www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Translated English of Chinese Standard: GB/T32917-2016

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 32917-2016

Information security technology - Security technique requirements and testing and evaluation approaches for WEB application firewall

信息安全技术 WEB 应用防火墙安全技术要求与测试评价方法

Issued on: August 29, 2016 **Implemented on: March 01, 2017**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;

Standardization Administration of PRC.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Table of Contents

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Information security technology - Security technique requirements and testing and evaluation approaches for WEB application firewall

1 Scope

This standard specifies the security function requirements, self-security protection requirements, performance requirements, security assurance requirements of WEB application firewalls; provides corresponding test evaluation methods.

This standard applies to the design, production, testing and procurement of WEB application firewalls.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 25069-2010 Information security technology - Glossary

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1

WEB application firewall

It is an information security product that performs protocol and content filtering on all WEB server access requests to WEB servers and WEB server responses based on pre-defined filtering rules and security protection rules, thereby realizing security protection functions for WEB servers and WEB

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

b) Record alarm events, including: the date and time of the event, matching rules, description of the alarm event, etc.

4.1.2 Self-security protection

4.1.2.1 Identification and authentication

4.1.2.1.1 Unique identification

Authorized administrators shall be provided with a unique identity; at the same time, the authorized administrator's identity shall be associated with all auditable events of the authorized administrator.

4.1.2.1.2 Identity authentication

Before performing any operations related to security functions, identify any administrator who claims to perform the duties of an authorized administrator.

4.1.2.1.3 Authentication data protection

It shall be ensured that the authentication data is not accessed and modified without authorization.

4.1.2.1.4 Authentication failure handling

When the administrator fails to reach the specified number of authentication attempts, he shall be able to:

a) Terminate the session.

4.1.2.2 Security audit

4.1.2.2.1 Audit data generation

The following audit logs shall be generated:

a) For all successful and failed WEB access events, audit records shall be generated. The audit log content shall include: the date, time, IP address, requested URL, success or failure identification, matching rules of each event;

b) The administrator's success and failure identification log; the audit log content shall include: the date, time, IP address, username, success or failure identification of each event.

4.1.2.2.2 Audit log management function

Management functions such as backup and query of audit data shall be provided.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

b) Describe the security domain of the product security function consistent with the security function requirements;

c) Describe why the product security function's initialization process is secured;

d) Verify that the product security function can prevent damage;

e) Verify that the product security function can prevent the security feature from being bypassed.

4.1.3.1.2 Functional specification

The developer shall provide a complete functional specification; the functional specification shall meet the following requirements:

a) Fully describe the security function of the product;

b) Describe the purpose and usage of all security function interfaces;

c) Identify and describe all parameters related to each security function interface;

d) Describe the execution behavior of the security function requirements related to the security function interface;

e) Describe direct error messages caused by security function's implementation behaviors and exceptions;

f) Describe the security function demand' s support and irrelevant behavior related to the security function interface;

g) Verify that the security function requires traceability to the security function interface.

4.1.3.1.3 Product design

Developers shall provide product design documents; the product design documents shall meet the following requirements:

a) Describe the product structure according to the subsystem;

b) Identify all subsystems of the product security function;

c) Describe the behavior of each sub-system that is not related to security function requirements in sufficient detail, to determine that it is not related to security function requirements;

d) Summarize the security function demand support and irrelevant behavior

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

a) Describe all the steps necessary to securely receive the delivered product consistent with the developer's delivery procedure;

b) Describe all the steps necessary to securely install the product and its operating environment.

4.1.3.3 Life cycle support

4.1.3.3.1 Configuration management capabilities

The developer's configuration management capabilities shall meet the following requirements:

a) Provide unique identification for different versions of the product;

b) Use the configuration management system to maintain all configuration items that make up the product; uniquely identify the configuration items;

c) Provide configuration management documents, which describe methods for uniquely identifying configuration items;

d) The configuration management system shall provide measures so that only authorized changes can be made to configuration items;

e) The configuration management document includes a configuration management plan, which describes how to use the configuration management system to develop products;

f) The implemented configuration management is consistent with the configuration management plan.

4.1.3.3.2 Configuration management scope

The developer shall provide a list of product configuration items and indicate the developer of the configuration items. The list of configuration items shall contain the following:

a) Evaluation evidence of product and security assurance requirements and product components and realization expressions;

b) The configuration item list shall uniquely identify the configuration item;

c) For each security function-related configuration item, the configuration item list shall briefly describe the developer of the configuration item.

4.1.3.3.3 Delivery procedures

Developers shall use certain delivery procedures to deliver products and

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

h) Illegal upload protection;

i) Illegal download protection;

j) HTTP Flood protection;

k) Cookie injection attack protection;

l) Webshell identification and interception;

m) Protection against other WEB attacks.

4.2.1.3 Other functions

4.2.1.3.1 Custom error page function

It shall be possible to customize the error page returned by the WEB server.

4.2.1.3.2 Whitelist function

It shall support the whitelist function; only allow specific objects to access the specified WEB resources.

4.2.1.3.3 Support HTTPS

It shall be able to decode HTTPS-based WEB server access requests and provide the following functions for the decoded content: 4.2.1.1 HTTP filtering function, 4.2.1.2 security protection function, 4.2.1.3.1 custom error page function, 4.2.1.3.2 whitelist function.

4.2.1.3.4 Rule base management

It shall have the following rule base management functions:

a) According to the user's WEB application environment, provide a matching security protection rule base; it can be upgraded automatically or manually;

b) Add, delete, modify custom filter rules.

4.2.1.3.5 Alarm function

It shall be able to alert on violations and meet the following requirements:

a) Support at least one of screen alarm, email alarm, SNMP trap alarm, SMS alarm, etc.;

b) Record alarm events, including: the date and time of the event, matching rules, description of the alarm event, etc.;

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

d) Describe the security function's implementation behavior related to the security function interface;

e) Describe the direct error messages caused by the behavioral processing of the security function;

f) Verify the traceability of the security function requirements to the security function interface;

g) Describe **all** behaviors related to the security function interface during the implementation of the security function;

h) Describe all direct error messages that may be caused by the invocation of the security function interface.

4.2.3.1.3 Implementation representation

The developer shall provide an implementation representation of all security functions; the implementation representation shall meet the following requirements:

a) Provide the mapping between the product design description and the realization representation example; prove its consistency;

b) Define product security functions according to the level of detail; the level of detail reaches the level that security functions can be generated without further design;

c) Provided in the form used by developers.

4.2.3.1.4 Product design

Developers shall provide product design documents; product design documents shall meet the following requirements:

a) Describe the product structure according to the subsystem;

b) Identify **and describe** all sub-systems of product security functions;

c) Describe the interaction between all subsystems of the security function;

d) The provided mapping relationship can verify that all the behaviors described in the design can be mapped to the security function interface that calls it;

e) Describe the security function according to the module;

f) Provide the mapping relationship between security function

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

consistent with the developer's delivery procedure;

b) Describe all the steps necessary to securely install the product and its operating environment.

4.2.3.3 Life cycle support

4.2.3.3.1 Configuration management capabilities

The developer's configuration management capabilities shall meet the following requirements:

a) Provide unique identification for different versions of the product;

b) Use the configuration management system to maintain all configuration items that make up the product; uniquely identify the configuration items;

c) Provide configuration management documents, which describe methods for uniquely identifying configuration items;

d) Provide **automated** measures so that only authorized changes can be made to configuration items;

e) **The configuration management system provides an automatic way to support the production of products;**

f) The configuration management document includes a configuration management plan, which describes how to use the configuration management system to develop products. The implemented configuration management is consistent with the configuration management plan;

g) **The configuration management plan describes the procedures used to accept modified or newly created configuration items that are part of the product**.

4.2.3.3.2 Configuration management scope

The developer shall provide a list of product configuration items and indicate the developer of the configuration items. The list of configuration items shall contain the following:

a) Evaluation evidence of products and security assurance requirements, product components and realization expressions, **security defect reports and their resolution status**;

b) The configuration item list shall uniquely identify the configuration item;

c) For each security function-related configuration item, the configuration

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

analysis description shall meet the following requirements:

a) Verify the consistency between the test in the test document and the security function subsystem **and security function demand's execution module** in the product design;

b) Verify that all security function subsystems **and security function demand's execution modules** in the product design have been tested.

4.2.3.4.3 Function test

Developers shall test product security features, document the results and provide test documentation. The test document shall include the following:

a) Test plan: Identify the tests to be executed and describe the plan for executing each test. These plans include any sequential dependencies on other test results;

b) Expected test result: Indicate the expected output after the test is successful;

c) Actual test results: Be consistent with expected test results.

4.2.3.4.4 Independent test

Developers shall provide a set of resources equivalent to those used in self-testing security functions, for sampling tests of security functions.

4.2.3.5 Vulnerability assessment

Based on the identified potential vulnerabilities, the product can resist the following attacks:

a) Attacks by attackers with **enhanced** basic attack potential.

Note: To **resist** attacks by attackers with enhanced basic attack potential, it is necessary to comprehensively consider the following five specific factors: attack time, attacker ability, knowledge of the product, access time to the product or number of attack samples, attack equipment used, See Appendix B in Reference [10] for details.

4.3 Performance requirements

4.3.1 HTTP throughput

The HTTP throughput of the WEB application firewall shall not be less than 90% of the wire speed.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

The test evaluation methods and results of the content filtering returned by the WEB server are as follows:

a) Test evaluation method:

The management host configures the filtering rules based on the content keywords returned by the WEB server; initiates the corresponding HTTP request from the test terminal, to detect whether it can block the WEB server containing the keywords from returning the page according to the filtering rules.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.1.2 Security protection function

5.2.1.2.1 WEB application protection function

The test evaluation methods and results of WEB application protection function are as follows:

a) Test evaluation method:

1) Enable the WEB application protection function of the WEB application firewall through the management host; configure the corresponding application protection rules;

2) Initiate attacks against popular vulnerabilities in mainstream WEB server software (such as Apache, IIS, etc.) from the test terminal, to detect whether it can be protected;

3) Initiate attacks against popular vulnerabilities in mainstream WEB application development scripts (such as PHP, ASP, JavaScript, etc.) from the test terminal, to check whether it can be protected.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.1.2.2 WEB attack protection function

The test evaluation methods and results of the WEB attack protection function are as follows:

a) Test evaluation method:

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

1) The inspector attempts to log in to the product to be tested for management, to see whether it is prompted to perform identity authentication;

2) Enter the correct username and corresponding password, to try to log in;

3) Enter the correct username and wrong password, to try to log in;

4) Enter the wrong username, to try to log in.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.2.1.3 Authentication data protection

The test and evaluation methods and results for identifying data protection are as follows:

a) Test evaluation method:

1) Log in to the product to be tested as an authorized administrator and an unauthorized administrator, respectively, to modify the passwords of other administrators;

2) According to the document provided by the developer, open the file or database table of the authentication data storage, to verify whether the authentication data needs authorization; check whether the authentication data is stored encrypted.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.2.1.4 Authentication failure handling

The test evaluation methods and results for identifying failure handling are as follows:

a) Test evaluation method:

1) Set the maximum number of failed login attempts (fixed times are also available);

2) Simulate multiple administrator login failure events, until the test

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.2.2.3 Understandable format

The test evaluation methods and results in an understandable format are as follows:

a) Test evaluation method:

The inspector checks the product audit data stored in the permanent audit record, to check whether the audit data is understandable or not.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.2.2.4 Prevention of loss of audit data

The test evaluation methods and results to prevent the loss of audit data are as follows:

a) Test evaluation method:

1) The evaluator shall review what mechanism the product description manual has to ensure the availability of audit records;

2) Simulate abnormal shutdown, full disk space, etc., to check whether the product can take effective measures to prevent audit data loss.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.2.3 Statistics function

The test evaluation methods and results of statistical functions are as follows:

a) Test evaluation method:

1) Use different IP addresses to access protected resources;

2) Enter the statistical function interface, to verify whether the product can count the total number of accesses to WEB resources and the total number of accesses to a single IP address according to different time

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

a) Test evaluation method:

1) Check whether the product under test has dual-system hot backup function;

2) According to the document provided by the developer, set the two WEB application firewalls to the main and standby working modes, respectively;

3) Make the main WEB application firewall unable to work normally (such as power failure, network disconnection, etc.), to check whether the standby WEB application firewall can detect the abnormal working status of the main WEB application firewall in time, meanwhile take over the main WEB application firewall to work.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.3 Test evaluation methods for security assurance requirements

5.2.3.1 Development

5.2.3.1.1 Security architecture

The test and evaluation methods and results of the security architecture are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides evidence of the following security architecture; check whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- Be consistent with the level of abstract description of security functions implemented in product design documents;

- Describe the security domain of the product security function consistent with the security function requirements;

- Describe why the product security function initialization process is secured;

- Verify that product security functions can be prevented from being destroyed;

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

meet the corresponding security technical requirements.

5.2.3.3 Life cycle support

5.2.3.3.1 Configuration management capabilities

The test evaluation methods and results of configuration management capabilities are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides the following evidence of configuration management capabilities; check whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- Provide unique identification for different versions of the product;

- Use the configuration management system to maintain all the configuration items that make up the product; uniquely identify the configuration items;

- Provide configuration management documents, which describe methods for uniquely identifying configuration items;

- The configuration management system shall provide measures to make only authorized changes to configuration items;

- Configuration management documents include a configuration management plan, which describes how to use the configuration management system to develop products;

- The configuration management implemented is consistent with the configuration management plan.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.3.3.2 Configuration management scope

The test evaluation methods and results of the configuration management scope are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides a list of product

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

on other test results;

- Expected test result: Indicate the expected output after the test is successful;

- The actual test result: Be consistent with the expected test result.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.3.4.4 Independent test

The test evaluation methods and results of the independent test are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides a set of equivalent resources used in the self-testing of the security function for the sampling test of the security function; check whether the information provided by the developer meets all the requirements of the content and form of the evidence.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.2.3.5 Vulnerability assessment

The test and evaluation methods and results of vulnerability assessment are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides a vulnerability analysis document; the vulnerability analysis document shall identify potential vulnerabilities. Check whether the product can resist the attacks of attackers with basic attack potential.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

a) Test evaluation method:

Configure the filtering rules based on the suffix of the WEB resource file (such as zip, rar, doc, exe, asp, html, etc.) through the management host; initiate the corresponding HTTP request from the test terminal, to try to access or download the WEB resources with the above suffixes File, to check whether it can block the access request based on filtering rules.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.1.1.4 Support multiple HTTP request parameter encoding methods

The test evaluation methods and results that support multiple HTTP request parameter encoding methods are as follows:

a) Test evaluation method:

The test terminal initiates HTTP requests in different encoding formats (UNICODE, BASE64, binary, hexadecimal, etc.), to detect whether it can automatically convert client requests into ASCII plaintext.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.1.1.5 Identify and restrict HTTP response codes

The test evaluation methods and results for identifying and restricting HTTP response codes are as follows:

a) Test evaluation method:

Configure the filtering rules based on HTTP response codes through the management host; initiate HTTP requests from the test terminal, to detect whether it can recognize the response codes returned by the HTTP server, meanwhile allow or block the response page according to the filtering rules.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.1.1.6 URL content keyword filtering

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

detect whether it can be protected;

3) Initiate attacks against popular vulnerabilities in mainstream WEB application development scripts (such as PHP, JSP, ASP, JavaScript, etc.) from the test terminal, to check whether it can be protected.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.1.2.2 WEB attack protection function

The test evaluation methods and results of the WEB attack protection function are as follows:

a) Test evaluation method:

1) Enable the WEB attack protection function of the WEB application firewall through the management host; configure the corresponding attack protection rules;

2) Use POST and GET methods to perform SQL injection attacks from the test terminal, to detect whether it can be protected;

3) Attack the WEB server with various XSS cross-site scripts built on the test terminal, to detect whether it can be protected;

4) Access the constructed resource hotlink from the test terminal, to detect whether it can be protected, so that the stolen link WEB page is displayed abnormally, meanwhile the pictures and other resources of the stolen server cannot be displayed normally;

5) Use the scanning tool to scan the WEB application of the WEB server from the test terminal, to check whether it can be protected, so that the scanning tool cannot scan any results;

6) Attack the WEB server with a crawler tool from the test terminal, to check whether it can be protected, so that the crawler tool cannot obtain the server's information;

7) Perform CSRF attacks on the WEB server from the test terminal, to detect whether it can be protected;

8) Use POST and GET methods to perform command injection attacks from the test terminal, to detect whether it can be protected;

9) Use the POST method to upload files illegally from the test terminal, to

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

3) Initiate the same HTTP request from the test terminal; trigger an alarm, to detect whether the product can merge alarms for the same alarm events that occur frequently;

4) Check the alarm log content of the product, to see whether it contains information items such as date, time, matching rules, alarm event description, etc.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test and evaluation methods.

5.3.2 Test evaluation method of self-security protection

5.3.2.1 Identification and authentication

5.3.2.1.1 Unique identification

The test and evaluation methods and results of the unique identification are as follows:

a) Evaluation method:

1) Create a user; view the unique identifier of the user; log in to the product to be tested as the created user; perform a series of operations; view related logs;

2) Try to create a user with the same identity again.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.2.1.2 Identity authentication

The test evaluation methods and results of identification are as follows:

a) Test evaluation method:

1) The inspector attempts to log in to the product to be tested for management, to see whether it is prompted to perform identity authentication;

2) Enter the correct username and corresponding password, to try to log in;

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

a) Test evaluation method:

1) The evaluator shall review what mechanism the product description manual has to ensure the availability of audit records;

2) Simulate abnormal shutdown, full disk space, etc., to check whether the product can take effective measures to prevent audit data loss.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.2.3 Statistics function

The test evaluation methods and results of statistical functions are as follows:

a) Test evaluation method:

1) Use different IP addresses to access protected resources;

2) Enter the statistical function interface, to verify whether the product can count the total number of access to WEB resources and the total number of accesses to a single IP address according to different time periods;

3) Try to generate statistical analysis reports based on the number of accesses to see if it supports graphical display (such as pie charts, bar charts, etc.); meanwhile it can be exported in common ways (such as HTML format, DOC format, etc.).

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.2.4 Remote management encryption

The test evaluation methods and results of remote management encryption are as follows:

a) Test evaluation method:

1) Check whether the system under test needs to support remote management;

2) Remotely manage the system; use a data packet analysis tool to verify whether the remote management communication is non-plain text.

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

5.3.2.7 Load balancing

The test and evaluation methods and results of load balancing are as follows:

a) Test evaluation method:

1) Review the product documentation, to see whether the product supports load balancing function;

2) Configure a load balancing policy on the WEB application firewall, to balance the WEB access requests to multiple WEB servers;

3) Use the performance tester to simulate multiple HTTP clients for HTTP access through the WEB application firewall, to check whether the WEB application firewall can balance the WEB access requests to multiple WEB servers;

4) Count the total number of WEB accesses on each WEB server, to test whether the WEB application firewall achieves the load balancing effect.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test and evaluation methods.

5.3.3 Test evaluation method of security assurance requirements

5.3.3.1 Development

5.3.3.1.1 Security architecture

The test and evaluation methods and results of the security architecture are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides evidence of the following security architecture; check whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- Be consistent with the level of abstract description of security functions implemented in product design documents;

- Describe the security domain of the product security function consistent with the security function requirements;

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

- **Describe all direct error messages that may be caused by the call of the security function interface**.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.3.1.3 Implementation representation

The test evaluation methods and results of the realization representation are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides the evidence of the following realization representation; check whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- **Provide the mapping between the product design description and the implementation representation example; prove its consistency;**

- **Define product security functions according to the level of detail; the level of detail reaches the level that security functions can be generated without further design;**

- **Provided in the form used by developers.**

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.3.1.4 Product design

The test evaluation methods and results of product design are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides the following product design evidence; check whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- Describe the product structure according to the subsystem;

- Identify **and describe** all subsystems of product security functions;

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

configuration items and indicate the developer of the configuration items. The list of configuration items shall contain the following content; check whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- Evaluation evidence of products and security assurance requirements, product components and realization expressions, **security defect reports and their resolution status;**

- The list of configuration items shall uniquely identify the configuration items;

- For each configuration item related to security function, the configuration item list shall briefly describe the developer of the configuration item.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.3.3.3 Delivery procedures

The test evaluation methods and results of the delivery process are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides evidence of the following delivery procedures; whether the information provided by the developer meets all the requirements for the content and form of the evidence:

- Certain delivery procedures shall be used to deliver products and the delivery process shall be documented. When delivering each version of the product to the user, the delivery document shall describe all procedures necessary to maintain security.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.3.3.4 Development security

The development of secured testing and evaluation methods and results are as follows:

a) Test evaluation method:

www.ChineseStandard.net --> Buy True-PDF --> Auto-delivered in 0~10 minutes.

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.3.3.5 Vulnerability assessment

The test and evaluation methods and results of vulnerability assessment are as follows:

a) Test evaluation method:

The evaluator shall check whether the developer provides a vulnerability analysis document; the vulnerability analysis document shall identify potential vulnerabilities. Check whether the product can resist the attacks of attackers with **enhanced** basic attack potential.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

5.4 Performance test evaluation method

5.4.1 HTTP throughput

The test evaluation methods and results of HTTP throughput are as follows:

a) Test evaluation method:

1) Use the performance tester to simulate multiple HTTP clients accessing the simulated server through the WEB application firewall (the HTTP request generation rate shall be less than or equal to the product's maximum HTTP request rate); the HTTP payload for each request is 10 MB, for a duration of 30 min;

2) Calculate the average HTTP throughput of the WEB application firewall during the test;

3) Repeat the process more than 3 times; calculate the arithmetic average of the 3 results.

b) Test evaluation results:

Record the test results and make a judgment on whether the results fully meet the corresponding security technical requirements.

This is an excerpt of the PDF (Some pages are marked off intentionally)

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------