Web 应用的安全性防护策略

一、 web 安全的重要性

随着网络安全的发展，web 应用软件也变得越来越普及。然而一个好的 web 应用，十分重要的一点便是安全性问题。作为一个二手交易平台，既要保护用户的交易安全和信息安全也要保护好管理员的权限。

在用户交易时，要保证交易的内容与个人信息不泄露，付款时保证交易的安全性；用户上传内容时，保证用户所上传的内容与商品实际信息相符等。

整个网站的用户体验都是建立在安全的基础之上，所以保护 Web 应用的安全至关重要。

二、 保证 web 安全所用到的技术

1. Spring Security

Spring Security 是一个能够为基于 Spring 的企业应用系统提供声明式的安全访问控制解决方案的安全框架。、问控制功能，减少了为企业系统安全控制编写大量重复代码的工作。

Spring Security 安全框架主要包括两个操作“用户认证”与“用户授权”。

用户认证指的是验证某个用户是否为该 web 应用系统中的合法主体，也就是说用户能否访问该系统。用户认证一般要求用户提供用户名和密码。系统通过校验用户名和密码来完成认证过程。用户授权指的是验证某个用户是否为该系统的管理员，是否有权限执行某个操作或查看某些内容。在一个系统中，不同用户所具有的权限是不同的。比如对一个文件来说，有的用户只能进行读取，而有的用户可以进行修改。一般来说，系统会为不同的用户分配不同的角色，而每个角色则对应一系列的权限。

在该项目中我们定义两个角色，管理员和用户。Spring security 可以主要用于验证用户是否为该平台合法主体以及登录者是否拥有管理员权限。在管理员的相关页面插入 spring security 框架，筛选用户名或密码不正确的用户阻止进入该系统，同时如果使用者想要登录管理员界面，系统会自动调用相关文件中的信息查询用户是否有此权限，如果有权限那么会登入管理员界面进行相关的管理员操作；如果没有权限，那么则会转至“无此权限”的页面，阻止非管理员用户获得更多资源。

2. Shiro 安全框架

Apache Shiro 是 Java 的一个安全框架。功能强大，使用简单的 Java 安全框架，它为开发人员提供一个直观而全面的认证，授权，加密及会话管理的解决方

案。

Shiro 的主要功能是管理应用程序中与安全相关的全部，同时尽可能支持多种实现方法。Shiro 是建立在完善的接口驱动设计和面向对象原则之上的，支持各种自定义行为。Shiro 提供的默认实现，使其能完成与其他安全框架同样的功能。

Apache Shiro 相当简单，对比 Spring Security，可能没有 Spring Security 做的功能强大，但是在实际工作时可能并不需要那么复杂的东西，所以使用小而简单的 Shiro 就足够了。

在本项目中，我们主要使用 Shiro 安全框架来验证用户身份以及控制用户访问的内容，使用 Authentcation 和 Authorization 的功能来保证该二手物品交易平台的安全性。

a) Authentication：身份认证/登录，验证用户是不是拥有相应的身份；
b) Authorization：授权，即权限验证，验证某个已认证的用户是否拥有某个权限；即判断用户是否能做事情，常见的如：验证某个用户是否拥有某个角色。或者细粒度的验证某个用户对某个资源是否具有某个权限；

3. 对于 SQL 注入的防范

SQl 注入就是通过把 SQL 命令插入到 Web 表单递交或输入域名查或页面请求查询的字符串，最终达到欺骗服务器额、执行恶意的 SQL 命令。

当我们用参数拼接的方法构造此类 SQL 语句时，一旦黑客们在前台文本框或 URL 填上 Aaa’ or 1=1 一旦这个参数传入后代中，这一句 SQL 就会成立在假定系统的表结构或某些表的名称，甚至可以在后面加入删除表或数据的语句，后果不堪设想。

对于 SQL 注入的防范：

1) 永远不要信任用户的输入，对用户的输入进行校验，可以通过正则表达式，或者限制长度，对单引号和双“-”进行转换等。
2) 尽量不要使用拼装 SQL 的方式进行数据库操作。Java 可以采用预编译的方式也可以有效的防止 SQL 注入，或者使用一些持久层框架。
3) 没有必要不要使用管理员权限连接的数据库。
4) 对于异常信息不要暴漏给用户，防止不法分子利用异常测试表结构。

4. 用函数检查用户提交信息

在 web 攻击中最常见的方法之一是 xss 攻击，它获取用户的联系人列表，然后向联系人发送虚假诈骗信息，可以删除用户的日志等等，有时候还和其

他攻击方式同时实施比如 SQL 注入攻击服务器和数据库、Click 劫持、相对链接劫持等实施钓鱼。所以我们首先要避免的就是 xss 攻击。

我们需要在用户提交表单或留言内容时，过滤内容，检查其中是否有非法字符，可以编写一个过滤 html、css、jsp 字符之后检查提交的内容中的是否含有非法字符。如果含有非法字符那么就阻止内容的下一步提交，不含则允许内容提交。

可能需要用到的函数有以下这些：htmlspecialchars() 函数,用于转义处理在页面上显示的文本。

htmlentities() 函数,用于转义处理在页面上显示的文本。

strip_tags() 函数,过滤掉输入、输出里面的恶意标签。

header() 函数,使用 header("Content-type:application/json"); 用于控制 json 数据的头部，不用于浏览。

urlencode() 函数,用于输出处理字符型参数带入页面链接中。

intval() 函数用于处理数值型参数输出页面中。

自定义函数,在大多情况下，要使用一些常用的 html 标签，以美化页面显示，如留言、小纸条。那么在这样的情况下，要采用白名单的方法使用合法的标签显示，过滤掉非法的字符。

三、总结

对于二手物品交易平台，我们在 Web 应用的安全性方面做了基本的防范策略，主要集中在用户的身份验证，权限识别和数据保护方面，但对于在该平台上传的信息的验证等方面还需要进一步加强，进一步提高该系统的安全性。