ICS 03.120.20
CCS A 00

RB

中华人民共和国认证认可行业标准

RB/T 212—2023

网站安全测评服务安全评价要求

Requirements for evaluation of website security test services

2024-05-20 发布　　2024-07-01 实施

国家认证认可监督管理委员会　发布
中国标准出版社　出版

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规定》的规定起草。

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专利的责任。

本文件由国家认证认可监督管理委员会提出并归口。

本文件起草单位：中国网络安全审查认证和市场监管大数据中心、北京邮电大学、中国电子科技集团公司第十五研究所、北京信息安全测评中心、北京红戎信安技术有限公司、北京安信多乐科技有限公司。

本文件主要起草人：樊华、寇春晓、陆月明、锁延峰、李媛、何志明、杜霖、甘杰夫、胡石、郑潇潇、翟亚红、段静辉、阚明、刘珺珺、华铎。

引　言

2017年我国第一部网络安全领域的专门性立法《中华人民共和国网络安全法》实施，其第十七条提出“国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务”，从法律层面肯定了网络安全服务在保障国家网络安全方面起到的重要作用。网站系统是向用户提供信息共享、浏览、发布部署应用系统的容器，随着互联网技术的迅速发展，网站系统得到极大的普及，各类应用极大地丰富和便利了人们的生活和学习。网站系统包含了大量的可视网页、可执行程序、系统程序、服务程序、管理程序和数据等。这些重要资源面临被黑客非法篡改、被泄露、被丢失等安全威胁。网站安全测评通过技术手段对网站进行漏洞扫描，检测网页是否存在漏洞、网页是否挂马、网页有没有被篡改、是否有欺诈网站等，保障网站的安全运行，提高网站服务的安全质量。但由于安全测评服务需要对网站进行网页挂马、数据加密、网页篡改甚至CC、SQL注入攻击、XSS跨站等攻击测试，且不成熟的安全测评技术、工具，不规范操作都会引入新的安全问题，因此保证测评服务提供方工作的安全性和可靠性是网站进行安全测评的前提和基础。

网站安全测评服务安全评价要求

1 范围

本文件确立了网站安全测评服务的评价原则，规定了网站安全测评服务的评价方法、评价过程及评价内容。

本文件适用于第三方评价机构对网站安全测评服务提供方的安全水平进行评估。网站安全测评服务提供方、网站安全测评服务需求方自行参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 5271.8—2001 信息技术 词汇 第8部分：安全

GB/T 25069—2022 信息安全技术 术语

3 术语和定义

GB/T 5271.8—2001、GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

网站 website

利用网络发布信息，提供在线服务、开展在线互动交流的系统或平台。

注：包括为用户提供展示和交互功能的页面以及生成和处理页面的应用程序、中间件、服务器等。

3.2

网站安全 website security

采取一系列措施防止网站被挂马、网页被篡改、数据被泄露、流量被劫持等行为，从而保障网站的安全性、保密性、完整性及可用性。

3.3

网站安全测评 website security test

针对网站安全性，进行问题发现、符合性和有效性验证的活动。

3.4

网站安全测评服务提供方 website security test service provider

按照服务协议，通过专业的网站安全测评服务人员提供网站安全测评服务的组织。

[来源：GB/T 32914—2016，3.3，有修改]

3.5

网站安全测评服务需求方 website security test service demander

获取外部提供的网站安全测评服务，以满足网站安全需求，实现自身业务目标的组织（或个人用户）。

[来源：GB/T 32914—2016，3.2，有修改]