

ICS 03.120.20
CCS A 00



**CERTIFICATION AND ACCREDITATION INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

RB/T 212-2023

Requirements for evaluation of website security test services

网站安全测评服务安全评价要求

(English Translation)

Issued on: May 20, 2024

Implemented on: July 1, 2024

Issued by: National Certification and Accreditation Administration

Table of Contents

Preface
Introduction
1 Scope
2 Normative references
3 Terms and Definitions
4 Evaluation Principles
5 Evaluation Method
6 Evaluation process
7 Evaluation content
Appendix A (Informative) Website Security Assessment Service Security Risk Analysis
Reference

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting regulations for standardization documents" Drafting.

Introduction

In 2017, the first specialized legislation in the field of cybersecurity in my country, the Cybersecurity Law of the People's Republic of China, was implemented.

The State promotes the construction of a socialized network security service system and encourages relevant enterprises and institutions to carry out network security certification, testing and risk assessment.

Security Services", affirming the important role of network security services in ensuring national network security from a legal perspective. The website system is it provides users with a container for information sharing, browsing, publishing and deploying application systems. With the rapid development of Internet technology, website systems have been greatly the website system contains a large number of visual web pages, executable programs, and these important resources are at risk of being illegally tampered with, leaked, lost, etc.

The website security assessment uses technical means to scan the website for vulnerabilities, detect whether the webpage has vulnerabilities, whether the webpage is

infected with Trojans, and whether the website is infected with Trojans.

Check whether the page has been tampered with, whether there are fraudulent websites, etc. to ensure the safe operation of the website and improve the security quality of website services.

The evaluation service requires testing the website for web page Trojans, data encryption, web page tampering, and even CC, SQL injection attacks, XSS cross-site attacks, etc.

Immature security assessment technologies and tools, as well as irregular operations, will introduce new security issues. Therefore, it is important to ensure that the assessment service provider works the security and reliability of a website are the premise and basis for security assessment.

Website Security Assessment Service Security Evaluation Requirements

1 Scope

This document establishes the evaluation principles for website security assessment services, and specifies the evaluation methods, evaluation process and evaluation Price content.

This document is applicable to third-party evaluation agencies to evaluate the security level of website security evaluation service providers.

Service providers and parties requiring website security assessment services may use this information for their own reference.

2 Normative references

The contents of the following documents constitute essential clauses of this document through normative references in this document.

For referenced documents without a date, only the version corresponding to that date applies to this document; for referenced documents without a date, the latest version (including all amendments) applies to this document.

GB/T 5271.8-2001 Information technology vocabulary Part 8: Security GB/T 25069-2022 Information Security Technical Terminology

3 Terms and definitions

The terms and definitions defined in GB/T 5271.8-2001, GB/T 25069-2022 and the following apply to this document.

website

A system or platform that uses the Internet to publish information, provide online services,

and conduct online interactive communication.

Note: This includes pages that provide display and interaction functions for users, as well as applications, middleware, servers, etc. that generate and process pages.

website security website security Take a series of measures to prevent websites from being hacked, web pages from being tampered with, data from being leaked, traffic from being hijacked, etc., so as to ensure the security of the website.

security, confidentiality, integrity and availability.

Website security test Carry out activities to discover problems, verify compliance and effectiveness for website security.

An organization that provides website security assessment services through professional website security assessment service personnel in accordance with the service agreement.

[Source. GB/T 32914-2016, 3.3, modified] 3.5 Organizations (or individuals) that obtain externally provided website security assessment services to meet website security needs and achieve their own business goals household).

[Source. GB/T 32914-2016, 3.2, modified]