

ICS 35.020
CCS V 07

MH

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

MH/T 0067-2018

**Civil Aviation Web Application System Security Inspection
Guide**

(English Translation)

Issued on: December 14, 2018

Implemented on: April 1, 2019

Issued by: Civil Aviation Administration of China

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Basic principles and methods of civil aviation web application system safety inspection
4.1 Basic principles of testing
4.2 How the test works
5 Phased work of civil aviation web application system safety inspection
5.1 Testing process
5.2 Test preparation stage
5.3 Test plan preparation stage
5.5 Test report preparation stage

Foreword

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

This standard was proposed by the Department of Personnel, Science and Education, Civil Aviation Administration of China.

This standard is under the jurisdiction of the China Academy of Civil Aviation Science and Technology.

Drafting organization of this standard. Civil Aviation University of China.

1 Scope

This standard specifies the basic principles and working methods for civil aviation Web application system testing.

This standard is applicable to guide the security testing of Web application systems.

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 document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 28448 Information Security Technology Information System Security Level Protection Evaluation Requirements GB/T 22239 Information Security Technology Information System Security Level Protection Basic Requirements GB/T 20984 Information Security Technology Information Security Risk Assessment Specification GB/T 31509 Information Security Technology Information Security Risk Assessment Implementation Guide GB/T 25058 Information Security Technology Information System Security Level Protection Implementation Guide Terms and Definitions

3 Terms and definitions

The following terms and definitions apply to this document.

Software fault-tolerance the software can automatically recover from an error state to a normal state to a certain extent.

4.1.1 Standard principles

The safety inspection of civil aviation web application system shall meet the relevant requirements of the inspection process in GB/T 31509 and GB/T 25058.

4.1.2 The principle of controllability During the implementation of safety inspection projects, the service process, personnel and tools should be controlled strictly in accordance with standard project management methods.

To ensure the controllability and safety of the testing implementation process, the specific measures are as follows.

a) Personnel and information controllability. The personnel involved in the test should sign a confidentiality agreement to ensure the safety of the test item information;

The data generated in the process should be strictly managed to prevent data leakage;

b) Process controllability. in accordance with project management requirements, a project implementation team should be set up, and the project team leader should be responsible for the project process.

Control; before conducting a safety test, the tester should fully communicate with the tested party and inform the tested party before the test Test time and test strategy;

c) Tool controllability. Relevant tools that have been tested and approved by the state or civil aviation department should be used in the testing process.

4.1.3 The principle of least impact for the running civil aviation web application system, the tester should determine an appropriate test time window before testing to avoid business peaks at the same time, make an emergency plan for the business system.

4.2.1 Manual interview

Professional information security personnel communicate and exchange with Web application system management, operation and maintenance and users, and fully master the Web application system Information on all aspects of the unified business process, data process, network architecture, host system, operation and maintenance, management organization and management system, Have a comprehensive understanding of the security status of Web application systems.

4.2.2 Manual inspection

Use the expertise and experience of professionals to conduct security tests on civil aviation Web application systems.

4.2.3 Tool test

Using automated web scanning tools to conduct security tests on the detection targets can fully understand the current security status of the web system and Information on vulnerabilities, potential threats, possible impacts and risks.

4.2.4 Penetration test

Simulate hacker's attack method to conduct security test on civil aviation Web application system.

5.1 Testing process

The safety inspection of civil aviation web application system should be divided into four stages.

- Test preparation stage;
- Inspection plan preparation stage;
- The specific implementation stage of testing;
- Inspection report writing stage.

5.2.1 Test preparation

The main task of the test preparation phase is to determine the target and scope of the test, set up a test team, and master the civil aviation web application being tested Information about the system.

5.2.2 Determine the purpose of the test

The goal of the civil aviation web application system detection is to understand the security risks of the web application system, and propose corresponding measures to the security risks found Security hardening recommendations.

5.2.3 Determine the detection range

To test the civil aviation Web application system, the business characteristics of the system operation should be grasped, and the business logic boundary should be determined according to its characteristics.

5.2.4 Establish a testing team

A testing team should be formed for the testing project, and the testing party and the tested party should jointly form a project team, and clarify the responsibilities of the project team members.

5.2.5 System research

The civil aviation web application system to be tested should be investigated, and the third part of the programming language, middleware, and call used by the target should be mastered.

Fang library files and other information.

5.2.6 Determine the basis for testing

The test basis is.

- a) GB/T 28448
- b) GB/T 20984

5.2.7 Determine the principles of testing tools

The selection and use of testing tools should follow the following principles.

- a) The detection tool should have a more comprehensive vulnerability detection capability as much as possible;
- b) The detection strategies and methods used by the detection tools should not cause abnormal effects on the Web application system;
- c) Manual verification of tool test results should be performed as much as possible, and false alarms should be as few as possible;
- d) The selection and use of testing tools should comply with relevant national regulations.