الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1211

(2014/09)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني – الأمن السيبراني

تقنيات لمنع الهجمات من خلال شبكة الإنترنت

التوصيـــة ITU-T X.1211

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليـــل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب	X.1149–X.1140
بروتوكولات الأمن	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
أمن الفضاء السيبراني	
الأمن السيبراني	**X.1229–X.1200**
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339–X.1310
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1659–X.1640
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أشكال أخرى لأمن الحوسبة السحابية	X.1699–X.1680

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T X.1211

تقنيات لمنع الهجمات من خلال شبكة الإنترنت

ملخص

تصف التوصية ITU-T X.1211 تقنيات يمكن أن تخفف من الهجمات من خلال شبكة الإنترنت التي قد تحدث عندما تستغل مواطن ضعف مستضيفات مواقع الويب وتدخل فيها شفرات ضارة يمكن أن تصيب حاسوب المستعمل بفيروسات. وتتناول التذييلات المتعددة بالتوضيح كيفية وقوع الهجمات فضلاً عن خطوات العلاج.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1211	2014-09-26	17	11.1002/1000/12154

كلمات رئيسية

منع، حقن لغة الاستعلام البنيوية، برمجيات تجسس، محتوى مشبوه، نقاط ضعف، هجمة من خلال شبكة الإنترنت.

* للنفاذ إلى هذه التوصية، اطبع الموقع الإلكتروني http://handle.itu.int/ في حقل العنوان بمتصفح الويب لديك، متبوعاً بمعرف الهوية الفريد للتوصية، مثلاً، http://handle.itu.int/11.1002/1000/11830-en.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتـــويات

الصفحة

التوصيـــة ITU-T X.1211

تقنيات لمنع الهجمات من خلال شبكة الإنترنت

1 مجال التطبيق

تقدم هذه التوصية تقنيات لمنع الهجمات من خلال شبكة الإنترنت. وهي تصف سيناريوهات الاستخدام لتوزيع البرمجيات الضارة عن طريق الإنترنت فضلاً عن التقنيات الوظيفية ووظائف لمنع الهجمات من خلال شبكة الإنترنت.

2 المراجع

لا توجد.

3 المصطلحات والتعاريف

1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 الأصل [b-ISO/IEC 27000]: أي شيء ذي قيمة للمنظمة.

ملاحظـــة – هناك أنواع عديدة من الأصول، ومنها:

أ) المعلومات؛

ب) البرمجيات، مثل برنامج حاسوب؛

ج) الأصول المادية، مثل الحاسوب؛

د) الخدمات؛

هـ) الناس ومؤهلاتهم ومهاراتهم وخبراتهم؛

و) الأصول غير الملموسة، كالسمعة والصورة الذهنية.

2.1.3 حالة هجوم (attack instance) [b-ITU-T X.1544]: هجوم محدد بالتفصيل ضد تطبيق أو نظام يستهدف مواطن التعرض أو الضعف في ذلك النظام.

3.1.3 نمط الهجمات (attack pattern) [b-ITU-T X.1544]: تجريد لنُهُج الهجمات الشائعة التي تلاحظ عامة ضد التطبيقات أو الأنظمة (مثل حقن لغة SQL، أو هجوم لمتطفل بين طرفين، أو قرصنة الدورة، أو غير ذلك).

ملاحظـــة – يمكن أن يكون لنمط الهجمات الواحد حالات هجوم متغيرة كثيرة مرتبطة به.

4.1.3 لغة إلحاق النصوص التشعبية (HTML) [b-ITU-T M.3030]: نظام تشفير معلومات مستقاة من مجموعة واسعة من الميادين (مثل النصوص والرسومات ونتائج الاستعلام من قاعدة بيانات) كي تعرضها متصفحات شبكة الإنترنت العالمية. فتُدمج شفرات خاصة معينة في الوثيقة تدعى وسوم بحيث يمكن إعلام المتصفح بكيفية تقديم المعلومات.

5.1.3 البرمجيات الضارة [b-ISO/IEC 27033-1]: برمجيات خبيثة مصممة خصيصاً لإلحاق الضرر بنظام أو تعطيله، مهاجمةً الكتمان و/أو السلامة و/أو التيسر.

6.1.3 تقنية التمويه [b-NIST SP 800-83]: طريقة لبناء الفيروس تجعل كشفه أكثر صعوبة.

7.1.3 المعلومات المحددة لهوية شخص (PII) [b-ITU-T X.1252]: أي معلومات أ) تعرِّف أو يمكن استعمالها في التعرُّف على الشخص الذي تخصه هذه المعلومات أو الاتصال به أو تحديد موقعه؛ ب) أو يمكن من خلالها الحصول على معلومات التعرف على شخص أو بيانات اتصاله؛ أو ج) تكون مرتبطة أو يمكن ربطها بشخص طبيعي بطريقة مباشرة أو غير مباشرة.

8.1.3 التهديد [b-ITU-T X.800]: انتهاك محتمل للأمن.

9.1.3 ميدان الأمن [b-ITU-T T.411]: مجموعة الموارد التي تخضع لسياسة أمنية واحدة.

10.1.3 سلطة ميدان الأمن [b-ITU-T X.810]: سلطة أمن تتولى مسؤولية تنفيذ سياسة أمنية لميدان الأمن.

11.1.3 السياسة الأمنية [b-ITU-T T.411]: مجموعة من القواعد التي تحدد الإجراءات والخدمات اللازمة للحفاظ على المستوى المقصود من الأمن لمجموعة من الموارد.

12.1.3 التوقيع [b-NIST SP 800-83]: مجموعة خصائص حالات البرمجيات الضارة المعروفة التي يمكن أن تستخدم لتحديد البرمجيات الضارة المعروفة وبعض تنوعاتها الجديدة.

13.1.3 برمجيات التجسس [b-NIST SP 800-83]: برمجيات ضارة تهدف إلى انتهاك خصوصية المستخدم.

14.1.3 الإضافة المساعدة لمتصفح الإنترنت [b-NIST SP 800-83]: آلية لعرض أو تنفيذ أنواع معينة من المحتوى من خلال متصفح الإنترنت.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 الشذوذ: نمط في البيانات لا يتفق مع السلوك المتوقع.

2.2.3 هجمات التنزيل أثناء التنقل: نمط من الهجمات من خلال شبكة الإنترنت، أثناء زيارة مستخدم لموقع إلكتروني، يستغل نقاط ضعف المتصفح ويطلق تنزيلاً تلقائياً ويثبِّت برمجيات ضارة دون علم المستخدم أو إذنه.

3.2.3 هجوم من خلال شبكة الإنترنت: نمط من الهجمات يخرق فيه المهاجمون المواقع الإلكترونية المشروعة مما يؤدي إلى حقن شفرة ضارة في تطبيق يمكن أن تُستخدم بدورها لإصابة حاسوب المستخدم الزائر لتلك المواقع بالعدوى، أو لاستخدام نقاط ضعف المواقع الإلكترونية لشن هجمات على أنظمة حاسوب المستخدم الذي يزور تلك المواقع، يحدث دون استعمال برمجيات ضارة.

4.2.3 نظام الحماية من هجوم من خلال شبكة الإنترنت: مجموعة من الأنظمة تكشف نقاط الضعف أو البرمجيات الضارة أو الشفرات الخبيثة المندسة في موقع إلكتروني مشروع ويبلغ المشرف على الشبكة بنتيجة الكشف مما يؤدي إلى إزالتها في نهاية المطاف.
ملاحظـــة – يمكن التخطيط لأنشطة الكشف بواسطة جدول زمني، أو قد تتفعل بأحداث الشبكة أو بطلبات من أنظمة أخرى.

5.2.3 الحاسوب المسخَّر: حاسوب مُخترَق يسيطر عليه مهاجم ثبَّت برمجيات ضارة مثل فيروسات الحاسوب أو حصان طروادة أو برمجيات روبوتية، يمكن استخدامها لتنفيذ هجمات خبيثة مثل نشر البريد الإلكتروني الطفيلي وشن هجمات الحرمان من الخدمة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

CAPEC تعداد وتصنيف أنماط الهجمات الشائعة *(Common Attack Pattern Enumeration and Classification)*

CSRF طلب مزوَّر عابر للموقع *(Cross-Site Request Forgery)*

CWE تعداد مواطن الضعف الشائعة *(Common Weakness Enumeration)*

DDoS الحرمان من الخدمة الموزَّع *(Distributed Denial of Service)*

DOM نموذج كائن الوثيقة *(Document Object Model)*

HTML لغة إلحاق النصوص التشعبية *(HyperText Markup Language)*

HTTP بروتوكول نقل النصوص التشعبية *(HyperText Transfer Protocol)*

ID الهوية *(IDentity)*

IODEF نسق تبادل وصف كائن الحادث *(Incident Object Description Exchange Format)*

LDAP بروتوكول النفاذ الخفيف إلى الدليل *(Lightweight Directory Access Protocol)*

MITM الاعتراض الوسيط *(Man-in-the-Middle)*

OS نظام التشغيل *(Operating System)*

OWASP مشروع أمن تطبيقات الإنترنت المفتوحة *(Open Web Applications Security Project)*

PC حاسوب شخصي *(Personal Computer)*

PII المعلومات المحددة لهوية شخص *(Personally Identifiable Information)*

PUI البرنامج قيد التفتيش *(Program under Inspection)*

SNS خدمة الشبكة الاجتماعية *(Social Network Service)*

SQL لغة الاستعلام البنيوية *(Structured Query Language)*

SSL طبقة المقبس الآمنة *(Secure Socket Layer)*

SSRF طلب مزور من جانب المخدِّم *(Server-Side Request Forgery)*

S/W برمجيات *(Software)*

TLS أمن طبقة النقل *(Transport Layer Security)*

URI المعرف الموحد للمورد *(Uniform Resource Identifier)*

URL المحدد الموحد لموقع المورد *(Uniform Resource Locator)*

XSPA هجوم على المنفذ عابر للموقع *(Cross-site Port Attack)*

XSS برمجة عابرة للموقع *(Cross-Site Scripting)*

5 الاصطلاحات

لا توجد.

6 نظرة شاملة عامة

تعرَّف البرمجيات الضارة التي تستخدم بغرض انتهاك أصول المعلومات على أنها برمجيات مصممة خصيصاً لإلحاق ضرر بنظام أو تعطيله، مهاجمةً الكتمان و/أو السلامة و/أو التيسر. وهي تشمل فيروسات وديدان الحاسوب، وحصان طروادة، والبرمجيات التجسسية، وبرمجيات الإعلانات، ومعظم الجذور الخفية، وغيرها من البرامج الخبيثة.

والهجمات من خلال شبكة الإنترنت هي هجوم يحاول فيه المهاجمون اختراق المواقع الإلكترونية المشروعة باستخدام نقاط الضعف فيها، مما يؤدي إلى حقن شفرة ضارة في هذه المواقع، فيمكن أن تُستخدم بدورها لإصابة حاسوب المستخدم الزائر لتلك المواقع بالعدوى. وقد تتخذ الشفرة الضارة أشكالاً متعددة: فيمكن أن تكون وسم iframe مخفياً يوجه المستخدم لزيارة موقع الهجوم، أو يمكن أن تكون تطبيقات ضارة مكتوبة بلغة برنامج حاسوبي (مثل البرامج النصية أو صغار التطبيقات). ومن الأمثلة النمطية على نقاط الضعف في الهجمات من خلال شبكة الإنترنت، حقن لغة الاستعلام البنيوية (SQL) والطلب المزوَّر العابر للموقع.

نمط الهجمة الخاصة بطلب مزوَّر عابر للموقع [b-CAPEC-62] هو نوع من الهجمات من خلال شبكة الإنترنت حيث ترسَل أوامر غير مخوَّلة أو تُطلب إجراءات غير مرغوبة ليجري تنفيذها على موقع إلكتروني موثوق دون علم المستخدم بعد أن يكون قد سجل دخوله إلى موقع إلكتروني موثوق. ونمط الهجوم بحقن لغة الاستعلام البنيوية (SQL) [b-CAPEC-66] هو نوع آخر من الهجمات من خلال شبكة الإنترنت على موقع إلكتروني تحركه قاعدة بيانات، حيث يضيف المهاجم شفرة لغة الاستعلام البنيوية (SQL) إلى إطار مدخلات استمارة موقع إلكتروني للنفاذ إلى الموارد أو إحداث تغييرات في البيانات. ويُستخدم هذا الحقن لسرقة المعلومات من قاعدة بيانات لا تكون بياناتها متاحة عادة و/أو للنفاذ إلى أجهزة الحاسوب المضيفة للمؤسسة من خلال الحاسوب الذي يستضيف قاعدة البيانات. الوسم iframe [b-iframe] رتل في الخط، aka، يُستخدم لدمج وثيقة غير مرئية ضمن الوثيقة الراهنة بلغة إلحاق النصوص التشعبية (HTML) وخداع المستعمل للنقر على الوثيقة غير المرئية عن طريق التلاعب بالنقر [b-CAPEC-103].

وفي الآونة الأخيرة، تزايدت الهجمات من خلال شبكة الإنترنت تزايداً كبيراً بسبب تزايد استخدام أجهزة المستخدم النهائي الحاسوبية والعدد المتزايد للمواقع الإلكترونية المتضمنة لبرمجيات ضارة.

فعلى سبيل المثال، يمكن تنفيذ تقنيات مكافحة الفيروسات على جانب المخدم، ويمكن تنفيذ جدران الحماية لتطبيقات الويب عند الوكلاء من أجل التنفيذ الفعّال تكاليفياً لهذه التقنيات.

وفي الهجمات من خلال شبكة الإنترنت، قد لا يكون المشرفون على المواقع على علم بأن المواقع قد اختُرقت وحُقنت بشفرات ضارة وأنها تُستخدم لنشر الشفرات الضارة. وعلاوة على ذلك، لا يدرك المستخدمون أن حواسيبهم معرضة للإصابة بشفرات ضارة من المواقع التي زاروها. وإذ يمكن منع بعض الحوادث بتثبيت برمجيات مكافحة الفيروسات (S/W)، فإن ذلك لا يقدم حلولاً نهائية.

وفيما يلي أسباب زيادة الهجمات من خلال شبكة الإنترنت:

- تزايد هجمات التنزيل أثناء التنقل من المواقع الإلكترونية السائدة؛
- هجمات على درجة عالية من التمويه ومتغيرة دينامياً تجعل السبل التقليدية في كشف البرمجيات الضارة وفي الحلول الواقية منها عديمة الفعالية؛
- هجمات تستهدف الإضافات المساعدة لمتصفح الويب لدى المستخدمين النهائيين؛
- استخدام هجمات حقن لغة الاستعلام البنيوية (SQL) لتصيب المواقع الإلكترونية السائدة بالعدوى؛
- الإعلانات الخبيثة التي تعيد توجيه المستخدمين إلى مواقع إلكترونية خبيثة؛
- النمو الهائل في عينات البرمجيات الضارة الفريدة والمحددة الأهداف.

7 تقنيات أنظمة الحماية من هجوم من خلال شبكة الإنترنت

1.7 التقنيات العامة

تعد التقنيات التالية من خصائص أنظمة الحماية من الهجمات من خلال شبكة الإنترنت:

- يصمم النظام بحيث يكون متيناً وقادراً على استيعاب مختلف المقاييس وعلى النهوض من العثرات؛
- أن يشغل عبر ميادين أمنية متعددة يدير كل منها مشرف مسؤول عن الأمن؛
- يقوم بتبادل المعلومات عن ضعف المواقع الإلكترونية، وعن المواقع الإلكترونية المصابة بالبرمجيات الضارة (أي المواقع الإلكترونية ذات الرتل i-frame غير المرئي الذي يعيد توجيه المستخدمين إلى موقع إلكتروني مصاب ببرمجيات ضارة [b-CAPEC-103])؛

ملاحظـــة – يمكن أن يُستخدم نسق تبادل وصف الكائن المتعلق بالحادث (IODEF) [b-ITU-T X.1541] لتبادل المعلومات.

- يعمل واحد من نموذجي النشر: نموذج مركزي ونموذج موزع. وفي النموذج المركزي، ينبغي الإبلاغ عن جميع المعلومات عن المواقع الإلكترونية المصابة بالبرمجيات الضارة، وأنواع البرمجيات الضارة التي ينبغي أن تبلَّغ إلى مخدِّم مركزي، أو ينبغي أن يحفظها هذا المخدِّم أو يتحكم فيها. وفي النموذج الموزع، ينبغي لكل ميدان أمني أن يعيّن وكيلاً مسؤولاً وينبغي تبادل المعلومات، عن المواقع الإلكترونية المصابة بالبرمجيات الضارة وأنواع هذه البرمجيات الضارة، بين الوكلاء المسؤولين الموجودين في مواقع موزعة؛
- يُشكل بطريقة تراتبية لتسهيل التشغيل القادر على استيعاب مختلف المقاييس.

2.7 التقنيات الوظيفية

تعد التقنيات الوظيفية التالية من خصائص أنظمة الحماية من الهجمات من خلال شبكة الإنترنت:

- التقنيات التي تحدد البرمجيات الضارة المعروفة والمتأتية من المحتوى المشروع على شبكة الإنترنت وأن يمنع تثبيت المواقع الإلكترونية المصابة بالبرمجيات الضارة؛
- التقنيات التي تكتشف الرتل i-frame غير المرئي الذي يعيد توجيه المستخدمين إلى مواقع إلكترونية أخرى تثبِّت البرمجيات الضارة؛
- التقنيات التي تكتشف نقاط الضعف التي يمكن استخدامها لشن هجمات نمطية من خلال شبكة الإنترنت مثل حقن لغة الاستعلام البنيوية (SQL) والإحالة العابرة للموقع، وما إلى ذلك، على النحو الموضح في التذييل الرابع؛
- التقنيات التي تجري تحليلاً قائماً على التوقيع أو تحليلاً مكافئاً من أجل كشف البرمجيات الضارة المعروفة الموجودة في الموقع الإلكتروني؛
- التقنيات التي تجري تحليلاً قائماً على السلوك لتحديد البرمجيات الضارة المجهولة؛
- التقنيات التي تبلغ المشرف على الموقع الإلكتروني بالإصابة بالبرمجيات الضارة لإزالتها من المواقع الإلكترونية؛
- التقنيات التي تكتشف البرمجيات الضارة المموَّهة باستخدام تقسيم السلسلة وتشفير السلسلة وتشفير السلسلة المخصص وتعديل سلوك البرنامج النصي ووظائف تعديل نموذج كائن الوثيقة (DOM) والروابط المتخفية وراء الخدمات العامة وإعادة توجيه الصفحة في الموقع الإلكتروني؛
- التقنيات التي تكتشف البرمجيات الضارة التي يمكن استخدامها لشن هجمات تزوير الإحالة العابر للموقع في المواقع الإلكترونية؛
- التقنيات التي تقيّم سلوك البرمجيات الضارة المشبوهة في المواقع الإلكترونية؛
- التقنيات التي تبلغ المستخدمين عن المواقع الإلكترونية المصابة في حال قام أحد المستخدمين بزيارة تلك المواقع المصابة؛
- التقنيات التي تبلغ المشرف الأمني بأن الموقع مصاب بشفرات ضارة يمكن أن تُستخدم في نهاية المطاف لشن هجوم من خلال شبكة الإنترنت عند اكتشاف نظام الحماية وجود برمجيات ضارة في موقع إلكتروني؛
- التقنيات التي تقوم بتبادل المعلومات بشأن القوائم السوداء التي تضم المواقع الإلكترونية الضارة؛
- التقنيات التي تحدد نقاط الضعف في موقع إلكتروني بما فيها حقن لغة الاستعلام البنيوية (SQL) والبرمجة العابرة للموقع، وأن يُعلم المشرف على تلك المواقع الإلكترونية بشأن نقاط الضعف التي جرى تحديدها.

3.7 تقنيات الإدارة

تعد تقنيات الإدارة التالية من خصائص أنظمة الحماية من الهجمات من خلال شبكة الإنترنت:

- التقنيات التي تدعم إدارة الأمن على أساس السياسات الأمنية عند نشرها في ميادين أمنية مختلفة؛
- التقنيات التي تتضمن سطحاً بينياً موحداً لدعم الإدارة في نظام إدارة مركزي؛
- التقنيات التي تدعم إدارة الثقة ولا تقبل بيانات الحدث المتعلقة بهجوم إلا من ميادين أمنية موثوقة؛

- التقنيات التي تدعم إدارة موارد النظام وحماية النظام من الحمل الزائد؛
- التقنيات التي تدعم إدارة التشغيل والصيانة بما في ذلك إدارة تشكيلة النظام وإدارة السجل ومراقبة حالة النظام، وما إلى ذلك.

4.7 تقنيات الأمن والخصوصية

تقنيات الأمن والخصوصية التالية من خصائص أنظمة الحماية من الهجمات من خلال شبكة الإنترنت:

- التقنيات التي توفر السرية والاستيقان من أصل البيانات، وسلامة المعلومات المتبادلة بين ميادين أمنية، من خلال السطح البيني للاتصالات؛
- التقنيات التي تمنع تسرب المعلومات المحددة لهوية شخص (PII) التي يعالجها نظام المنع من خلال شبكة الإنترنت؛
- التقنيات التي توفر المرونة والقدرة على استعادة الموقف إزاء مختلف الهجمات من خلال الشبكة، مثل هجمات الحرمان من الخدمة الموزَّع (DDoS)؛
- التقنيات التي توفر وظيفة التدقيق التي يمكنها أن تتبع سوء أو إساءة استخدام جهات غير مخوَّلة للمعلومات التي جُمعت من أجل هذا النظام.

8 وظائف أنظمة الحماية من الهجمات من خلال شبكة الإنترنت

ينبغي لنظام الحماية من هجوم من خلال شبكة الإنترنت أن يوفر المهام التالية، دون أن يقتصر عليها:

- كشف جميع نقاط الضعف المعروفة في المواقع الإلكترونية؛
- كشف المواقع الإلكترونية التي تحتوي على برمجيات ضارة تُستخدم لتوزيع البرمجيات الضارة؛
- إخطار المشرف على المواقع الإلكترونية التي تحتوي على برمجيات ضارة ونقاط ضعف معروفة يمكن للمهاجمين استغلالها؛
- جمع المعلومات اللازمة عن نقاط ضعف المواقع الإلكترونية والبرمجيات الضارة التي تحتوي عليها؛
- تبادل المعلومات عن المواقع الإلكترونية المصابة بالبرمجيات الضارة وتلك التي تُستخدم لتوزيع البرمجيات الضارة بين الكيانات الموثوقة في ميدان أمني وبين ميادين متعددة؛
- تنفيذ سياسة أمنية لنظام الحماية من هجوم من خلال شبكة الإنترنت في ميدان ما؛
- الحماية من أي هجمات على نظام الحماية من هجوم من خلال شبكة الإنترنت.

9 نسق تبادل المعلومات

ينبغي تعزيز تبادل المعلومات بشأن تحليل البرمجيات الضارة (من قبيل تعداد نعوت البرمجيات الضارة وتشخيصها). ويمكن لمنفذي هذه التوصية استعمال التوصية [b-ITU-T X.1546] لتبادل معلومات تحليل البرمجيات الضارة.

التذييـــل الأول

سيناريوهات الهجمات من خلال شبكة الإنترنت

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.I سيناريو العدوى بالبرمجيات الضارة

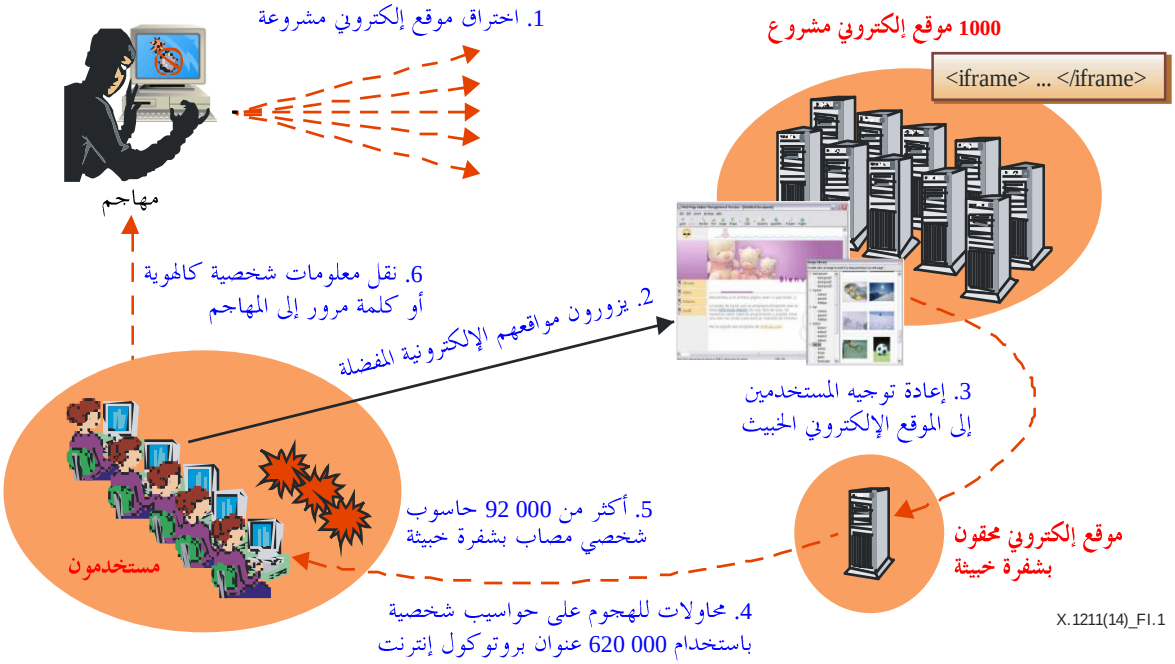
يصور الشكل I-1 السيناريو النمطي للهجمات من خلال شبكة الإنترنت.

1 يخترق المهاجمون موقعاً إلكترونياً مشروعاً فيه نقاط ضعف ثم يثبتون برمجيات ضارة أو برمجية نصية تُستخدم لمهاجمة حاسوب المستخدم أو لتثبيت وسوم تعيد توجيه نفاذ المستخدم إلى الموقع الإلكتروني الذي يحتوي على البرمجيات الضارة لمهاجمة حاسوب المستخدم الذي قام بزيارة ذلك الموقع الإلكتروني.

2 وعندما يزور المستخدم المهاجَم الموقع الإلكتروني الذي اخترقه المهاجمون، يهاجَم حاسوب المستخدم بالبرمجيات الضارة المندسة في الموقع أو يعاد توجيهه إلى موقع آخر يحتوي على البرمجيات الضارة لمهاجمة حاسوب المستخدم.

3 وعندما توجد نقاط ضعف في متصفح الحاسوب يمكن لبرمجيات ضارة معينة استخدامها، تثبَّت تلك البرمجيات الضارة في حاسوب المستخدم فيصبح مصاباً بها دون علم المستخدم أو إذن منه.

4 يمكن استخدام البرمجيات الضارة المثبتة في حاسوب المستخدم لشن هجمات الحرمان من الخدمة الموزَّع (DDoS) أو لسرقة معلومات شخصية مثل الهوية (ID) وكلمة المرور وإحالتها إلى المهاجمين.



الشكل I-1 السيناريو النمطي للهجمات من خلال شبكة الإنترنت

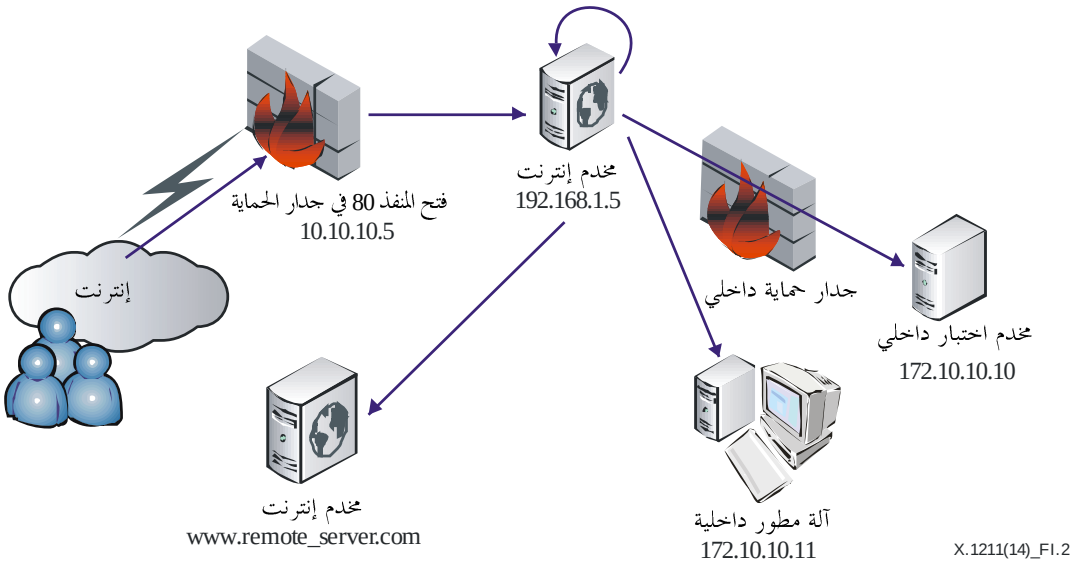
2.I طلب مزوَّر عابر للموقع (CAPEC-62)

قد يحمل طلب مزوَّر عابر للموقع (CSRF) ضحيته على أن تقدم عن غير قصد واحداً أو أكثر من طلبات بروتوكول نقل النصوص التشعبية (HTTP) إلى موقع إلكتروني غير حصين يثق به المستخدم. ويمكن لهجوم في شكل طلب مزوَّر عابر للموقع أن ينال من سلامة البيانات وفقاً لذلك، وأن يمكِّن المهاجم من تعديل المعلومات المخزنة في موقع إلكتروني غير حصين.

وعندما يتطلب موقع إلكتروني الاستيقان من المستخدم، فإنه غالباً لا يُلزم المستخدم بكتابة كلمة المرور الخاصة به لكل طلب HTTP؛ بل يتعرّف الموقع الإلكتروني على حالة الاستيقان من المستخدم بين طلبات HTTP متعددة عن طريق تأشيرات مثل ملفات تعريف ارتباط الجلسة أو رأسية تخويل HTTP. ولكن هناك مشكلة في ذلك: فمتصفحات الإنترنت تحفظ غيباً التأشيرة المرتبطة بالمحدد الموحد لموقع المورد (URL) وتُرفق التأشيرة تلقائياً عند إصدار طلب HTTP جديد إلى الموقع الإلكتروني، حتى لو لم يكن الطلب مقصوداً من المستخدم. فيستغل الطلب المزوَّر العابر للموقع (CSRF) سلوك المتصفح. وبهذا الطلب، لا يحتاج المستخدم إلا لزيارة موقع إلكتروني خبيث يمكنه أن يدرج منطق برمجيات جافا النصية (JavaScript) الذي يصدر طلبات HTTP (يحتمل أن تكون مخفية) إلى مواقع إلكترونية أخرى (مثل مصرف المستخدم)، وقد يخوِّل الموقع الإلكتروني طلبات HTTP هذه بسبب وجود التأشيرات. ويمكن الطلب المزوَّر العابر للموقع من شن أنواع مختلفة من الهجمات المختلفة، مثل إرسال رسائل البريد الإلكتروني من خدمة بريد على شبكة الإنترنت، أو نشر تعليق على مدونة نيابةً عن المستخدم، أو تغيير قائمة أصدقاء المستخدم في خدمة شبكة اجتماعية (SNS)، أو تغيير الإعدادات في جهاز مسيِّر منزلي.

3.I الهجمات على المنفذ العابرة للموقع/الطلبات المزوَّرة من جانب المخدِّم

إن الهجمات على المنفذ العابرة للموقع/الطلبات المزوَّرة من جانب المخدِّم (XSPA/SSRF) هي أسلوب لإساءة استخدام تطبيقات الإنترنت التي تعالج عناوين URL المقدمة من مدخلات متصفح الإنترنت. ويستهدف هجوم XSPA/SSRF النمطي شبكة إنترانت التطبيق غير الحصينة. وقد يسبب الهجوم مسح المَنْفَذ ويهتك كتمان البيانات ويؤدي إلى تنفيذ شفرة غير مخوَّلة ويستغل موارد الإنترانت غير الحصينة. ويُعتبر التطبيق عرضة للهجمات على المنفذ العابرة للموقع/الطلبات المزوَّرة من جانب المخدِّم عندما لا يتحقق من صحة المخرجات الواردة من مضيف بعيد والمدخلات المقدمة من المستخدم النهائي. وكمثال على ذلك، يمكن لتطبيق، يقوم بتحميل صورة من URL يقدمه مستخدم، أن ينفُذ إلى مورد إنترانت عندما ينشر المستخدم URL بصيغة 'http://localhost/secret.txt'. وفي بعض الحالات، قد تُستخدم أنماط من المعرف الموحد للمورد (URI) بحيث يرسل تطبيق غير حصين طلباً إلى خدمات خاصة مثل 'https' أو 'gopher' أو 'ftp' أو 'ldap'. ويمكن أيضاً استخدام أنماط خاصة بلغة معينة مثل 'php://fd' أو 'php://memory'.



الشكل I-2 – سيناريو نموذجي للهجمات على المنفذ العابرة للموقع/الطلبات المزوَّرة من جانب المخدِّم (XSPA/SSRF)

4.I حقن اللغة SQL (CAPEC-66)

يقوم السيناريو النمطي لحقن اللغة SQL على فحص ردئ لسلامة البيانات المدخلة لتطبيقات الويب. وقد تختلف قنوات الدخل بحيث تأخذ أحد الأشكال: طلبات GET وPOST HTTP وملفات بيانات المتصفح (cookies) وحمولة نافعة قائمة على اللغة XML ومدخلات ملفات وغيرها.

ويحقن الدخل المستهدف في استفسار للغة SQL. وفيما يلي مثال أساسي على الحقن SQL في معلمة "GET" HTTP":

- باعتبار الاستفسار الأصلي – "SELECT title, content FROM table1 WHERE id=%d"

حيث "id" المعلمة المستهدفة.

وفي ظل الظروف الطبيعية يكون "id" أحد الأعداد الطبيعية. ولكن بسبب عدم إجراء فحص السلامة، يطرح القائم بالهجمة بدلاً من العدد الدخل التالي:

- "1 UNION SELECT user, password FROM secret_table" = %d

ويؤدي ذلك إلى نفاذ غير مخول إلى "secret_table" ومن ثم الكشف عن بيانات حساسة عند دخل المتصفح مباشرةً.

وحسب تنفيذ قاعدة بيانات اللغة SQL، يمكن لهذه الهجمة أن تؤدي إلى:

- الكشف عن بيانات حساسة من قاعدة البيانات أو نظام الملفات؛
- فقدان/تعديل البيانات؛
- حقن أبواب خلفية للتلصص وزيادة الامتيازات؛
- نشر برمجيات ضارة لدى المستعملين النهائيين الذين يزورون الموقع.

5.I كشف البرمجيات الضارة في المواقع الإلكترونية

يمكن تصنيف التقنيات المستخدمة لكشف البرمجيات الضارة في فئتين: الكشف القائم على الشذوذ والكشف القائم على التوقيع [b-NA].

وفي تقنية الكشف القائم على الشذوذ، تكون معايير تحديد إمكانية الإضرار في البرنامج قيد التفتيش هي التي تشكل السلوكيات العادية. ويشار إلى نوع خاص من الكشف القائم على الشذوذ بالكشف القائم على التوصيف. وتستخدم تقنيات الكشف القائم على التوصيف مجموعة ما من المواصفات أو القواعد للسلوك الصالح من أجل البت في إمكانية الإضرار في البرنامج قيد التفتيش. وتعتبر البرامج المنتهكة لمجموعة القواعد أو المواصفات هذه برامج خبيثة.

وفي الكشف القائم على التوقيع، تتمثل معايير تحديد إمكانية الإضرار في البرنامج قيد التفتيش في توصيف ما هو معروف على أنه ضار. وتشخيص أو توقيع السلوك الضار هو المفتاح لفعالية أسلوب الكشف القائم على التوقيع.

ويمكن لكل من تقنيتي الكشف أن تستخدم واحداً من ثلاثة نُهُج مختلفة: ساكن أو دينامي أو هجين. فيتحدد النهج أو التحليل المحدد للتقنية القائمة على الشذوذ أو على التوقيع بالكيفية التي تجمع فيها التقنيةُ المعلومات لكشف البرمجيات الضارة. فيستخدم تحليل الساكن الخصائص النحوية أو الهيكلية للبرنامج (نهج ساكن)/العملية قيد التفتيش (PUI) (نهج دينامي) لتحديد إمكانية الإضرار. فعلى سبيل المثال، لا يستخدم النهج الساكن في الكشف القائم على التوقيع إلا المعلومات الهيكلية (كتتابع البايتات مثلاً) لتحديد إمكانية الإضرار، في حين أن النهج الدينامي يستخدم معلومات وقت التشغيل (كالأنظمة المرئية على كدسة وقت التشغيل مثلاً) في العملية قيد التفتيش.

وبوجه عام، يحاول النهج الساكن كشف البرمجيات الضارة قبل تنفيذ البرنامج قيد التفتيش. وعلى العكس من ذلك، يحاول النهج الدينامي كشف السلوك الضار أثناء تنفيذ البرنامج أو بعد تنفيذه.

وهناك تقنيات هجينة تجمع بين النهجين. وفي هذه الحالة، تُستخدم المعلومات الساكنة والدينامية لكشف البرمجيات الضارة.

وهناك عدة تقنيات لكشف البرمجيات الضارة في المواقع الإلكترونية، ويرد وصفها في التذييل الثالث.

التذييـــل الثاني

أسلوب إصابة حاسوب المستخدم بالبرمجيات الضارة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

القصد من هذا التذييل هو وصف السيناريوهات النموذجية التي يمكن أن يستخدمها المهاجمون، لإعانة المشرفين في فهمها.

الخطوة الأولى للهجوم من خلال شبكة الإنترنت هو تثبيت وتشغيل مختلف الشفرات الضارة على حاسوب المستخدم. ويمكن أن تشمل هذه الشفرات شفرات تسجيل المدخلات عبر لوحة المفاتيح والجذور الخفية (والتي يمكن أن تحول حواسيب المستخدمين إلى حواسيب مسخَّرة أو تسرب معلومات المستخدم الحساسة إلى المهاجمين).

ويمكن تحقيق الهدف من الهجوم إما عن طريق استكشاف بضع نقاط الضعف المعروفة في مكونات البرمجيات المختلفة التي يمكن النفاذ إليها عبر متصفح (مثل مكونات نظام التشغيل التي يمكن النفاذ إليها عبر متصفح من خلال مكون ActiveX، وما إلى ذلك)، أو عن طريق تقنيات الهجوم التي تستخدم الهندسة الاجتماعية لخداع المستخدمين وحملهم على تركيب وتشغيل برمجيات ضارة على النظام الخاص بهم. وبالإضافة إلى ذلك، يحاول هذا الهجوم سرقة بيانات اعتماد المستخدم من خلال تقنيات التصيّد أو هجمات البرمجة العابرة للموقع المشغَّلة في إطار iframe خفي.

وهناك عدد من التقنيات التي تستخدم لتصيب حاسوب المستخدم بالبرمجيات الضارة: استغلال مكون ActiveX، وتقنيات الهندسة الاجتماعية، ونقص الكودك، وتقنيات أداة إزالة البرمجيات الضارة، وهجمات الطلب المزوَّر العابر للموقع. ويمكن تقديم معلومات مفصلة عن ذلك في المرجع [b-NTOBJECTives]. وبالإضافة إلى ذلك، ترد قائمة من أنماط الهجوم الشائعة إلى جانب قائمة كاملة بالأنماط والتصنيفات في المرجع [b-ITU-T X.1544].

التذييـــل الثالث

أمثلة نمطية عن تقنيات التمويه

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يستخدم المحتوى الضار المحقون تقنيات تمويه من أجل إخفاء البرمجيات الضارة عن العين البشرية وعن برمجيات كشف نقاط الضعف على حد سواء [b-ITU-T X.1520]. وتقنيات التمويه فعالة جداً للأسباب التالية:

- يتخوف العديد من المشرفين على المواقع الإلكترونية من حذف شفرات البرمجة النصية التي لا يفهمونها.
- يصعب على المشرفين على قواعد البيانات المصابة القيام بتنظيفها، حيث يجهلون ماهية الأنماط التي يتعين البحث عنها.
- تعتمد العديد من أساليب الكشف على أساليب الصيغة العادية أو الأساليب الأخرى المرتبطة ببحث السلسلة، وبالتالي فهي تعاني من مشاكل تحديد لغة HTML المموَهة.

وتتعدد تقنيات التمويه: تقسيم السلسلة وتشفير السلسلة وتشفير السلسلة المخصص وتعديل سلوك البرنامج النصي ووظائف تعديل نموذج كائن الوثيقة (DOM) والروابط المتخفية وراء الخدمات العامة وإعادة توجيه الصفحة. ويرد وصف معلومات مفصلة في المرجع [b-NTOBJECTives].

التذييـــل الرابع

تقنيات الوقاية من هجمات تشَّن من خلال شبكة الإنترنت

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

القصد من هذا التذييل هو عرض عدة تقنيات لكشف البرمجيات الضارة في المواقع الإلكترونية [b-NTOBJECTives]. ويمكن كشف المحتوى الضار بمطابقة توقيع المحتوى، أو إدراج المواقع الإلكترونية للهجمات في قائمة سوداء، أو بتحليل المحتوى ذي السلوك المشبوه بواسطة خوارزميات مسجلة الملكية.

1.IV إزالة نقاط ضعف الموقع الإلكتروني

تتمثل أبسط طريقة في إزالة نقاط ضعف المواقع الإلكترونية، بما في ذلك حقن لغة الاستعلام البنيوية (SQL) والبرمجة العابرة للموقع. فإذا عجز المهاجم عن دس المحتوى الضار في الموقع الإلكتروني، لن ينفِّذ متصفح العميل البرمجيات الضارة المندسة في الموقع. ولذلك، تتمثل الطريقة الأكثر فعالية لمنع الهجمات من خلال شبكة الإنترنت في إزالة نقاط الضعف كافة من المواقع الإلكترونية.

2.IV مطابقة التوقيع

نظراً لتعدد تقنيات التمويه وأدوات الأتمتة المستخدمة لتمويه البرمجيات الضارة، من غير العملي السعي لكشف المحتوى الضار في الموقع الإلكتروني باستخدام أسلوب الكشف القائم على التوقيع. ومن المعروف جيداً أن المهاجمين قادرون على أتمتة تشفير المحتوى الضار بمفتاح جديد لكل موقع إلكتروني، مما يؤدي إلى استحداث توقيع مختلف للبرمجيات الضارة في كل موقع. ولكن المحتوى العادي للبرمجيات الضارة لا يكثر تغيّره، وبالتالي يمكن كشف البرمجيات الضارة في موقع إلكتروني بتوقيع. وإذا تم الحصول على المحتوى الضار العادي عن طريق فك تشفير البرمجيات الضارة وحُسب توقيع البرمجيات الضارة العادية من البرمجيات الضارة العادية، يمكن لهذا الأسلوب أن يكشف البرمجيات الضارة عن طريق مقارنة توقيع البرمجيات الضارة المحسوب مع قائمة مجمعة مسبقاً لجميع توقيعات المحتويات الضارة المعروفة سلفاً.

3.IV إدراج المواقع في قائمة سوداء

إن إدراج مواقع إلكترونية في قائمة سوداء هو من بين تقنيات الكشف الأكثر قيمة. وعلى الرغم من أن المحتوى الضار يمكن استضافته تماماً في موقع إلكتروني جيد (خالٍ من متطلبات التحميل التلقائي لأي برمجيات نصية أو أطر iframes من موقع الهجوم، وهكذا يخفي صلته بموقع الهجوم)، فمن الضروري تبادل بعض البيانات مع الموقع الإلكتروني للهجوم لاستكمال الهجوم المقصود. وقد يتخذ هذا التبادل الضروري للبيانات العديد من الأشكال المختلفة: إذ يحتاج هجوم البرنامج النصي لتنزيل البرمجيات الضارة من الموقع الإلكتروني للهجوم، أو يحتاج لإرسال البيانات الخاصة التي جُمعت من مستخدمي النظام إلى مهاجمي الموقع، أو يحتاج لشيء آخر. وفي أي حال، يحتاج البرنامج النصي المهاجم لإقامة توصيل مع موقع الهجوم.

وفي حال وجود خوارزمية لكشف الموارد الخارجية الواردة في قائمة المواقع المدرجة على القائمة السوداء، يمكن أن تبدي الشك بوجود برمجيات ضارة في الموقع. وبالتالي، فإن أي استعلامات بشأن المواقع المدرجة في القائمة السوداء ستشي بوجود محتوى ضار على صفحة يجري تحليلها.

4.IV كشف تقنيات التمويه

إذا تضمن الموقع الإلكتروني صفحة محتواها مشفر بتقنيات التمويه، يمكن أن يكون ذلك مؤشراً معقولاً إلى أن لهذا الموقع له نية خبيثة. فعلى سبيل المثال، إذا وُجد في موقع إلكتروني محتوىً ذو سلسلة طويلة مشفرة، فإنه يمكن أن يكون محتوى ضاراً. ولكن رغم الشبهة التي تثيرها سلسلة طويلة مشفرة، لا يمكن الافتراض دوماً أن الموقع الإلكتروني يحتوي على محتوى ضار حتى تُفكَك شفرته ويُحلَل فعله.

5.IV تقييم التصرفات المشبوهة للمحتوى

تتمثل الطريقة الأكثر كفاءة في تحليل سلوك المحتويات المشبوهة. فإذا كان نشاط المحتوى مشبوهاً، يمكن أن يكون ذلك مؤشراً على نوايا خبيثة. وتشمل التصرفات النمطية التي يمكن اعتبارها خبيثة، النفاذ إلى القرص الصلب المحلي، واستحضار كائن تطبيق من مخدم بعيد، وتنزيل (أو النفاذ إلى) محتوى خارجي قابل للتنفيذ.

التذييـــل الخامس

أمثلة نمطية من مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP) بشأن المخاطر الأمنية المحدقة بالتطبيقات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

إن مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP) هو تعاون مفتوح المصادر بين أدوات وتكنولوجيات ومنهجيات الأمن على شبكة الإنترنت المتأتية من قادة الصناعة والمنظمات التعليمية والأفراد من جميع أنحاء العالم. وترد في الجدول 1.V أكبر 10 هجمات من خلال شبكة الإنترنت نشرها مشروع أمن تطبيقات الإنترنت المفتوحة [b-OWASP] وCWE-928 [b-ITU-T X.1524] CWE: مواطن الضعف في أكبر 10 هجمات للمشروع OWASP [b-CWE].

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-1- حقن	أي شخص يمكن أن يرسل بيانات غير موثوقة إلى النظام، بما في ذلك المستخدمون الخارجيون والمستخدمون الداخليون والمشرفون.	يرسل المهاجمون هجمات بسيطة قائمة على النصوص تستغل قواعد النظم اللغوي للمترجم المستهدف. ويمكن أن يكون أي مصدر بيانات تقريباً ناقلاً للحقن، بما في ذلك المصادر الداخلية	تحدث عيوب الحقن عندما يرسل تطبيقٌ بيانات غير موثوقة إلى مترجم. وتشيع عيوب الحقن كثيراً، لا سيما في الشفرات القديمة، التي غالباً ما توجد في استعلامات SQL واستعلامات LDAP واستعلامات XPath وأوامر نظام التشغيل، وعُمدات برنامج، إلخ. ويسهل اكتشاف عيوب الحقن عند تفحص شفرة، ولكنه يصبح أكثر صعوبة عن طريق الاختبار. ويمكن للماسحات والاختبارات البرمجية أن تساعد المهاجمين في العثور عليها.	يمكن أن يؤدي الحقن إلى فقدان البيانات أو إفسادها أو انعدام المساءلة أو الحرمان من النفاذ. ويمكن أن يؤدي الحقن في بعض الأحيان إلى السيطرة الكاملة على المضيف.	يتعين النظر في القيمة التجارية للبيانات المتضررة ومنصة تشغيل المترجم. إذ يمكن أن تُسرق جميع البيانات أو تُعدل أو تمحى. هل يمكن أن تتضرر السمعة جراء ذلك؟	CWE-929، CWE-77، CWE-78، CWE-89، CWE-90، CWE-91

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-2- انقطاع الاستيقان وإدارة الدورة	يتعين النظر في المهاجمين المجهولين من الخارج، وكذلك المستخدمين أصحاب الحسابات الذين يمكن أن يحاولوا سرقة حسابات من الآخرين. ويتعين النظر أيضاً في رغبة الجهات العاملة من الداخل في إخفاء أفعالها.	يستخدم المهاجم التسريبات أو العيوب في الاستيقان وإدارة الدورة (مثل الحسابات وكلمات المرور وهويات الدورة المكشوفة) لتقمص شخصية المستخدمين.	كثيراً ما يعد المطورون خططاً مخصصة للاستيقان وإدارة الدورة، ولكن يصعب إعدادها على الوجه الصحيح. ونتيجة لذلك، تعاني هذه الخطط المخصصة في كثير من الأحيان من عيوب في مجالات مثل تسجيل الخروج وإدارة كلمة المرور وانقضاء المهل الزمنية وتذكر إعدادات المستخدم والسؤال السري وتحديث الحساب، وما إلى ذلك. وقد يصعب أحياناً العثور على مثل هذه العيوب، لأن كل تنفيذ هو تنفيذ فريد من نوعه.	يمكن لمثل هذه العيوب أن تعرض بعض أو حتى جميع الحسابات للهجوم. وحالما ينجح، مرة واحدة ناجحة، يمكن للمهاجم أن يفعل أي شيء يمكن أن تفعله الضحية. وكثيراً ما تُستهدف الحسابات المكتومة.	يتعين النظر في القيمة التجارية للبيانات المتضررة أو وظائف التطبيق. ويتعين النظر أيضاً في التأثير التجاري لانكشاف نقطة الضعف على العلن.	CWE-930، CWE-256، CWE-287، CWE-522، CWE-613، CWE-384، CWE-311، CWE-319، CWE-523، CWE-620، CWE-640

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-3- البرمجة العابرة للموقع (XSS)	يتعين النظر في أي شخص يمكن أن يرسل بيانات غير موثوقة إلى النظام، بما في ذلك المستخدمون الخارجيون والمستخدمون الداخليون والمشرفون.	يرسل المهاجم مخطوطات هجوم قائمة على النصوص تستغل المترجم في المتصفح. ويمكن أن يكون أي مصدر بيانات تقريباً ناقلاً للهجوم، بما في ذلك المصادر الداخلية كالبيانات من قاعدة البيانات.	البرمجة العابرة للموقع(XSS) هي الثغرة الأمنية الأكثر انتشاراً في تطبيقات الإنترنت. وتحدث ثغرات XSS عندما يتضمن التطبيق بيانات ورَّدها المستخدم في صفحة مرسَلة إلى المتصفح من دون التحقق من صحة ذلك المحتوى أو الخروج منه على الوجه الصحيح. وهناك ثلاث أنواع معروفة من ثغرات XSS: 1) XSS المخزنة، 2) XSS المنعكسة، و3) XSS القائمة على نموذج كائن الوثيقة (DOM). ويسهل إلى حد ما كشف معظم ثغرات XSS عن طريق الاختبار أو تحليل الشفرة.	يمكن للمهاجمين تنفيذ البرامج النصية في متصفح الضحية لخطف دورات المستخدم، وتشويه المواقع الإلكترونية، وإدراج محتوى عدائي، وإعادة توجيه المستخدمين وخطف متصفح المستخدم باستخدام البرمجيات الضارة، إلخ.	يتعين النظر في القيمة التجارية للنظام وجميع البيانات التي يعالجها. ويتعين النظر أيضاً في التأثير التجاري لانكشاف نقطة الضعف على العلن.	CWE-931، CWE-79
A-4- الإحالات المباشرة غير المأمونة إلى كائن	يتعين النظر في أنواع المستخدمين لنظامك. هل يمكن لأي من المستخدمين النفاذ جزئياً فقط إلى أنواع معينة من بيانات النظام؟	المهاجم هو مستخدم مخوَّل للنظام يقوم بمجرد تغيير قيمة المعلمة من تلك التي تحيل مباشرة إلى كائن في النظام إلى أخرى تحيل إلى كائن آخر غير مخوَّل للمستخدم. فهل مُنح إذن النفاذ؟	كثيراً ما تستخدم التطبيقات اسم كائن أو مفتاحه الفعلي عند إنشاء صفحات إلكترونية. ولا تتحقق التطبيقات دائماً من كون المستخدم مخولاً بالنفاذ إلى الكائن المستهدف. وهو ما يؤدي إلى ثغرة الإحالة المباشرة غير المأمونة إلى كائن. وتسهل على المختبرين المناورة بقيم المعلمة لكشف مثل هذه الثغرات. ويبين تحليل الشفرة بسرعة ما إذا جرى التحقق من التخويل على الوجه الصحيح.	يمكن لمثل هذه الثغرات أن تفسد جميع البيانات التي يمكن للمعلمة أن تحيل إليها. وما لم يتعذر التنبؤ بالإحالات إلى الكائن، يسهل على مهاجم النفاذ إلى جميع البيانات المتاحة من ذلك النمط.	يتعين النظر في القيمة التجارية للبيانات المكشوفة. ويتعين النظر أيضاً في التأثير التجاري لانكشاف نقطة الضعف على العلن.	CWE-932، CWE-22، CWE-99، CWE-639

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-5- سوء تشكيلة الأمن	يتعين النظر في المهاجمين المجهولين من الخارج وكذلك المستخدمين أصحاب الحسابات الخاصة الذين قد يحاولون اختراق النظام. ويتعين النظر أيضاً في الجهات العاملة من الداخل الراغبة في إخفاء أفعالها.	ينفذ المهاجم إلى الحسابات المبدئية والصفحات غير المستخدمة والعيوب غير المصححة، والملفات والدلائل غير المحمية، وغير ذلك، من أجل النفاذ غير المخوَّل إلى النظام أو التعرف عليه.	يمكن أن تساء التشكيلة في أي مستوى من كدسة التطبيق، بما في ذلك المنصة والمخدم على شبكة الإنترنت ومخدم التطبيق وقاعدة البيانات والإطار والشفرة المخصصة. ويتعين على المطورين والمشرفين على النظام العمل معاً لضمان تشكيل الكدسة بأكملها على الوجه الصحيح. ويستفاد من الماسحات المؤتمتة في كشف نقص البرمجيات التصحيحية وسوء التشكيلات واستخدام الحسابات المبدئية والخدمات غير الضرورية، وغير ذلك.	يمكن اختراق النظام بالكامل دون علمك. وقد تُسرق جميع بياناتك أو تعدَّل ببطء على مر الزمن. وقد تكون تكلفة إعادة النظام إلى سابق عهده مكلفة.	يمكن اختراق النظام بالكامل دون علمك. وقد تُسرق جميع بياناتك أو تعدَّل ببطء على مر الزمن. وقد تكون تكلفة إعادة النظام إلى سابق عهده مكلفة.	CWE-933، CWE-2، CWE-16، CWE-209، CWE-215، CWE-548

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-6- انكشاف البيانات الحساسة	يتعين النظر فيمن يمكنه النفاذ إلى البيانات الحساسة وأي نسخ احتياطية من تلك البيانات. ويشمل ذلك البيانات الساكنة والعابرة، وحتى تلك الموجودة في متصفحات عملائك. ويتعين إدراج التهديدات الخارجية والداخلية على السواء.	لا يكسر المهاجمون التجفير مباشرةً في العادة. بل يكسرون شيئاً آخر، من قبيل سرقة المفاتيح أو شن هجمات الاعتراض الوسيط أو سرقة بيانات النص غير المشفر من المخدِّم، أثناء العبور، أو من متصفح المستخدم.	الثغرة الأكثر شيوعاً هي مجرد عدم تجفير البيانات الحساسة. فعند استخدام التجفير، يشيع استخدام توليد المفاتيح الضعيف والإدارة الضعيفة والخوارزمية الضعيفة، وبوجه خاص تقنيات ضعيفة في اختزال كلمة المرور. ولئن شاعت كثيراً أوجه ضعف المتصفح فإن كشفها سهل واستغلالها صعب على نطاق واسع. ويصعب على المهاجمين الخارجيين كشف الثغرات في جانب المخدّم نظراً لمحدودية النفاذ إليه وصعوبة استغلال هذه الثغرات عادةً.	كثيراً ما ينال العطل من حصانة جميع البيانات التي ينبغي أن تكون محمية. وعادةً ما تتضمن هذه المعلومات بيانات حساسة من قبيل السجلات الصحية وبيانات الاعتماد والبيانات الشخصية وبطاقات الاعتماد وما إلى ذلك.	يتعين النظر في قيمة البيانات المفقودة وتأثيرها على السمعة، وفي ماهية المسؤولية القانونية إذا انكشفت هذه البيانات. ويتعين النظر في الضرر الذي تتعرض له السمعة.	CWE-934، CWE-311، CWE-310، CWE-312، CWE-319، CWE-325، CWE-326

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-7- التحكم في النفاذ على مستوى الوظيفة	يمكن لأي شخص نافذ إلى الشبكة أن يرسل طلباً إلى تطبيقك. هل يمكن لمستخدمين مجهولي الهوية النفاذ إلى الخواص الوظيفية الخاصة أو يمكن لمستخدمين عاديين النفاذ إلى وظيفة مكتومة؟	يقوم مهاجم، هو مستخدم مخوَّل للنظام، بمجرد تغيير URL أو معلمة أو وظيفة مكتومة. هل يمكنه القيام بذلك؟ ويمكن لمستخدمين مجهولي الهوية النفاذ إلى وظائف خاصة غير محمية.	لا تحمي التطبيقات دائماً وظائف التطبيق على الوجه المناسب. وأحياناً تدار الحماية على مستوى الوظيفة عبر التشكيلة، وتساء تشكيلة النظام. ويجب على المطورين أحياناً أو يضمِّنوا ضوابط الشفرة المناسبة، ويفوتهم ذلك. ويسهل كشف مثل هذه الثغرات. وأصعب ما في الأمر هو تحديد أي من الصفحات (URL) أو الوظائف الموجودة سيتعرض لهجوم.	تسمح هذه الثغرات للمهاجمين بالنفاذ إلى خواص وظيفية غير مخوَّلة لهم. والوظائف الإدارية هي أهداف رئيسية لهذا النوع من الهجمات.	يتعين النظر في القيمة التجارية للوظائف المكشوفة والبيانات التي تعالجها. ويتعين النظر أيضاً في التأثير على السمعة إذا ظهرت نقطة الضعف هذه على العلن.	CWE-935، CWE-285، CWE-287

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-8- طلب مزوَّر عابر للموقع (CSRF)	يتعين النظر في أي شخص يمكنه أن ينزل محتوى في متصفحات المستخدمين ليجبرهم بذلك على تقديم طلب إلى موقعك الإلكتروني. ويمكن لأي موقع إلكتروني أو مصدر تغذية HTML آخر ينفذ إليه مستخدموك أن يقوم بذلك.	ينشئ المهاجم طلبات HTTP مزورة ويحتال على الضحية كي تقدمها عبر وسوم صور أو XSS أو العديد من التقنيات الأخرى. فإذا تم الاستيقان من المستخدم، يُفلح الهجوم.	يستغل طلب CSRF سماح معظم تطبيقات الإنترنت للمهاجمين بتوقع جميع تفاصيل إجراء معين. ونظراً إلى أن المتصفحات ترسل تلقائياً بيانات اعتماد مثل ملفات ارتباط الدورة، يمكن للمهاجمين إنشاء صفحات إلكترونية خبيثة تولد طلبات مزورة يتعذر تمييزها عن الطلبات المشروعة. ويسهل كشف ثغرات CSRF إلى حد ما عبر اختبار الانتشار أو تحليل الشفرة.	يمكن للمهاجمين أن يحتالوا على الضحايا لحملهم على القيام بأي عملية تغيير حالة يحق لهم القيام بها، مثل تحديث تفاصيل الحساب، والشراء عبر الإنترنت، وتسجيل الخروج وحتى تسجيل الدخول.	يتعين النظر في القيمة التجارية لما تضرر من بيانات أو وظائف تطبيق. وتصور عدم التيقن من أن المستخدمين يريدون فعلاً القيام بهذه الإجراءات. ويتعين النظر في تأثير ذلك على سمعتك.	CWE-935، CWE-352، CWE-346، CWE-441، CWE-346، CWE-642
A-9- استخدام مكونات ذات نقاط ضعف معروفة	يمكن التعرف على بعض المكونات غير الحصينة (مثل مكتبات الإطار) واستغلالها بأدوات مؤتمتة، على نحو يوسع رقعة واسطة التهديد إلى ما هو أبعد من المهاجمين المستهدفين لتشمل جهات فاعلة عشوائية.	يتعرف المهاجم على المكون الضعيف عن طريق المسح أو التحليل اليدوي. ويفصِّل مقاس الاستغلال حسب الحاجة وينفذ الهجوم. ويزداد الأمر صعوبة إذا كان موقع المكون المستخدَم عميقاً في التطبيق.	يعاني كل تطبيق عملياً من هذه الإشكالات لأن معظم فرق التطوير لا تركز على ضمان مواكبة مكوناتها/مكاتبها لآخر التحديثات. وفي العديد من الحالات، لا علم للمطورين حتى بالمكونات التي يستخدمونها، ناهيك عن إصداراتها. ويزداد الأمر سوءاً بتابعيات المكونات.	يمكن أن تكون هناك مجموعة كاملة من نقاط الضعف، بما في ذلك الحقن وانقطاع التحكم في النفاذ وXSS، وما إلى ذلك. ويمكن أن يتراوح التأثير بين حده الأدنى والاستيلاء الكامل على المضيف وهتك سرية البيانات.	يتعين النظر فيما تعنيه كل نقطة ضعف لمصلحة الأعمال التي يتحكم فيها التطبيق المتضرر. فقد يكون الأمر غير ذي بال أو قد يعني تعرضاً كاملاً للخطر.	CWE-937

الجدول 1.V – أكبر 10 مخاطر أمنية تتهدد التطبيقات وفق مشروع أمن تطبيقات الإنترنت المفتوحة (OWASP)

نمط الهجوم	واسطة التهديد	ناقل الهجوم	الثغرة الأمنية	التأثير التقني	التأثير التجاري	المراجع
A-10- عمليات إعادة التوجيه وإعادة التسيير غير المتحقَق من صحتها	يتعين النظر في أي شخص يمكنه أن يحتال على المستخدمين لديك ليحملهم على تقديم طلب إلى موقعك الإلكتروني. ويمكن لأي موقع إلكتروني أو مصدر تغذية HTML آخر ينفذ إليه مستخدموك أن يقوم بذلك.	يقيم المهاجم وصلة مع عمليات إعادة التوجيه وإعادة التسيير غير المتحقَق من صحتها ويحتال على الضحايا ليحملهم على نقر الوصلة. ويرجح أن ينقرها الضحايا لأن الوصلة تؤدي إلى موقع صحيح. ويستهدف المهاجم إعادة التسيير غير الآمنة ليتجاوز الضوابط الأمنية.	كثيراً ما تقوم التطبيقات بإعادة توجيه المستخدمين إلى صفحات أخرى، أو تستخدم إعادة تسيير داخلية بالطريقة نفسها. وتحدَد الصفحة المستهدفة أحياناً بمعلمة غير متحقَق من صحتها مما يتيح للمهاجمين اختيار صفحة المقصد. ويسهل كشف عمليات إعادة التوجيه بالبحث عنها حيثما يمكن إعداد محدد URL الكامل. أما عمليات إعادة التسيير غير المتحقَق منها فهي أصعب، لأنها تستهدف صفحات داخلية.	يمكن لعمليات إعادة التوجيه هذه أن تحاول تثبيت برمجيات ضارة أو تحتال على الضحايا لحملهم على إفشاء كلمات المرور أو معلومات حساسة أخرى. ويمكن لعمليات إعادة التسيير غير المأمونة أن تسمح بتجاوز التحكم في النفاذ.	يتعين النظر في القيمة التجارية للحفاظ على ثقة المستخدمين لديك. فماذا لو استولت البرمجيات الضارة عليهم؟ وماذا لو تمكن المهاجمون من النفاذ إلى الوظائف الداخلية فقط؟	CWE-938، CWE-601

بيبليوغرافيا

[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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكةص الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2015