

源码如下

```
1 <?php
2 show_source("13.php");
3 echo '<br>';
4 require 'flag.php';
5 $md51 = md5('QNKCDZO');
6 $a = @$_GET['a'];
7 $md52 = @md5($a);
8 if(isset($a)){
9 if ($a != 'QNKCDZO' && $md51 == $md52) {
10 echo "$flag";
11 } else {
12 echo "false!!!";
13 }}
14 else{echo "please input a";}
15
16 ?>
```

通过读源码可以发现

是将QNKCDZO的md5值和传入a的md5值比较

由于QNKCDZO的md5值是0e开头，会被php的弱类型比较认为是0的很多很多次幂

所以可以用另一些0e开头的md5原文来是指相等

所以payload:

```
1 a=s878926199a
```