技术选型表-Version1

2017.04.09 白微，李伽泽

项目	Mobile App	Web App	备注
1 终端支持	□ Android	□ PC □ Pad □ Phone	执行人： 白微，李伽泽
1.1 开发语言框架	□ Java □ Android	□ HTML 5 □ CSS 3 □ JavaScript	
1.2 响应式布局框架	□RxJava	□ BootStrip	
1.3 传感器	□ GPS □ 距离	□ GPS	
2.服务端支持			
2.1 语言	□ JAVA	□ JAVA	
2.2 web 框架	□ SpringMVC	□ SpringMVC	
2.3 ORM 框架		□ Hibernate	
2.4 关系数据库	□ SQLiteDatabase	□ MySQL	
2.5 数据缓存（非关系）	□ SharedPreference	□ NoSQL □ Redis □ MangoDB	
2.7 负载均衡机制	□ Ngin	□ Ngin	

2.8 消息中间件	□ ZeroMQ	□ ZeroMQ	
2.9 其他第三方组件	□ 百度地图 API	□ 百度地图地图 API	
3.开发平台工具			
3.1 IDE	Intelliji IDEA		
3.2 集成与测试			
3.3 源代码管理	□ Github	□ Github	

2、技术原型开发内容

2.1 列出项目技术风险元素。例如：获取手机 ID 或 Mac；印刷体识别等等

1. 隐私数据

   外部存储安全和内部存储安全

   用户名、密码、聊天记录、配置信息等隐私信息是否被保存在本地，是否加密保存

   使用数据前都判断信息是否被篡改

2. 权限攻击

   检查 App 所在的目录，其权限必须为不允许其他组成员读写

   检查系统权限是否受到攻击

3. 数据通信

   软件与软件的通信安全，主要是意图不被其他程序截获

   软件与网络服务器的通信安全，即检查敏感信息在网络传输中是否做了加密处理

   防止暴力破解用户名、密码

4. 运行时解释保护

   对于嵌有解释器的软件，检查是否存在 XSS、SQL 注入漏洞

使用 webiew 的 App，检查是否存在 URL 欺骗漏洞

5. Android 组件权限保护

禁止 App 内部组件被任意第三方程序调用

禁止 Activity 被任意第三方程序调用

禁止 Activity 劫持

Broadcast 的接收和发送安全，只能接收本程序发出的广播，发送的内容不想让第三方获得

禁止恶意的启动或者停止 service

Content provider 的操作权限

若需要供外部调用的组件，应检查对调用者是否做了签名限制

6. 升级

检查是否对升级包的完整性、合法性进行了校验，避免升级包被劫持

7. 第三方库

如果使用了第三方库，需要跟进第三方库的更新并且检查第三方库的安全性

8. ROM 安全

使用官方 ROM 或者权威团队提供的 ROM，避免 ROM 中被添加了植入广告、木马等

9. 对抗反破解

对抗反编译，即无法通过反编译工具对其进行反编译，或者反编译之后无法得到正确的反汇编代码

对抗静态分析，采用代码混淆技术，代码加密

对抗动态调试，在软件中加入检测调试器和模拟器的代码

防止重编译，检查签名、校验编译之后 dex 文件的 Hash 值

名称	含义
detect_addJavascriptInterface	Webview组件远程代码执行漏洞
detect_openFileOutput	全局文件可读写漏洞
detect_AllowAllHostnameVerifier	HTTPS关闭主机名验证
detect_Intent_parserUri	Intent Scheme URL攻击漏洞
detect_onReceivedSslError	WebView忽略SSL证书错误
detect_intent_action	APP存在隐式意图调用
detect_custom_x509_trust_manager	自定义SSL x509 TrustManager，信任任意证书漏洞
detect_dexclassloader	Dex文件动态加载风险
detect_getSharedPreferences	配置文件可读写漏洞
detect_securerandom	随机数不安全使用风险
detect_unsecure_encrypt	加密方法不安全使用风险
detect_webview_searchboxjavabridge	Webview组件系统隐藏接口漏洞
readable	App存在全局可读文件
writable	App存在全局可写文件
sql_inject	本地sql注入漏洞
Logcat_Dos_Service	拒绝服务漏洞

2.2 给出验证性的程序开发方案或技术原理

1.影院售票系统的架构是基于 Jsp/JavaBean 的模式，这种模式以其稳定性和优越的速度，被全球企业证明公认为可以高效稳定的进行企业运算开发的平台。

2.本平台　利用现在比较广泛的 JSP+Oracle 数据库的架构实现的。完成一个完整的影院售票系统，分为影院内部管理和网络服务 2 个系统，影院内部管理子系统主要实现影院售票员对影院的售票功能，网络服务实现网上查询浏览约定电影院功能。这些功能可以分为以下二部个部分：前台管理，后台管理。

前台现场售票：电影名称，票价，票价打折，售票，座位，打印票，结帐

后台管理模块： 管理员主要用于电影类型管理：添加电影种类，介绍，票价，

放映场次，放映时间，放映大厅，近几日放映订划管理。具体的功能可以分为以下几个部分：影院介绍，预订电影

3.系统的建设关键在于其所使用的架构，而影院网上售票这种基于 web 的系统，传统的 c/s 架构已经不能满足大量用户的访问和操作，b/s 基于浏览器的架构则是目前网络系统应用的主流，它将大量的数据处理工作交给服务器端来处理，客户端只用通过普通的 IE 浏览器即可访问系统，方便快捷而且利于系统的更新和维护，java 语言在该方面更是得天独厚，j2ee 规范的出现则使系统的开发更加规范，层次更加清楚，更利于对复杂事务的处理，而且在安全性方面也做的更好。基于 mvc 的开发流程则使开发过程更加清晰明了，利于做一些复杂的逻辑实现，从而节省了开发周期和开发成本。