Task 12

随着计算机应用的普及和网络的不断发展，网络和信息的安全问题日益突出，网络入侵、攻击和病毒以及不良的有害信息给Web应用的安全性带来了严峻的挑战，因此，基于Web安全性的研究应运而生。

Web应用的安全是Web应用构建、运行、维护与管理过程中最重要的任务之一。它是指一种能够识别和消除网络上对Web应用的硬件、软件、数据等造成破坏的不安全因素的能力，凡是涉及网络上的信息保密性、完整性、可用性、真实性和可控性的相关技术和理论都是Web应用安全的研究领域。

针对Web应用特性及其存在的安全威胁，有一些好的技术和方法可以预防或缓解这些攻击和漏洞：

1. Cloud Security：

云安全技术是P2P技术、[网格](https://baike.baidu.com/item/%E7%BD%91%E6%A0%BC)技术、[云计算](https://baike.baidu.com/item/%E4%BA%91%E8%AE%A1%E7%AE%97)技术等[分布式计算技术](https://baike.baidu.com/item/%E5%88%86%E5%B8%83%E5%BC%8F%E8%AE%A1%E7%AE%97%E6%8A%80%E6%9C%AF)混合发展、自然演化的结果。它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

“云安全”同事也是“云计算”技术的重要分支，它已经在反病毒领域当中获得了广泛应用。云安全技术通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。整个互联网，变成了一个超级大的杀毒软件，这就是云安全计划的宏伟目标。

“云安全”可以是个开放性的系统，其“探针”应当与其他软件相兼容，即是用户使用不同的杀毒软件，也可以享受“云安全”系统带来的成功。

尽管“云安全”系统构建困难，但是“云安全”却给用户带来了巨大的好处。主要表现在病毒查杀能力全面提升，杀毒效率极大提升以及智能帮助用户做出正确的安全决策。

1. Spring Security：

Spring 是一个非常流行和成功的 Java 应用开发框架。Spring Security 基于 Spring 框架，提供了一套 Web 应用安全性的完整解决方案。一般来说，Web 应用的安全性包括用户认证（Authentication）和用户授权（Authorization）两个部分。用户认证指的是验证某个用户是否为系统中的合法主体，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有权限执行某个操作。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。

对于上面提到的两种应用情景，Spring Security 框架都有很好的支持。在用户认证方面，Spring Security 框架支持主流的认证方式，包括 HTTP 基本认证、HTTP 表单验证、HTTP 摘要认证、OpenID 和 LDAP 等。在用户授权方面，Spring Security 提供了基于角色的访问控制和访问控制列表（Access Control List，ACL），可以对应用中的领域对象进行细粒度的控制。

1. Shiro ：

是一个功能强大且易于使用的Java安全框架，可执行身份验证，授权，加密和会话管理，并可用于保护任何应用程序 - 从命令行应用程序，移动应用程序到最大的Web和企业应用程序。

Shiro提供了应用程序安全API来执行以下方面：

（1） 身份验证 - 证明用户身份，通常称为用户“登录”。

（2）授权 - 访问控制

（3） 密码学 - 保护或隐藏窥探数据的数据

（4）会话管理 - 每用户时间敏感状态

Shiro还支持一些辅助功能，例如Web应用程序安全性，单元测试和多线程支持，但这些有助于强化上述四个主要问题。

1. VPN :

VPN(Virtual Private Network，虚拟专用网络)是目前解决信息安全问题的比较新颖、或成功的技术课题之一，是利用密码技术和访问控制技术在公共网络上建立专用信息网络，使数据通过安全的“加密通道”在公共网络中传播。在公共通道上建立VPN有两种主流的机制，这两种机制为路由过滤技术和隧道技术。

VPN主要采取了如下4种技术来保障安全：隧道技术、加解密技术、密匙管理技术、以及使用者与设备身份认证技术。

1. 安全脆弱性扫描技术：

安全脆弱性扫描技术是能针对网络分析系统当前的设置和防御手段，指出系统存在或潜在的安全漏洞，以改进系统对网络入侵能力的一种安全技术。

1. 网络数据储存、备份级容灾规划：

网络数据存储、备份与容灾计划是当系统或设备不幸遇到灾难后就可迅速地恢复数据，使整个系统在最短的时间内重新投入正常运行的一种安全技术方案。

除了上述的方案外，还有其他多种Web安全技术，针对安全威胁，可以采取的安全策略也有很多，比如在web客户机方面，短期可以对浏览器进行设置，如关闭Javascript功能，地址可见等等；长期可以使浏览器具有反应URL信息的功能；设置访问限制等等。在web服务器方面，要保证账户的时效性以及及时删除死账户；要求用户使用安全性好的密码；不要保留不用的服务；定期检查系统日志与web记录以及系统文件；及时对版本进行更新以及打补丁。

没有一种安全技术可以完美解决Web上的所有安全问题，各种安全技术必须相互关联，相互补充，形成Web安全的立体纵深、多层次防御体质。