**威海南海房产交易及产权管理平台系统安全测试报告**

**系统名称：威海南海房产交易及产权管理平台**

**版本号：v1.0**

**测试时间：2019年4月10日**

目录

**[1. 测试目的](#_Toc15600_WPSOffice_Level1)** **[5](#_Toc15600_WPSOffice_Level1)**

**[2. 测试依据](#_Toc24963_WPSOffice_Level1)** **[6](#_Toc24963_WPSOffice_Level1)**

[2.1. 参考依据](#_Toc24963_WPSOffice_Level2) [6](#_Toc24963_WPSOffice_Level2)

[2.2. 用户文档](#_Toc18266_WPSOffice_Level2) [6](#_Toc18266_WPSOffice_Level2)

**[3. 测试范围及对象](#_Toc18266_WPSOffice_Level1)** **[6](#_Toc18266_WPSOffice_Level1)**

[3.1. 系统概述](#_Toc28739_WPSOffice_Level2) [6](#_Toc28739_WPSOffice_Level2)

[3.2. 测试方法和测试工具](#_Toc25777_WPSOffice_Level2) [7](#_Toc25777_WPSOffice_Level2)

[3.3. 验证输入安全](#_Toc32410_WPSOffice_Level2) [7](#_Toc32410_WPSOffice_Level2)

[3.4. 访问控制安全](#_Toc15669_WPSOffice_Level2) [7](#_Toc15669_WPSOffice_Level2)

[3.5. 安全配置错误](#_Toc18069_WPSOffice_Level2) [7](#_Toc18069_WPSOffice_Level2)

[3.6. 缓冲区溢出](#_Toc23631_WPSOffice_Level2) [8](#_Toc23631_WPSOffice_Level2)

[3.7. 敏感数据泄露](#_Toc16704_WPSOffice_Level2) [8](#_Toc16704_WPSOffice_Level2)

[3.8. 不安全的配置管理](#_Toc11520_WPSOffice_Level2) [8](#_Toc11520_WPSOffice_Level2)

[3.9. 注入式漏洞](#_Toc13108_WPSOffice_Level2) [9](#_Toc13108_WPSOffice_Level2)

[3.10. 不恰当的异常处理](#_Toc14514_WPSOffice_Level2) [9](#_Toc14514_WPSOffice_Level2)

[3.11. 不安全的存储](#_Toc17052_WPSOffice_Level2) [9](#_Toc17052_WPSOffice_Level2)

[3.12. 跨站脚本（XSS）](#_Toc28063_WPSOffice_Level2) [9](#_Toc28063_WPSOffice_Level2)

[3.13. 使用含有已知漏洞的组件](#_Toc2693_WPSOffice_Level2) [10](#_Toc2693_WPSOffice_Level2)

[3.14. 不足的日志记录和监控](#_Toc12662_WPSOffice_Level2) [10](#_Toc12662_WPSOffice_Level2)

[3.15. 不安全的反序列化](#_Toc32106_WPSOffice_Level2) [11](#_Toc32106_WPSOffice_Level2)

**[4. 测试工具](#_Toc28739_WPSOffice_Level1)** **[11](#_Toc28739_WPSOffice_Level1)**

**[5. 测试环境与配置](#_Toc25777_WPSOffice_Level1)** **[11](#_Toc25777_WPSOffice_Level1)**

[硬件环境](#_Toc27173_WPSOffice_Level2) [11](#_Toc27173_WPSOffice_Level2)

[软件环境](#_Toc14684_WPSOffice_Level2) [11](#_Toc14684_WPSOffice_Level2)

**[6. 测试结论](#_Toc32410_WPSOffice_Level1)** **[11](#_Toc32410_WPSOffice_Level1)**

# 测试目的

本报告对威海南海房产交易及产权管理平台项目在应用安全和数据安全两个方面进行安全测评，目的在考察系统安全性、稳定性、健壮性，根据被测系统的安全现状，给出测评结果并提出整改意见。

# 测试依据

## 参考依据

开放式Web应用程序安全项目（OWASP，Open Web Application Security Project）十大web漏洞

## 用户文档

《威海南海房产交易及产权管理平台需求规格说明书》、《威海南海房产交易及产权管理平台使用手册》

# 测试范围及对象

本次测评在测试环境中进行，安全测试范围包括应用安全和数据安全两个方面。

## 系统概述

在有效保障建设方现有信息化建设基础投资成本，业务数据及业务流程平滑过渡的前提下，针对房屋交易业务对数据、业务一体化存储及动态实时检索的要求，以楼盘表为核心对现有数据存储及业务支持平台进行升级改造，要求系统数据库及程序以升扩模式进行从而保障升级后系统数据的完整及业务连续，并完成相应的数据调查迁移整合入库工作，全面适应威海市房屋交易与产权管理工作的新需求。

系统建设内容包含商品房销售管理系统、楼盘管理系统、资金监管系统、测绘成果管理系统、商品房销售许可证管理系统。子系统之间的数据调用接口，包括：威海市不动产系统的数据接口开发、维修基金系统数据接口开发、硬件设备数据接口开发、其他第三方系统的对接。

系统采用JAVA语言开发遵循J2EE规范，基于B/S架构，服务器采用windows服务器和Oracle数据库。

## 测试方法和测试工具

威海南海房产交易及产权管理平台系统主要使用了验证输入安全、访问控制安全、安全配置错误、缓冲区溢出、敏感数据泄露、不安全的配置管理、注入式漏洞、使用含有已知漏洞的组件、不足的日志记录和监控、不安全的反序列化等安全测试方案。针对以上提供的测试方案进行对应的测试用例和测试脚本编写，并使用Websecurify作为测试工具。

## 验证输入安全

威海南海房产交易及产权管理平台统主要对没有被验证的输入进行如下测试：数据类型（字符串，整型，实数，等）、允许的字符集、最小和最大的长度、是否允许空输入、参数是否是必须的、重复是否允许、数值范围、特定的值（枚举型）、特定的模式（正则表达式）。

测试结果：测试通过。

## 访问控制安全

需要验证用户身份以及权限的页面，复制该页面的url地址，关闭该页面以后，查看是否可以直接进入该复制好的地址

例：从一个页面链到另一个页面的间隙可以看到URL地址直接输入该地址，可以看到自己没有权限的页面信息。

测试结果：测试通过。

## 安全配置错误

安全配置错误是最常见的安全问题，这通常是由于不安全的默认配置、不完整的临时配置、开源云存储、错误的 HTTP 标头配置以及包含敏感信息的详细错误信息所造成的。因此，我们不仅需要对所有的操作系统、框架、库和应用程序进行安全配置，而且必须及时修补和升级它们。

## 缓冲区溢出

没有加密关键数据

例：view－source：http地址可以查看源代码

在页面输入密码，页面显示的是 \*\*\*\*\*, 右键，查看源文件就可以看见刚才输入的密码。

## 敏感数据泄露

许多Web应用程序和API都无法正确保护敏感数据，例如：财务数据、医疗数据和PII数据。攻击者可以通过窃取或修改未加密的数据来实施信用卡诈骗、身份盗窃或其他犯罪行为。未加密的敏感数据容易受到破坏，因此，我们需要对敏感数据加密，这些数据包括：传输过程中的数据、存储的数据以及浏览器的交互数据。

测试结果：测试通过。

## 不[安全](http://security.chinaitlab.com/" \t "_blank)的配置管理

Config中的链接字符串以及用户信息，邮件，数据[存储](http://www.storworld.com/" \t "_blank)信息都需要加以保护

程序员应该作的： 配置所有的[安全](http://security.chinaitlab.com/" \t "_blank)机制，关掉所有不使用的服务，设置角色权限帐号，使用日志和警报。

用户使用缓冲区溢出来破坏web应用程序的栈，通过发送特别编写的代码到web程序中，攻击者可以让web应用程序来执行任意代码。

测试结果：测试通过。

## 注入式漏洞

将不受信任的数据作为命令或查询的一部分发送到解析器时，会产生诸如SQL注入、NoSQL注入、OS注入和LDAP注入的注入缺陷。攻击者的恶意数据可以诱使解析器在没有适当授权的情况下执行非预期命令或访问数据：

　　如果使用的sql语句为：

　　Select \* from table A where username＝’’ + username+’’ and pass word …..

　　Sql 输入 ‘ or 1＝1 ―― 测试是否可以不输入任何password进行攻击或者是半角状态下的用户名与密码均为：‘or’‘=’。

测试结果：对sql进行拦截过滤，测试通过。

## 不恰当的异常处理

程序在抛出异常的时候给出了比较详细的内部错误信息，不应该暴露显示的执行细节，检测网站是否存在潜在漏洞。

测试结果：测试通过。

## 不安全的[存储](http://www.storworld.com/" \t "_blank)

帐号列表：系统不应该允许用户浏览到网站所有的帐号，如果必须要一个用户列表，推荐使用某种形式的假名（屏幕名）来指向实际的帐号。

浏览器缓存：认证和会话数据不应该作为GET的一部分来发送，应该使用POST。

测试结果：测试通过。

## 跨站脚本（XSS）

1、跨网站的入侵字串(Cross Site Scripting，简称XSS，亦称為跨站脚本攻击)：Web应用程式直接将来自使用者的执行请求送回浏览器执行，使得攻击者可窃取使用者的Cookie或Session资料而能假冒直接登入为合法使用者。

测试方法：

　　● HTML标签：<…>…</…>

　　● 转义字符：&(&)；<(<)；>(>)； (空格) ；

　　● 脚本语言：

　　<script. language=‘javascript’>

　　…Alert(‘’)

　　</script>

　　● 特殊字符：‘ ’ < > /

　　● 最小和最大的长度

　　● 是否允许空输入

测试结果：测试通过。

## 使用含有已知漏洞的组件

组件（例如：库、框架和其他软件模块）拥有和应用程序相同的权限。如果应用程序中含有已知漏洞的组件被攻击者利用，可能会造成严重的数据丢失或服务器接管。同时，使用含有已知漏洞的组件的应用程序和API可能会破坏应用程序防御、造成各种攻击并产生严重影响。

测试结果：测试通过。

## 不足的日志记录和监控

不足的日志记录和监控，以及事件响应缺失或无效的集成，使攻击者能够进一步攻击系统、保持持续性或转向更多系统，以及篡改、提取或销毁数据。大多数缺陷研究显示，缺陷被检测出的时间超过200天，且通常通过外部检测方检测，而不是通过内部流程或监控检测。

测试结果：测试通过。

## 不安全的反序列化

不安全的反序列化会导致远程代码执行。即使反序列化缺陷不会导致远程代码执行，攻击者也可以利用它们来执行攻击，包括：重播攻击、注入攻击和特权升级攻击。

测试结果：测试通过。

# 测试工具

|  |  |  |  |
| --- | --- | --- | --- |
| **工具名称** | **用途** | **生产厂商** | **版本** |
| Websecurify | 安全测试工具 | Parasoft | 0.9 |

# 测试环境与配置

在此次项目的测试中，所使用到的环境和配置见下表：

**硬件环境**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **服务器** | **厂商/型号** | **配置/数量** | **IP** | **操作系统** |
| 1 | 云主机 | 20008R2 | 1 | 192.168.192.202 | windowsServer |

**软件环境**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **系统软件** | **厂商** | **版本** | **备注** |
| 1 | JDK | Oracle | 1.8.0\_191-b12 |  |
| 2 | Tomcat | apache | 8.5.39 |  |
| 3 | Oracle | Oracle | 11g |  |

# 测试结论

1、本次测试覆盖全面，测试数据基础合理，测试有效。

2、SQL注入测试，已执行测试用例，问题回归后测试通过

3、跨站脚本测试，测试发现文本框对尖括号、百分号、单引号、圆括号、双引号进行了转义，测试通过。

4、跨目录测试，已执行测试用例，路径已加密，无漏洞，测试通过。

5、用户权限控制和权限数据控制安全测试，已执行测试用例，问题经回归后测试通过。

6、应用系统提供专用的登录控制模块对登录的用户进行身份识别和鉴别，对用户口令有复杂度要求，有登录失败处理功能；系统访问控制功能有效，限制了非法用户的访问权限；系统有安全审计功能，审计策略覆盖用户登入登出、用不操作等等。

7、应用系统将用户信息的MD5值存储于数据库中以实现数据信息的存储保密性，每天定时对数据库中的数据进行全量备份。

综合以上结论得出本次安全测试通过。