国 际 电 信 联 盟

ITU-T X.1524

(03/2012)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络安全信息交换 – 脆弱性/状态信息交换

通用缺陷列表

ITU-T X.1524 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定安全	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
网络安全信息交换	
网络安全概述	X.1500–X.1519
脆弱性/状态信息交换	**X.1520–X.1539**
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1524 建议书

通用缺陷列表（CWE）

摘要

本建议书涉及通用缺陷列表（CWE）的使用，提供了一种用于交流信息安全缺陷的结构化手段，其中包含了通信网络、最终用户设备或任何其它类型能够运行软件的信息通信技术使用的商业或开源软件中已知问题的通用名称。CWE的目标是使人们实现更有效地讨论、描述、选择和使用能够在源代码和操作系统中发现这些缺陷的软件安全工具和服务，以及更好地了解和管理与架构和设计相关的软件缺陷。本建议书定义了CWE的使用，提供了一种能使软件安全工具、服务、知识库和其它功能同时使用的机制，方便了安全工具和服务的比较。CWE还提供了有关可能出现的风险、影响、修复程序信息的背景信息，以及有关软件缺陷可能对软件系统产生的影响的详细技术资料。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1524	2012-03-02	17

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2013

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页码

1 范围 1
2 参考文献 1
3 定义 1
3.1 其它地方定义的术语 1
3.2 本建议书中定义的术语 1
4 缩略语和首字母缩写 2
5 用法惯例 3
6 高层管理要求 3
7 精确度 4
8 有效性 5
9 文档 5
10 CWE版本的使用 5
11 CWE兼容性的撤销 6
12 审核机构 7
附件A 针对具体类型的要求 8
A.2 工具要求 8
A.3 安全服务要求 9
A.4 在线能力要求 9
附件B 媒体要求 11
B.3 电子文件（HTML、文字处理器、PDF、ASCII文本等） 11
B.4 图形用户界面（GUI） 11
附录一 CWE标识符及相关背景信息贮存库列表 12
附录二 审核机构名单 13
参考资料 14

引言

通用缺陷列表（CWE）建议书对CWE的使用方法做了说明，它是一个交流统一和可测量的软件缺陷的结构性手段，旨在为众所周知的问题提供通用名称。CWE的目标是便于更有效地讨论、描述、选择和使用软件安全工具和服务，以便在源代码和操作系统中发现这些缺陷，并更好地了解和管理与架构和设计相关的软件缺陷。

CWE的目的在于全面了解所有众所周知的弱点和敞口背后的起因，无论它们存在于软件架构、设计、代码当中，还是部署当中。虽然CWE旨在涵盖成熟信息，但其首要目标是发现导致弱点和敞口的缺陷。如本建议书所定义的，CVE标识符使用的一致性由审核机构决定。

CWE利用网络安全界的现有工作成果，例如的ITU-T X.1520建议书—常见漏洞和敞口（CVE）提及的大量现实存在的不同漏洞。许多来源和实例被用于确定具体明确的CWE清单内容和分类树形结构的定义。此外，还对CWE和CVE标识符进行了适当映射，使每个CWE组或成分都拥有一份属于该具体CWE类型的软件安全漏洞的详细CVE标识符列表。在构建CWE列表和分类树形图时，力求最大限度地全面覆盖相关的概念、业务和技术领域。

ITU-T X.1524建议书 – 通用缺陷列表（CWE）是在MITRE 公司的协作下制定的，期间考虑到了在ITU-T X.1524建议书 – 通用缺陷列表（CWE）与 2011年7月28日的《对CWE兼容性和有效性的要求和建议》（1.0版）[https://cwe.mitre.org/compatible/requirements_v1.0.html]之间尽可能保持技术兼容的重要性。

ITU-T X.1524 建议书

通用缺陷列表（CWE）

1 范围

有关使用CWE的本建议书为全球信息交换提供了一种“结构性手段”，以便对存在于架构、设计、代码或部署工作中并可能导致软件系统不安全、不可靠和易受攻击的软件安全漏洞做出说明。安全工具、评估服务和某些类型的安全审查可以发现这类软件漏洞。这种“结构性手段”通常被称为“CWE兼容性”，并规定了CWE的正确使用方法。信息安全漏洞是一种软件错误，黑客可利用它所导致的脆弱性打入系统或网络。CWE标识符的分配超出了本建议书的职责范围。有关CWE标识符及相关背景信息贮存库列表见附录一。

本建议书明确界定了CWE的使用，CWE的目的在于全面介绍导致漏洞和敞口的根本原因，无论它们存在于软件架构、设计、代码当中，还是部署当中。虽然CWE旨在涵盖成熟信息，但其首要目标是发现、教导并说明那些导致漏洞和敞口的根本原因，使其能够被软件开发人员所避免、对其进行测试，并使开发团队能够驾驭这些漏洞和敞口，同时也使安全工具和业务能够不断地就这些漏洞和敞口做出报告。

ITU-T X.1524建议书 – 通用缺陷列表（CWE）是在MITRE公司的协作下制定的，期间考虑到了在ITU-T X.1524建议书 – 通用缺陷列表（CWE）与2011年7月28日的《对CWE兼容性和有效性的要求和建议》（1.0版）[https://cwe.mitre.org/compatible/requirements_v1.0.html]之间尽可能保持技术兼容的重要性。

2 参考文献

无。

3 定义

3.1 其它地方定义的术语

无。

3.2 本建议书中定义的术语

本建议书中定义了如下术语：

3.2.1 准确率：审核抽样中参照正确CWE标识符的安全要素的比例。

3.2.2 能力：评估工具、综合开发环境（IDE）、编码审核工具、编码检查编辑器、数据库、网站、通报或提供有关在实施、设计和架构层导致可被利用的软件安全弱点的漏洞信息服务。

3.2.3 CWE兼容性要求评估表：本评估表包含一系列问题，要求能力拥有者以文本、图像或网络参考文献的形式记录其与本建议书的兼容性要求的合规情况，以及有关如何提交填妥表格的说明，或请审核机构就如何填写评估表做出澄清。

3.2.4 CWE有效性要求评估表：本评估表包含一系列问题，要求能力拥有者以文本、图像或网络参考文献的形式记录其与本建议书的有效性要求的合规情况，以及有关如何提交填妥的表格，或请审核机构就如何填写评估表做出澄清。

3.2.5 有效性测试：确定能力是够具有CWE效率的程序。

3.2.6 映像/映射：对贮存器中的漏洞要素和与这些要素相关的CWE项目之间关系的规范。

3.2.7 拥有者：对能力负有责任的管理方（个人或公司）。

3.2.8 贮存器：安全弱点数据库、编码分析器的一套图形或网站等可向能力提供支持的一系列暗示或明示的与安全相关的软件漏洞要素。

3.2.9 审核：判定能力是否与CWE兼容的程序。

3.2.10 审核机构：从事审核或有效性测试并有权授予CWE兼容或CWE有效状态的实体（MITRE是目前唯一的审核机构）。

注意，附录二含有一份审核机构名单。

3.2.11 审核版本：用于确定能力具有CWE兼容性或CWE有效性的注明日期的CWE版本。

3.2.12 安全要素：与具体安全漏洞相关的数据库记录、评估调查、签名等。

3.2.13 任务：工具的调查、检查、签名等功能，可从事某些安全信息生成工作（如安全要素）。

3.2.14 测试结果：提出有效性测试结果的数据。

3.2.15 工具：一种软件应用和装置，负责检查一个软件、二进制或其它人工制品，并生成有关源代码安全分析器、代码质量评估工具、代码检查编辑器或发展环境等安全漏洞的信息。

3.2.16 用户：能力的消费者或潜在消费者。

3.2.17 漏洞：所有可被用来破坏系统或系统所存信息的软件弱点（根据ITU-T X.1500建议书）。

3.2.18 缺陷：软件编码、设计、架构或部署中的缺点或瑕疵，它们可在某个时候成为漏洞，或催生其它漏洞。

4 缩略语和首字母缩写

本建议书使用下述缩略语和首字母缩写：

ASCII 美国信息交换标准代码

CCR 覆盖主张表达

CGI 通用网关接口

CWE 通用缺陷列表

GUI 图形用户接口

HTML 超文本标识语言

HTTP 超文本传输协议

ICT 信息通信技术

PDF 便携文件格式

POC 联系人

URL 统一资源定位符

XML 可扩展标记语言

5 用法惯例

无。

6 高层管理要求

以下各段定义了与正确使用CWE标识符相关的概念、作用和责任，以便在各个安全漏洞能力（工具、贮存器和服务）之间共享信息，使这些安全漏洞能力得到集中使用，并便于对安全漏洞工具和服务进行比较。

6.1 能力的拥有者应是有效的法人实体，如拥有有效电话号码、电子邮件地址和街区邮政地址的机构或具体个人。

6.2 除CWE自身提供的信息（即姓名、说明、参考和相关的漏洞数据）之外，该能力应当提供附加的含义或信息。

6.3 能力拥有者应向审查机构提供一名技术联系人，此人有资格回答与映射准确性和所有与CWE相关的能力功能的问题，并协调能力测试，以支持CWE有效确定的评估。

6.4 这一能力应以产品或公共版本向公众或向一些消费者提供，例如，在公共网站上提供、作为开源软件开放使用、可供购买或可通过合同获得服务）。

6.5 就CWE兼容性而言，能利拥有者应向审查机构提供完整的“CWE兼容性要求评估表”。

6.6 能力拥有者应允许审核机构自由访问贮存器，从而使机构能够确认贮存器全部达到了相关的映射准确性要求。

6.7 能力拥有者应允许审核机构利用贮存器应纳入CWE的所有漏洞。

6.8 为使CWE发挥效力，该能力应做到CWE兼容。

6.9 为使CWE发挥效力，能力拥有者应向审核机构提供一份填好的“CWE有效性要求评估表”。

6.10 为使CWE发挥效力，能力拥有者应向审核机构提有效性测试结果，使该机构能够确定该能力达到了所有相关有效性要求。

6.11 能力拥有者应同意遵守所有强制性的CWE兼容性和有效性要求，其中包括对能力具体类型的强制性要求。

6.12 为实现CWE的兼容性，能力应允许用户利用CWE标识符（“CWE-搜索”）定位安全要素。

6.13 为实现CWE的兼容性，当能力向用户介绍安全要素时，应允许用户获取相关的CWE标识符（“CWE-输出”）。

6.14 为实现CWE的兼容性，能力的映射应准确地将安全要素与相应的CWE标识符准确挂钩（“映射精度”）。

6.15 为实现CWE的兼容性，能力文档应充分介绍CWE、CWE兼容性和能力中与CWE相关功能的使用方法（“CWE-文档”）。

6.16 为实现CWE的兼容性，能力对外提供的文档应明确列出CWE标识符，而能力拥有者将涉及的能力视为其功能性的一部分（“CWE-覆盖”）。

6.17 为实现CWE兼容性，能力对外提供的网站应将提供的能力的CWE覆盖做为CWE-覆盖主张表达（CCR）XML文档。

6.18 为发挥CWE的有效性，应在CWE网站张贴能力针对CWE标识符得出的评估结果（列为能力的CWE覆盖）（“CWE-测试结果”）。

6.19 能力应指出CWE的更新日期（“数据使用”）。

6.20 能力应满足具体类型能力的所有补充要求，如附件A所述。

6.21 能力应满足其分配媒介的所有要求，如附件B所述。

6.22 不应对能力提出如下要求：

- 使用与CWE相同的说明或参考
- 在其数据库中包括所有CWE标识符

6.23 如能力不能全部满足上述可行要求（6.1至6.22），那么能力拥有者就不能宣称它具有CWE兼容性或CWE有效性。

7 精确度

只有能力映射准确时，CWE兼容性才能促进数据共享。因此，CWE兼容性能力必需满足最低的精确度要求。

7.1 贮存库的精确率应为100%。

7.2 在审核期内，能力拥有者应更正审核机构发现的所有映射错误。

7.3 审核期过后，能力拥有者应当在该差错上报后的合理时段内更正映射差错，即贮存库的两（2）个版本或六（6）个月之内，以先到者为准。

7.4 能力拥有者应当准备并签署一份声明，尽其所能确保映射中不存在差错。

7.5 如果某项能力是基于或使用了另一种CWE兼容能力（“源”能力），且能力拥有者意识到源能力中存在映射差错，则该拥有者应向源能利拥有者报告这些差错。

8 有效性

有效性侧重于使能力的潜在用户了解能力所及领域，以确定软件中的相应漏洞。当潜在用户考虑使用一种能力或依赖于利用能力的其它人的成果时，了解能力所及领域以发现不同复杂度的漏洞对于他们十分重要。因此，CWE-有效性能力必须满足以下最低限度的有效性要求。

8.1 能力拥有者应利用“CWE有效性要求评估表”适当部分公布，他们认为其能力能够有效地定位哪些CWE标识符。这项工作可通过采用CWE覆盖主张表达（CCR） XML文档完成。

8.2 就公布的CWE标识符而言，能力拥有者应提出相应测试题的要求，使拥有者能够利用能力评估与公布的CWE标识符相应的所有漏洞的测试集。

8.3 在商定的时间范围内，能力拥有者应提交他们利用其能力评估测试集的结果。

8.4 该结果应列出每项经评估的测试集文档，以及与相应CWE标识符共置的每项漏洞的行编码。

8.5 能力拥有者应拟定和签署一项声明，同意在CWE网站张贴其能力测试结果。

8.6 能力拥有者应提交一份经修订的“CWE有效性要求评估表”，其中包括一份经更新的他们认为其能力可有效定位的CWE标识符列表，以便针对不同CWE标识符集重新进行有效性测试。这项工作可通过经更新的CWE覆盖主张表达（CCR）XML文档完成。

9 文档

下述要求适用于能力提供的文档。

9.1 文档的内容应包括CWE和CWE兼容性的简要描述，其内容可从CWE网站中的文件逐字照搬。

9.2 文档应当描述用户如何能够利用CWE标识符从能力贮存库中找到独立的安全要素。

9.3 文档应当描述用户如何能够从能力贮存库中的独立要素中获得CWE标识符。

9.4 如果文档包括索引，则该文档应在“CWE”术语项下包含CWE相关文档的参考。

10 CWE版本的使用

用户必需了解能力贮存库在CWE映射方面的“更新”程度。能力拥有者需指出映射的更新程度，其方式是提供其最后一次CWE信息更新的日期并指出其使用哪部分CWE内容及其采集CWE内容的位置。

10.1 各新版本的能力均应至少通过下述方法之一来标识创建、更新和映射所用CWE内容的最新日期：变更日志、新功能清单、帮助文件或其它机制。能力与此日期“保持一致”。

10.2 各新版本的能力均应与公布的CWE日期保持同步，该日期不得超过向用户提供此项能力后的四（4）个月。如果某项能力无法满足这一要求，则可认为其已“过期”。

10.3 拥有者应当描述其选择将某类CWE信息纳入能力时所采用的标准和机制。

11 CWE兼容性的撤销

以下说明了审核机构在撤销CWE兼容性方面的职责。

11.1 如果审核机构已经验证某能力为CWE兼容，但后来该审核机构有证据表明这些要求并未得到满足，则审核机构可撤销其批准。

11.1.1 审核机构应当指出未得到满足的具体要求。

11.2 审核机构应当判定拥有者的行为或声明是否为“有意误导”。

11.2.1 审核机构可自行对“有意误导”一词做出解释。

11.3 审核机构审议是否撤销某特定能力CWE兼容性的审查周期不得短于六（6）个月。

11.4 审核机构应当至少在取消计划实施日期之前两（2）个月，向能力拥有者和技术联系人提出撤销警告

11.4.1 如果审核机构发现拥有者的行为或声明为故意误导，则审核机构可忽略警告期的规定。

11.5 如果拥有者坚信所有要求均得到了满足，则拥有者可对撤销警告做出响应，提供详细信息说明其能力可满足这些要求的理由。

11.6 如果拥有者对能力进行了修改，使能力能够在警告期内满足相关要求，则审核机构应当终止针对该能力的撤销行动。

11.7 审核机构可以推迟撤销的日期。

11.8 审核机构应当公布某项能力的CWE兼容性已被取消。

11.9 如果审核机构发现拥有者在CWE兼容性要求方面所采取的行动是故意进行误导，则撤销至少应持续一年。

11.10 审核机构可以公布撤销的原因。

11.11 能力拥有者可在同一网站发布有关撤销的声明。

11.12 如果批准被撤销，拥有者在撤销期内不得申请重新审核。

12 审核机构

12.1 审核机构可针对具体的CWE版本，即审核版本，进行CWE兼容性审核。

12.2 审核机构应当明确指出用于判定能力兼容性的审核版本。

12.3 审核机构应当明确指出用于判定能力兼容性或有效性的CWE兼容性要求和有效性文件的版本。

12.4 审核机构可对能力贮存库中的各个要素进行审核。

12.5 审核机构应至少每年一次地检查能力的映射精确度。

附件A

针对具体类型的要求

（此附件是本建议书不可分割的组成部分）

由于许多能力均在使用CWE，因此某些类型的能力可能拥有特殊功能，需要对其CWE兼容性予以特别关注。

A.1 能力应当满足与特定类型相关的所有附加要求。

A.1.1 如果能力是一种评估工具、源或二进制编码安全分析器、编码质量评估工具、编码检查编辑器、开发环境或整合一个或多个此类项目的产品，它就必需满足工具要求A.2.1 - A.2.8的规定。

A.1.2 如果能力是一项服务（例如安全评估服务、教育或培训服务或编码和设计审核服务），它就必需满足安全服务要求A.3.1 - A.3.5的规定。

A.1.3 如果能力是一安全问题或应用软件漏洞的网上数据库或、基于网络的资源或信息站点，它就必需满足网络能力要求A.4.1 - A.4.3的规定。

A.2 工具要求

以下是对工具的特定要求。

A.2.1 工具应当允许用户使用CWE标识符在工具内部定位相关的任务（“CWE-搜索”），其方式是至少提供下述功能之一：“查找”或“搜索”功能、该工具任务名称与CWE标识符之间的映射或审核机构认为适用的其它机制。

A.2.2 对确定独立安全要素的报告而言，该工具应当通过使用下述方式之一使用户能够判定这些要素的相关CWE标识符（“CWE-输出”）：将CWE标识符直接纳入报告、在工具任务名称与CWE标识符之间提供映射或审核机构认为适用的其它机制。

A.2.3 公开提供的文档应明确列出能力拥有者认为其工具可在软件中有效定位的CWE标识符（“CWE兼容性主张覆盖”）。

A.2.4 功能的对外网站可提供CWE兼容性要求覆盖作为覆盖主张表达（CCR）XML文档。

A.2.5 所有必要的报告或映射都应满足附录B提出的媒体要求。

A.2.6 工具或能力拥有者应当为用户提供与工具任务相关的所有CWE标识符清单。

A.2.7 工具应当以提供包含CWE标识符清单文件的方式，使用户能够选择任务级。

A.2.8 工具接口可以利用独立的CWE标识符，使用户能够浏览，选择或取消任务集。

A.2.9 如果工具中没有与用户在工具的A.2.5或A.2.6要求中提出的CWE标识符相关的任务，则工具应通知用户其无法执行相关任务。

A.2.10 能力拥有者应当保证（1）误报率小于100%，即如果工具报告某特定安全要素，则其至少在某些时候是正确的，且（2）漏报率低于100%，即当与特定安全要素相关的事件发生时，有时工具会报告该事件。

A.3 安全服务要求

安全服务会在工作中使用CWE兼容和CWE有效工具，但它们可能不会允许用户直接使用这些工具。因此，客户可能很难确定并比较不同业务的能力。安全业务要求旨在解决这一潜在限制。

A.3.1 安全业务应当能够通过下述一种或多种方式，利用CWE标识符告诉用户该服务测试、检测或覆盖了哪些安全要素（“CWE-可搜索”）：为用户提供CWE标识符的清单指出该业务测试、检测或覆盖的要素、为用户提供业务要素与CWE标识符之间的映射、以明确该业务测试、检测或覆盖的CWE标识符的方式或利用其它某种机制，对用户提交的CWE标识符清单做出响应。

A.3.2 对于确定单独安全要素的报告，服务应当通过下述一种或多种方式允许用户判定这些要素的相关CWE标识符（“CWE-输出”）：允许用户将CWE标识符直接纳入报告、为用户提供安全要素与CWE标识符间的映射或通过其它某种机制实现。

A.3.3 公开提供的文档应明确列出能力拥有者认为安全服务可在其业务提供中有效覆盖的CWE标识符（“CWE兼容性要求覆盖”）。

A.3.4 能力对外提供的网站可提供能力的CWE兼容性主张覆盖，作为CWE覆盖主张表达（CCR）XML文档。

A.3.5 服务提供的所有规定报告或映射均应满足附录B规定的媒体要求。

A.3.6 如果服务允许用户直接使用列出安全要素的产品，则该产品应为CWE兼容和CWE有效。

A.3.7 能力拥有者应当保证（1）误报率小于100%，即如果工具报告某特定安全要素，则其至少在某些时候是正确的，且（2）漏报率低于100%，即当与特定安全要素相关的事件发生时，有时工具会报告该事件。

A.4 在线能力要求

以下是对在线能力的特定要求。

A.4.1 在线能力通过提供下述功能，允许用户从在线能力贮存库（“CWE-可搜索”）中查找相关的安全要素：能够将CWE标识符退给相关要素的搜索功能、将各要素与相关CWE标识符连接在一起的映射或某种其它机制。

A.4.1.1 在线能力应当提供一个URL“模板”，使计算机程序能够方便地建立链接，以利用A.4.1在线能力要求中描述的搜索功能。

示例：

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

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

A.4.1.2 如果网站无需登陆就可公开访问，cgi程序就应接受“GET”方法。

A.4.2 对于标识独立安全要素的报告，在线能力应当通过下述一种或几种方式允许用户判定这些要素的相关CWE标识符（“CWE-输出”）：允许用户将CWE标识符直接纳入报告、为用户提供安全要素与CWE标识符之间的映射或通过某种其它机制实现。

A.4.3 对外提供的文档应明确列出能力拥有者认为在线能力贮存器可覆盖的CEW标识符（“CWE兼容性主张覆盖”）。

A.4.4 能力对外提供的网站可提供能力的CEW兼容性主张覆盖，作为CWE覆盖主张表达（CCR）XML文档。

A.4.5 如果在线能力不提供单独安全要素的详细信息，在线能力则应提供将各元素与相关CWE标识符连接在一起的映射。

附件B

媒体要求

（此附件是本建议书不可分割的组成部分）

B.1 CWE兼容能力使用的传播媒体应采用本附件中包括的媒体格式。

B.2 媒体格式应当满足对该格式的具体要求。

B.3 电子文件（HTML、文字处理器、PDF、ASCII文本等）

B.3.1 文件应使用常用的格式，其阅读器支持“查找”或“搜索”功能（“CWE-可搜索”），例如原始ASCII文本、HTML或PDF。

B.3.2 如果文件仅提供针对单独要素的短名称或标题，它应列出与这些要素相关的CWE 名称（“CWE-输出”）。

B.3.3 文件应当包括要素与CWE标识符之间的映射，列出各要素的相应页数。

B.4 图形用户界面（GUI）

以下是对图形用户界面的特定要求。

B.4.1 GUI应当为用户提供搜索功能，允许用户输入CWE标识符并对相关要素进行检索（“CWE-可搜索”）。

B.4.2 如果GUI列出了单独要素的详细内容，则其应当列出映射至该要素的CWE标识符（“CWE-输出”）。否则，GUI应以符合B.3.1电子文件要求的格式向用户提供映射。

B.4.3 GUI应以符合B.3.1电子文件要求的格式，导出或访问CWE相关数据。

附录一

CWE标识符及相关背景信息贮存库列表

（此附录并非是本建议书不可分割的组成部分）

MITRE 公司	cwe.mitre.org/data

附录二

审核机构名单

（此附录并非是本建议书不可分割的组成部分）

1 MITRE 公司，联系方式：cwe@mitre.org。

参考资料

[b-ITU-T X.1500] ITU-T X.1500 建议书 (2011)，网络安全信息交换概述。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2013年，日内瓦