SECUINFOR

Centro de Operaciones
de Ciberseguridad

#SiempreAlerta

REVISANDO TÉCNICAMENTE CADA UNO DE LOS RIESGOS PRESENTES EN LAS APLICACIONES WEB

A2 PÉRDIDA DE AUTENTICACIÓN Y GESTIÓN DE SESIONES

Autor: Christian Mendoza Bonzo.

Objetivo: Describirles a los desarrolladores y gerentes de proyectos en desarrollo en qué consiste el riesgo de Pérdida de autenticación y gestión de sesiones, alternativas para detectarlo y los mecanismos de protección,

Fecha: Septiembre 26, 2016.

Continuando con la descripción de los riesgos en aplicaciones, ahora desarrollaremos la descripción de cada uno de los riesgos, cómo identificarlas y qué acciones podemos tomar.

A2- Pérdida de autenticación y gestión de sesiones.-

Recordemos que esta vulnerabilidad ocurre cuando en una aplicación los mecanismos que proveen autenticación y gestión de sesiones son implementados incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, sesiones o explorar otras fallas para asumir la identidad de otros usuarios.

Revisemos paso a paso cómo se puede generar este tipo de amenazas antes que se transformen en un riesgo.

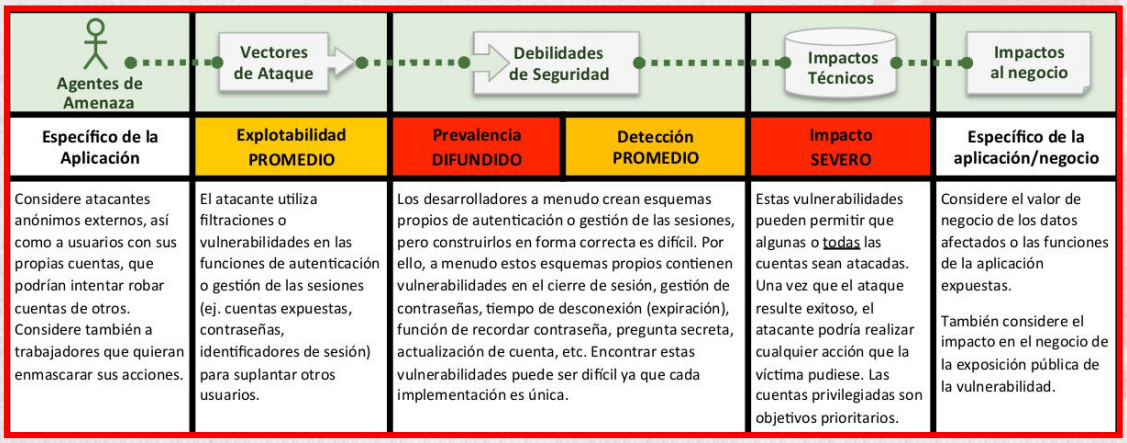

Fig 1. Pérdida de autenticación y gestión de sesiones. Copyright por: Owasp. Re-impreso con Permiso

¿Cómo conocer si soy vulnerable?

Existen varias formas de conocer si eres o no vulnerable, te presentamos algunas opciones que te permitirán conocerlo:

- √ Se es vulnerable cuando se almacena credenciales cifradas de los usuarios.
- √ Son vulnerables si es posible adivinar o sobrescribir las credenciales a través de funciones débiles de gestión de la sesión, como: creación de usuarios, cambio de contraseñas, recuperación de contraseñas, id de sesiones débiles.
- √ También son vulnerables si los identificadores (ID) de sesión son expuestos en la URL.

- √ Se es vulnerable cuando los identificadores (ID) de sesión, las sesiones de usuarios o los tokens de autenticación no expiran.
- √ Los identificadores de sesión son vulnerables a ataques de fijación de la sesión.
- √ Las claves, identificadores de sesión y otras credenciales que son transmitidos a través de canales no cifrados, son vulnerables.

¿Cómo prevenirlo?

Para evitar pérdida de autenticación y gestión de sesiones se recomienda los siguientes ítems:

1. Un único grupo de controles de autenticación y gestión de sesiones fuerte.
2. Cumplir con todos los requisitos de autenticación y gestión de sesiones definidos en el *Application Security Verification Standard (ASVS*) de *OWASP*.
3. Tener una interfaz sencilla para los desarrolladores, considerar el uso de ESAPI authenticator[1] y la APIs de usuarios como buenos ejemplos a seguir.
4. Ejecutar pruebas estáticas y dinámicas sobre el software desarrollado.

Si desea conocer cómo podemos ayudarlo a proteger su información confidencial contáctenos a:

Email: info@secuinfor.com
PBX: +593-4-3726620
Website: http://www.secuinfor.com

[1] *La ESAPI es una colección gratis y abierta de todos los métodos de seguridad que un desarrollador necesita para construir una aplicación Web segura. Usted puede usar solo las interfases y construir su propia implementación usando la infraestructura de su compañía.*