Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1211

(09/2014)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Ciberseguridad

Técnicas para prevenir ataques en la web

Recomendación UIT-T X.1211

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1211

Técnicas para prevenir ataques en la web

Resumen

La Recomendación UIT-T X.1211 describe técnicas que pueden atenuar los ataques en la web que ocurren cuando se explotan las vulnerabilidades de los servidores de sitios web y se introducen códigos malignos que pueden infectar la computadora del usuario. Varios apéndices ilustran de qué manera pueden tener lugar esos ataques así como las medidas para resolverlos.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1211	2014-09-26	17	11.1002/1000/12154

Palabras clave

Ataque web, contenido sospechoso, inyección SQL, prevención, software espía, vulnerabilidad

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1211

Técnicas para prevenir ataques en la web

1 Alcance

En esta Recomendación se facilitan técnicas para prevenir ataques en la web. Se describen hipótesis para la distribución de software maligno a través de la web, así como técnicas funcionales y funciones para prevenir los ataques en la web.

2 Referencias

Ninguna.

3 Términos y definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 activo [b-ISO/IEC 27000]: Todo lo que tiene valor para la organización.

NOTA – Hay muchos tipos de activos y entre ellos se cuentan:

a) la información;

b) el software, como los programas informáticos;

c) los físicos, como las computadoras;

d) los servicios;

e) las personas y sus calificaciones, conocimientos y experiencias; y

f) los intangibles, como la reputación y la imagen.

3.1.2 instancia de ataques [b-UIT-T X.1544]: Ataque pormenorizado concreto contra una aplicación o sistema que busca vulnerabilidades o debilidades en ese sistema.

3.1.3 pauta de ataque [b-UIT-T X.1544]: Abstracción de planteamientos de ataques comunes observados en el mundo contra aplicaciones o sistemas (por ejemplo, inyección SQL, de intermediarios, robo de sesión, etc.).

NOTA – Una sola pauta de ataque puede tener potencialmente muchas instancias de ataque variables asociadas a ella.

3.1.4 lenguaje de marcaje de hipertexto (HTML) [b-UIT-T M.3030]: Sistema de codificación de información de una amplia gama de dominios (por ejemplo, texto, gráficos, resultados de indagaciones a bases de datos) para visualización con navegadores World Wide Web. Algunos códigos especiales, denominados etiquetas, están insertados en el documento para poder indicar al navegador cómo presentar la información.

3.1.5 malware [b-ISO/IEC 27033-1]: Software maligno diseñado específicamente para dañar o interrumpir un sistema atacando su confidencialidad, integridad y/o disponibilidad.

3.1.6 técnica de ocultación [b-NIST SP 800-83]: Manera de crear un virus para hacer más difícil su detección.

3.1.7 información de identificación personal (PII) [b-UIT-T X.1252]: Toda información a) que identifica a una persona y que puede utilizarse para identificar, contactar o localizar a la misma; b) que puede utilizarse para obtener información de identificación o de contacto sobre una determinada persona; c) que puede relacionarse directa o directamente con una persona.

3.1.8 amenaza [b-UIT-T X.800]: Posible violación de la seguridad.

3.1.9 dominio de seguridad [b-UIT-T T.411]: Conjunto de recursos sometidos a una única política de seguridad.

3.1.10 autoridad del dominio de seguridad [b-UIT-T X.810]: Autoridad de seguridad responsable de la aplicación de una política de seguridad en un dominio de seguridad.

3.1.11 política de seguridad [b-UIT-T T.411]: conjunto de normas que especifica los procedimientos y servicios necesarios para mantener el nivel de seguridad deseado de un conjunto de recursos.

3.1.12 firma [b-NIST SP 800-83]: Conjunto de características de los malware conocidos que pueden utilizarse para identificar malware conocidos y algunas nuevas variantes de malware conocidos.

3.1.13 spyware [b-NIST SP 800-83]: Malware destinado a violar la privacidad del usuario.

3.1.14 aplicativo de navegador web [b-NIST SP 800-83]: Mecanismo para visualizar o ejecutar ciertos tipos de contenido con un navegador web.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 anomalía: Patrón en los datos que no se ajusta al comportamiento previsto.

3.2.2 ataque por descarga: Patrón de ataque web que ocurre cuando un usuario visita un sitio web que explota las vulnerabilidades del navegador y lanza la descarga e instalación automática de malware sin el conocimiento o permiso del usuario.

3.2.3 ataque web: Patrón de ataque en que los atacantes ponen en peligro sitios web legítimos inyectando códigos malignos en una aplicación, que causan a su vez la infección de la computadora del usuario que visita esos sitios web, o utilizan las vulnerabilidades de los sitios web para lanzar ataques a los sistemas informáticos de los usuarios que visitan esos sitios web, que tienen lugar sin la intervención de malware.

3.2.4 sistema de protección contra ataques web: Una serie de sistemas que detectan las vulnerabilidades, malware o códigos malignos incorporados en sitios web legítimos y que informan al administrador web de dicha detección, permitiendo en último término su eliminación.

NOTA – La detección puede estar planificada de antemano o efectuarse en respuesta a eventos de la red o peticiones de otros sistemas.

3.2.5 computadora zombi: Computadora intervenida y controlada por un atacante que ha instalado malware, como virus, troyanos o botnet (red robot), que puede utilizar para llevar a cabo sus ataques, como el envío de spam (correo basura) o lanzar ataques de denegación de servicio.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

CAPEC Enumeración y clasificación de pautas de ataque comunes (*common attack pattern enumeration and classification*)

CSRF Falsificación de petición en sitios cruzados (*cross-site request forgery*)

CWE Enumeración de debilidades comunes (*common weakness enumeration*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DOM Modelo de objeto de documento (*document object model*)

HTML Lenguaje de marcaje de hipertexto (*hypertext markup language*)

HTTP	Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)
ID	Identidad (*identity*)
IODEF	Formato para el intercambio de descripciones de objetos de incidentes (*incident object description exchange format*)
LDAP	Protocolo ligero de acceso al directorio (*lightweight directory access protocol*)
MITM	Punto intermedio (*man-in-the-middle*)
OS	Sistema operativo (*operating system*)
OWASP	Proyecto abierto de seguridad de aplicaciones web (*open web applications security project*)
PC	Computadora personal (*personal computer*)
PII	Información de identificación personal (*personally identifiable information*)
PUI	Programa en inspección (*program under inspection*)
SNS	Servicio de red social (*social network service*)
SQL	Lenguaje de consulta estructurado (*structured query language*)
SSL	Capa de conexión segura (*secure socket layer*)
SSRF	Falsificación de petición en el servidor (*server-side request forgery*)
S/W	Software
URI	Identificador uniforme de recursos (*uniform resource identifier*)
URL	Localizador uniforme de recursos (*uniform resource locator*)
XSPA	Ataque de puerto en sitios cruzados (*cross-site port attack*)
XSS	Secuencias de comandos en sitios cruzados (*cross-site scripting*)

5 Convenios

Ninguno.

6 Aspectos generales

El malware, utilizado con el propósito de poner en peligro recursos de información, se define como un software diseñado específicamente para dañar o interrumpir un sistema, atacando su confidencialidad, integridad y/o disponibilidad. Se incluyen en esta categoría los virus informáticos, los gusanos, los troyanos, el spyware (software espía), el adware (software publicitario), la mayoría de rootkits y otros programas malignos.

Los ataques web son aquéllos en que los atacantes tratan de intervenir en sitios web legítimos aprovechando sus vulnerabilidades para inyectar en ellos códigos malignos que, a su vez, pueden utilizarse para infectar la computadora del usuario que visita esos sitios web. Los códigos malignos pueden adoptar múltiples formas: pueden estar escondidos en una etiqueta *iframe* que obligue al usuario a visitar el sitio atacado; o pueden ser aplicaciones malignas escritas en lenguaje de programación informática (por ejemplo, secuencias de comandos o applets). Ejemplos típicos de ataques web como la inyección SQL y la falsificación de petición en sitios cruzados.

El patrón de ataque falsificación de petición en sitios cruzados [b-CAPEC-62] es un tipo de ataque web en el cual se transmiten instrucciones no autorizadas o se solicita la ejecución de acciones no deseadas en un sitio web fiable sin que el usuario lo sepa mientras el usuario está conectado al sitio web fiable. El patrón de ataque inyección de lenguaje de consulta estructurado (SQL) [b-CAPEC-66] es otro tipo de ataque web en un sitio web de base de datos donde el atacante añade un código de lenguaje de consulta estructurado (SQL) en una casilla del formulario web para acceder a los recursos o modificar los datos. Se utiliza para robar información de una base de datos cuyos datos normalmente no están a disposición y/o para acceder a los anfitriones de una organización a través de la computadora que alberga la base de datos. La etiqueta *iframe*, *in-line frame* y *aka* [b-iframe] se utiliza para incorporar un documento invisible en el documento en lenguaje de marcaje de hipertexto (HTML) en uso y engañar al usuario, que pulsa sin advertirlo (*clickjacking*) el documento invisible [b-CAPEC-103].

Últimamente se ha visto un drástico incremento del número de ataques web motivado por la utilización creciente de dispositivos informáticos de usuario y un mayor número de sitios web con malware.

Por ejemplo, podrían aplicarse técnicas antivirus en el servidor y cortafuegos de aplicaciones web en intermediarios para facilitar una implementación rentable de estas técnicas.

En caso de ataque web, es posible que los administradores de los sitios web no sepan que sus sitios han sido pirateados y se les han inyectado códigos malignos que se utilizan para difundir otros códigos malignos. Además, los usuarios también desconocen que sus computadoras han sido infectadas por los códigos malignos inyectados en los sitios que han visitado. La instalación de software antivirus puede evitar algunos incidentes, pero no ofrece una solución definitiva.

El aumento de ataques web se debe a los siguientes factores:

- están aumentando los ataques por descarga desde sitios web populares;
- los ataques están muy ocultos y cambian dinámicamente, lo que hace que las soluciones tradicionales de detección y prevención de malware sean ineficaces;
- los ataques se dirigen a los aplicativos del navegador web de los usuarios extremos;
- se utilizan ataques de inyección SQL para infectar sitios web populares;
- los anuncios malignos redirigen a los usuarios hacia sitios web malignos; y
- hay un crecimiento exponencial de muestras de malware únicos y con objetivos muy definidos.

7 Técnicas del sistema de protección contra ataques web

7.1 Técnicas generales

Las siguientes técnicas son características del sistema de protección contra ataques web:

- lograr un diseño adaptable, robusto y resistente;
- funcionar en múltiples dominios de seguridad, cada uno de los cuales estará gestionado por un administrador de seguridad responsable, e
- intercambiar información sobre las vulnerabilidades de los sitios web o sitios web infectados con malware (es decir, los sitios web con etiquetas *i-frame* invisibles que redirigen a los usuarios a sitios web infectados con malware) [b-CAPEC-103].

  NOTA – Para intercambiar información puede utilizarse el formato para el intercambio de descripciones de objetos de incidentes (IODEF) existente [b-UIT-T X.1541].

- funcionar en uno de los dos tipos de modelos de implantación: centralizado y distribuido. En el modelo centralizado, toda la información sobre sitios web infectados con malware y tipos de malware debe comunicarse al servidor central, que la mantendrá o controlará. En el modelo distribuido, cada dominio de seguridad deberá tener un agente responsable, y serán los agentes responsables de cada ubicación distribuida los que intercambiarán la información sobre los sitios web infectados con malware y los tipos de malware;
- configurarse de manera jerárquica para facilitar su funcionamiento adaptable.

7.2 Técnicas funcionales

Las siguientes técnicas funcionales son características del sistema de protección contra ataques web:

- identificar el malware conocido en el contenido web legítimo y evitar la instalación del malware en los sitios web;
- detectar etiquetas *i-frame* invisibles que redirigen al usuario a otros sitios web que instalan el malware;
- detectar las vulnerabilidades que se pueden aprovechar para lanzar ataques web típicos, como la inyección SQL, la referencia entre sitios cruzados, etc., como se describe en el Apéndice IV;
- efectuar un análisis de firmas o un análisis equivalente para detectar el malware en el sitio web;
- efectuar un análisis de comportamiento para identificar el malware desconocido;
- informar al administrador del sitio web de la infección de malware para proceder a su eliminación de los sitios web;
- detectar el malware oculto que utiliza la división de cadenas, la codificación de cadenas, la codificación de cadenas personalizada, la modificación del comportamiento de comandos, la ocultación de funciones de modificación del modelo de objeto de documento (DOM), escondiendo enlaces detrás de servicios públicos y redireccionamientos de páginas en los sitios web;
- detectar el malware que puede utilizarse para lanzar ataques de falsificación de referencia en sitios cruzados en los sitios web;
- evaluar el comportamiento del malware sospechoso en los sitios web;
- informar a los usuarios de los sitios web infectados en caso de que el usuario los visite;
- informar al administrador de seguridad de que el sitio web ha sido infectado con códigos malignos que pueden, en último término, utilizarse para lanzar un ataque web, cuando un sistema de protección contra ese tipo de ataques detecta un malware en un sitio web;
- intercambiar información sobre listas negras de sitios web malignos; e
- identificar las vulnerabilidades de un sitio web, incluida la inyección SQL y las secuencias de comandos en sitios cruzados, y comunicar al administrador de ese sitio web las vulnerabilidades identificadas.

7.3 Técnicas de gestión

Las siguientes técnicas de gestión son características del sistema de protección contra ataques web:

- soportar la gestión de seguridad basada en políticas de seguridad cuando está implantado en diversos dominios de seguridad;
- disponer de una interfaz unificada para soportar la gestión desde un sistema de gestión centralizado;
- soportar la gestión fiable y aceptar únicamente datos sobre ataques procedentes de dominios de seguridad fiables;

- soportar la gestión de recursos del sistema y protegerlo contra las sobrecargas, y
- soportar la gestión de funcionamiento y mantenimiento, incluida la gestión de configuración del sistema, la gestión del registro cronológico, la supervisión del estado del sistema, etc.

7.4 Técnicas de seguridad y privacidad

Las siguientes técnicas de seguridad y privacidad son características del sistema de protección contra ataques web:

- facilitar la confidencialidad, la autentificación del origen de los datos y la integridad de la información intercambiada entre dominios de seguridad;
- evitar la filtración de información de identificación personal (PII) que el sistema de prevención web procesa;
- ofrecer resistencia ante diversos ataques en la red, por ejemplo, ataques de denegación de servicio distribuida (DDoS); y
- disponer de una funcionalidad de auditoria que pueda rastrear toda utilización indebida o abuso de la información recopilada para el sistema de protección contra ataques web por entidades no autorizadas.

8 Funciones del sistema de protección contra ataques web

El sistema de protección contra ataques web debe ofrecer como mínimo las siguientes funciones:

- detección de todas las vulnerabilidades conocidas en los sitios web;
- detección de sitios web que contienen malware utilizado para la distribución de malware;
- notificación al administrador de los sitios web que contienen malware y tienen vulnerabilidades conocidas que pueden explotar los atacantes;
- recopilación de la información necesaria sobre las vulnerabilidades de los sitios web y del malware que contienen;
- compartición de la información sobre sitios web infectados con malware y aquéllos que se utilizan para la distribución de malware entre entidades fiables y un dominio de seguridad, y entre múltiples dominios;
- aplicación de la política del sistema de protección contra ataques web en un dominio; y
- protección del sistema de protección contra ataques web contra todo ataque.

9 Formato de intercambio de información

Debe reforzarse el intercambio de información sobre análisis de malware (por ejemplo, enumeración y caracterización de atributos de malware). Los usuarios de esta Recomendación pueden utilizar [b-UIT-T X.1546] para intercambiar información sobre análisis de malware.

Apéndice I

Hipótesis de ataques web

(Este Apéndice no forma parte integrante de la presente Recomendación.)

I.1 Hipótesis de infección con malware

En la Figura I-1 se muestra un caso típico de ataque web:

1) Los atacantes intervienen en un sitio web legítimo que tiene vulnerabilidades e instalan un malware o una cadena de comandos que se utilizan para atacar la computadora del usuario o instala etiquetas para redirigir el acceso del usuario al sitio web que contiene el malware para atacar la computadora del usuario que ha visitado el sitio web.

2) Cuando el usuario víctima visita el sitio web intervenido por los atacantes, su computadora se ve atacada por el malware incorporado o redirigida a otro sitio web que contiene el malware para atacar la computadora del usuario.

3) Cuando la computadora del usuario tiene vulnerabilidades de navegador que puede utilizar un malware específico, éste se instala en la computadora del usuario y se convierte en una computadora infectada con malware sin que el usuario lo sepa o haya dado su permiso.

4) El malware instalado en la computadora del usuario puede emplearse para lanzar un ataque de denegación de servicio distribuida (DDoS) masivo o para robar información personal, como la identidad (ID) y la contraseña, que se transmite a los atacantes.

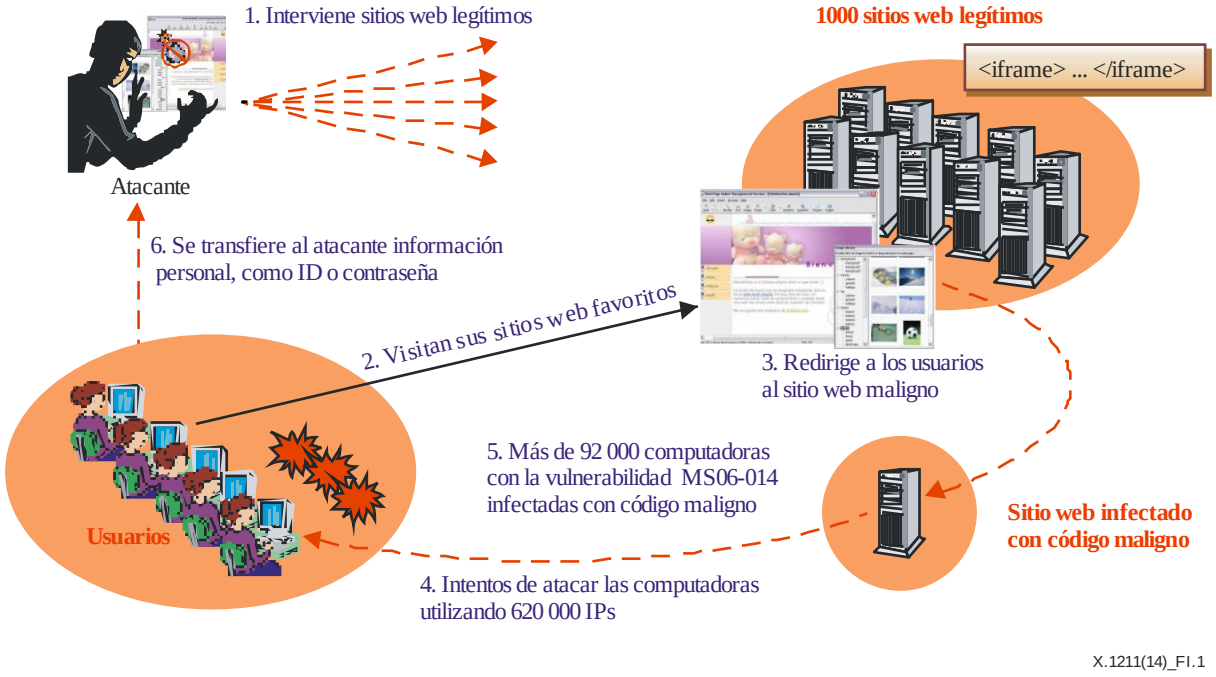

Figura I-1 – Caso típico de ataque web

I.2 Falsificación de petición en sitios cruzados (CAPEC-62)

La falsificación de petición en sitios cruzados (CSRF) puede hacer que una víctima efectúa inocentemente una o más peticiones en protocolo de transferencia de hipertexto (HTTP) a un sitio web vulnerable en el que el usuario confía. Un ataque de falsificación de petición en sitios cruzados típico puede poner en peligro la integridad de los datos y dar al atacante la capacidad de modificar la información almacenada en un sitio web vulnerable.

Cuando un sitio web exige la autentificación del usuario, con frecuencia no le exige introducir su contraseña a cada petición http, sino que el sitio web identifica el estado de autentificación del usuario entre múltiples peticiones HTTP con testigos como las *cookies* de sesión o el encabezamiento de autorización http. Sin embargo, hay un problema: los navegadores web memorizan el testigo asociado a un localizador uniforme de recursos (URL) y automáticamente anexan el testigo cuando se presenta una nueva petición new HTTP al sitio web, incluso si el usuario no pretende formular esa petición. La CSRF se aprovecha del comportamiento del navegador. En caso de CSRF, un usuario sólo necesita visitar un sitio web maligno que puede incluir una lógica JavaScript que formula peticiones HTTP (posiblemente ocultas) a otros sitios web (como el banco del usuario), y el sitio web puede autorizar tales peticiones HTTP gracias a la presencia de los testigos. La CSRF permite realizar diversos tipos de ataque, como el envío de correos-e desde un servicio de correo web, la publicación de un comentario en un blog en nombre del usuario, la alteración de la lista de amigos del usuario en un servicio de red social (SNS), o la modificación de la configuración de encaminador doméstico.

I.3 Ataque de puerto en sitios cruzados/falsificación de petición en el servidor

El ataque de puerto en sitios cruzado/falsificación de petición en el servidor (XSPA/SSRF) es un método de abusar de las aplicaciones web que procesa las URL facilitadas por una entrada de navegador web. En un ataque XSPA/SSRF típico el objetivo es la intranet de la aplicación vulnerable. El ataque puede desencadenar la exploración de puertos, poner en peligro la confidencialidad de los datos, desencadenar la ejecución de códigos no autorizados y explotar los recursos de intranet vulnerables. Una aplicación se considera vulnerable a XSPA/SSRF cuando no valida la salida recibida desde un anfitrión remoto y la entrada facilitada por el usuario extremo. Por ejemplo, la aplicación que descarga una imagen de un URL facilitado por el usuario puede acceder a un recurso de intranet cuando el usuario escribe el URL, como 'http://localhost/secret.txt'. En algunos casos, se pueden utilizar esquemas de identificador uniforme de recursos (URI) especiales a fin de que la aplicación vulnerable envíe una petición de servicios especiales, como 'https', 'gopher', 'ftp', 'ldap'. También se pueden utilizar esquemas de lenguajes específicos como 'php://fd', 'php://memory'.

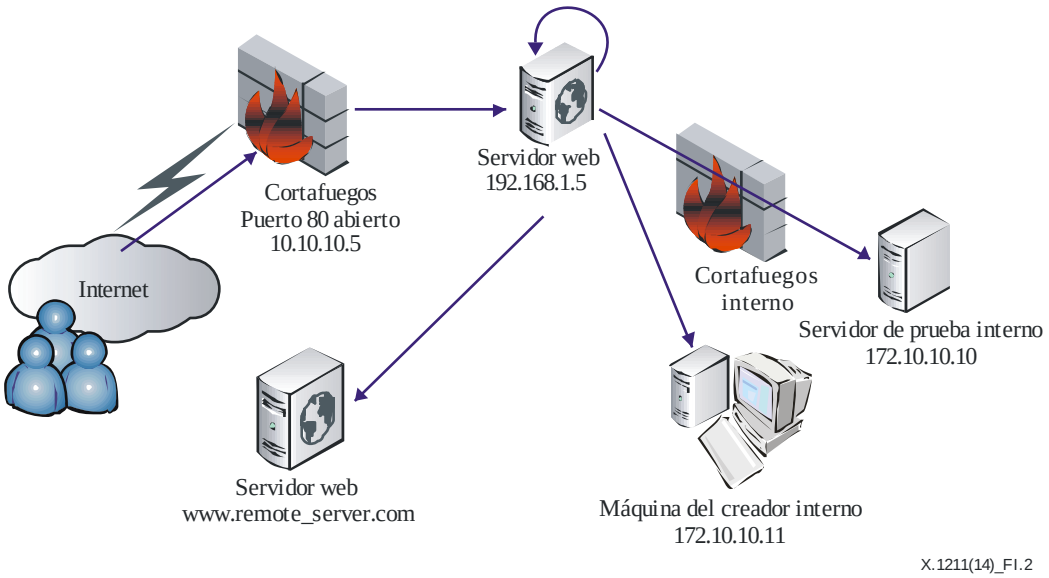

Figura I-2 – Caso típico de ataque de puerto en sitios cruzados/ falsificación de petición en el servidor

I.4 Inyección SQL (CAPEC-66)

La hipótesis habitual de inyección SQL está basada en una verificación incompleta de la validez de los datos de entrada de las aplicaciones web. Los canales de entrada pueden variar de peticiones GET y HTTP POST a cookies del navegador, cargas útiles basadas en XML, entradas de archivos y otros.

La entrada específica se inyecta entonces en una indagación SQL. Este es el ejemplo básico de inyección SQL en el parámetro "GET" HTTP:

- Dada la indagación original – "SELECCIONAR título, contenido DESDE cuadro 1 DONDE id=%d"

donde "id" es el parámetro objetivo.

En condiciones normales, "id" es un cierto número natural. Pero debido a la falta de comprobación de la validez, en lugar de un número el atacante puede proporcionar la siguiente entrada:

- %d = "1 usuario UNION SELECT, contraseña FROM secret_table"

Habría de esta forma un acceso no autorizado al "secret table" dando lugar a la revelación de datos sensibles directamente a la salida del navegador.

Según la implantación de la base de datos SQL, ese ataque podría llevar a:

- revelación de datos sensibles de la base de datos o del sistema de ficheros;
- pérdida/modificación de datos;
- inyección de "puertas traseras" (backdoors) y escalado basado en privilegios; e
- implantación de malware a los usuarios extremos que visitan el sitio.

I.5 Detección de malware en sitios web

Las técnicas utilizadas para detectar el malware pueden dividirse en dos categorías: detección de anomalías y detección de firmas [b-NA].

Con la técnica de detección de anomalías, los criterios para determinar la malignidad del programa que se inspecciona son los comportamientos normales. Hay un tipo especial de detección de anomalías denominado detección de especificación. Estas técnicas utilizan algún tipo de especificaciones o normas de comportamiento válido para determinar la malignidad del programa que se inspecciona. Los programas que violan esas normas o especificaciones se consideran malignos.

Con la detección de firmas, los criterios para determinar la malignidad del programa que se inspecciona son las características de lo que se conoce como maligno. La caracterización o firma del comportamiento maligno es la clave de la eficacia del método de detección de firmas.

Cada técnica de detección puede adoptar uno de tres posibles enfoques diferentes: estático, dinámico o híbrido. El método o análisis específico que se realiza con una técnica de detección de anomalías o de firmas está determinado por cómo se obtiene la información para detectar el malware. El análisis estático utiliza las propiedades sintácticas o estructurales del programa (estático)/proceso (dinámico) que se inspecciona para determinar su malignidad. Por ejemplo, para la detección de firmas estática sólo se utilizará la información estructural (por ejemplo, secuencia de bytes) para determinar la malignidad, mientras que con un enfoque dinámico se utilizará la información del tiempo de ejecución (por ejemplo, los sistemas presentes en la pila de tiempo de ejecución) del programa que se inspecciona.

En general, con el enfoque estático se intenta detectar el malware antes de que se ejecute el programa en inspección. Por el contrario, con el enfoque dinámico se quiere detectar el comportamiento maligno durante la ejecución del programa o después de la misma.

Hay técnicas híbridas que combinan ambos enfoques. En ese caso, se utiliza la información estática y dinámica para detectar el malware.

En el Apéndice III se describen varias técnicas de detección de malware en sitios web.

Apéndice II

Método para infectar una computadora de usuario con malware

(Este Apéndice no forma parte integrante de la presente Recomendación.)

El objetivo de este Apéndice es describir casos típicos de ataques a fin de que los administradores puedan entenderlos mejor.

El primer paso de un ataque web es la instalación y ejecución de diversos códigos malignos en la computadora de un usuario. Entre tales códigos se cuentan los registradores de teclas y rootkits (que pueden transformar la computadora del usuario en zombie o filtrar a los atacantes información sensible del usuario).

El objetivo del ataque puede lograrse explorando diversas vulnerabilidades conocidas de diversos componentes de software accesibles desde un navegador (por ejemplo, componentes del sistema operativo accesibles desde un navegador a través de ActiveX, etc.), o mediante técnicas de ataque que utilizan la ingeniería social para engañar a los usuarios y que ellos mismos instalen y ejecuten el malware en su sistema. Además, con este ataque se intentan robar las credenciales del usuario mediante técnicas de peska (phishing) o secuencias de comandos en sitios cruzados que se ejecutan en una *iframe* oculta.

Se pueden utilizar diversas técnicas para infectar la computadora de un usuario con malware: explotar el componente ActiveX, técnicas de ingeniería social, códecs perdidos, herramientas de supresión de malware y ataques de falsificación de petición en sitios cruzados. Puede encontrarse información detallada al respecto en [b-NTOBJECTives]. Además, puede encontrarse una lista de patrones comunes de ataque y una lista complete de esquemas y clasificación en [b-UIT-T X.1544].

Apéndice III

Ejemplos típicos de técnicas de ocultación

(Este Apéndice no forma parte integrante de la presente Recomendación.)

El contenido maligno inyectado utiliza una técnica de ocultación a fin de esconderlo al ojo humano y al software de detección de vulnerabilidades [b-UIT-T X.1520]. Las técnicas de ocultación son bastante eficaces por los siguientes motivos:

- Muchos administradores de sitios web no se atreven a borrar códigos de comandos que no entienden.
- Los administradores de bases de datos tienen dificultades para limpiar bases de datos infectadas sin saber qué patrones buscar.
- Muchos métodos de detección se basan en la búsqueda de expresiones regulares o cadenas por lo que tienen problemas para identificar HTML oculto.

Hay varios tipos de métodos de ocultación: división de cadenas, codificación de cadenas, codificación personalizada de cadenas, modificación del comportamiento de comandos, funciones de ocultación de modificaciones de DOM, ocultación de enlaces tras servicios públicos y redireccionamiento de página. Puede encontrarse información detallada al respecto en [b-NTOBJECTives].

Apéndice IV

Técnicas de prevención de ataques web

(Este Apéndice no forma parte integrante de la presente Recomendación.)

El objetivo de este Apéndice es presentar diversas técnicas de detección de malware en sitios web [b-NTOBJECTives]. El contenido maligno puede detectarse mediante la correspondencia de firmas de contenido, la realización de listas negras de sitios atacantes o el análisis del contenido en busca de comportamientos sospechosos con algoritmos propios.

IV.1 Eliminar vulnerabilidades de los sitios web

La manera más simple es eliminar las vulnerabilidades de los sitios web, incluidas la inyección SQL y las secuencias de comandos en sitios cruzados. Si el atacante no puede insertar el contenido maligno en el sitio web, el navegador del cliente no ejecutará el malware insertado en el sitio web. Por consiguiente, la manera más eficaz de evitar ataques web es eliminar todas las vulnerabilidades de los sitios web.

IV.2 Correspondencia de firmas

Dado que existen diversas técnicas de ocultación y herramientas automáticas para ocultar el malware, no resulta práctico detectar el contenido malware en un sitio web utilizando el método de detección de firmas. Es bien sabido que los atacantes pueden automatizar la codificación de contenido maligno con una nueva clave para cada sitio web, haciendo así que el malware tenga una firma distinta en cada sitio web. Sin embargo, el contenido malware simple no se cambia con frecuencia, por lo que puede detectarse en un sitio web por su firma. Si el contenido malware simple se obtiene descodificando el malware codificado y se calcula su firma, este método puede detectar el malware comparando la firma calculada con una lista previamente establecida de todas las firmas de malware conocidas hasta el momento.

IV.3 Lista negra de sitios

Realizar una lista negra de sitios web atacantes es la técnica de detección más valiosa. Aunque el contenido maligno puede estar completamente albergado en un sitio web adecuado (sin requisitos de carga automática de comandos o *iframes* desde el sitio atacante, escondiendo así su conexión con el sitio atacante), es necesario intercambiar ciertos datos con el sitio web atacante para completar el ataque previsto. Este intercambio de datos necesario puede darse de muy diversas formas: el comando atacante debe descargar malware desde el sitio web atacante, o enviar los datos privados extraídos del sistema del usuario al sitio atacante, o cualquier otra variante. En cualquier caso, el comando atacante tiene que establecer una conexión con el sitio atacante.

Si hay un algoritmo de detección de recursos externos vinculado a la lista negra, puede sospechar que un sitio web tiene un malware. Por consiguiente, toda correspondencia con los sitios de la lista negra indicará la presencia de contenido maligno en la página analizada.

IV.4 Detección de técnicas de ocultación

Si un sitio web tiene el contenido de la página codificado con técnicas de ocultación, puede razonablemente pensarse que el sitio web tiene intenciones malignas. Por ejemplo, si un sitio web tiene contenido con una cadena codificada larga, puede ser contenido maligno. Sin embargo, aunque las cadenas codificadas largas son sospechosas, no siempre puede suponerse que el sitio web tiene contenido maligno hasta que se descodifica y se analiza su acción.

IV.5 Evaluación de comportamientos del contenido sospechoso

La manera más eficaz es analizar el comportamiento del contenido sospechoso. Si la actividad del contenido es sospechosa, puede indicar que su intención es maligna. Los comportamientos tópicos que pueden considerarse malignos son, entre otros, el acceso al disco duro local, la instanciación de un objeto de aplicación intérprete de comandos y la descarga (acceso) de contenido ejecutable externo.

Apéndice V

Ejemplos típicos de riesgos de seguridad de aplicaciones por OWASP

(Este Apéndice no forma parte integrante de la presente Recomendación.)

El Proyecto abierto de seguridad de aplicaciones web (OWASP), conjunto de herramientas, tecnologías y metodologías web de fuente abierta resultado de la colaboración entre líderes de la industria, organizaciones docentes y particulares de todo el mundo, publicó la lista OWASP de 10 ataques web más eficaces [b-OWASP] y CWE [b-UIT-T X.1524] CWE-928: Puntos débiles en la lista OWASP de 10 ataques web más eficaces [b-CWE], que se reproduce en el Cuadro V.1.

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-1 – Inyección	Toda persona que pueda enviar datos no fiables al sistema, incluidos los usuarios externos, los usuarios internos y los administradores.	Los atacantes envían ataques de texto simple que explotan la sintaxis del intérprete objetivo. Prácticamente todas las fuentes de datos pueden ser vector de inyección, incluidas las internas.	Los errores de inyección ocurren cuando una aplicación envía datos no fiables a un intérprete. Los errores de inyección están muy presentes, sobre todo el códigos heredados, y se encuentran con frecuencia en búsquedas SQL, búsquedas LDAP, búsquedas XPath, instrucciones del OS, argumentos de programas, etc. los errores de inyección son fáciles de descubrir al examinar el código, pero difíciles cuando se recurre a las pruebas. Los atacantes pueden servirse de un escáner o un fuzzer para encontrarlos.	La inyección puede causar la pérdida o la corrupción de los datos, una falta de responsabilidad, o la denegación del acceso. En ocasiones una inyección puede llevar a una toma de control total sobre el anfitrión.	Considérese el valor comercial de los datos afectados y de la plataforma que ejecuta el intérprete. Todos los datos pueden ser robados, modificados o suprimidos. ¿Puede quedar dañada su reputación?	CWE-77, CWE-78, CWE-89, CWE-90, CWE-91, CWE-929

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-2 – Rotura de la gestión de autentificación y sesión	Pueden ser atacantes externos anónimos, y también usuarios con sus propias cuentas, que intentan robar las cuentas ajenas. También pueden ser atacantes internos que quieran encubrir sus acciones.	El atacante utiliza filtraciones o fallos en las funciones de gestión de autentificación o sesión (por ejemplo, cuentas, contraseñas, ID de sesión a la vista) para hacerse pasar por los usuarios.	Los creadores suelen crear esquemas de gestión de autentificación y sesión personalizados, pero hacerlo correctamente es difícil. Así, estos esquemas personalizados suelen tener fallos en, por ejemplo, la desconexión, la gestión de contraseñas, la expiración de los temporizadores, la memoria de contraseñas, las preguntas secretas, la actualización de cuentas, etc. en ocasiones puede resultar difícil encontrar esos fallos, puesto que cada aplicación es única.	Estos fallos pueden permitir que se ataquen algunas, o incluso todas, las cuentas. Cuando el ataque se realiza con éxito, el atacante puede realizar las mismas acciones que la víctima. Suelen ser objetivo de los ataques las cuentas con privilegios.	Considérese el valor comercial de los datos o funciones de aplicación afectadas. Considérese asimismo la repercusión comercial de que se haga pública la vulnerabilidad.	CWE-256, CWE-287, CWE-384, CWE-311, CWE-319, CWE-522, CWE-523, CWE-613, CWE-620, CWE-640, CWE-930

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-3 – Secuencias de comandos en sitios cruzados (XSS)	Toda persona que pueda enviar datos no fiables al sistema, incluidos los usuarios externos, los usuarios internos y los administradores.	El atacante envía secuencias de comandos de ataque textuales que explotan el intérprete del navegador. Prácticamente todas las fuentes de datos pueden ser vector de ataque, incluidas las internas, como los datos de una base de datos.	XSS es el error de seguridad de aplicación web que más presente está. Los errores XSS ocurren cuando una aplicación incluye los datos facilitados por un usuario en una página enviada al navegador sin validar adecuadamente el contenido o sin obviarlo. Hay tres tipos conocidos de errores XSS: 1) almacenado, 2) reflejado, y 3) XSS en DOM. La mayoría de fallos XSS se detectan fácilmente con pruebas o análisis de código.	Los atacantes pueden ejecutar secuencias de comandos en el navegador de la víctima para piratear las sesiones de usuario, cambiar la apariencia de sitios web, insertar contenido hostil, redirigir a los usuarios, piratear el navegador del usuario con malware, etc.	Considérese el valor comercial del sistema afectado y de todos los datos que procesa. Considérese también la repercusión comercial de hacer pública la vulnerabilidad.	CWE-79, CWE-931

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-4 – Referencia a objeto directo insegura	Considérese los tipos de usuarios de su sistema. ¿Hay usuarios que sólo tienen acceso parcial a ciertos tipos de datos del sistema?	El atacante, que es un usuario autorizado del sistema, simplemente modifica un valor de parámetro que remite directamente a un objeto del sistema a otro objeto al que el usuario no está autorizado a acceder. ¿Se le concede el acceso?	Las aplicaciones suelen utilizar el nombre real o la clave de un objeto cuando generan páginas web. Las aplicaciones no siempre verifican que el usuario está autorizado para acceder al objeto en cuestión. Esto hace posible el ataque por referencia a objeto directo insegura. Los probadores pueden fácilmente manipular los valores de los parámetros para detectar esos fallos. Con un análisis de código se ve rápidamente si la autorización está adecuadamente verificada.	Esos fallos pueden poner en peligro los datos que pueden referenciarse con ese parámetro. A menos que las referencias a objetos sean impredecibles, un atacante puede fácilmente acceder a todos los datos disponibles de ese tipo.	Considérese el valor comercial de los datos en peligro. Considérese también la repercusión comercial de hacer pública la vulnerabilidad.	CWE-22, CWE-99, CWE-639, CWE-932

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-5 – Configuración de seguridad errónea	Pueden ser atacantes externos anónimos, así como usuarios con cuenta que intentar poner en peligro el sistema. También pueden ser usuarios internos que quieran encubrir sus acciones.	El atacante accede a las cuentas defectuosas, las páginas no utilizadas, las brechas de seguridad sin parchar, los ficheros y directorios no protegidos, etc., para obtener acceso no autorizado al sistema o conocerlo.	Una configuración errónea puede darse en cualquier nivel de la pila de aplicación, incluida la plataforma, el servidor web, el servidor de aplicación, la base de datos, el marco y el código personalizado. Los creadores y administradores del sistema deben colaborar para asegurarse de que toda la pila está adecuadamente configurada. Los escáneres automatizados son útiles para detectar los parches que faltan, las configuraciones erróneas, la utilización de cuentas defectuosas, los servicios innecesarios.	El sistema puede estar íntegramente en peligro sin que se sepa. Todos los datos pueden robarse o modificarse lentamente con el paso del tiempo. Los costos de recuperación pueden ser muy elevados.	El sistema puede estar íntegramente en peligro sin que se sepa. Todos los datos pueden robarse o modificarse lentamente con el paso del tiempo. Los costos de recuperación pueden ser muy elevados.	CWE-2, CWE-16, CWE-209, CWE-215, CWE-548, CWE-933

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-6 – Exposición de datos sensibles	Considérese quién puede acceder a los datos sensibles y realizar copias de seguridad de los mismos. Se incluyen los datos en reposo, en tránsito e, incluso, en los navegadores de los clientes. Se incluyen amenazas internas y externas.	Los atacantes no suelen romper directamente la criptografía, sino que suelen robar claves, realizar ataques por intermediario o robar texto sin encriptar del servidor, mientras está en tránsito o cuando está en el navegador del usuario.	El fallo más común es la no encriptación de datos sensibles. Cuando se utiliza la criptografía se suelen emplear una gestión y generación de claves débiles y se utiliza un algoritmo débil, en particular técnicas de troceado de contraseñas débiles. Es muy común que el navegador tenga puntos débiles, comunes y fáciles de detectar, pero difíciles de explotar a gran escala. Los atacantes externos suelen tener dificultades para detectar los fallos del servidor al tener un acceso limitado, y también porque suelen ser difíciles de explotar.	Los fallos frecuentemente ponen en peligro todos los datos que deberían estar protegidos. Normalmente esta información incluye datos sensibles como expedientes sanitarios, credenciales, datos personales, tarjetas de crédito, etc.	Considérese el valor comercial de los datos perdidos y la repercusión para su reputación. ¿Cuál es la responsabilidad jurídica si esos datos quedan expuestos? Considérense también los daños que puede sufrir su reputación.	CWE-310, CWE-311, CWE-312, CWE-319, CWE-325, CWE-326, CWE-934

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-7 – Control de acceso a nivel de función	Toda persona con acceso a la red puede enviar una petición a su aplicación. ¿Pueden los usuarios anónimos acceder a funcionalidades privadas o los usuarios normales acceder a funciones privilegiadas?	El atacante, que es un usuario autorizado del sistema, simplemente modifica el URL o un parámetro para acceder a una función privilegiada. ¿Se le concede ese acceso? Los usuarios anónimos pueden acceder a funciones privadas que no estén protegidas.	Las aplicaciones no siempre protegen adecuadamente las funciones de aplicación. En ocasiones, la protección del nivel de función se gestiona mediante la configuración y, el sistema está configurado erróneamente. A veces, los creadores deben incluir las verificaciones de código adecuadas y se olvidan. Detectar esos fallos es fácil. Lo difícil es identificar qué páginas (URL) o funciones existen para atacar.	Los fallos permiten a los atacantes acceder a funcionalidades no autorizadas. Las funciones administrativas son los principales objetivos de este tipo de ataques.	Considérese el valor comercial de las funciones expuestas y de los datos que se procesan. Considérense también las repercusiones para su reputación de que se haga pública la vulnerabilidad.	CWE 285, CWE-287, CWE-935

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-8 –Falsificación de petición en sitios cruzados (CSRF)	Toda persona que pueda cargar contenido en los navegadores de los usuarios y forzarlos a presentar peticiones al sitio web. Todo sitio web o flujo HTML al que pueden acceder los usuarios puede realizar esa función.	El atacante crea peticiones HTTP falsas y engaña a la víctima para que las envíe en etiquetas de imagen, XSS o por diversas otras técnicas. Si el usuario está autentificado, el ataque tiene éxito.	CSRF se aprovecha de que la mayoría de aplicaciones web permiten a los atacantes predecir todos los detalles de una acción concreta. Dado que los navegadores envían credenciales, como las cookies de sesión, automáticamente, los atacantes pueden crear páginas web malignas que generan peticiones falsas que no se pueden distinguir de las legítimas. La detección de errores CSRF es relativamente fácil mediante una prueba de penetración o un análisis de código.	Los atacantes engañan a las víctimas para que realicen operaciones de cambio de estado para las que están autorizadas, por ejemplo, actualización de datos de cuenta, realización de compras, desconexión e, incluso, conexión.	Considérese el valor comercial de los datos afectados o las funciones de aplicación. Imagínese la inseguridad de no saber si los usuarios van a realizar esas acciones. Considérese la repercusión para su reputación.	CWE-346, CWE-352, CWE-441, CWE-642, CWE-935

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-9 – Utilización de componentes con vulnerabilidad es conocidas	Es posible identificar y explotar algunos componentes vulnerables (por ejemplo, bibliotecas marco) con herramientas automáticas, ampliando el número de agentes amenazadores a cualquier persona aleatoria.	El atacante identifica un componente débil mediante escaneado o análisis manual. Adapta la explotación en función del resultado y ejecuta el ataque. Resulta más difícil si el componente utilizado está en las profundidades de la aplicación.	Prácticamente todas las aplicaciones tienen este problema, porque la mayoría de equipos creadores no se centran en garantizar que sus componentes/bibliotecas estén actualizados. En muchos casos, los creadores ni siquiera conocen todos los componentes que utilizan, y mucho menos las versiones. Las dependencias del componente agravan la situación.	Puede darse toda la gama de vulnerabilidades, incluida la inyección, la rotura del control de acceso, XSS, etc. La repercusión puede ser mínima o la toma de control total del anfitrión y la puesta en peligro de los datos.	Considérese qué repercusión puede tener cada vulnerabilidad para las funciones controladas por la aplicación afectada. La puesta en peligro puede ser muy leve o total.	CWE-937

Cuadro V.1 – Lista OWASP de 10 ataques web más eficaces

Tipo de ataque	Agente amenazador	Vector del ataque	Puntos débiles de seguridad	Repercusiones técnicas	Repercusiones para la empresa	Referencias a los identificadores CWE
A-10 – Reenvío y redireccionamiento no validado	Toda persona que pueda engañar a los usuarios para que presenten una petición al sitio web. Todo sitio web o flujo HTML que pueden utilizar los usuarios puede realizar esa función.	El atacante crea enlaces a redireccionamientos no validados y engaña a las víctimas para que los utilicen. Probablemente las víctimas lo utilizarán, pues se trata de un enlace a un sitio válido. El atacante pretende realizar un reenvío no seguro para evitar las verificaciones de seguridad.	Las aplicaciones suelen redireccionar a los usuarios a otras páginas o utilizar, de manera semejante, el reenvío interno. En ocasiones la página objetivo está especificada en un parámetro no validado, lo que permite a los atacantes elegir la página de destino. Es fácil detectar redireccionamientos no verificados. Se han de buscar los redireccionamientos en que se puede indicar todo el URL. Los reenvíos no verificados son más difíciles, pues su objetivo son páginas internas.	Estos redireccionamientos pueden intentar instalar malware o engañar a las víctimas para que descubran su contraseña o demás información sensible. Los reenvíos no seguros pueden ayudar a evitar el control de acceso.	Considérese el valor comercial de mantener la confianza de los usuarios. ¿Qué pasa si el malware toma el control? ¿Qué pasa si los atacantes sólo pueden acceder a funciones exclusivamente internas?	CWE-601, CWE-938

Bibliografía

[b-UIT-T M.3030] Recomendación UIT-T M.3030 (2002), *Marco para un lenguaje de marcaje en telecomunicaciones*.

[b-UIT-T T.411] Recomendación UIT-T T.411 (1993) | ISO/IEC 8613-1:1994, *Tecnología de la información – Arquitectura de documento abierta y formato de intercambio: Introducción y principios generales*.

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[b-UIT-T X.810] Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[b-UIT-T X.1520] Recomendación UIT-T X.1520 (2014), *Vulnerabilidades y exposiciones comunes*.

[b-UIT-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*.

[b-UIT-T X.1541] Recomendación UIT-T X.1541 (2012), *Formato para el intercambio de descripciones de objetos de incidentes*.

[b-UIT-T X.1544] Recomendación UIT-T X.1544 (2013), *Enumeración y clasificación de pautas de ataques comunes*.

[b-UIT-T X.1546] Recomendación UIT-T X.1546 (2014), *Enumeración y caracterización de atributos de malware*.

[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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2015