Session and cookie

学号：161250128

姓名：唐诗林

安全性：

1、数据库直接存放 md5 加密后的密码，进行加密后判断

```
var d = getMD5Password(testuser.password);
testuser.password = d;
User.find(testuser, function (err, detail) {
    if (detail.length) {
        console.log("loggedIn!");
        signinCheckSuccess(detail, req, res)
    } else {
        console.log("wrong!");
        errorInfo = "用户名不存在或密码错误";
        res.render('login.ejs', {
            errorInfo:errorInfo
        })
    }
})
```

2、通过设置 Cookie 的 HttpOnly 为 true，可以防止客户端脚本访问这个 Cookie，从而有效的防止 XSS 攻击

```
// session时限为5分钟
app.use(session({ secret: 'keyboard cat', cookie: { httpOnly: true, maxAge: 300000 }}));
```

3、过滤和净化用户输入，防御跨站点脚本编制（XSS）和命令注入攻击。

4、关闭透明化 Session ID。透明化 Session ID 指当浏览器中的 Http 请求没有使用 Cookie 来存放 Session ID 时，Session ID 则使用 URL 来传递。

备注：

进入项目目录运行 node signin.js，打开 http://127.0.0.1:8000/进入登陆页面