



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	I
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	3
4 概述	3
5 安全功能实现	4
5.1 数据清洗	4
5.2 数据加密与保护	5
5.3 访问控制	6
5.4 日志安全	8
6 代码实现安全	9
6.1 面向对象程序安全	9
6.2 并发程序安全	10
6.3 函数调用安全	10
6.4 异常处理安全	11
6.5 指针安全	11
6.6 代码生成安全	11
7 资源使用安全	12
7.1 资源管理	12
7.2 内存管理	12
7.3 数据库管理	13
7.4 文件管理	13
7.5 网络传输	14
8 环境安全	15
8.1 第三方软件使用安全	15
8.2 开发环境安全	15
8.3 运行环境安全	16
附录 A (资料性附录) 代码示例	17
A.1 概述	17
A.2 安全功能实现	17
A.3 代码实现安全	48
A.4 资源使用安全	98
A.5 环境安全	129
参考文献	131

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、王鹏翮、李燕伟、高强、杨鹏、陈亮、范乐君、张晓娜、杜薇、夏剑锋、李晔、张淼、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。