关于建立“高校在线答疑系统”

安全性防护策略

西安电子科技大学软件学院

二O一八年六月

**安全性防护策略**

1. 应用系统存在的安全问题分析

Web应用系统存在着诸多威胁，例如：被恶意篡改网页内容、窃取重要内部数据、植入恶意代码等。操作系统和后台数据库的漏洞和配置不当，发布系统存在安全漏洞，都会导致黑客和病毒可以利用这些缺陷攻击网站。开发人员在编程过程中忽略安全方面的考量，也会给入侵者可趁之机。因此，在Web应用开发过程中，对Web应用平台安全防护性的设计和开发尤为重要。

1. 主要的安全性防护策略

为了保证整个答疑系统的安全，可以从以下几个方面加强防护:

1. 使用Spring Security实现安全访问控制。对系统中的每个操作定义权限，为系统设置管理员和权限组。建立登录验证过滤器，该过滤器可用于在管理员登录时进行日志记录等相关操作。
2. 通过部署在服务端，保障Web服务器平台的安全，防御攻击者破坏平台或者窃取重要数据，同时保障平台对外提供服务的正常运行，不影响用户的正常使用。
3. 获取服务器运行状态系统信息，以便于管理员了解当前运行状态，包括实时性能、进程运行状态、TCP和UDP网络连接状态等，以便于管理员定位安全问题的来源。
4. 结合应用开发周期，通过安全检查、人工检查、渗透测试、代码审计、架构分析等方法，全面发现Web应用本身的脆弱性及系统架构导致的安全问题。应用程序的安全问题可能是在软件生命周期的各个阶段产生的。
5. 对应用代码、数据库等进行加固，改善其应用部署的合理性，从补丁、管理接口、账号权限、文件权限、通信加密、日志审核等方面对应用支持环境和应用模块间部署方式划分的安全性进行增强。
6. 持续地检测被保护应用页面的当前状态，判断页面是否被攻击者加入恶意代码，通过检测Web访问日志及Web程序存放目录，检测是否存在文件篡改及是否被加入Web Shell一类的网页后门。
7. 经常对数据进行备份，并将数据存放在安全的场所。
8. 运行监视入站和出站通信的病毒检查程序。
9. 提高Web应用程序的安全系数，开发过程前要设计出周密详细的思路对Web页面进行加密与验证处理，只有部署安全系数较高的Web应用才能从根本上解决Web应用层面的安全问题。
10. 根据业务需求配置安全系数相对较高的Web服务。
11. 创建Web防御检测系统，使用该系统对Web应用的运行情况进行实时监控，快速掌握Web应用安装运行状况并及时采取有针对性的应对策略，将风险降至最低。
12. 建立用户分级和审核制度，对普通用户和管理员分区管理，并设置高安全系数的密码。
13. 开发人员和运维人员了解掌握相关知识，在系统建设阶段和运维阶段同步考虑安全问题，在应用发布前最大程度地减少脆弱点。