源码如下

```php
<?php
 show_source("09.php");
   echo '<br>';
error_reporting(0);

require 'flag.php';

if($_POST[user] && $_POST[pass]) {

 require('config.php');
 }
 else{
     echo "Sons of bitch!";
 }
 $user = $_POST[user];
 $pass = md5($_POST[pass]);

 $sql = "select pwd from userinfo where uname='$user'";
 $query = mysql_query($sql);
 if (!$query) {
     printf("Error: %s\n", mysql_error($con));
     exit();
 }
 $row = mysql_fetch_array($query, MYSQL_ASSOC);
   if (($row[pwd]) && (!strcasecmp($pass, $row[pwd]))) {
     echo "<p>Logged in! Key:  $flag </p>";
 }
 else {
     echo("<p>Log in failure!</p>");

   }
 mysql_close($con);
 ?>
```

但是做了半天，无解

上网查询是使用了union联合注入，但是我并没有做出来