### 文献综述

对于银行系统来说，快捷方便有效的操作流程是构建银行系统的目的，但网络安全是系统正常运行的首要前提。在目前所能选择的技术实现方案里，或多或少都会存在一定得漏洞，如果没有做好对漏洞的防御，如果被黑客攻击，轻则造成系统崩溃，使用者无法正常使用本系统，重则会篡改数据库中所存储的用户数据，对银行造成重大损失。本系统运行在浏览器上，浏览器是本系统的载体，所以web安全是系统安全中最重要的组成部分，所以如何避免web中存在系统漏洞，以及做好对攻击者的防御是银行系统的重中之重。通过对文献的阅读整理，对于系统漏洞与防御方案，归纳总结为以下几点内容：

1.跨站脚本攻击  
 跨站脚本攻击是指黑客通过“HTML注入”篡改了页面，插入了恶意的脚本，从而在用户浏览网页时，控制用户浏览器的一种攻击。比较常见的场景就是，黑客将包含恶意的Javascript代码的内容在银行系统的客户端中保存，当银行管理员通过浏览器查看黑客用户所保存的内容时，会在管理员的浏览器中执行这段恶意的javascript代码，这段恶意的javascript代码，可能包含很多恶意攻击，比如窃取用户权限，当黑客窃取了管理员的权限后，可以恶意修改用户的数据。  
 对于跨站脚本攻击，可以通过输入检查的方式对黑客输入的恶意javascript代码进行过滤，由于javascript代码在html中执行需要包裹在<script></script>标签内，所以在用户提交数据时检查用户输入是否包含字符'<'和'>'，在发现用户的输入中包含这两种字符后，对这两种字符进行转义。转义后管理员在通过浏览器查看用户输入内容时，由于恶意javascript代码没有了运行的载体，所以可以避免攻击的出现。

2.SQL注入  
 SQL注入指的是把黑客输入的数据当做代码来执行，当黑客输入的数据内容为一段数据库操作的sql语句，原本系统需要通过黑客的数据对数据进行操作，但由于黑客输入的数据为sql语句，导致在正常数据操作的时候混杂了黑客输入的操作语句。通过SQL注入的方式，黑客可以攻击数据库的存储过程，导致数据库瘫痪，系统无法正常运行；也可以恶意篡改正常用户的数据，导致系统数据错乱。  
 对应SQL注入的攻击方式，可以通过对黑客的输入内容进行检查，判断是否为sql语句的方式来防御，但这种防御方式并不完善，由于数据库的字符编码与系统的字符编码可能并不统一，黑客可以通过转码的方式来进行破解。目前主流的防御方式是对输入内容进行检查，并且使用预编译语句的方式来防御。  
使用预编译语句，SQL语句的语意不会发生变化，而且攻击者无法改变SQL的结构，以达到防御的目的。

3.权限管理  
 在系统中，由于业务的需要，可能划分为若干模块，每个模块的操作内容不同，而对应每个模块的操作人可能也不同，所以要区分不同模块使用者的权限，不同模块的使用者不能操作其他模块的内容。  
 当黑客通过某种方式入侵至系统中时，由于黑客获取的可能是某个单一模块的权限，所以黑客只能操作本模块的内容，无法操作其他模块的内容，可以限制黑客的攻击范围，将损失尽量减少。  
 甚至可以将模块的操作分为读权限和写权限，并降低黑客获取写权限的几率，以达到最大程度上限制黑客的攻击范围。

4.加密算法与随机数  
 当黑客已某种方式入侵了系统时，为了防止黑客通过系统的业务接口修改业务数据，可以将重要的业务接口使用加密算法与随机数的方式来校验。系统使用一套唯一的加密算法，当调用系统业务接口时，校验接口参数是否包含的唯一的加密信息。由于黑客只是入侵到系统中，但是并不知道系统唯一加密算法，所以黑客无法通过系统的业务接口调用篡改系统数据。  
 在制定加密算法时，使用随机数与秘钥绑定的方式，由于随机数本身是随机生成的，秘钥又是加密生成的，二者结合后，黑客难以通过常规手段破译加密算法。

5.MVC框架安全  
 在现代web开发中，使用MVC架构是一种流行的做法。MVC架构思想将Web应用分为三层，View层负责用户视图层；controller负责应用的实现，接受View层传入的用户请求，并转发给Model做处理；Model层则负责试下你模型，完成数据处理。  
 在View层中，可以解决跨站脚本攻击的问题，在渲染页面时，使用View层的模板引擎技术，将数据进行转码，避免黑客的恶意javascript脚本攻击，达到防御跨站脚本攻击的目的。  
 在Model层中，使用ORM框架解决SQL注入的问题，由于它是基于sqlmap的，生成的SQL语句都能结构化的写在XML文件中。在SQL中如果包含动态变量，并且黑客能够控制这个变量，则会存在一个SQL注入的漏洞。所以只要搜索所有的sqlmap文件，查看其中是否包含了动态变量，当出现了动态变量，在上层的代码逻辑中对变量进行严格控制，以保证不会出现SQL注入问题。

在以上防御方式完成后，还要制定监控系统，随时监听系统是否被黑客入侵，及时的了解黑客的入侵方式，快速将漏斗降低，最大程度上减少损失。