国 际 电 信 联 盟

ITU-T X.1211

(09/2014)

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

网络空间安全 – 计算网络安全

防止网络攻击的技术

ITU-T X.1211 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
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和导则	X.1640–X.1659
云计算安全的落实工作	X.1660–X.1679
其他云计算安全问题	X.1680–X.1699

欲了解更详细信息，请查阅 ITU-T建议书目录。

ITU-T X.1211 建议书

防止网络攻击的技术

摘要

ITU-T X.1211建议书阐述了能够缓解网络攻击的技术，这些网络攻击出现在网络主机漏洞被利用并引入了可能会影响用户计算机的恶意代码的情况之下。多个附录展示了攻击出现的方式以及补救措施的步骤。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1211	2014-09-26	17	11.1002/1000/12154

关键词

防止、SQL插入、间谍软件、可疑内容、漏洞、网络攻击。

* 欲查阅建议书，请在您的网络浏览器地址域键入URLhttp://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

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/。

目录

ITU-T X.1211 建议书

防止网络攻击的技术

1 范围

本建议书介绍了防止网络攻击的技术，阐述了恶意软件网络传播的使用情境以及防止网络攻击的功能性技术与功能。

2 参考文献

无。

3 术语和定义

3.1 在其它文件中定义的术语

本建议书中使用了下述在其它文件中定义的术语：

3.11 资产[b-ISO/IEC 27000]：一切对组织有价值的东西。

注 – 资产存在多种类型，其中包括：

a) 信息；

b) 计算机程序等软件；

c) 物理硬件，如计算机；

d) 服务；

e) 人员及其资质、技能和经验，以及

f) 声誉和形象等无形资产。

3.12 攻击实例 [b-ITU-T X.1544]：针对应用程序或系统，利用系统中的漏洞或薄弱环节进行的特定、详细的进攻。

3.13 攻击模式 [b-ITU-T X.1544]：在自然情况下观察到的针对应用程序或系统的常见攻击方法的抽象（例如，SQL注入攻击，中间人攻击，会话劫持等）。

注 – 一个单一的攻击模式可能潜在关联许多不同的攻击实例。

3.14 超文本标识语言（HTML）[b-ITU-T M.3030]：来自多个领域（例如，文字、图像、数据库查询结果）用于万维网浏览器显示的编码信息系统。文件内嵌有某些称为标记的特殊编码，用于指导浏览器如何提供信息。

3.15 恶意软件 [b-ISO/IEC 27033-1]：旨在专门破坏或干扰系统，攻击其保密性、完整性和/或可用性的恶意软件。

3.16 迷惑技术 [b-NIST SP 800-83]：生成病毒，为检测增加难度的方法。

3.17 个人可识别信息（PII）[b-ITU-T X.1252]：任何信息a) 识别或能用于识别、联系或定位与该信息相关的个人；b) 从这些信息能够获得某个人的识别或联系信息；或c) 该信息能够直接或间接与一个自然人相关联。

3.18 威胁 [b-ITU-T X.800]：破坏安全性的潜在可能。

3.19 安全域 [b-ITU-T T.411]：遵循同一安全政策的一批资源。

3.1.10 安全域管理机构 [b-ITU-T X.810]：负责安全域安全政策实施的安全管理机构。

3.1.11 安全政策 [b-ITU-T T.411]：维持一批资源的目标安全水准所需的程序和服务规则。

3.1.12 签名 [b-NIST SP 800-83]：已知恶意软件实例的一系列特性，可用于确定已知恶意软件或其部分新的变种。

3.1.13 间谍软件[b-NIST SP 800-83]：意在侵犯用户隐私的恶意软件。

3.1.14 网络浏览器植入机制[b-NIST SP 800-83]：通过网络浏览器显示或执行某类内容的机制。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 异常：与预期行为不符的数据模式。

3.2.2 偷渡式下载攻击：一种当用户访问网站时引起的网络攻击模式，在用户不知情或不允许的情况下利用浏览器的漏洞启动自动下载并安装恶意软件。

3.2.3 网络攻击：网络攻击是攻击者利用网络漏洞对合法网络进行的攻击模式，导致某项应用被注入恶意代码，这种代码反过来可用于感染访问这些网站的用户计算机或利用网站的漏洞攻击用户的计算机系统（其发生不会涉及恶意软件）。

3.2.4 网络攻击保护系统：检测合法网站所嵌入漏洞、恶意软件或恶意代码，并将检测结果通知网络管理员，从而最终将其移除的一套系统。

注 – 检测活动可能按规划实施、由网络事件触发或由其它系统提出申请。

3.2.5 僵尸计算机：受到攻击者破坏和控制的计算机。攻击者将计算机病毒、特洛伊木马或僵尸网等恶意软件植入计算机，用于实施恶意攻击，例如传播电子邮件垃圾信息及开发拒绝服务攻击。

4 缩略语和首字母缩写词

本建议书使用了如下缩略语和首字母缩写词：

CSRF 跨网站请求伪造

CAPEC 常见攻击方式列举和分类

CWE 常见弱点列举

DDoS 分布式拒绝服务

DOM 文件对象模型

HTML 超文本标识语言

HTTP 超文本传输协议

ID 身份（Identity）

IODEF 事件对象描述交换格式

LDAP 轻权目录访问协议

MITM 中间人

OS 操作系统

OWASP 开放网络应用安全计划

PC 个人计算机

PII 个人可识别信息

PUI 在查程序

SNS 社交网络服务

SQL 结构化查询语言

SSL 安全套接层

SSRF 服务器侧请求造假

S/W 软件

TLS 传输层安全

URI 统一资源标识符

URL 统一资源定位符

XSPA 跨网站端口攻击

XSS 跨网站脚本攻击

5 排印惯例

无。

6 概述

用于危及信息资产的恶意软件旨在专门破坏或干扰系统，攻击其保密性、完整性和/或可用性。此类软件包括计算机病毒、蠕虫、特洛伊木马、间谍软件、广告软件、多数隐匿程式和其它恶意程序。

网络攻击中的攻击者试图利用合法网络的漏洞攻击这些网络，在这些网站植入恶意代码，并以此感染访问这些网站的其它用户的计算机。恶意代码可能存在多种形式：既可能是用于指挥用户访问攻击网站的隐藏iframe标记，也可能是以计算机程序语言（例如脚本或小应用程序）编写的恶意应用程序。典型的网络攻击漏洞示例包括SQL植入和跨网站请求伪造。

跨网站请求伪造攻击模式[b-CAPEC-62]是一种网络攻击，当用户登录信任网站后，在其不知情的情况下，发出未经授权的命令或实施有违本意的操作。结构化查询语言（SQL）植入攻击模式[b-CAPEC-66]属于针对数据库驱动网站的网络攻击，攻击者在网上表格输入框内加入结构化查询语言（SQL），以获取资源或修改数据。此攻击用于从通常并不开放的数据库窃取信息和/或通过载有该数据库的计算机进入某一组织的主机。Iframe标记[b-iframe]作为一种线内帧，用于在超文本标识语言（HTML）文件内嵌套不可见的文件，通过点击劫持（clickjacking）引诱用户点击不可见文件[b-CAPEC-103]。

近来，由于最终用户计算设备使用的增长以及包含恶意软件的网站数量的上升，网络攻击始终呈大幅上升之势。

例如，可在服务器端实施防病毒技术或在代理服务器安装网络应用防火墙，从而以高成本效益的方式使用这些技术。

在网络攻击中，网站管理员可能并未意识到网络受到黑客攻击，被植入恶意代码并被用于传播这些恶意代码。此外，用户可能也未意识到其已受到所访网站恶意代码的感染。安装防病毒软件（S/W）能够防止部分事件，但无法提供最终解决方案。

网络攻击增加的原因如下：

- 从主流网站进行偷渡下载攻击的现象在增加；
- 攻击的迷惑性明显增强并动态变化，致使传统恶意软件的测防方案失效；
- 攻击目标是最终用户的网络浏览器插件；
- SQL植入攻击被用于感染主流网站；
- 恶意广告将用户引导至恶意网站；且
- 独特且有针对性的恶意软件事例出现了爆炸性增长。

7 网络攻击保护系统的技术

7.1 一般技术

网络攻击保护系统具有下列技术和特性：

- 可扩展性、强健性和弹性；
- 跨多安全域使用，由负责安全的管理员管理各域；且
- 就网站的漏洞或受恶意软件感染的网站（即使用不可见iframe的网站将用户重新引导至受恶意软件感染的网站[b-CAPEC-103]）交流信息。

注 – 现有的事件对象描述交换格式（IODEF）[b-ITU-T X.1541]可用于交换信息。

- 可能使用两类部署模式中的一种：一种集中模式和一种分布模式。在集中模式中，所有有关受恶意软件感染的网站以及各类恶意软件的信息，均应上报给集中式服务器并由其维护或控制。在分布模式中，各安全域应建立主管代理，并在各分散位置的主管代理间交流有关受恶意软件感染网站和恶意软件类型的信息。
- 可能会配置为分层的方式，以促进可扩展的操作。

7.2 功能性技术

下列功能性技术属于网络攻击保护系统的特性：

- 从合法网络内容中辨认出已知恶意软件，防止网站被安装恶意软件；
- 检测出将用户重新引导至受恶意软件感染网站的不可见iframe；
- 检测出可用于诸如SQL植入、跨网站引用等附录IV所述典型网络攻击的漏洞；
- 使用签名分析或对等分析，检测网站内的已知恶意软件；
- 开展确定已知恶意软件的行为分析；
- 通知网站管理员，其网站已被恶意软件感染并请其删除该网站的恶意软件；

- 检测出迷惑性的恶意软件，使用的方法包括字符串分割、字符串编码、自定义字符串编码、脚本行为修改、迷惑文件对象模型（DOM）修改功能、将链接隐藏于公共服务之后，以及网站的页面重定向；
- 检测出可用于跨网站引用伪造攻击的恶意软件；
- 评估网站可疑恶意软件的行为；
- 在用户访问受感染网站时通知其该网站已受感染；
- 当网络攻击保护系统在某网站检测到恶意软件时，通知安全管理员，该网站已受感染且其感染的恶意代码最终可用于网络攻击；
- 交换有关恶意网站黑名单的信息；
- 确定网站的漏洞，其中包括SQL植入及跨网站脚本攻击，此外还应将确定的这些漏洞通知相关网站的管理员。

7.3 管理技术

下列管理技术属于网络攻击保护系统的特性：

- 部署在不同安全域内的网络攻击保护系统，支持基于安全政策的安全管理；
- 拥有统一的接口，用于支持集中管理系统的管理；
- 支持信任管理，仅接受来自受信任安全域与攻击相关的事件数据；
- 支持系统资源管理，保护系统不出现过载的情况；且
- 支持操作与维护管理，其中包括系统配置管理、日志管理和系统状态监测等。

7.4 安全性和隐私保护技术

下列安全性和隐私保护技术属于网络攻击保护系统的特性：

- 通过安全域间的通信提供保密性、数据来源认证和保证信息交换的完整性；
- 防止泄漏个人可识别信息（PII）的风险。此类信息由网络防护系统处理；
- 提供应对各类网络攻击所需的弹性，例如DDoS攻击；和
- 提供审计功能，该功能能够追踪未经授权实体对网络攻击保护系统所采集信息的误用和滥用。

8 网络攻击保护系统的功能

网络攻击保护系统应至少，但不限于提供以下功能：

- 检测网站的所有已知漏洞；
- 检测网站的相关恶意软件，由这些恶意软件实施的其它恶意软件的传播；

- 通知网站管理员，其网站包含恶意软件和可供攻击者利用的已知漏洞；
- 采集有关网站漏洞及其所包含恶意软件的必要信息；
- 分享关于受恶意软件感染网站的信息，以及在安全域和多个域内可信任实体间传播恶意软件的信息；
- 在域内实施网络保护系统安全政策；和
- 使网络攻击保护系统免受任何攻击。

9 信息交换格式

应当强化恶意软件分析信息（例如，恶意软件属性的列举和特性化）的交流。实施本建议书的用户可将[b-ITU-T X.1546]用于交换恶意软件分析信息。

附录 I

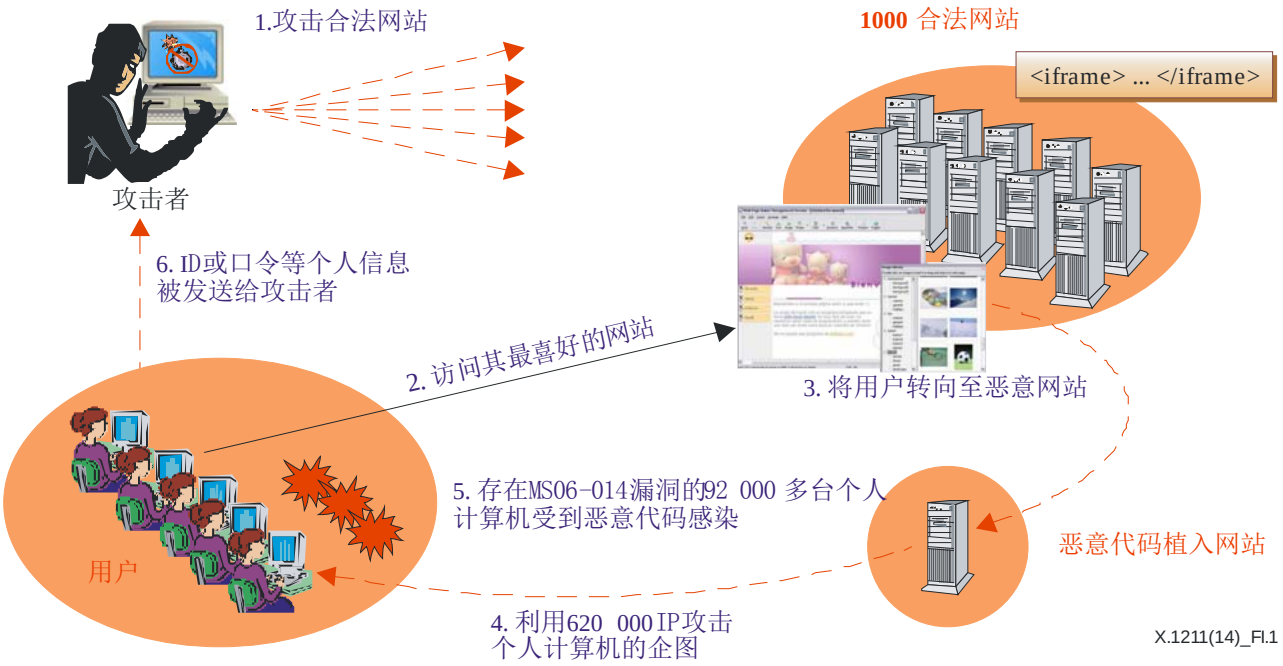
网络攻击情景

（本附录并非此建议书不可或缺的组成部分）

I.1 恶意软件感染的情景

图I-1描述了典型的网络攻击情景。

1. 攻击者感染有漏洞的合法网站后安装恶意软件或脚本，用以攻击用户的计算机或以安装标记的手段将用户访问转向包含恶意软件的网站，随后攻击该恶意网站采访用户的计算机。
2. 当用户，即受害者访问了被攻击者感染的网站后，用户的计算机会受到内置恶意软件的攻击，或被转向至包含有会攻击用户计算机的恶意软件的网站。
3. 当用户计算机存在可供特定恶意软件利用的浏览器漏洞时，该恶意软件将安装于用户计算机之上，在用户不知情或用户未允许的情况下，成为受恶意软件感染的计算机。
4. 安装于用户计算机上的该恶意软件可用于发起大规模分布式拒绝服务（DDoS）攻击或窃取身份（ID）和口令等个人信息，并将其转给攻击者。



图I.1 – 典型网络攻击方案

I.2 跨网站请求伪造（CAPEC-62）

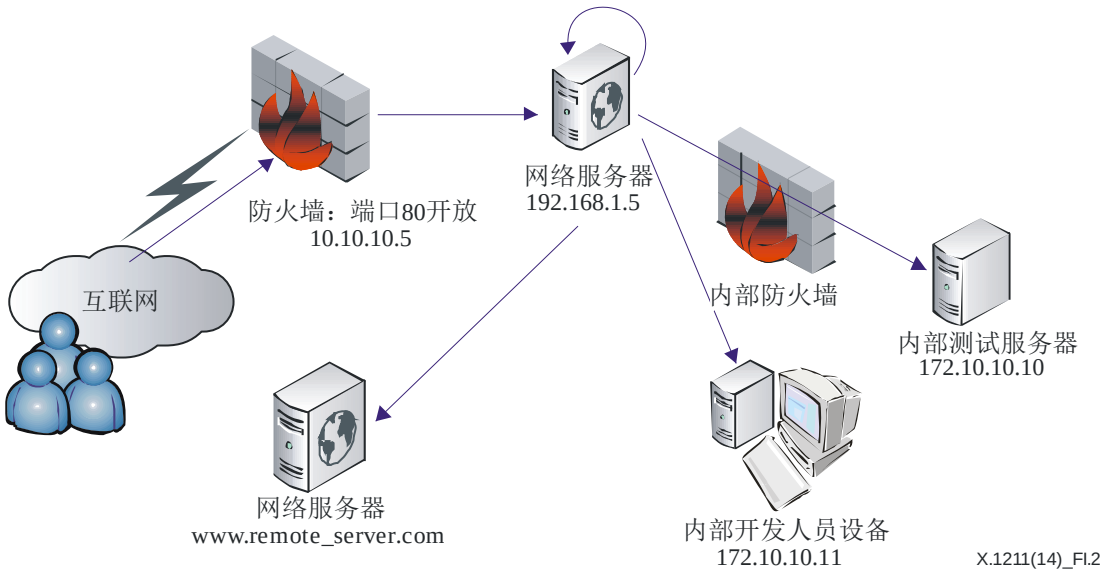
跨网站请求伪造（CSRF）可能会造成受害者不自觉地向用户信任且存在漏洞的网站提交一个或多个超文本传输协议（HTTP）请求。典型跨网站请求伪造攻击可能会相应的破坏数据完整性，赋予攻击者修改该有漏洞网络所存储信息的能力。

当网站要求用户认证时，其通常不会规定用户就每一HTTP请求输入口令。与之相反，网络采用会话标签（cookies）或HTTP认证报头确认多个HTTP请求的用户认证状态。但是，这存在一个问题：网络浏览器会记忆与统一资源定位符（URL）相关联的令牌，当向网站发送新HTTP请求时会自动附着，即便该请求并非用户的本意。CSRF会利用浏览器的行为方式。有了CSRF，用户只要访问包含有JavaScript逻辑、向其它网站（例如用户的银行）发出（可能是隐藏状态）HTTP请求的恶意网站，则由于令牌的存在，那些HTTP请求可能要经网站授权。CSRF支持各类攻击，例如通过网上邮件服务发送电子邮件、以用户身份对博客发表评论、改变用户在社交网络服务（SNS）中的朋友列表或改变归属路由器的设置。

I.3 跨网站端口攻击/服务器侧请求伪造

跨网站端口攻击/服务器侧请求伪造（XSPA/SSRF）是一种滥用网络应用的方法，此类网络应用负责处理网络浏览器输入所提供的URL。典型的XSPA/SSRF攻击是针对存在漏洞应用的内部网。攻击可能会引发端口扫描、破坏数据保密性、执行未经授权的代码和利用存在漏洞的内部网资源。

如果应用不批准对从远程主机收到的输出内容和最终用户所提供输入内容的认证，则应认为其存在XSPA/SSRF漏洞。例如，从用户提供的URL下载图片的应用，在用户公布URL‘http://localhost/secret.txt ’后，可以访问内部资源。在某些情况下，可使用特殊的统一资源标识符（URI）模式，使有漏洞的应用能够发送‘https’、‘gopher’、’ftp’、’ldap’等特殊服务请求。此外，还可使用‘php://fd’、’php://memory’等与特定语言相关的模式。



图I.2 – 典型的跨网站端口攻击/服务器侧请求伪造方案

I.4 SQL插入（CAPEC-66）

典型的SQL插入情景是基于网络应用输入数据的不良健康状况检查。输入的渠道多种多样，既包括GET和POST HTTP请求、浏览器cookie、基于XML的净荷和文件输入，也包含其它渠道。

接下来，目标输入内容被插入SQL查询。下文列出了HTTP“GET”参数的SQL插入基本示例：

- 原始查询的内容为 –“SELECT title，content FROM table1 WHERE id = %d”

其中“id”为目标参数。

在正常条件下，“id”为某个自然数。但由于缺乏健康检查，攻击者或可提供如下输入：

- %d =“1 UNION SELECT user，password FROM secret_table”。

这将导致“secret_table”的非授权使用，从而造成在浏览器输出中直接披露敏感数据。

根据所用SQL数据库不同，此类攻击可能会导致：

- 披露数据库或文件系统内的敏感数据；
- 数据损失/修改；
- 插入后门和权限升级；以及
- 对访问该网络的用户部署恶意软件。

I.5 检测网站中的恶意软件

检测恶意软件的技术可分为两类：异常检测和签名检测[b-NA]。

在异常检测技术中，判定在查程序是否存在恶意的标准是正常行为的构成。一种特殊类型的异常检测被称为基于规范的检测。基于规范的检测技术使用某些规范或有效行为规则集合来判定在查程序是否存在恶意。违反规则集合或规范的程序被视为恶意程序。

在签名检测中，判定在查程序是否存在恶意的标准是已知恶意程序的特征。恶意行为的特征性或签名是签名检测方法是否有效的关键。

各种检测技术可采用三种不同方法之一：静态、动态或混合态。异常检测或签名检测的具体方法或分析由技术如何采集信息进行恶意软件检测来决定。静态分析使用在检程序（静态）/进程（动态）的句法或结构特性来判定其是否存在恶意。例如，签名检测静态方法仅使用结构性信息（例如，字节顺序）来判定是否存在恶意，而动态方法将使用PUI运行时间信息（例如，运行时间栈上所见的系统）。

总而言之，静态方法试图在执行在查程序前检测恶意软件。与之相反，动态方法尝试在程序执行期间或之后检测恶意行为。

混合技术将两种方法结合在一起。在此情况下，采用静态和动态信息检测恶意软件。

检测网站恶意软件有多种技术；请参见附录III。

附录 II

恶意软件感染用户计算机的方法

（本附录并非此建议书不可或缺的组成部分）

本附录旨在阐述攻击者常用的典型方案，为管理员了解这些方案提供帮助。

网络攻击的第一步是在用户计算机上安装并运行各类恶意代码。这些代码可能包括键盘记录软件和隐匿程式（可将用户计算机变为僵尸计算机或向攻击者泄露敏感的用户信息）。

攻击目标的实现方式既可以是利用可通过浏览器访问的不同软件的若干已知漏洞（例如，ActiveX等通过浏览器操作系统访问的组件），也可是使用社会工程学手段诱骗用户在其系统上安装并运行恶意软件。另外，此攻击试图用钓鱼技术窃取用户证书，或利用隐藏于iframe的方式发动跨网站脚本攻击。

目前存在多种使用恶意软件感染用户计算机的技术：利用ActiveX组件、社会工程学技术、编解码缺失、恶意软件删除工具技术和跨网站请求伪造攻击。详细信息可通过[b-NTOBJECTives]提供。此外，[b-ITU-T X.1544]还提供了一批通用攻击模式，列出了模式和分类的完整清单。

附录 III

迷惑技术的典型示例

（本附录并非此建议书不可或缺的组成部分）

植入的恶意内容采用迷惑技术，使人类的眼睛和漏洞[b-ITU-T X.1520]检测软件无法发现恶意软件。鉴于以下原因，迷惑技术非常有效：

- 许多网站管理员对删除不理解的脚本代码非常警惕。
- 数据库管理员在清理受感染数据方面存在问题，对该寻找哪些模式无所事从。
- 许多检测方法依赖常规表述或其它与搜索字符串相关的方法，因此在确定受迷惑的HTML方面存在问题。

迷惑方法有多种：字符串分隔、字符串编码、自定义字符串编码、脚本行为修改、迷惑DOM修改功能、将链接隐藏于公共服务之后和页面转向。详细信息请参见[b-NTOBJECTives]。

附录 IV

防止网络攻击的技术

（本附录并非此建议书不可或缺的组成部分）

本附录旨在介绍若干网站恶意软件检测技术[b-NTOBJECTives]。恶意内容的检测可能通过内容签名匹配、攻击网站黑名单或通过专用算法对可疑行为开展内容分析。

IV.1 消灭网站漏洞

最简单的方法是删除网站漏洞，包括消灭SQL植入和跨网站脚本攻击。如果攻击者 不能向网站植入恶意内容，则客户端浏览器将不能执行植入网站的恶意软件。因此，防止网络攻击最效的方法是消除网站所有的漏洞。

IV.2 签名匹配

鉴于目前有多种迷惑技术和自动化工具可用于生成迷惑性恶意软件，因此使用签名检测方法检测网站内的恶意软件内容不切实际。众所周知，攻击者可利用针对每个网站的新密钥实现恶意内容的自动编码，从而为各网站的恶意软件创建一个不同的签名。

但是，普通恶意软件内容并不会经常改变，因此网站中的恶意软件可用签名来检测。如果普通恶意软件内容是通过恶意软件编解码获取，且普通恶意软件的签名是在普通恶意软件基础上计算得出，则此方法可以通过将计算得出的恶意软件签名与事先编辑的恶意软件完整清单加以比对，检测出恶意软件。

IV.3 网站黑名单

列出攻击网站黑名单是最有价值的检测技术之一。尽管恶意内容可完全隐匿于善意网站（不要求从攻击网站自动加载任何脚本或iframe，因此隐藏了其与攻击网站的连接），但其必须与攻击网站交换部分数据，方能完成意向中的攻击。这种必要的数据交换可能出现多种形式：攻击脚本需要从攻击网站下载恶意软件，或将收集到的私人数据从用户系统发送至攻击者的网站，抑或采用其它某种形式。无论如何，攻击脚本需与攻击网站建立连接。

如果检测算法能够检测到与黑名单所列站址外部资源相关的信息，则可怀疑该网站有恶意软件。因此，点击黑名单所列网站后该算法将指出，正在分析的网页存在恶意内容。

IV.4 检测迷惑技术

如果某网站网页包含用迷惑技术编码的内容，则有理由认为该网站存在恶意目的。例如，如果某网站包含长编码字符串内容，则此内容可能是恶意内容。但是，尽管长编码字符串内容可疑，但在解码并对其行为加以分析之前不能始终假设该网站有恶意内容。

IV.5 可疑内容行为的评估

最有效的方法是分析可疑内容的行为。如果该内容的活动可疑，则其可能是存在邪恶意图的指标。可被视作恶意的典型行为包括，访问本地硬盘、壳应用对象的实例化以及下载（访问）外部可执行内容。

附录 V

OWASP应用安全风险的典型示例

（本附录并非此建议书不可或缺的组成部分）

开放网络应用安全计划（OWASP）是一种开放源协作，其协作对象包括由业届领袖、教育组织和世界各地个人提供的网络安全工具、技术和方法，该计划公布的OWASP十类成功网络攻击[b-OWASP]和常见弱点列举（CWE）[b-ITU-T X.1524] CWE-928：表V.1所示为OWASP弱点排名的前十名[b-CWE]。

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-1 – 植入	能够向系统发送非受信数据的任何人，包括外部用户、内部用户和管理员。	攻击者利用目标解析程序的句法漏洞，发送简单的文本攻击。包括内部源在内的几乎所有数据源均可成为植入向量。	植入缺陷出现在应用向解析程序发送非受信数据时。植入缺陷非常普遍，特别是在传统代码中，并经常出现在诸如SQL查询、LDAP查询、XPath查询、OS命令、程序参量中。在审核代码时很容易发现植入缺陷，但通过测试检测难度越高。扫描程序和漏洞检查工具可帮助攻击者找到植入缺陷。	植入可能会造成数据丢失或损坏，缺乏可靠性或造成拒绝接入。植入有时会导致主机的全面接管。	会对受影响的数据和运行解析器平台的商业价值产生影响。所有数据均存在被盗、篡改或被删除的风险。您的声誉或许也会受到损害？	CWE-929， CWE-77， CWE-78， CWE-89， CWE-90， CWE-91

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-2 – 中断认证和会话管理	匿名的外部攻击者以及有自身账户并可能窃取它人账户者。另外，还应考虑希望掩盖其行动的内部人员。	攻击者使用认证或会话管理功能中泄露的信息或缺陷（例如，暴露账户、口令和会话ID）假冒用户。	开发人员经常建立自定义的认证和会话管理模式，但要确保其正确却并非易事。因此自定义模式在退出、口令管理、超时、用户记忆、账户更新等方面存在缺陷。鉴于每项实施均具有唯一性，寻找此类缺陷有时非常困难。	此类缺陷可能会使部分甚至是所有账户受到攻击。一旦成功，攻击者就可以完成受害者能够进行的任何操作。特权账户经常成为攻击目标。	这方面应考虑到受影响数据或应用功能的商业价值。 亦应考虑漏洞被公之于众产生的商业影响。	CWE-930， CWE-256， CWE-287， CWE-522， CWE-613， CWE-384， CWE-311， CWE-319， CWE-523， CWE-620， CWE-640

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-3 – 跨网站脚本攻击(XSS)	能够向系统发送非受信数据的任何人，包括外部用户、内部用户和管理员。	攻击者利用目标解析程序的句法漏洞，发送简单的文本攻击。包括数据库内部源在内的几乎所有数据源均可成为攻击向量。	XSS是最普遍的网络应用安全缺陷。当应用在向浏览器发送的页面内纳入用户提供的数据但未经验证或逃避对该内容的验证时，将出现XSS缺陷。目前有三种已知XSS缺陷：1）存储、2）反射和3）基于XSS的DOM。 通过检测或代码分析容易检测出大多数XSS缺陷。	攻击者可在受害者浏览器内执行脚本，以劫持用户会话、改变网站的外观、插入有敌意的内容、使用户转向、使用受恶意软件支持用户的浏览器等。	这方面应考虑到受影响系统及其所处理的全部数据的商业价值。 亦应考虑漏洞被公之于众产生的商业影响。	CWE-931 CWE-79
A-4 – 不安全的对象直接引用	请审核您系统用户的类型。是否有些用户只能部分访问某些类型的系统数据?	攻击者为经授权的系统用户，其仅是改变了参数值，将直接引用的系统对象改为另一未授权其使用的对象。接入是否获得批准？	应用在生成网页时经常使用实际名称或对象密钥。这些应用并不总是验证用户是否被授权访问目标对象。这就产生了“不安全的对象直接引用”缺陷。测试人可轻松地利用参数值检测出此类缺陷。代码分析会很快显示授权是否得到了恰当验证。	此缺陷将影响相关参数可引用的全部数据。除非对象引用不可预测，否则攻击者很容易访问该类型的所有可用数据。	这方面应考虑到曝光数据的商业价值。 亦应考虑漏洞被公之于众产生的商业影响。	CWE-932 CWE-22， CWE-99， CWE-639

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-5 – 不当的安全配置	匿名的外部攻击者以及有自身账户并可能企图破坏系统者。另外，还应考虑希望掩盖其行动的内部人员。	攻击者访问缺省账户、未使用的页面、未修补的缺陷、无保护的文件和目录等，以便在未授权的情况下访问或了解相关系统。	不当的安全配置可能出现在应用栈的任何层面，包括平台、网络服务器、应用服务器、数据库、框架和自定义码。开发人员需要与系统管理员合作，确保整个栈得到恰当配置。自动扫描程序在检测丢失补丁、不当配置、缺省账户使用和不必要业务等方面十分有用。	系统可能在用户不知情的情况下被全部感染。用户的全部数据都可能被盗或被逐渐修改。恢复成本可能非常高昂。	系统可能在用户不知情的情况下被全部感染。用户的全部数据都可能被盗或被逐渐修改。恢复的成本可能非常高昂。	CWE-933 CWE-2， CWE-16， CWE-209， CWE-215， CWE-548

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-6 – 敏感数据曝光	可访问用户敏感数据和一切数据备份者。这包括静止数据、转移中的数据甚至是客户浏览器中的数据。同时包括内外两种威胁。	攻击者通常不会直接破解加密。它们会破解其它一些内容，例如在传输过程中或从用户浏览器盗取密钥、实施中间人攻击或从服务器盗取明确的文本数据。	最常见的缺陷是不对敏感数据加密。加密后，低级别的密钥生成与管理以及低强度算法的使用非常普遍，特别是低强度口令破解技术。浏览器的弱点十分普遍，易于发现但很难大规模利用。由于访问的限制，外部攻击者很能检测服务器一侧，且服务器通常很难被利用。	故障经常会影响那些本应受到保护的数据。一般此类信息包含敏感数据，例如医疗病历、证书、个人数据和信用卡。	这方面应考虑到丢失数据的商业价值及其对用户声誉的影响。如果此数据曝光，您应承担什么法律责任？亦应考虑对用户声誉造成的影响。	CWE-934 CWE 311， CWE-310， CWE-312， CWE-319， CWE-325， CWE-326

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-7 – 功能层接入控制	拥有网络接入能力的所有人均可向用户的应用发出请求。匿名用户是否能够使用专项功能，常规用户是否拥有特权功能？	攻击者为经授权的系统用户，其仅将URL或参数改为指向特权功能。接入是否获得批准？匿名用户能够使用未加保护的专用功能。	应用并非总能适当地保护各项应用功能。有时功能层的保护是通过配置管理，而系统配置并不恰当。有时开发人员必须进行适当的代码检查，但他们却可能会忘记。检测此类缺陷很容易。最难的部分是确定哪些现有页面（URL）或功能可用于攻击。	此类缺陷允许攻击者使用未授权的功能。管理功能是此类攻击的主要目标。	这方面应考虑到暴露功能及其处理数据的商业价值。 亦应考虑如果漏洞曝光对用户声誉造成的影响。	CWE-935 CWE 285， CWE-287

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-8 – 跨网站请求伪造(CSRF)	可将内容上载至用户浏览器并因此强制它们向用户网站发送请求的任何一方。您所属用户接入的任何网站或其它HTML均可执行此操作。	攻击者伪造HTTP请求并欺骗受害者通过图像标记、XSS或多种其它技术提交这些请求。如果用户得到认证，则攻击取得成功。	CSRF利用了大多数网络应用允许攻击者预测特定操作细节这一事实。鉴于浏览器自动发送会话cookies等证书，攻击者可创建恶意的网页，生成与合法请求无法区分的伪造请求。通过渗透检测或代码分析很容易查出CSRF缺陷。	攻击者可诱骗受害者执行其已获得授权的改变状态操作，例如更新详细账户信息，购物、退出甚至是登录。	这方面应考虑到受影响数据或应用功能的商业价值。设想一下无法确定用户是否确实有意愿进行此类操作的情景。考虑对您声誉的影响。	CWE-935 CWE-352 CWE 346， CWE-441， CWE-346， CWE-642
A-9 – 使用有已知漏洞的组件	部分存在漏洞的组件（例如框架库）可通过自动化工具确定并加以利用，从而将造成威胁媒介的范围从目标攻击者扩大至包括行为无序的参与者在内的更多媒介。	攻击者通过扫描或人工分析确定存在弱点的组件，按需对这些组件进行自定义并发起攻击。如所用组件位于应用中很深的位置，则此攻击会变得更困难。	几乎所有应用都有此类问题，因为大多数研发团队并不关注确保其组件/库及时更新。很多时候开发者甚至不知晓其使用的全部组件，更不用说这些组件的版本了。组件间的相互依赖性使事情变得更糟。	弱点可能存在于各个方面，其中包括植入、中断接入控制、XSS等。其影响范围可从最轻微的影响一直到完全被主机接管和数据感染。	这方面应考虑到各漏洞可能给受影响应用所控制业务造成的后果。这种影响既可能微不足道，也可能是彻底的灾难。	CWE-937

表 V.1 – OWASP的十大应用安全性风险

攻击的类型	造成威胁的媒介	攻击向量	安全弱点	技术影响	业务影响	对CWE标识符的参引
A-10 – 未经验证的转向和前转	所有诱骗您用户向贵网站提交请求者。您所属用户使用的任何网站或其它HTML均可执行此操作。	与未经验证的网站相连的攻击者链接，将用户转向至并诱骗用户点击该链接。受害者很可能点击该链接，因为该链接与有效网站相连。攻击者以不安全的前转为目标，藉此绕过安全检查。	相关应用经常将用户转向至其它网页，或在类似情况下使用内容前转功能。有时目标网页使用未经验证的参数加以规范，使攻击者可选择最终的目的地网页。检测未经核查的转向并非难事。当您能够设置完成URL时，请查找是否存在转向。未核对的前转更难检测，因为它们的目标是内部网页。	此类转向可能意在安装恶意软件或诱骗受害者披露密码或其它敏感信息。不安全的前转可能允许接入控制被绕开。	这方面应考虑到维持用户信任的商业价值。如果恶意软件将其控制会产生什么影响？ 如果攻击者能够接入仅供内部使用的功能会产生什么影响？	CWE-938 CWE-601

参考资料

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications Markup Language (tML) framework.*

[b-ITU-T T.411] Recommendation ITU-T T.411 (1993) | ISO/IEC 8613-1:1994，*Information technology − Open Document Architecture (ODA) and interchange format: Introduction and general principles.*

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology − Open Systems Interconnection − Security frameworks for open systems: Overview*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions.*

[b-ITU-T X.1520] Recommendation ITU-T X.1520 (2014), *Common vulnerabilities and exposures.*

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration.*

[b-ITU-T X.1541] Recommendation ITU-T X.1541 (2012), *Incident object description exchange format.*

[b-ITU-T X.1544] Recommendation ITU-T X.1544 (2013), *Common attack pattern enumeration and classification.*

[b-ITU-T X.1546] Recommendation ITU-T X.1546 (2014), *Malware attribute enumeration and characterization*.

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2009, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

[b-CAPEC-62] CAPEC-62: *Cross Site Request Forgery (aka Session Riding).*
https://capec.mitre.org/data/definitions/62.html

[b-CAPEC-66] CAPEC-66: *SQL Injection*.
https://capec.mitre.org/data/definitions/66.html

[b-CAPEC-103] CAPEC-103: *Clickjacking.*
https://capec.mitre.org/data/definitions/103.html

[b-CWE] CWE-928: *Weaknesses in OWASP Top Ten (2013).*
http://cwe.mitre.org/data/graphs/928.html

[b-iframe] W3C (2014), *HTML <iframe> Tag*.
http://www.w3schools.com/tags/tag_iframe.asp

[b-NA] Idika, Nwokedi, and Mathur, Aditya P. (2007), *A Survey of Malware Detection Techniques*, Department of Computer Science, Purdue University, 2 February.
http://www.serc.net/system/files/SERC-TR-286.pdf

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling.*

[b-NTobjectives] Kuykendall, Dan (2009), *Is Your Website Already Infected? Analyzing and Detecting Malicious Content*, 20 March.
http://www.manvswebapp.com/is-your-website-already-infected

[b-OWASP] OWASP (2013), *OWASP Top 10 application security risks*.
https://www.owasp.org/index.php/Top_10_2013-Top_10

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
2014年，日内瓦