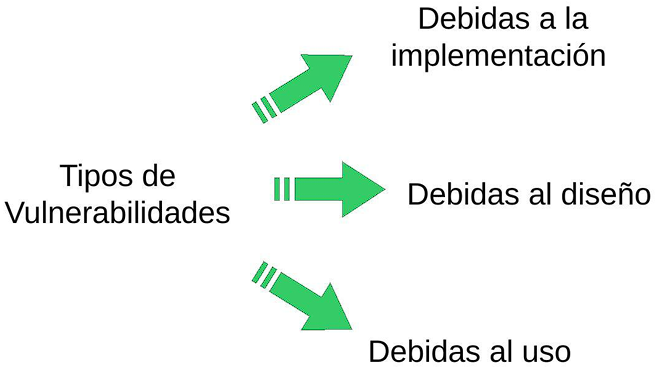
Unidad 2 – ULTRA RESUMEN

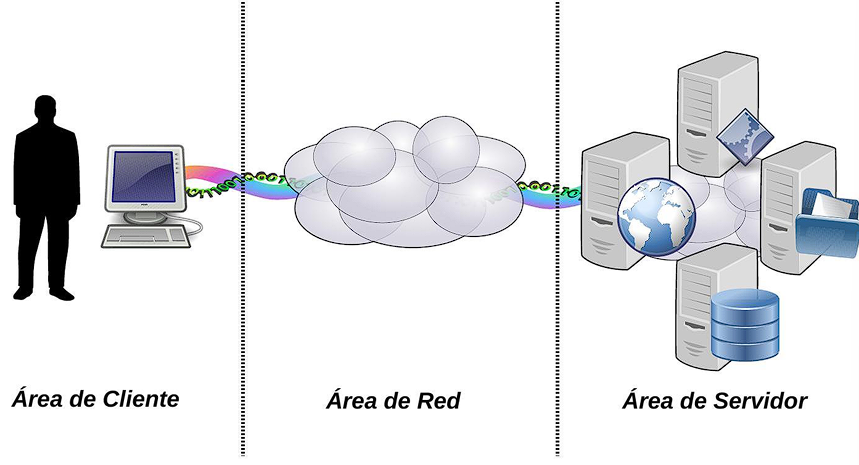
**DAÑO;** Prejuicio que se produce cuando un sistema informático falla. Dicho prejuicio debe ser cuantificable.

**RIESGO;** Producto entre la magnitud de un daño, y a la probabilidad de que este tenga lugar.

**AMENAZA;** Situación de daño cuyo riesgo de producirse es significativo

**VULNERABILIDAD**; Deficiencia en un sistema susceptible de producir un fallo en el mismo

**EXPLOIT;** Cualquier técnica que permita aprovechar una vulnerabilidad de un sistema para producir un daño en el mismo.



**LA NUBE**

*Ventajas*

* Facilidad de acceso a la información desde diferentes ubicaciones y dispositivos
* Infraestructura flexible y escalable basada en servicios
* Reducción de costos por infraestructura y servicios
* Centralización de administración y gestión de datos

*Desventajas*

* Dependencia en la infraestructura y servicios externos
* Dependencia en servicios de comunicación externos para acceder a los sistemas y datos propios
* Pérdida del control de la seguridad de la información.

**Ataques a aplicación conocidas**

* *Common Vulnerabilities and Exposures* o *CVE* es un código asignado a una vulnerabilidad que le permite ser identificada de forma univoca. <https://cve.mitre.org/>
* *Common Weakness Enumeration* o *CWE* es una lista de tipos de debilidades de software y hardware, las mismas se encuentran clasificadas y con identificadores del tipo CWE – numero.

<https://cwe.mitre.org/>

* *NVD, National Vulnerability Database*, del *NIST* es el repositorio del gobierno de EEUU para la gestión de datos de vulnerabilidades basados en los estándares.

<http://nvd.nist.gov/home.cfm>

* *CVSS, Common Vulnerability Scoring System*, es un conjunto de estándares abiertos para asignar un valor o puntaje de severidad a una vulnerabilidad. Este puntaje va desde 0.0 a 10.0, siendo este último el de mayor severidad.

**Prevencion de vulnerabilidades**

* Listas bugtraq
* Sistrmas automáticos de análisis
  + DATS; scanners de vulnerabilidades
  + SAST; auditoria automática de código
  + IAST; detectan vulnerabilidades en tiempo real durante la ejecución de una aplicación.
  + Redes trampa

**CERT; Computer Emergency Response Team**

**CSIRT; Centro de respuesta a incidentes de seguridad informática**

Son equipos reconocidos por la dirección de su organización como responsables de gestionar indicentes de seguridad informática que le competen según su alcance y comunidad.

Interactúan entre si a fin de facilitar información oportuna para actuar frente a diferentes tipos de incidentes, determinar su impacto, alcance y naturaleza.

Funciones;

* Ayudar al publico objetivo a atenuar y prevenir incidentes graves de seguridad
* Ayudar a proteger informaciones valiosas
* Coordinar de forma centralizada la seguridad de la información
* Guardar evidencias, por si hubiera que recurrir a pleitos.
* Apoyar y prestar asistencia a usuarios para recuperarse de las consecuencias de los incidentes de seguridad
* Dirigir de forma centralizada la respuesta a los incidentes de seguridad.

**DOS – DENEGACION DE SERVICIO**

Ataque a un sistema que causa que un servicio sea inaccesible a los usuarios. Provoca la perdida de la conectividad de la red por el consumo del ancho de banda de la red de la victima o sobrecarga de los recursos computacionales del sistema de la víctima.

*Tipos:*

Volume-based DDoS attacks: El atacante inunda a la víctima con un gran volumen de paquetes o conexiones de red, sobrecargando el equipamiento de la red servidores o ancho de banda.

Application DDoS attacks: El atacante opera a nivel de aplicación usualmente por HTTP intentando saturar el servidor y/o un servicio que este presta.

Low-rate DOS (LDoS) attacks: El atacante utiliza una vulnerabilidad en el diseño o implementación de la aplicación.

**FLOODING**

La técnica de Flooding o Inundación busca generar solicitudes maliciosas a un servicio con la finalidad de hacer que el mismo se sature o entre en un modo de espera, de esta forma anula o limita su funcionamiento.

**BOTNET**

Conjunto de terminales que ejecutan software que permite su control total o parcial desde ubicaciones remotas

**SNIFFERS**

Programa de captura de las tramas de red, se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

Para redes Ethernet (LAN); Ethereal, WinPcap, Ettercap, RCPDump, WinDump, WinSniffer, Hunt, Darkstat, Traffic-vis.

Redes inalámbricas (wireless); Kismet, Network, Stumbler.

**Atacando a navegadores;**

*Tampering o Data Diddling:*

Se refiere a la modificación no autorizada de la información. Por ejemplo, múltiples sitios web han sido afectados al detectar cambios en el contenido de sus páginas.

*Ataques Mediante JavaScript:*

JavaScript es un lenguaje de programación usado por los diseñadores de sitios web. Este tipo de programas son utilizados para explotar fallas de seguridad de navegadores web y servidores de correo.

Ataques drive-by download

Infectan de forma masiva a los usuarios, simplemente ingresando a un sitio web determinado. Mediante esta técnica, los desarrolladores de malware

*Hijackers:*

Son programas que alteran el funcionamiento o configuración del cliente para que el atacante pueda "secuestrar" información de interés Ejemplo, Page hijacking, Session hijacking, Browser hijacking...

*Rootkits:*

Son programas que permiten que una aplicación maliciosa permanesca oculta en el sistema operativo o que la misma no pueda ser eliminada normalmente. Ejemplo, procesos fantasmas en paralelo.

*Backdoors:*

Son programas que habilitan un acceso alternativo al sistema permitiendo evitar el método de autenticación principal. Normalmente se instalan en los sistemas comprometidos para facilitar su posterior uso (local o remoto) por parte del atacante.

*Stealers:*

Son programas que acceden a la información almacenada en el equipo para facilitársela al atacante. Su principal objetivo son contraseñas almacenadas o recordadas en navegadores y clientes de email o mensajería

*Keyloggers:*

Son programas o dispositivos físicos que registran la actividad de los dispositivos de entrada, comúnmente el teclado.

*Ransomware:*

Son programas que retienen el control del equipo o cifran información almacenada en el mismo para que no pueda ser accedida, en muchos casos solicitan un pago para que sean desactivados. Algunos ejemplos son "Virus Ukash", "WannaCry", "Petya/NotPetya", "Cryptolocker" y "Cryptowall".

**ANEXO SAST -> PMD**

**OWASP – RIESGO DE SEGURIDAD EN APLICACIONES**

Organización que facilita el desarrollo de proyectos de seguridad.

*Proveedores de datos;*

* AppSec Labs, Cobalt.io, Constrast Security, GitLab, etc.

*Principales fuentes de datos;*

* Herramienta asisitifa por humanos
* Humano asisitio por herramientas
* Herramientas en bruto

La tasa de incidencia se refiere al porcentaje de la población de aplicaciones que tiene al menos una instancia de un tipo de vulnerabilidad. No importa si fue algo puntual o sistémico; sino que se considera cuántas aplicaciones tenían al menos una instancia.

Se analizaron las ocho categorías con las tasas de incidencia más altas, luego se evaluaron los resultados de la encuesta a la comunidad del Top 10 para ver cuáles ya se encuentran presentes en los datos. Las dos más votadas que no están presentes fueron seleccionadas para los otros dos puestos del Top 10. Una vez seleccionadas las diez, se determinan los factores generalizados de explotabilidad e impacto, y por último se procede a ordenarlas en función del riesgo.

*Factores de datos;*

* CWEs mapeadas: El número de CWEs asignadas a una categoría.
* Tasa de incidencia: Es el porcentaje de aplicaciones vulnerables a esa CWE de la población analizada por esa organización para ese año.
* Cobertura (de pruebas): El porcentaje de aplicaciones que han sido testadas por todas las organizaciones para una determinada CWE.

Explotabilidad ponderada: La sub-puntuación de Explotabilidad de las puntuaciones CVSSv2 y CVSSv3 asignadas a las CVEs mapeadas a las CWEs, normalizados y colocados en una escala de 10 puntos.

Impacto ponderado: La sub-puntuación de Impacto de las puntuaciones CVSSv2 y CVSSv3 asignadas a las CVEs mapeadas a las CWEs, normalizados y colocados en una escala de 10 puntos.

Total de ocurrencias: Número total de aplicaciones en las que se han encontrado las CWEs asignados a una categoría.

Total de CVEs: Número total de CVEs en la base de datos del NVD que fueron asignadas a las CWEs asignados a una categoría.

**TOP 10 WEB APPLICATION SECURITY RISKS 2021**

1. AOI - Pérdida de Control de Acceso

El atacante simplemente navega forzosamente a la URL objetivo. Considere las siguientes URLs las cuales se supone que requieren autenticación. Para acceder a la página "admin\_getapplnfo" se necesitan permisos de administrador.

http://ejemplo.com/app/getapplnfo <http://ejemplo.com/app/admin_getapplnfo>

Si un atacante no autenticado puede acceder a cualquiera de estas páginas entonces se ha permitido acceso no autorizado. Si un usuario autorizado, no administrador, puede acceder a la página "admin\_getapplnfo", esto es un fallo, y puede llevar al atacante a otras páginas de administración que no están debidamente protegidas.

Este tipo de vulnerabilidades se encuentran con frecuencia cuando links y botones simplemente se ocultan a usuario no autorizados, pero la aplicación no protege adecuadamente las páginas de destino.

La aplicación utiliza datos no verificados en una llamada SQL que accede a información sobre la cuenta:

*string query = "SELECT \* FROM accts WHERE account = Q"; PreparedStatement pstmt = connection.prepareStatement(query , ... ); pstmt.setString( 1, request.getparameter("acct")); ResultSet results = pstmt.executeQuery( );*

El atacante simplemente modificaría el parámetro "acct" en su navegador para enviar cualquier número de cuenta que quiera. Si esta acción no se verifica, el atacante podría acceder a cualquier cuenta de usuario, en vez de a su cuenta de cliente correspondiente.

*Medidas de prevención:*

' Utilizar referencias indirectas por usuario o sesión

' Comprobar el nivel de acceso al objeto

Control de acceso único y reutilizado en toda la aplicación. Minimizar el control de acceso HTTP (CORS).

Deshabilitar el listado de directorios del servidor web y asegurar que los metadatos de archivos

Limite la tasa de acceso a APIs y al control de acceso

1. A02 - Fallas Criptográficas
2. A03 – Inyección
3. A04 - Diseño Inseguro
4. A05 - Configuración de Seguridad Incorrecta
5. A06 - Componentes Vulnerables y Desactualizados
6. A07 - Fallas de Identificación y Autenticación
7. A08 - Fallas en el Software y en la Integridad de los Datos
8. A09 - Fallas en el Registro y Monitoreo
9. AIO - Falsificación de Solicitudes del Lado del Servidor