ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39412—2020

信息安全技术　代码安全审计规范

Information security technology—Audit specification of code security

2020-11-19 发布　　2021-06-01 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:信息安全共性技术国家工程研究中心、中国科学院信息工程研究所、国家保密科技测评中心、北京信息安全测评中心、中国信息安全测评中心、中国电子技术标准化研究院、公安部第三研究所、国家计算机网络应急技术处理协调中心。

本标准主要起草人:王彦杰、胡建勋、徐根炜、高振鹏、伊鹏达、肖树根、康蕊、霍玮、朴爱花、李丰、何建波、刘国乐、刘海峰、赵章界、李晨旸、王嘉捷、辛伟、孙彦、孙永清、郭运尧、王博、吴倩。

信息安全技术　代码安全审计规范

1　范围

本标准规定了代码安全的审计过程以及安全功能缺陷、代码实现安全缺陷、资源使用安全缺陷、环境安全缺陷等典型审计指标及对应的证实方法。

本标准适用于指导代码安全审计相关工作。

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 15272—1994　程序设计语言 C

GB/T 25069　信息安全技术　术语

GB/T 35273—2020　信息安全技术　个人信息安全规范

3　术语、定义和缩略语

3.1　术语和定义

GB/T 15272—1994、GB/T 25069 和 GB/T 35273—2020 界定的以及下列术语和定义适用于本文件。

3.1.1

代码安全审计　code security audit

对代码进行安全分析，以发现代码安全缺陷或违反代码安全规范的动作。

3.1.2

安全缺陷　security defect

代码中存在的某种破坏软件安全能力的问题、错误。

3.1.3

跨站脚本攻击　cross site script

攻击者向 Web 页面里面插入恶意 HTML 代码，当用户浏览该页面时，嵌入到 Web 里面的 HTML 代码会被执行，从而达到攻击者的特殊目的。

3.1.4

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。

3.1.5

死锁　deadlock

两个或两个以上的进程在执行过程中，因竞争资源或彼此通信而造成的一种阻塞现象。