International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1524

(03/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity information exchange – Vulnerability/state exchange

Common weakness enumeration

Recommendation ITU-T X.1524

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	**X.1520–X.1539**
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1524

Common weakness enumeration

Summary

Recommendation ITU-T X.1524 on the use of the common weakness enumeration (CWE) provides a structured means to exchange information security weaknesses that provides common names for publicly known problems in the commercial or open source software used in communication networks, end user devices, or any of the other types of information and communications technology (ICT) capable of running software. The goal of CWE is to enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source codes and operational systems as well as better understanding and management of software weaknesses related to architecture and design. This Recommendation defines the use of CWE to provide a mechanism for software security tools, services, knowledge bases and other capabilities to be used together, and to facilitate the comparison of security tools and services. CWE also offers supportive context information about possible risks, impacts, fix information, and detailed technical information about what the software weaknesses could mean to a software system.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1524	2012-03-02	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

The common weakness enumeration (CWE) Recommendation describes the use of CWE, a structured means to exchange unified, measurable sets of software weaknesses that aims to provide common names for publicly known problems. The goal of CWE is to make it easier to enable more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as to promote better understanding and management of software weaknesses related to architecture and design.

The intention of CWE is to be comprehensive with respect to the causes behind all publicly known vulnerabilities and exposures, whether from weaknesses in the software's architecture, design, code, or deployment. While CWE is designed to contain mature information, the primary focus is on identifying the weaknesses that can cause vulnerabilities and exposures. The review authority determines conformance on the use of CWE identifiers, as defined in this Recommendation.

CWE gives leverage to existing work from within the cybersecurity community such as the large number of diverse real-world vulnerabilities specified in Recommendation ITU-T X.1520 – Common vulnerabilities and exposures (CVE). Many sources and examples are leveraged to develop the specific and succinct definitions of the CWE list elements and classification tree structures. In addition, appropriate mappings are created between CWEs and CVE names so that each CWE identifier has a list of the specific CVE names that belong to that particular CWE category of software security weaknesses. In constructing the CWE list and classification tree, maximum comprehensive coverage across appropriate conceptual, business, and technical domains is sought.

This Recommendation is technically equivalent to and compatible with the "Requirements and Recommendation for CWE Compatibility and Effectiveness", version 1.0, dated July 28, 2011 https://cwe.mitre.org/compatible/requirements_v1.0.html.

Recommendation ITU-T X.1524

Common weakness enumeration

1 Scope

This Recommendation on the use of the common weakness enumeration (CWE) provides a "structured means" for the global exchange of information about software security weaknesses in architecture, design, code, or deployment that can make software systems insecure, unreliable and vulnerable to attack. Security tools, assessment services, and some types of security reviews can detect these types of software weaknesses. This "structured means" is often referred to as "CWE Compatibility" and defines the correct use of CWE. An information security weakness is a mistake in the software that could result in a vulnerability that can be used by a hacker to gain access to a system or network. The assignment of CWE identifiers is not within the scope of this Recommendation. A list of repositories for CWE identifiers and the associated context information is available in Appendix I.

The intention of CWE, the use of which is defined in this Recommendation, is to be comprehensive with respect to the software architecture, design, coding, and deployment errors that are the root causes of vulnerabilities and exposures. While CWE is designed to contain mature information, the primary focus is on identifying, educating, and describing these root causes of vulnerabilities and exposures so they can be avoided by developers, tested for, and managed by development teams as well as consistently reported by security tools and services.

This Recommendation is technically equivalent to and compatible with the "Requirements and Recommendation for CWE Compatibility and Effectiveness", version 1.0, dated July 28, 2011 https://cwe.mitre.org/compatible/requirements.html.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 accuracy percentage: The percentage of security elements in the review sample that reference the correct CWE identifiers.

3.2.2 capability: An assessment tool, Integrated Development Environment (IDE), code review tool, code checking compiler, database, website, advisory, or service that provides information about implementation, design, or architecture-level weaknesses that can lead to an exploitable security vulnerability in software.

3.2.3 CWE compatibility requirements evaluation form: This evaluation form contains a series of questions asking the capability's owner to document their conformance to the compatibility requirements of Recommendation ITU-T X.1524 in text, image or web references, as well as instructions on where to submit the completed form or to ask the review authority for clarification on how to complete the evaluation form.

3.2.4 CWE effectiveness requirements evaluation form: This evaluation form contains a series of questions asking the capability's owner to document their conformance to the effectiveness requirements of this Recommendation in text, image or web references, as well as instructions on where to submit the completed form, request tests, or to ask the review authority for clarification on how to complete the evaluation form.

3.2.5 effectiveness testing: The process of determining whether a capability is CWE effective.

3.2.6 map/mapping: The specification of relationships between weakness elements in a repository and the CWE items that are related to those elements.

3.2.7 owner: The custodian (real person or company) having responsibility for the capability.

3.2.8 repository: An implicit or explicit collection of security-related software weakness elements that supports a capability, e.g., a database of security weaknesses, the set of patterns in a code analyser, or a website.

3.2.9 review: The process of determining whether a capability is CWE-compatible.

3.2.10 review authority: An entity that performs a review or effectiveness testing and is authorized to grant CWE-compatible or CWE-effective status.

Note that Appendix II contains a list of review authorities.

3.2.11 review version: The dated version of CWE that is being used for determining the CWE compatibility or CWE effectiveness of a capability.

3.2.12 security element: A database record, assessment probe, signature, etc., that is related to a specific security weakness.

3.2.13 task: A tool's probe, check, signature, etc., that performs some action that produces security information (i.e., the security element).

3.2.14 test results: Data representing the outcome of effectiveness testing.

3.2.15 tool: A software application or device that examines a piece of software, binary, or other artefact and produces information about security weaknesses, e.g., a source code security analyser, a code quality assessment tool, code checking compiler or a development environment.

3.2.16 user: A consumer or potential consumer of the capability.

3.2.17 vulnerability: Any weakness in software that could be exploited to violate a system or the information it contains (based upon [b-ITU-T X.1500]).

3.2.18 weakness: A shortcoming or imperfection in the software code, design, architecture, or deployment that, could, at some point become a vulnerability, or contribute to the introduction of other vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASCII American Standard Code for Information Interchange

CCR Coverage Claim Representation

CGI Common Gateway Interface

CWE	Common Weakness Enumeration
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
PDF	Portable Document Format
POC	Point of Contact
URL	Uniform Resource Locator
XML	Extensible Markup Language

5 Conventions

None.

6 High-level requirements

The following items define the concepts, roles, and responsibilities related to the proper use of CWE identifiers to share data across separate security weakness capabilities, (tools, repositories, and services) to allow these security weakness capabilities to be used together, and to facilitate the comparison of security weakness tools and services.

6.1 The capability owner shall be a valid legal entity, i.e., an organization or a specific individual, with a valid phone number, email address, and street mail address.

6.2 The capability shall provide additional value or information beyond that which is provided in CWE itself (i.e., name, description, risks, references, and associated weakness information).

6.3 The capability owner shall provide the review authority with a technical point of contact who is qualified to answer questions related to the mapping accuracy, any CWE-related functionality of the capability, and to coordinate the testing of the capability in support of assessing its effectiveness in identifying CWEs.

6.4 The capability shall be available to the public, or to a set of consumers, in a production or public version, such as either being available on a public website, being offered for use as an open source, being available for purchase or as a service available for contract.

6.5 For CWE compatibility the capability owner shall provide the review authority with a completed "CWE compatibility Requirements Evaluation Form".

6.6 The capability owner shall provide the review authority with free access to the capability's repository so that the authority can determine that the capability's repository satisfies all associated mapping accuracy requirements.

6.7 The capability owner shall allow the review authority to use the repository to identify any weaknesses that should be added to CWE.

6.8 For CWE effectiveness the capability shall be CWE compatible.

6.9 For CWE effectiveness the capability owner shall provide the review authority with a completed "CWE effectiveness Requirements Evaluation Form".

6.10 For CWE effectiveness the capability owner shall provide the review authority with effectiveness testing results as part of their "CWE effectiveness Requirements Evaluation Form" so that the authority can determine that the capability satisfies all associated effectiveness requirements.

6.11 The capability owner shall agree to abide by all of the mandatory CWE compatibility and effectiveness requirements, which include the mandatory requirements for the specific type of capability.

6.12 For CWE compatibility the capability shall allow users to locate security elements using CWE identifiers ("CWE-Searchable").

6.13 For CWE compatibility when the capability presents security elements to the user, it shall allow the user to obtain the associated CWE identifiers ("CWE-Output").

6.14 For CWE compatibility the capability's mapping shall accurately link security elements to the appropriate CWE identifiers ("Mapping Accuracy").

6.15 For CWE compatibility the capability's documentation shall adequately describe CWE, CWE compatibility, and how the CWE-related functionality in the capability is used ("CWE-Documentation").

6.16 For CWE compatibility the capability's publicly available documentation shall explicitly list the CWE identifiers that the capability owner considers the capability to cover as part of its functionality ("CWE-Coverage").

6.17 For CWE compatibility the capability's publicly available website should provide the capability's CWE-Coverage as a CWE Coverage Claim Representation (CCR) XML document(s).

6.18 For CWE effectiveness the results from the capability's assessing the test sets for the CWE identifiers (listed as the capability's CWE-Coverage) shall be posted on the review authority's CWE website. ("CWE-Test Results").

6.19 The capability shall denote the dated CWE version used ("Version Usage").

6.20 The capability shall satisfy the following additional requirements for the specific type of capability, as specified in Annex A.

6.21 The capability shall satisfy all requirements for its distribution media, as specified in Annex B.

6.22 The capability is not required to do any of the following:

- use the same descriptions or references as CWE;
- include every CWE identifier in its repository.

6.23 If the capability does not satisfy all of the applicable requirements above (clauses 6.1 to 6.22), then the capability owner shall not advertise that it conforms to the CWE-compatible or CWE-effective portions of this Recommendation.

7 Accuracy

CWE compatibility only facilitates data sharing and correlation if the capability's mapping is accurate. Therefore, CWE-compatible capabilities must meet the following minimum accuracy requirements.

7.1 The Repository shall have an accuracy of 100 per cent.

7.2 During the review period, the capability owner shall correct any mapping errors found by the review authority.

7.3 After the review period, the capability owner should correct a mapping error within a reasonable time frame after the error was initially reported, i.e., within two versions of the capability repository or six months, whichever is shorter.

7.4 The capability owner should prepare and sign a statement that, to the best of the capability owner's knowledge, there are no errors in the mapping.

7.5 If the capability is based on, or uses, another CWE-compatible capability (the "Source" capability), and the capability owner becomes aware of mapping errors in the Source capability, then the capability owner shall report those errors to the capability owner of the Source capability.

8 Effectiveness

Effectiveness is focused on providing transparency for prospective users of a capability so that the corresponding weaknesses in software can be identified. Insight into the ability of a capability to find weaknesses in the face of different levels of complexity is of interest to users when they are considering using a capability or relying on the results of someone else using a capability. Therefore, CWE-effective capabilities must meet the following minimum effectiveness requirements.

8.1 Using the appropriate portion of the "CWE Effectiveness Requirements Evaluation Form" the capability owner shall declare which CWE identifiers they claim their capability is effective in locating. This can be accomplished through the use of a CWE coverage claim representation (CCR) XML document(s).

8.2 For the CWE identifiers declared, the capability owner shall request the appropriate test sets so that the capability owner can use the capability to assess the test sets for all of the weaknesses corresponding to the declared CWE identifiers.

8.3 Within an agreed time-frame, the capability owner shall submit the results they obtained from assessing the test sets with their capability.

8.4 The results shall list each assessed test set file, and the line number for each weakness located along with the appropriate CWE identifier.

8.5 The capability owner shall prepare and sign a statement agreeing to the posting of their capabilities test results on the CWE website.

8.6 The capability owner shall submit a revised "CWE Effectiveness Requirements Evaluation Form" with an updated listing of the CWE identifiers they claim their capability is effective in locating in order to retake the effectiveness tests for a different set of CWE identifiers. This can be accomplished through the use of an updated CWE coverage claim representation (CCR) XML document(s).

9 Documentation

The following requirements apply to documentation that is provided by the capability owner with their capability.

9.1 The documentation shall include a brief description of CWE and CWE compatibility, which can be based on verbatim portions of documents from the review authority's CWE website.

9.2 The documentation shall describe how the user can find individual security elements in the capability's repository by using CWE identifiers.

9.3 The documentation shall describe how the user can obtain CWE identifiers from individual elements in the capability's repository.

9.4 If the documentation includes an index, then it should include references to CWE-related documentation under the term "CWE".

10 CWE version usage

Users must know what version of CWE is used in a capability's repository with respect to its mapping to CWE. The capability owner can indicate the currency of a mapping by using the CWE version or date the mapping was updated.

10.1 The capability shall identify the CWE version or update the date that was used in creating or updating the mapping through at least one of the following: change logs, new feature lists, help files, or some other mechanism. The capability is "up-to-date" with respect to that version or update date.

10.2 Each new version of the capability should be up-to-date with respect to a CWE version that was released no more than four months before the capability was made available to its users. If a capability does not satisfy this requirement, then it is "out-of-date".

10.3 The capability owner should publicize to its users and prospective users how quickly it will update the capability's repository after a new CWE version or update becomes available on the CWE website.

11 Revocation of CWE compatibility

The following describes the responsibilities of the review authority with respect to revoking CWE compatibility.

11.1 If a review authority has verified that a capability is CWE-compatible or CWE-effective, but at a later time the review authority has evidence that the requirements are not being met, then the review authority may revoke its approval.

11.1.1 The review authority shall identify the specific requirements that are not being met.

11.2 The review authority shall determine if the actions or claims of the capability owner are "intentionally misleading".

11.2.1 The review authority may interpret the phrase "intentionally misleading" at its discretion.

11.3 The review authority should not consider revoking CWE compatibility for a particular capability more often than once every six months.

11.4 The review authority shall provide the capability owner and technical POC with a warning of revocation at least two months before revocation is scheduled to occur.

11.4.1 If the review authority has found that the capability owner's actions or claims are intentionally misleading, then the review authority may disregard the warning period.

11.5 If the capability owner believes that the requirements are being met, then the capability owner may respond to the warning of revocation by providing specific details that indicate why the capability meets the requirements under question.

11.6 If the capability owner modifies the capability so that it complies with the requirements in question during the warning period, then the review authority should end the revocation action for the capability.

11.7 The review authority may delay the date of revocation.

11.8 The review authority shall publicize that CWE compatibility or CWE effectiveness has been revoked for the capability on the review authority's CWE website.

11.9 If the review authority finds that the capability owner's actions with respect to CWE compatibility or CWE effectiveness requirements are intentionally misleading, then revocation should last a minimum of one year.

11.10 The review authority may publicize the reason for revocation.

11.11 The capability owner may post a public statement regarding the revocation on the same site.

11.12 If the approval is revoked, the capability owner shall not apply for a new review during the period of revocation.

12 Review authority

12.1 A review authority shall review the capability for CWE compatibility or CWE effectiveness with respect to a specific CWE version, i.e., the review version.

12.2 A review authority shall clearly identify the review version that was used to determine compatibility or effectiveness for the capability.

12.3 A review authority shall clearly identify the version of the CWE compatibility requirements and effectiveness document that was used to determine compatibility or effectiveness for the capability.

12.4 A review authority shall review every element in the capability's repository for CWE mapping accuracy.

12.5 A review authority should review a capability for mapping accuracy at least once per year.

Annex A

Type-specific requirements

(This annex forms an integral part of this Recommendation.)

Since a wide variety of capabilities use CWE, certain types of capabilities may have unique features that require special attention with respect to CWE compatibility.

A.1 The capability shall satisfy all of the following additional requirements that are related to the specific type of capability.

A.1.1 If the capability is an assessment tool, source or binary code security analyser, a code quality assessment tool, code checking compiler, development environment, or a product that integrates the results of one or more of these types of items, then it must satisfy the tool requirements, A.2.1-A.2.8.

A.1.2 If the capability is a service (such as a security assessment service, an education or training service, or a code and design review service) then it must satisfy the security service requirements, A.3.1-A.3.5.

A.1.3 If the capability is an online database of security issues or weaknesses in application software, a web-based resource, or an information site, then it must satisfy the online capability requirements, A.4.1-A.4.3.

A.2 Tool requirements

The following are the tool specific requirements.

A.2.1 The tool shall allow the user to use CWE identifiers to locate associated tasks in that tool ("CWE-Searchable") by providing at least one of the following: a "find" or "search" function, a mapping between that tool's task names and CWE identifiers, or another mechanism determined to be sufficient by the review authority.

A.2.2 For any report that identifies individual security elements, the tool shall allow the user to determine the associated CWE identifiers for those elements ("CWE-Output") by doing at least one of the following: including CWE identifiers directly in the report, providing a mapping between the tool's task names and CWE identifiers, or using some other mechanism determined to be sufficient by the review authority.

A.2.3 The publicly available documentation shall explicitly list the CWE identifiers that the capability owner considers the tool effective at locating in software ("CWE-Compatibility Claim Coverage").

A.2.4 The capability's publicly available website may provide the capability's CWE compatibility claim coverage as a CWE coverage claim representation (CCR) XML document(s).

A.2.5 Any required reports or mappings shall satisfy the media requirements as specified in Annex B.

A.2.6 The tool, or the capability owner, should provide the user with a list of all CWE identifiers that are associated with the tool's tasks.

A.2.7 The tool should allow the user to select a set of tasks by providing a file that contains a list of CWE identifiers.

A.2.8 The interface of the tool should allow the user to browse, select, and deselect a set of tasks by using individual CWE identifiers.

A.2.9 If the tool does not have a task that is associated with a CWE identifier as specified by the user in the A.2.5 or A.2.6 tool requirements, then the tool should notify the user that it cannot perform the associated task.

A.2.10 The capability owner shall warrant that (1) the rate of false positives is less than 100 per cent, i.e., if the tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 per cent, i.e., if an issue is in the artefacts of the system that is related to a specific security element, then sometimes the tool reports that issue.

A.3 Security service requirements

Security services might use CWE-compatible and CWE-effective tools in their work, but they may not provide their customers with direct access to those tools. Thus it could be difficult for customers to identify and compare the capabilities of different services. The security service requirements address this potential limitation.

A.3.1 The security service shall be able to use CWE identifiers to tell a user which security elements are tested, detected, or covered by the service offering ("CWE-Searchable") by doing one or more of the following: providing the user with a list of CWE identifiers that identify the elements that are tested, detected, or covered by that service; providing the user with a mapping between the service's elements and CWE identifiers; responding to a user-supplied list of CWE identifiers by identifying which of the CWE identifiers are tested, detected, or covered by the service; or by using some other mechanism.

A.3.2 For any report that identifies individual security elements, the service shall allow the user to determine the associated CWE identifiers for those elements ("CWE-Output") by doing one or more of the following: allowing the user to include CWE identifiers directly in the report, providing the user with a mapping between the security elements and CWE identifiers, or by using some other mechanism.

A.3.3 The publicly available documentation shall explicitly list the CWE identifiers that the capability owner considers the security service to effectively cover in its offering ("CWE-Compatibility Claim Coverage").

A.3.4 The capability's publicly available website may provide the capability's CWE-compatibility claim coverage as a CWE coverage claim representation (CCR) XML document(s).

A.3.5 Any required reports or mappings that are provided by the Service shall satisfy the media requirements as specified in Annex B.

A.3.6 If the service provides the user with direct access to a product that identifies security elements, then that product should be CWE-compatible and CWE-effective.

A.3.7 The capability owner shall warrant that (1) the rate of false positives is less than 100 per cent, i.e., if a tool reports a specific security element, it is at least sometimes correct, and (2) the rate of false negatives is less than 100 per cent, i.e., if an issue is in the artefacts of the system that is related to a specific security element, then sometimes the service reports that issue.

A.4 Online capability requirements

The following are the online capability specific requirements.

A.4.1 The online capability shall allow a user to find related security elements from the online capability's repository ("CWE-Searchable") by providing one of the following: a search function that returns CWE identifiers for related elements, a mapping that links each element with its associated CWE identifier(s), or some other mechanism.

A.4.1.1 The online capability should provide a URL "template" that allows a computer program to easily construct a link that accesses the search function as outlined in online capability requirements A.4.1.

Examples:

http://www.example.com/cgi-bin/db-search.cgi?cweid=XXX

http://www.example.com/cwe/xxx.html

A.4.1.2 If the site is publicly accessible without requiring login, then the cgi program should accept the "GET" method.

A.4.2 For any report that identifies individual security elements, the online capability shall allow the user to determine the associated CWE identifiers for those elements ("CWE-Output") by doing at least one of the following: by allowing the user to include CWE identifiers directly in the report, providing the user with a mapping between the security elements and CWE identifiers, or by some other mechanism.

A.4.3 The publicly available documentation shall explicitly list the CWE identifiers that the capability owner considers the online capability's repository to cover ("CWE-Compatibility Claim Coverage").

A.4.4 The capability's publicly available website may provide the capability's CWE-compatibility claim coverage as a CWE coverage claim representation (CCR) XML document(s).

A.4.5 If the online capability does not provide details for individual security elements, then the online capability shall provide a mapping that links each element with its associated CWE identifier(s).

Annex B

Media requirements

(This annex forms an integral part of this Recommendation.)

B.1 The distribution media that is used by a CWE-compatible capability shall use a media format that is covered in this annex.

B.2 The media format shall satisfy the specific requirements for that format.

B.3 Electronic documents (HTML, word processor, PDF, ASCII text, etc.)

B.3.1 The document shall be in a commonly available format that has readers, which support a "find" or "search" function ("CWE-Searchable"), such as raw ASCII text, HTML, or PDF.

B.3.2 If the document only provides short names or titles for individual elements, then it shall list the CWE identifiers that are related to those elements ("CWE-Output").

B.3.3 The document should include a mapping from elements to CWE identifiers, which lists the appropriate pages for each element.

B.4 Graphical user interface (GUI)

The following are the graphical user interface specific requirements.

B.4.1 The GUI shall provide the user with a search function that allows the user to enter a CWE identifier and retrieve the related elements ("CWE-Searchable").

B.4.2 If the GUI lists details for an individual element, then it shall list the CWE identifiers that map to that element ("CWE-Output"). Otherwise, the GUI shall provide the user with a mapping in a format that satisfies the B.3.1 electronic documents requirement.

B.4.3 The GUI should allow the user to export or access CWE-related data in an alternate format that satisfies the B.3.1 electronic documents requirement.

Appendix I

List of CWE repositories for identifiers and the associated context information

(This appendix does not form an integral part of this Recommendation.)

MITRE Corporation	cwe.mitre.org/data

Appendix II

List of review authorities

(This appendix does not form an integral part of this Recommendation.)

1. MITRE Corporation, contact via cwe@mitre.org.

Bibliography

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012