DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Jornadas de
Visibilidad Web UNAM 2022

Principales vulnerabilidades en aplicaciones web y recomendaciones de mitigación

Ing. Angie Aguilar Domínguez

Visibilidad Web UNAM

Agenda

- Seguridad en aplicaciones web
- Principales vulnerabilidades en aplicaciones web
- Elementos adicionales
- Recomendaciones de mitigación

¿Por qué pensar en seguridad en aplicaciones web?

- Cualquier sitio está expuesto a ataques, modificaciones, minado…
- Factores como: el tamaño del sitio, la cantidad de usuarios, las transacciones que se realizan
- Objetivo para uso de recursos del servidor y/o robo de información
- No siempre el ataque viene de afuera

- En el peor escenario: ¿Cuánto tiempo puede estar el sitio fuera de línea?
  - Recuperar el sitio en tiempo récord, ¿con los mismos problemas?
- ¿Estoy preparado para enfrentarlo?
  - Conocer el entorno: software, versiones, fallos conocidos…
- Entender que la seguridad debe ser preventiva:
  - Si yo creo que mi sitio no es importante, ¿qué es lo peor que puede pasar?

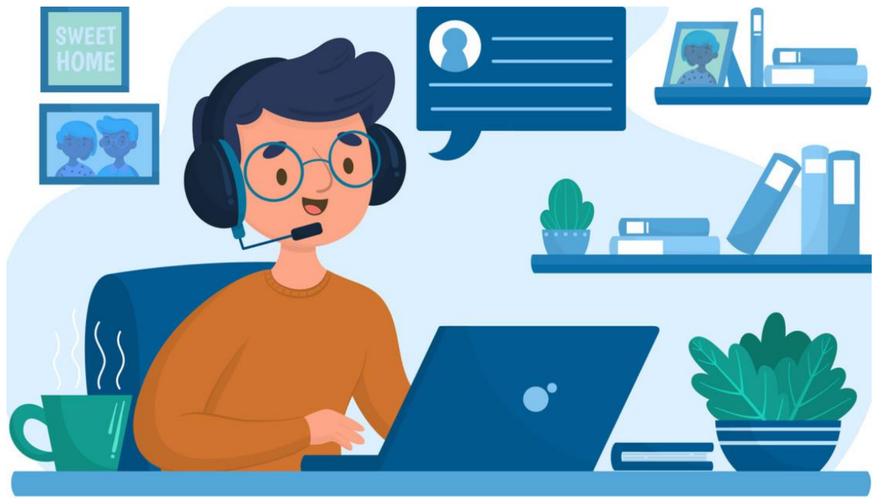
Algunos datos

- En 2021 aumentó la cantidad de ataques dirigidos a aplicaciones web en un 600% hacia sitios de América Latina respecto a 2020

- Una de las vulnerabilidades que los atacantes buscaron explotar es Log4J, la cual permite la ejecución remota de código malicioso

- También hubo ataques distribuidos de denegación de servicio, así como intentos de instalar herramientas de minería de criptomonedas

(Fuente: Fortinet)



- Algunos eventos que se presentaron en fechas recientes:
- Log4shell: vulnerabilidad en la biblioteca Log4j de Apache
- Exchange: vulnerabilidad en el servidor Microsoft Exchange Server
- Aún más: ¿Qué sucedió en pandemia?

OWASP

- OWASP, Open Web Application Security Project, es un grupo de seguridad y profesionales dedicados a la seguridad de las aplicaciones web

- Sitio oficial:

https://www.owasp.org

OWASP

- Promueve el mejor uso de los recursos y la implementación de buenas prácticas

- Cuenta con guías gratuitas para el desarrollo y prueba de distintos escenarios: OWASP Web Security Testing Guide
  - https://owasp.org/www-project-web-security-testing-guide/

- Algunas herramientas disponibles: ZAP, Burp, w3af, complementos para navegador…

- 10 de las vulnerabilidades mas comunes en las aplicaciones web: última actualización en 2021
- El objetivo principal es educar y difundir información sobre las vulnerabilidades más importantes
- Esta publicación proporciona información y recomendaciones sobre las medidas que se pueden implementar

A01:2021 Pérdida de control de acceso

- Fallo que conduce a la divulgación, modificación o destrucción de información no autorizada, a realizar una función de negocio fuera de los límites del usuario

- Incluye elementos como:
  - Violación del principio del menor privilegio
  - Omisión de las verificaciones de control de acceso

A01:2021 Pérdida de control de acceso

- Consecuencias:
  - Omitir comprobaciones de control de acceso modificando la URL
  - Elevación de privilegios: actuar como un usuario sin iniciar sesión o actuar como administrador siendo usuario estándar
- Acciones:
  - Restringir el acceso a todo lo que no sean recursos públicos
  - Implementar mecanismos de control de acceso de acuerdo al perfil del usuario (usuarios y privilegios) y realizar pruebas del correcto funcionamiento de esta implementación

A02:2021 Fallas criptográficas

- Fallas relacionadas con la criptografía o su ausencia, conduciendo a la exposición de datos confidenciales

- Incluye elementos como:
  - Transmisión de texto en claro, ausencia de directivas y encabezados de seguridad
  - Uso de SSL o TLS anterior a 1.3
  - Uso de funciones hash en desuso, como MD5 o SHA1

A02:2021 Fallas criptográficas

- Consecuencias:
  - Exposición/robo de contraseñas, tarjetas de crédito, registros de salud, información personal, secretos de la organización…
  - Violación a las leyes vigentes
- Acciones:
  - Implementar algoritmos, protocolos y claves estándar sólidos y actualizados; utilizar una gestión de claves adecuada
  - Cifrar todos los datos en tránsito con protocolos seguros como TLS
  - Deshabilitar el almacenamiento en caché para las respuestas que contienen datos confidenciales
  - Aplicar los controles de seguridad requeridos según la clasificación de datos

A03:2021 Inyección

- La aplicación no valida, filtra ni “sanitiza” los datos proporcionados por el usuario

- Incluye elementos como:
  - Consultas dinámicas o no parametrizadas sin escape que se utilizan directamente por la aplicación
  - No sólo es SQL, también: llamadas a sistema, Java Script, LDAP, XML, entre otros

A03:2021 Inyección

- Consecuencias:
  - Pérdida y/o corrupción de datos
  - Pérdida de acceso a recursos: base de datos, aplicación, sistema operativo

Acciones:

- Implementar código seguro: validación de entradas, incluso de otros sistemas
- Uso de herramientas para realizar la búsqueda de puntos de inyección
- Uso de módulos, complementos, bibliotecas y otros elementos actualizados y verificados

A04:2021 Diseño inseguro

- Riesgos relacionados con los defectos de diseño y arquitectura, dejando de lado el modelado de amenazas, patrones de diseño seguro y arquitecturas de referencia

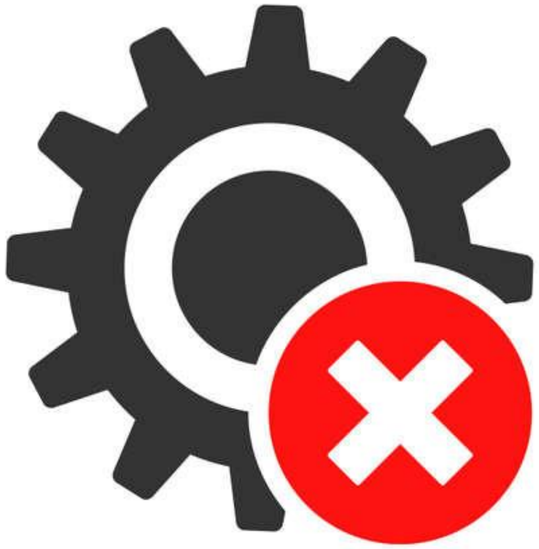
- Incluye elementos como:
  - Fallos de diseño: ausencia de controles de seguridad para defenderse de ataques específicos
  - No considera que el código se diseñe y pruebe de manera sólida para evitar métodos de ataque conocidos

A04:2021 Diseño inseguro

- Consecuencias:
  - Problemas con el flujo de datos, control de acceso, controles de seguridad.
  - Exposición de datos de configuración y/o personales, gestión inadecuada de privilegios, fallo en el cifrado, almacenamiento inadecuado (texto en claro, disponible para todos/nadie, etc.)
- Acciones:
  - Incluir la seguridad en el ciclo de vida de las aplicaciones web
  - Emplear componentes que han sido revisados y actualizados

A05:2021 Configuración de seguridad incorrecta

- Ausencia o error en el proceso de configuración de seguridad de aplicaciones concertado y repetible.



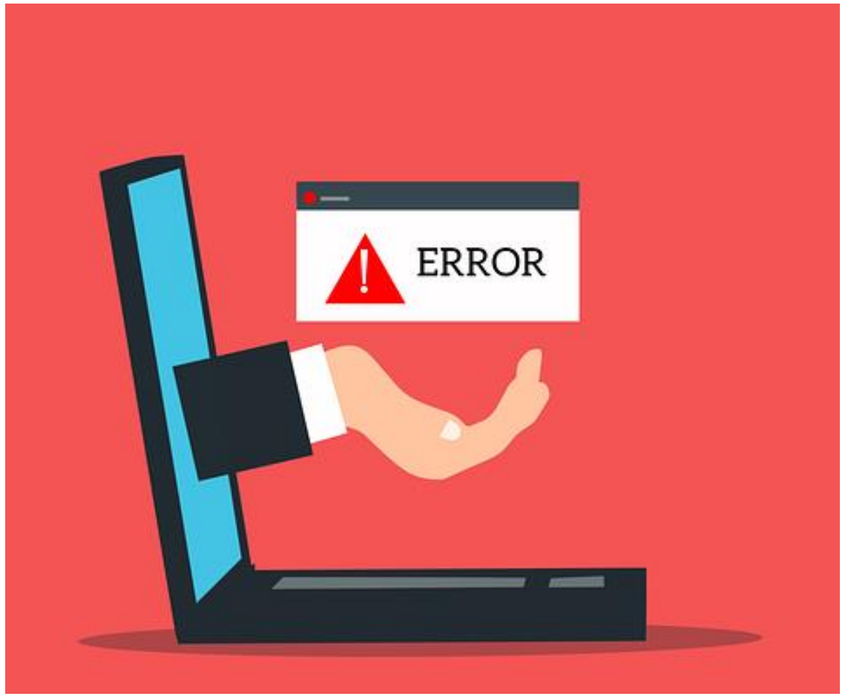
- Incluye elementos como:
  - Uso de funciones innecesarias, uso de cuentas y contraseñas predeterminadas
  - Fallo inseguro de las aplicaciones
  - Ausencia de encabezados o directivas de seguridad
  - Software desactualizado y/o vulnerable

A05:2021 Configuración de seguridad incorrecta

- Consecuencias:
  - Acceso a secciones restringidas del sitio
  - Exposición de información: configuraciones, documentación, instaladores, datos sensibles…
- Acciones:
  - Asegurar el entorno: desarrollo, pruebas, producción
  - Revisar y actualizar las configuraciones y accesos

Elementos adicionales

- Uso de componentes vulnerables y desactualizados
- Fallas de identificación y autenticación
- Falla en el software y en la integridad de los datos



Elementos adicionales

- Fallas en el registro y monitoreo
- Falsificación de solicitud del lado del servidor
- 0-day

Seguridad por capas

- Defensa en profundidad:
  - Las medidas que ayudan a proteger los datos, usuarios, servidores y servicios pueden aplicarse en distintos niveles


Datos
Aplicación
Host
Red interna
Perímetro
Seguridad física
Directivas, procedimientos y concienciación

Recomendaciones generales

- Conexiones sólo a servidores y usuarios autorizados:
  - Desactivar todas las conexiones que no se estén empleando.
  - Utilizar un mecanismo de autenticación que soliciten contraseña a los usuarios.
- Establecer roles y privilegios de acceso: BD, Aplicación, Servidor, Red…
- Implementar SSL para cifrar las conexiones
- Implementación de captchas y tokens anti-CSRF

- Generación y prueba de respaldos de forma periódica.
- Control de versiones sobre fuente del sitio.
- Uso de herramientas para la detección de intrusos (IDS, IPS).
- Protección adicional: fail2ban, WAF.

- Uso de alguna herramienta de monitoreo del servidor: logcheck, logwatch.

- Suscripción a las listas de seguridad de los servicios empleados.

- Realización de pruebas de seguridad de manera periódica: análisis dinámico y estático

- Documentarse sobre la legislación vigente en materia de seguridad

- Generación de una política y lineamientos de seguridad física y lógica que respalden las acciones a nivel organizacional y técnico que se lleven a cabo.

- Mantenerse actualizado en temas de seguridad: ser proactivos en las medidas que se pueden tomar, capacitarse y buscar la mejora constante.

Algunos recursos adicionales

- Portal Seguridad:

www.seguridad.unam.mx -> Divulgación

- CERT MX:

www.gob.mx/gncertmx

- Qualys SSL:

www.ssllabs.com/ssltest

DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Gracias por su atención

Ing. Angie Aguilar Domínguez
Coordinación de Seguridad de la Información
DGTIC UNAM

angie.aguilar@cert.unam.mx

2022

Visibilidad Web UNAM