cookie-session

cookie和session的区别及使用

众所周知，HTTP 是一个无状态协议，所以客户端每次发出请求时，下一次请求无法得知上一次请求所包含的状态数据，如何能把一个用户的状态数据关联起来呢?

cookie

首先产生了 cookie 这门技术来解决这个问题，cookie 是 http 协议的一部分，它的处理分为如下几步：

服务器向客户端发送 cookie。
通常使用 HTTP 协议规定的 set-cookie 头操作。
规范规定 cookie 的格式为 name = value 格式，且必须包含这部分。
浏览器将 cookie 保存。
每次请求浏览器都会将 cookie 发向服务器。
其他可选的 cookie 参数会影响将 cookie 发送给服务器端的过程，主要有以下几种：

`path：表示 cookie 影响到的路径，匹配该路径才发送这个 cookie。`
`expires 和 maxAge：告诉浏览器这个 cookie 什么时候过期，expires 是 UTC 格式时间，maxAge 是 cookie 多久后过期的相对时间。`
`当不设置这两个选项时，会产生 session cookie，session cookie 是 transient 的，当用户关闭浏览器时，就被清除。`
`一般用来保存 session 的 session_id。`
`secure：当 secure 值为 true 时，cookie 在 HTTP 中是无效，在 HTTPS 中才有效。`
`httpOnly：浏览器不允许脚本操作 document.cookie 去更改 cookie。一般情况下都应该设置这个为 true，这样可以避免被 xss 攻击拿到 cookie。`

express 中的 cookie

express 在 4.x 版本之后，session管理和cookies等许多模块都不再直接包含在express中，而是需要单独添加相应模块。

express4 中操作 cookie 使用 cookie-parser 模块(https://github.com/expressjs/cookie-parser)。
```
var express = require('express');
```