****

**微信城市服务**

**安全开发规范**

**1、背景说明**

为减少城市服务业务开发过程中产生的安全漏洞问题，特制定本规范。

本文档主要包括安全开发的原则、流程以及安全检查表等，提出城市服务业务应达到的安全要求，并提出安全开发的方法和流程，保障业务的安全性。适用于城市服务中涉及的web程序、web应用。

**2、常见安全检查**表

对每个漏洞没有做详细的阐述，这里只列举在城市服务中出现的漏洞以及简单的介绍。

### 2.1 XSS

* 输入校验：长度限制、值类型是否正确、是否包含特殊字符（如<>’”等）
* 输出编码：根据输出的位置进行相应的编码，如HTML编码、JavaScript编码、URL编码。
* 输出到HTML标签之间时，对这些数据进行HTML Entity编码。
* 输出到HTML属性里时，特殊字符编码为 &#xHH;
* 输出到SCRIPT里时，对这些数据进行SCRIPT编码，除了阿拉伯数字和字母，对其他所有的字符进行编码，只要该字符的ASCII码小于256。编码后输出的格式为 \xHH
* 输出到Style属性里时，对这些数据进行CSS编码，除了阿拉伯数字和字母，对其他所有的字符进行编码，只要该字符的ASCII码小于256。编码后输出的格式为 \HH
* 输出到HTML URL里时，对这些数据进行URL编码，当需要往HTML页面中的URL里插入不可信数据的时候，需要对其进行URL编码

### 2.2 SQL注入

* 最佳方式就是使用预编译语句，绑定变量
* 检查数据类型
* 使用安全函数，例如php的mysql\_real\_escape\_string
* 从数据库自身来说，应使用最小权限原则，切记不要使用dba权限

### 2.3 上传漏洞

* 在客户端和服务器端对用户上传的文件名和文件路径等项目分别进行严格的检查，尤其是服务端检测不能少
* 服务器端的检查最好使用白名单过滤的方法，比如只允许jpg文件上传等
* 上传目标路径尽量不在web目录下，如果在web目录下去掉该目录的可执行权限
* 慎用Fckeditor、ewebeditor等第三方上传组建，历史上曾出现多个漏洞

### 2.4 Struts2

历史上Struts2框架出过多个高危漏洞，这些漏洞足以黑掉一个网站，要尽量使用最新版本。

### 2.5信息泄漏

* 线上机器删掉测试页面，例如test.html，phpinfo.php等
* 禁掉详细的错误提示
* 禁止显示调试信息
* 禁止将svn相关的文件更新到线上机器，例如.svn/entries

### 2.6 登录安全

* 登录页面最好加入验证码
* 尽量使用https协议

### 2.7 会话安全

公众号开发中通常将openid作为用户身份标识，使用openid时要将openid设置到cookie中不要拼接到URL中例如http://www.qq.com/getuser?code=aaaaaa

### 2.8管理页面

Tomcat、jboss、weblogic等管理页面可以做以下加个方面的安全策略

* 使用白名单的方式限制可以登录的IP
* 如果不使用这些管理界面直接删掉

### 2.9 平行权限问题

像订单等场景需要格外注意平行权限问题，例如order?Id=111，是否order?Id=112就可以看到其他的订单。对于这种情况的防御，可以加入校验参数，order?Id=111&sign=hash(字符串常量+id)

### 2.10 支付金额

* 涉及到微支付的web应用一定要严格按照https://pay.weixin.qq.com/wiki/doc/api/index.html的文档设计
* 确定用户的支付金额与应付金额是否相等