

ICS 03.060
CCS A 11

JR

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

JR/T 0191-2020

**Software Testing Guide for Securities and Futures Industry
Software Security Testing
(English Translation)**

Issued on: July 10, 2020

Implemented on: July 10, 2020

Issued by: People's Bank of China

Table of Contents

- Foreword
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Software security test content and process
- 5 Software Security Testing Technology
- 6 Basic testing methods for software security testing
- 7 Specific test methods for mobile application security testing
- Appendix A (Informative Appendix) Software Security Test Template
 - A.1. Software security testing program
 - A.2. Software security test cases
 - A.3. Software Security Test Report

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Securities Technical Committee of the National Financial Standardization Technical Committee (SAC/TC180/SC4).

This standard is under the jurisdiction of the National Financial Standardization Technical Committee (SAT/TC180).

Drafting organizations of this standard. Information Center of China Securities Regulatory Commission, Dalian Commodity Exchange, Information Technology Testing of Securities and Futures Industry Center (Dalian), China Securities Information Technology Service Co., Ltd., Shanghai Stock Exchange, Shenzhen Stock Exchange, Shanghai Futures Exchange, China Financial Futures Exchange, Guotai Junan Securities Co., Ltd., Hang Seng Electronics Co., Ltd., Beijing Bangbang Security Technology Co., Ltd.

Division.

1 Scope

This standard specifies the software security testing objectives and procedures, software security testing techniques, Basic testing methods for software security testing and specific testing methods for mobile application security testing.

This standard is applicable to guide the market core institutions of the securities and futures industry (hereinafter referred to as core institutions), securities and futures fund management institutions (to Hereinafter referred to as operating institutions) and securities and futures information technology service institutions (hereinafter referred to as service institutions) to implement computer software and Security testing of external information systems.

Note 1: Core institutions, such as securities and futures exchanges, securities registration and settlement institutions, futures market monitoring centers, etc.;

Note 2: Operating institutions, such as securities companies, futures companies, fund companies, etc.;

Note 3: Service organizations are software developers, information providers, and service providers.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this article Pieces. For undated references, the latest version (including all amendments) applies to this document.

GB/T 20271-2006 Information Security Technology Information System General Security Technical Requirements GB/T 25069-2010 Information Security Technical Terms JR/T 0060-2010 Basic requirements for security level protection of information systems in the securities and futures industry (for trial implementation) JR/T 0067-2011 Securities and Futures Industry Information System Security Level Protection Evaluation Requirements (Trial) JR/T 0146-2016 (all parts) Guidelines for the Audit of Securities and Futures Industry Information Systems JR/T 0175-2019 Software Testing Specification for Securities and Futures Industry

3 Terms and definitions

The following terms and definitions defined in GB/T 25069-2010 apply to this document.

Software security testing in the life cycle of information system software products, the software products are inspected to verify that the software products meet the security requirements and software production the process of quality standards.

Penetration testing

By using unauthorized actions to bypass the security mechanism of a certain system, check the security function of the data processing system to discover the information system Means to manage security issues.

[GB/T 25069-2010, definition 2.3.87] 3.3 Fuzz testing the technology of discovering software vulnerabilities by providing unexpected input to the target system and monitoring

abnormal results.

Sensitive information Once leaked or modified, information that will affect the identified information subject.

Note: Sensitive information in the securities and futures industry includes the customer's name, customer's detailed address, customer's contact phone number, customer ID number, customer's bank and account number, and Member transaction status, number of positions held by members, available funds for members, etc.

Mobile internet application Application software that is acquired and run on mobile smart terminals through pre-installation, downloading, etc., to provide users with information services.

4.1 Test content

The content of software security testing includes.

- a) Make sure that the safety features of the software are consistent with the expected design;
- b) Detect potential vulnerabilities and risks in the software;
- c) Verify that the software product can continue to run correctly under malicious attacks and ensure that the software is within the authorized scope Ability to use law;

4.2.1 System analysis

Evaluate the system under test and analyze the components, network topology, system configuration, and security of the system from the perspectives of physical architecture and logical architecture.

Full defense measures and other information.

- a) Physical architecture. According to the components used in the system, the physical architecture is obtained, including databases, control components, front-end libraries, and communication to understand the structure of the system;
- b) Logical architecture. According to the business logic of the system, the logical architecture is obtained, and then the data flow inside the system is understood.

4.2.2 Threat analysis

According to the results of system analysis, select an appropriate threat model and analyze the main security threats facing the system. Risk analysis should comply with GB/T 20271-2006. Such as the common data stream-based threat analysis model STRIDE, which contains six dimensions (counterfeiting, tampering, denial, information the threats of leakage, denial of service, and elevation of privileges are usually combined with data flow

diagrams (DFD) to assist STRIDE analysis and divide the system into Decompose into components and prove that each component is not vulnerable to related threats.

After the system analysis and threat analysis are completed, a security test plan should be produced. The content of the plan includes the physical structure and logic of the system analysis stage.

The structure, as well as the data flow diagram of the threat analysis stage, the technical plan, the implementation plan, etc., the report format can refer to the template output (see See Figure A.1 in Appendix A).

4.2.3 Develop test cases

Write test cases based on the results of threat analysis. For each data flow diagram decomposed, for each data flow diagram element, map pairs in response to threats, write test cases. Use cases can refer to the template output (see Figure A.2 in Appendix A).

4.2.4 Test execution

Test execution includes automated tool execution and manual execution. In this process, various automated or manual tests are required.

Test tools. For the test process of each use case, a corresponding operation screenshot is required. If you can obtain the application source code, you can enter Conduct source code security audits.

4.2.5 Report output

The output documents of each stage of the software security testing process, including the following basic content (see Table 1), can be appropriately tailored according to actual needs Cut, refer to Appendix A for specific templates.

5.1 Safety function check

Make manual inspections and audits on security strategies, progress, and technical decisions (such as development models, etc.) involved in the software development process Perform a safety function check.

The inspection content includes documents, code security policies, security requirements, architecture security, etc. The inspection forms include manual file analysis, visits Wait. See JR/T 0175-2019 for the relevant requirements of the safety test.

5.2 Code Security Test

Through the security scan and audit of the software source code, locate the location of the vulnerable code.