

1、知识点

Null

2、源码

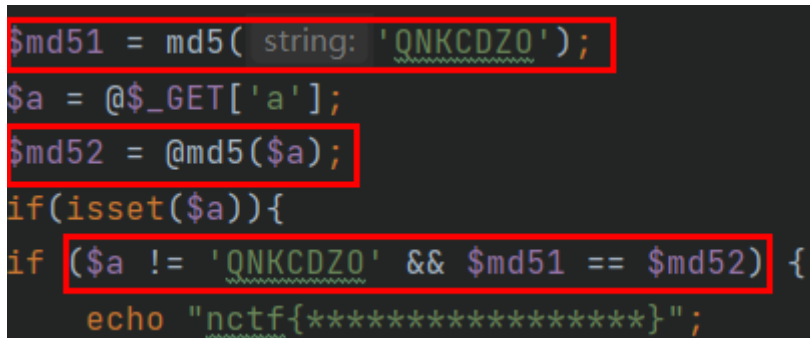
```
<?php

$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
    if ($a != 'QNKCDZO' && $md51 == $md52) {
        echo "nctf{*****}";
    } else {
        echo "false!!!";
    }
}
else{echo "please input a";}

?>
```

3、分析

1) 程序通过GET接收参数a，并对其进行md5加密。随后使用==进行比较，如果md5加密后的a，和md5加密后的'QNKCDZO'相等，就返回flag。



```
$md51 = md5( string: 'QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
    if ($a != 'QNKCDZO' && $md51 == $md52) {
        echo "nctf{*****}";
    }
}
```

2) 由于程序使用的==弱类型比较，在比较字符串时，会将其转换成数字进行比较，那么此时'QNKCDZO'的md5值是 0e830400451993494058024219903391，0e开头表示科学计数法，所以值转换成了0；然后只要传入的a的值经过md5加密后也是0e开头，即可绕过该比较，得到flag。

← → ↻ ⚠ 不安全 | x.com/13.php?a=240610708

nctf{*****}

4、利用

?a=240610708