        }
    }
    return $number == '54975581388';
}

$flag='*****';
if(nother_says_correct($_GET['key']))
    echo "flag is ".$flag;
else
    echo 'access denied';
?> access denied
```

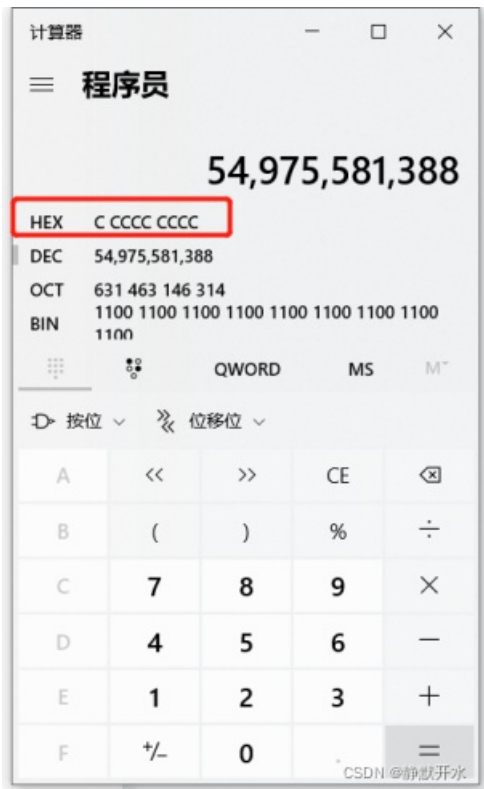
输入值不能是数字1-9

输入值需弱等于这个数

GET方式传入

CSDN @静默开水

要传入一个没有1到9数字的字符串，但值要等于54975581388，可以使用进制转换来代替



将得到的十六进制GET传入得flag

```
<?php
highlight_file('2.php');
function nother_says_correct($number)
{
    $some = ord('1');
    $nine = ord('9');
    for ($i = 0; $i < strlen($number); $i++)
    {
        $digit = ord($number[$i]);
        if ( ($digit >= $some) && ($digit <= $nine) )
        {
            return false;
        }
    }
    return $number == '54975581388';
}

$flag = '*****';
if(nother_says_correct($_GET['key']))
    echo "Flag is ".$flag;
else
    echo 'access denied';
?> flag is (ddefjagaergha)
```