1、知识点

```
Null
```

2、源码

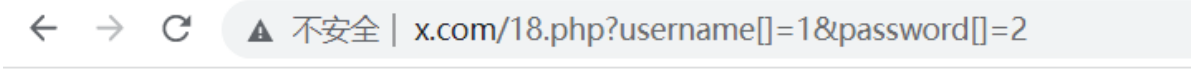
```
<?php
error_reporting(0);
$flag = 'flag{test}';
if (isset($_GET['username']) and isset($_GET['password'])) {
    if ($_GET['username'] == $_GET['password'])
        print 'Your password can not be your username.';
    else if (md5($_GET['username']) === md5($_GET['password']))
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}
?>
```

3、分析

1）程序通过GET方法接收username和password的值，username和password的值不能相等，但是双方经过md5加密后的值又必须相等。

```
$flag = 'flag{test}';
if (isset($_GET['username']) and isset($_GET['password'])) {
    if ($_GET['username'] == $_GET['password'])
        print 'Your password can not be your username.';
    else if (md5($_GET['username']) === md5($_GET['password']))
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}
```

2）如果==，可以使用 username=QNKCDZO&password=240610708，因为==比较时会进行数据转换，0exxxx转换成0，可以绕过。这里是===，需要使用数组类型进行绕过，因为md5无法加密数组，会返回null的空，null===null，也就绕过了检测。



Flag: flag{test}

4、利用

```
?username[]=1&password[]=2
```