**北京科技大学实验报告**

学院：计通学院 专业：信息安全 班级：信安182

姓名： 梁逸飞 学号：41824141 实验日期： 2020年 12月 25日

**实验名称：互认证web登录系统**

**实验目的：**通过设计Web登陆界面和登陆方法，满足多种安全性要求。

**实验原理：**为了设计一个有安全性的登录界面，设置了多种安全机制。本次实验制作的登录网页具有5个安全机制：双向认证、一次性口令、登录权限验证、服务端密码加密存储、建立会话机制。

**实验环境：**tomcat、java、eclipse

**实验内容与步骤：**

一、网页的总体设计

总体设计了5个安全策略，详情请见“网页设计说明文档.docx”文件。

根据每部分安全策略，设计的网页后端包括如下几个部分。



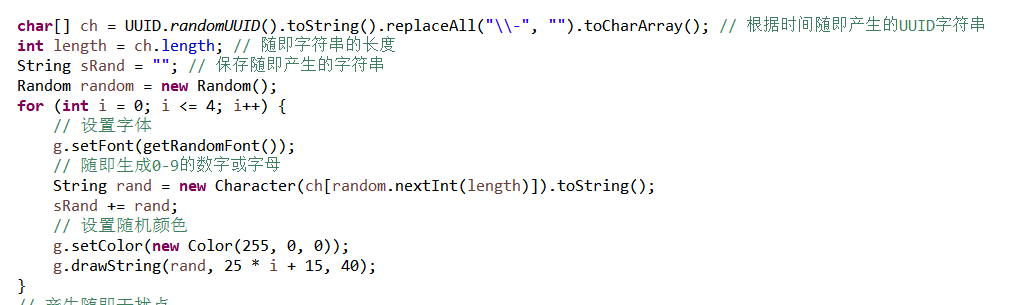
二、网页的详细设计

1、双向认证功能

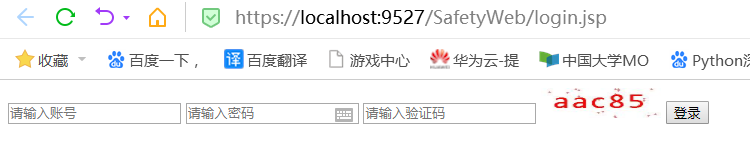
即启用tomcat的HTTPS的双向认证协议。其过程为先生成客户端和服务端的证书并导入，再配置服务器的信息。其详细过程见“网页设计说明文档.docx”中的第一条。

2、一次性口令设计

一次性口令可以防止重放攻击，通过RandomCodeFilter.java过滤器制作一次性口令验证码。核心代码如下。



根据时间变换生成基于时间的UUID字符串，并随机获取其中的5个字符，然后通过java的绘图工具将其绘制成图片。登录界面效果图如下图所示。

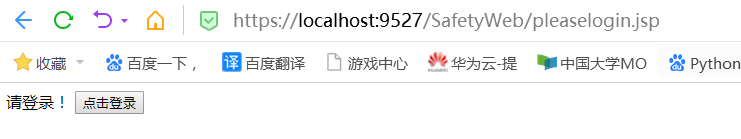


3、登录权限验证

登录权限验证主要是用于保护用户信息和资源。其主要是通过UserLoginFilter.java过滤器实现的登录拦截。

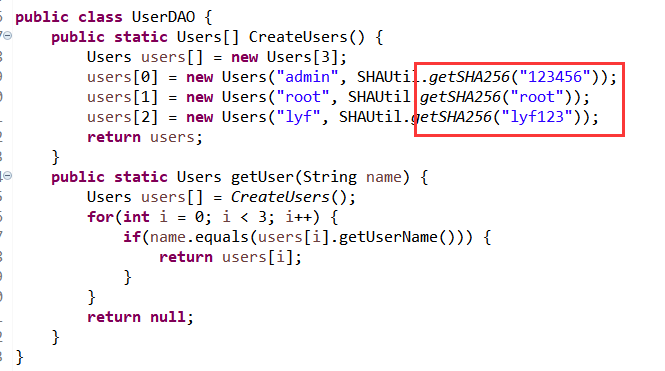


在没有登录的情况下，直接访问位于users下的loginSuccess.jsp页面，即https://localhost:9527/SafetyWeb/users/loginSuccess.jsp这个url地址，会被拦截并跳转到拦截界面pleaselogin.jsp，提示登录。



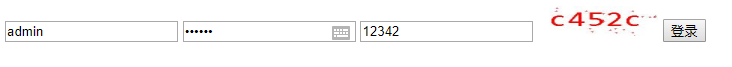
4、服务器端用户密码加密存储

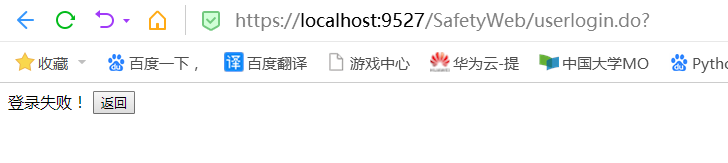
在UserDAO.java中创建用户信息，其密码是利用SHAUtil.java这个工具类通过SHA256进行加密存储。如果有盗取后端存储的账户密码，会得到密文而无法推出明文，是对用户账户的保护。



5、登录验证

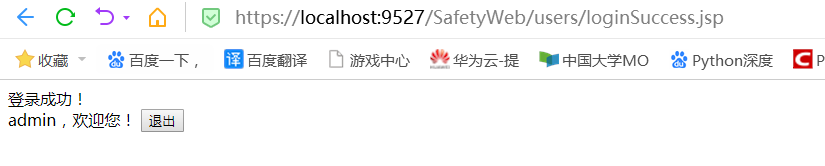
在登录界面，只有输入正确的账号、密码和验证码才能实现登录跳转到users下的loginSuccess.jsp页面，否则会跳转到loginFailed.jsp页面。如果验证码输入错误，也会跳转到登录失败界面。



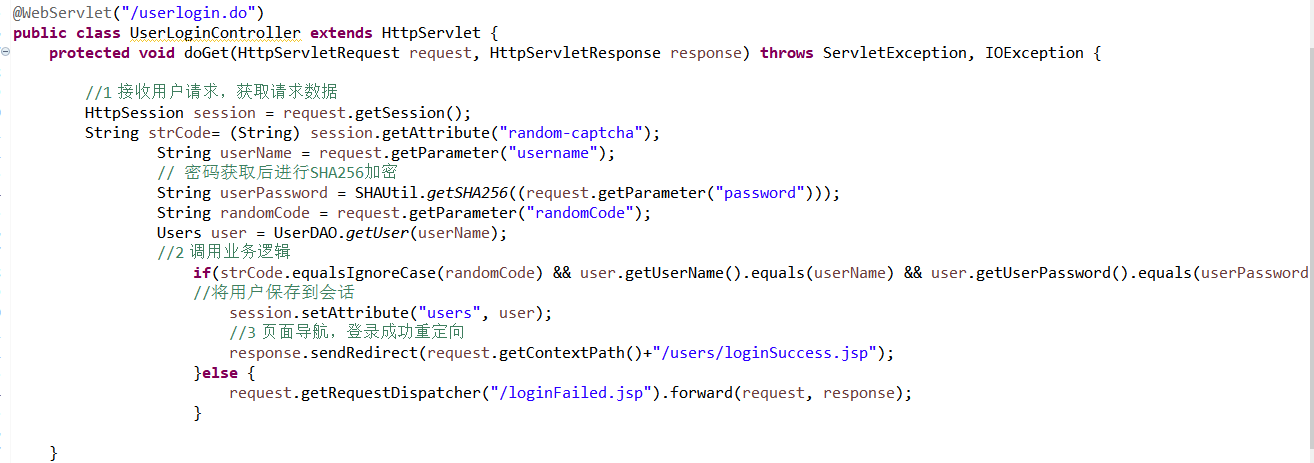


只有三个都输入正确时，才会跳转登录成功。





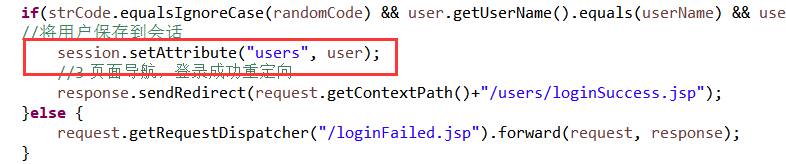
登录验证功能是在登录控制器UserLoginController.java中实现的，代码如下。



控制器会根据网页前端获取输入的账户、密码和验证码，根据输入的账户获取后端存储的对应的密码，然后判断密码和验证码是否与正确的相同。由于前端密码是明文，后端密码是密文，所以需要将前端获取的密码通过SHA256进行加密，将二者密文进行比较，如果密文相同，则说明密码输入正确。

6、建立会话机制

登录成功后，在登录控制器UserLoginController.java中会将用户信息保存到session当中，退出的时候会在退出控制器UserLogoutController.java中清除session当中的用户信息。





**实验结果与分析：**

通过自己设计互认证web登录系统，实现各种安全策略，对各种安全性检测和设置有了更深的认识和了解，同时也明白了网页制作中需要考虑的诸多安全隐患，避免这些不安全设计，才能更好的保护用户资源信息，被用户信赖使用。