1、知识点

知识点	说明
strcasecmp()	比较两个字符串并返回整型值

2、源码

```
<?php

//配置数据库
if($_POST[user] && $_POST[pass]) {
    $conn = mysql_connect("localhost", "root", "xxx");
    mysql_select_db("mysql") or die("Could not select database");
    if ($conn->connect_error) {
        die("Connection failed: " . mysql_error($conn));
}

//赋值

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

$sql = "select `user` from `users` where user='$user'";
$query = mysql_query($sql);
if (!$query) {
    printf("Error: %s\n", mysql_error($conn));
    exit();
}
$row = mysql_fetch_array($query, MYSQL_ASSOC);
//echo $row["user"];

  if (($row[user]) && (!strcasecmp($pass, $row[user]))) {

//如果 str1 小于 str2 返回 < 0； 如果 str1 大于 str2 返回 > 0；如果两者相等，返回 0。


    echo "<p>Logged in! Key:*************** </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，并拼接到SQL语句中进行查询。

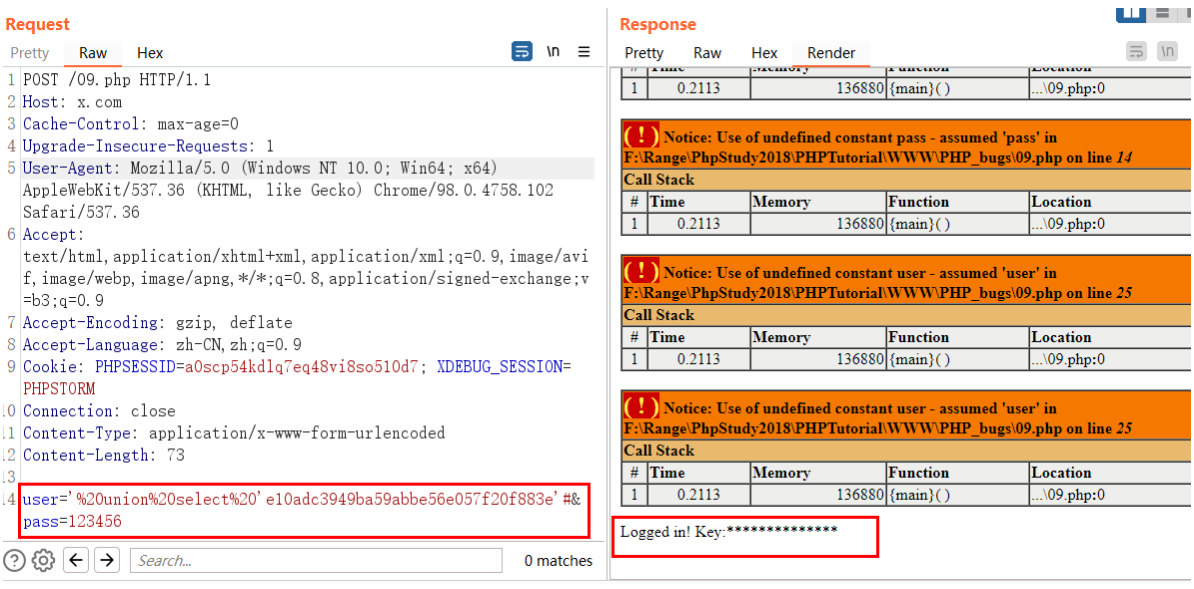
```php
$user = $_POST[user];
$pass = md5($_POST[pass]);

$sql = "select `user` from `users` where user='$user'";
$query = mysql_query($sql);
if (!$query) {
    printf( format: "Error: %s\n", mysql_error($conn));
    exit();
}
```

2）将查询到的结果返回到$row数组中，如果数组中的user值为真，并且pass和user的值相等，就输出key。

```php
$row = mysql_fetch_array($query, result_type: MYSQL_ASSOC);
//echo $row["user"];

 if (($row[user]) && (!strcasecmp($pass, $row[user]))) {

//如果 str1 小于 str2 返回 < 0； 如果 str1 大于 str2 返回 > 0；如果两者相等，返回 0。


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

3）由于接收到的GET参数没有经过过滤，直接就拼接到SQL语句中进行查询，所以这里可以通过')闭合，造成注入；其次这里的要求是$user和$pass（$pass是经过md5加密的，图1可以看到）进行比较，如果为真就返回key。

那么此时通过传入md5加密后的pass值作为user的值，然后')闭合并注释，再传入pass的值，即可成功拿到key。



4、利用

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