ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38674—2020

信息安全技术　应用软件安全编程指南

Information security technology—Guideline on secure coding of application software

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家计算机网络应急技术处理协调中心、北京邮电大学、北京奇虎测腾安全技术有限公司、中国电力科学研究院有限公司、上海计算机软件技术开发中心、海通证券股份有限公司、北京银行股份有限公司、信息安全共性技术国家工程研究中心。

本标准主要起草人:舒敏、王博、吴倩、王文磊、黄元飞、张家旺、林星辰、陈禹、王鹏翩、李燕伟、高强、杨鹏、陈亮、范乐君、张晓娜、杜薇、夏剑锋、李晔、张森、徐国爱、郭燕慧、李祺、杨昕雨、王晨宇、葛慧晗、黄永刚、韩建、章磊、王彦杰、胡建勋、李凌。

信息安全技术　应用软件安全编程指南

1　范围

本标准提出了应用软件安全编程的通用框架，从提升软件安全性的角度对应用软件编程过程进行指导。

本标准适用于客户端/服务器架构的应用软件开发，其他架构的应用软件开发也可参照使用，并根据其应用环境的特性补充必要的安全防护措施。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010　信息安全技术　术语

3　术语和定义、缩略语

3.1　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069—2010 中的某些术语和定义。

3.1.1

缓冲区溢出　buffer overflow

向程序的缓冲区写入超出其长度的内容，从而破坏程序堆栈，使程序转而执行其他指令，以获取程序或系统的控制权。

3.1.2

命令注入　command injection

通过应用程序将用户输入的恶意内容拼接到命令中，并提交给后台引擎执行的攻击行为。

3.1.3

应用软件日志　application softwarelog

用于记录系统操作事件的文件集合。

3.1.4

线程安全　thread safe

某个函数、函数库在多线程环境中被调用时能够正确地处理多个线程之间的共享变量，使程序功能正确执行的能力。

3.1.5

线程同步　thread synchronization

多个线程通过特定手段来控制线程之间执行顺序的一种机制。

注：当有一个线程在对内存进行操作时，其他线程就不能对该内存地址执行操作，直到该线程操作完成，此时，其他线程被设置处于等待状态。