1、知识点

```
Null
```

2、源码

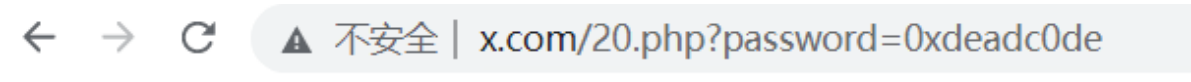
```
<?php

error_reporting(0);
function noother_says_correct($temp)
{
    $flag = 'flag{test}';
    $one = ord('1');  //ord — 返回字符的 ASCII 码值
    $nine = ord('9'); //ord — 返回字符的 ASCII 码值
    $number = '3735929054';
    // Check all the input characters!
    for ($i = 0; $i < strlen($number); $i++)
    {
        // Disallow all the digits!
        $digit = ord($temp{$i});
        if ( ($digit >= $one) && ($digit <= $nine) )
        {
            // Aha, digit not allowed!
            return "flase";
        }
    }
    if($number == $temp)
        return $flag;
}
$temp = $_GET['password'];
echo noother_says_correct($temp);

?>
```

3、分析

1) 程序通过GET方法接收password的值，并使用for循环对password的值进行校验，只要其中存在数字就报错。并且只有当password的值等于'3735929054'时，才输出flag。

```php
function noother_says_correct($temp)
{
    $flag = 'flag{test}';
    $one = ord( character: '1');  //ord — 返回字符的 ASCII 码值
    $nine = ord( character: '9'); //ord — 返回字符的 ASCII 码值
    $number = '3735929054';
    // Check all the input characters!
    for ($i = 0; $i < strlen($number); $i++)
    {
        // Disallow all the digits!
        $digit = ord($temp{$i});
        if ( ($digit >= $one) && ($digit <= $nine) )
        {
            // Aha, digit not allowed!
            return "flase";
        }
    }
    if($number == $temp)
        return $flag;
}
$temp = $_GET['password'];
echo noother_says_correct($temp);
```

2）这里使用的==，又是一个弱类型比较，也就是可以传入16进制的 3735929054 进行绕过，然后比较，最后拿到flag。



flag{test}

4、利用

```
?password=0xdeadc0de
```