|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **年级、专业、班级** | | **2018级计算机科学与技术04班/2018级信息安全专业02班/2018级信息安全专业02班** | | | **姓名** | **蒋莹倩/廖然/王青** |
| **实验题目** | **单点登录系统的设计与实现** | | | | | |
| **实验时间** | **2020.9.29~2020.10.29** | | **实验地点** | **DS3 401** | | |
| **实验成绩** |  | | **实验性质** | **□验证性 □设计性 ■综合性** | | |
| 教师评价：  □算法/实验过程正确；□源程序/实验内容提交 □程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； □报告规范；  其他：  评价教师签名： | | | | | | |
| 一、实验目的  利用Java EE技术实现一个单点登录系统，用户仅需要在该系统中登录一次，即可以访问互信的多个应用系统。 | | | | | | |
| 二、实验项目内容  1、实现2个简单的、需要用户登录才能使用的应用系统，这2个应用称为系统A和系统B。  2、设计实现一个单点登录系统。  3、将系统A和系统B与单点登录系统进行集成。  4、从单点登录系统登录后，可以直接访问系统A和系统B。  5、未登录状态下访问系统A或者系统B，跳转到单点登录系统。  6、在实验中使用git进行源代码管理。  7、在实验中用maven打包构建应用程序。  8、程序采用MVC架构。 | | | | | | |
| 1. 实验过程或算法（源程序）   本组实现基于OAuth2.0协议的SSO单点登陆系统。   1. OAuth2.0 协议   1.1 基本概念  OAuth2.0是OAuth协议的延续版本，但不向前兼容OAuth 1.0。OAuth 2.0关注客户端开发者的简易性。要么通过组织在资源拥有者和HTTP服务商之间的被批准的交互动作代表用户，要么允许第三方应用代表用户获得访问的权限。  1.2 协议的参与者  从基本概念中得出OAuth的参与实体有如下四个：  ·RO (resource owner): 资源所有者，对资源具有授权能力的人。即用户。  · RS (resource server): 资源服务器，它存储资源，并处理对资源的访问请求。如Google资源服务器，它所保管的资源就是用户Alice的照片。  · Client: 第三方应用，它获得RO的授权后便可以去访问RO的资源。如网易印像服务。  · AS (authorization server): 授权服务器，它认证RO的身份，为RO提供授权审批流程，并最终颁发授权令牌(Access Token)。  1.3 授权类型  OAuth2.0为了支持这些不同类型的第三方应用，提出了多种授权类型，如授权码 (Authorization Code Grant)、隐式授权 (Implicit Grant)、RO凭证授权 (Resource Owner Password Credentials Grant)、Client凭证授权 (Client Credentials Grant)。本组则实现授权码(Authorization Code Grant)类型。  授权码类型的开放授权流程图如下：    具体描述如下：  (1) Client初始化协议的执行流程。Redirect\_URI中应包含如下参数：client\_id, scope (描述被访问的资源), redirect\_URI (即Client的URI), state (用于抵制CSRF攻击). 此外，请求中还可以包含access\_type和approval\_prompt参数。  (2) AS认证RO身份，并提供页面供RO决定是否批准或拒绝Client的此次请求。  (3) 若请求被批准，AS使用步骤(1)中Client提供的redirect\_URI重定向RO用户代理到Client。若请求被拒绝，AS将通过redirect\_URI返回相应的错误信息。  (4) Client拿authorization\_code去访问AS以交换所需的access\_token。Client请求信息中应包含用于认证Client身份所需的认证数据，以及上一步请求authorization\_code时所用的redirect\_URI。  (5) AS在收到authorization\_code时需要验证Client的身份，并验证收到的redirect\_URI与第3步请求authorization\_code时所使用的redirect\_URI相匹配。如果验证通过，AS将返回access\_token，以及refresh\_token（交换并刷新令牌）。  1.4授权码类型的时序图     1. 类的UML图   以下为授权码参与者和SSO中对应情况  Client -- 项目APP8081、项目APP8082  RS、AS -- 项目Server  RO -- 项目Server中User类  APP8081：      Server：    Server 实现包装   1. 数据库相关   数据库使用MySQL，并采用JDBC对接远程数据库完成操作。  主要步骤为:  ·注册驱动  ·获得链接  ·得到操作数据库sql语句的对象  ·执行  ·获得结果 集合  ·关闭资源 | | | | | | |
| 四、实验结果及分析和（或）源程序调试过程  见 SSO结果演示.mp4 | | | | | | |