RESUMEN PRIMER PARCIAL SEGURIDAD Y CALIDAD EN APLICACIONES WEB

Unidad N°1: Introducción a la Seguridad

Información

Es un grupo de datos ya procesados y ordenados, que sirven para construir un mensaje que cambia el estado de conocimiento del sujeto o sistema que lo recibe.

Características de la información

- Crítica: Es indispensable para la operación de la organización
- Valiosa: Es un activo apreciado por la organización y sus operaciones.
- Sensitiva: Debe de ser conocida por las personas autorizadas

Seguridad

Desde el punto de vista psicosocial se puede considerar como un estado mental que produce en los individuos un particular sentimiento de que se está fuera o alejado de todo peligro ante cualquier circunstancia.

- **Seguridad de la Información**
  Es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.
  - **Política de seguridad**
    Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.
  - **Plan director de seguridad**
    Proyecto consistente en la definición y priorización de un conjunto de medidas en materia de seguridad de la información, con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.
  - **Análisis de riesgos**
    Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

La seguridad de la información se articula sobre tres dimensiones, que son los pilares sobre los que aplicar las medidas de protección de nuestra información:

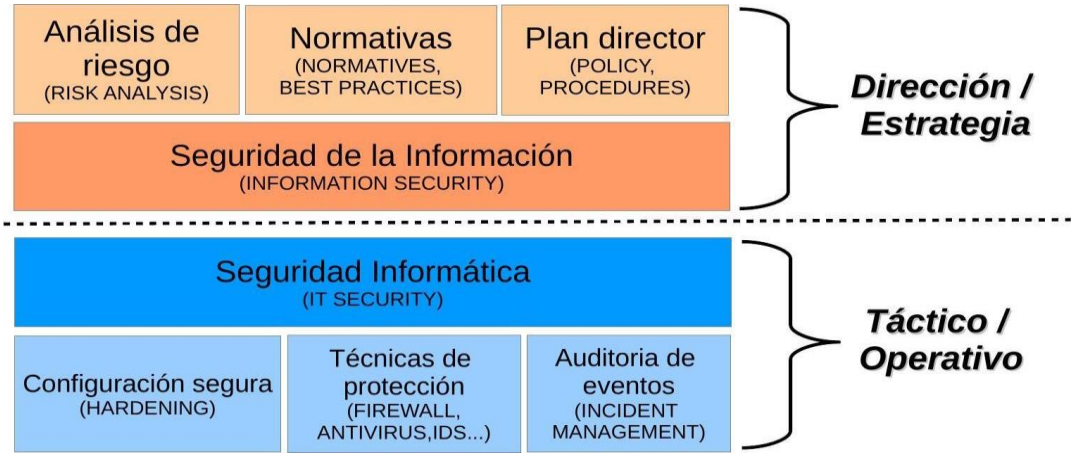
La **disponibilidad** de la información hace referencia a que la información esté accesible cuando la necesitemos.

La **integridad** de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella.

La **confidencialidad** implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.

La evaluación de los activos de información de la organización en relación a estas tres dimensiones de la seguridad determina la dirección a seguir en la implantación y selección de medidas, también denominadas controles o salvaguardas. También debemos tener en cuenta que la adopción de un determinado control para mejorar la seguridad en una dimensión puede afectar de forma negativa o positiva a otra de las dimensiones, por ello, es esencial conocer cuál de estas dimensiones es más importante proteger en cada sistema de información.

- **Seguridad Informática**
  Se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que — articulados con prácticas de gobierno de tecnología de información — establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.
- **Seguridad aplicada**



Incidentes de seguridad

Son violaciones de la seguridad que ocasionan la destrucción, acceso no autorizado, pérdida o alteración (accidental o deliberada) de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos.

Origen de los incidentes:

- **Accidente**
- **Interno** (miembros de la organización)
- **Ciberataque**
  Intento deliberado de obtener acceso a un sistema informático sin autorización en base al uso de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.
- **Intrusión**
  Acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivo sin autorización con el objetivo de realizar actividades ilegítimas.

Términos relevantes

- **Riesgo:** Definiremos el riesgo como el producto entre la magnitud de un daño, y la probabilidad de que este tenga lugar.
- **No repudio:** Que el usuario asuma todas las responsabilidades derivadas de la información que haya podido enviar. Es decir que no pueda negar su autoría sobre el mismo.
- **Amenazas:** Entendemos por amenaza aquella situación de daño cuyo riesgo de producirse es significativo.
- **Vulnerabilidades:** Una vulnerabilidad es una deficiencia en un sistema susceptible de producir un fallo en el mismo.
- **Anonimato:** No poder identificar a quien realiza la acción.

Las causas de inseguridad

- Un **estado de inseguridad activo**; es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, activar servicios de red que el usuario no necesita)
- Un **estado de inseguridad pasivo**; es decir, la falta de conocimiento de las medidas de seguridad disponibles (por ejemplo, cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan)

Requisitos funcionales para la seguridad

- **Auditoría de Seguridad**, registro de actividades.
- **Soporte de cifrado**, uso de criptografía para la protección de datos.
- **Gestión de seguridad**, gestión de perfiles de usuario y niveles de acceso vinculados a los mismos.
- **Privacidad**, soporte del anonimato de los usuarios.
- **Autodefensa**, controles para fallar de manera contenida o prevista.
- **Control de acceso**, manejo de la cantidad y tiempo de las sesiones, concurrencia e información sobre sesiones previas.
- **Rutas o canales fiables**, mecanismos que permitan confiar en los recursos accedidos, como los certificados.

Referencia: Función de Hash

Se define como una función o método no reversible para generar un valor que represente de manera casi unívoca a un dato.

Información de entrada de tamaño variable / función hash / Información de salida de tamaño fijo y reducido

Seguridad Lógica

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo

- Modalidad de Acceso
    - Lectura
    - Escritura
    - Ejecución
    - Borrado
- Control de Acceso Interno
    - Palabras Claves (Passwords)
    - Cifrado
    - Listas de Control de Accesos
    - Límites sobre la Interfaz de Usuario
    - Etiquetas de Seguridad
- Control de Acceso Externo
    - Dispositivos de Control de Puertos
    - Firewalls o Puertas de Seguridad
    - Acceso de Personal Contratado o Consultores
    - Accesos Públicos

Niveles de Seguridad (Orange Book - 1985)

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo.

- **Nivel D: División Simple**
  Este nivel contiene una sola división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.
- **Nivel C1: Protección Discrecional**
  Se requiere identificación de usuarios que permite el acceso a distinta información.
- **Nivel C2: Protección de Acceso Controlado**
  Este subnivel fue diseñado para solucionar las debilidades del C1. Se debe llevar una auditoria de accesos e intentos de accesos fallidos a objetos.
- **Nivel B1: Seguridad Etiquetada**
  Soporta seguridad multinivel como la secreta y ultrasecreta. A cada objeto del sistema se le asigna una etiqueta, con un nivel de seguridad jerárquico y con unas categorías.
- **Nivel B2: Protección Estructurada**
  Requiere que se etiquete a cada objeto de nivel superior por ser padre de un objeto inferior.
- **Nivel B3: Dominios de Seguridad**
  Refuerza a los dominios con la instalación de hardware.
- **Nivel A: Protección Verificada**
  Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales para asegurar todos los procesos que realiza un usuario sobre el sistema.

Estos son otros elementos comunes en el manejo de la seguridad lógica de sistemas:

Firewalls

Es un dispositivo de red que crea una separación entre redes públicas (no confiables) y redes privadas (confiables).

Características básicas:

- No protegen de ataques internos
- No protegen de accesos no autorizados
- No protegen de la totalidad de ataques dañinos
- Filtran el tráfico dependiendo de reglas predefinidas

Funcionalidades accesorias:

- Alta disponibilidad (AD)
- Balanceo de carga (BCFW)
- Filtrado de contenidos / Anti-Spam
- Escaneo de virus

Honeypots

Es un sistema informático que se “sacrifica” para atraer ciberataques, como un señuelo. Simula ser un objetivo para los hackers y utiliza sus intentos de intrusión para obtener información sobre los cibercriminales y la forma en que operan o para distraerlos de otros objetivos.

Honeynets

Son un tipo especial de Honeypots de alta interacción que actúan sobre una red entera, diseñada para ser atacada y recobrar así mucha más información sobre posibles atacantes. Se usan equipos reales con sistemas operativos reales y corriendo aplicaciones reales.

IDS – Sistema de Detección de intrusiones

Analiza el tráfico de red para tratar de detectar patrones sospechosos que indiquen ataques o intenciones de ataques contra algún recurso. Una vez identificados, puede tomar ciertas medidas contra ese tipo de tráfico, como generar alertas o inclusive bloquear o descartar el tráfico que viene de ese origen.

Modelo de funcionamiento general

1. Recolección de datos
2. Analisis
3. Respuesta

Clasificaciones

- HIDS (Sistema de Detección de Intrusiones de Maquina)
  Utilizan los registros de auditoría, registros del sistema, registros de aplicaciones, sistema de archivos.
- NIDS (Sistema de Detección de Intrusiones de Red) y NNIDS (Sistema de Detección de Intrusiones de Nodo de Red) Utilizan paquetes de red.

IPS - Sistemas de Prevención de Intrusiones

Es el resultado de la combinación de IDS + Firewall en respuesta activa, estos dispositivos identifican el curso de un ataque y lo bloquean antes de que suceda-

WAF - Web Application Firewall

Dispositivo físico o lógico que analiza el tráfico web, los datos recibidos por parte del usuario y protege de diferentes ataques web como: SQL injection, Cross Site Scripting, etc. Este dispositivo trata de proteger de los ataques dirigidos al servidor web que los IDS/IPS no nos pueden defender.

Proceso de aprendizaje implementado en WAF

Se denomina Learning mode al modo de operación donde la herramienta registra la actividad normal de la aplicación para que posteriormente pueda ser utilizada a fin de generar reglas. El WAF detectará una anomalía y tomará las medidas necesarias, que suelen ser, la denegación de la petición o el redireccionamiento a una página previamente configurada.

NGFW – Next Generation Firewalls

Se basa en la inspección profunda de paquetes, sumada a las tecnologías para evitar intrusiones y de firewalls tradicionales

DMZ – Zona Desmilitarizada

Es un área de configuración de firewall con reglas específicas orientada a manejar equipos que deben tener mayor exposición en la infraestructura, como por ejemplo los servidores web, de correo y otros.

Referencia: BYOD (Bring your own device)

Es una política empresarial para el uso de dispositivos tecnológicos que se caracteriza por permitir a los empleados el uso de sus propios dispositivos personales (portátiles, smartphones, tablets) para el trabajo, así como también el acceso desde los mismos a las redes corporativas, aceptando su uso compartido para las tareas profesionales como para las personales.

Referencia: VPN

Una estructura de red que con soporte lógico que permite el tráfico de información privada sobre una infraestructura de red pública mediante el uso de criptografía.

Protocolos

- IPSec
- SSL / TLS
- PPTP, L2TP

Seguridad Física

Consiste en mecanismos destinados a proteger físicamente cualquier recurso del sistema de amenazas producidas tanto por el hombre como por la naturaleza; en general serán prevención y detección.

- Tipos de Desastres
    - Desastres naturales, incendios accidentales tormentas e inundaciones
    - Disturbios, sabotajes internos y externos deliberados.
    - Amenazas ocasionadas por el hombre.
- Acciones Hostiles
    - Robo
    - Fraude
    - Sabotaje
- Control de Accesos
    - Utilización de Guardias
    - Utilización de Detectores de Metales
    - Utilización de Sistemas Biométricos
    - Verificación Automática de Firmas (VAF)
    - Seguridad con Animales
    - Protección Electrónica

Sistema biométricos

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a una persona por lo que es.

- Emisión de calor
- Huella digital
- Verificación de voz
- Verificación de patrones oculares

Unidad N°2: Amenazas a la seguridad

Términos relevantes

- **Daño**
  Definiremos como daño el perjuicio que se produce cuando un sistema informático falla. Dicho perjuicio debe de ser cuantificable.
- **Exploit**
  Llamaremos exploit a cualquier técnica que permita aprovechar una vulnerabilidad de un sistema para producir un daño en el mismo.

Tipos de vulnerabilidades

- Debidas a la implementación
- Debidas al diseño
- Debidas al uso

Áreas de vulnerabilidades en entornos Web

- Área de cliente
- Área de red
- Área de servidor

Ataques a aplicaciones conocidas

CVE - Common Vulnerabilities and Exposures (Vulnerabilidades y amenaza común) es un código asignado a una vulnerabilidad que le permite ser identificada de forma univoca. El código identificador es del modo CVE - año - número.

CWE - Common Weakness Enumeration (Enumeración de debilidades comunes) es un código asignado a una debilidad que le permite ser identificada de forma univoca. Es una lista de tipos de debilidades de software y hardware, las mismas se encuentran clasificadas y con identificadores del tipo CWE número.

NVD - National Vulnerability Database del NIST es el repositorio del gobierno de Estados Unidos para la gestión de datos de vulnerabilidades basados en los estándares.

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.

Prevención de vulnerabilidades

- Listas bugtraq, es una lista de notificación sobre vulnerabilidades encontradas en software y hardware.
- Sistemas automáticos de análisis.
    - DAST (Dynamic Application Security Testing). Scanners de vulnerabilidades.
    - SAST (Static Application Security Testing). Auditoria automática de código.
    - IAST (Interactive Application Security Testing). Detectan vulnerabilidades tiempo real durante la ejecución de una aplicación.
    - Redes Trampa.

CERT / CSIRT

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 los incidentes de seguridad informática que le competen según su alcance y comunidad.

Funciones

- Ayudar al público objetivo a atenuar y prevenir incidentes 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 - Promover confianza, que alguien controla la situación

Denegación de servicio (DOS)

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

- **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.

Referencia: 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.

Referencia: BotNet

Es un conjunto de terminales que ejecutan software que permite su control total o parcial desde ubicaciones remotas. Las terminales se denominan bots o zombies.

Referencia: Sniffer

Un sniffer es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

Atacando a los navegadores (clientes)

- **Tampering o Data Diddling**: Se refiere a la modificación no autorizada de la información. Sitios web han sido afectados al detectar cambios en su contenido.
- **Ataques Mediante JavaScript**: 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 (programas maliciosos) propagan sus creaciones e inyectan código dañino entre su código original.

Otras tecnologías generadoras de riesgos

- Javascript
- ActiveX
- Shockwave
- Java Applets
- Microsoft Silverlight
- Portable Document Format (PDF) Flash
- Plugins de navegador

Otros ataques a clientes

- **Hijackers**: Son programas que alteran el funcionamiento o configuración del cliente para que el atacante pueda "secuestrar" información de interés.
- **Rootkits**: Son programas que permiten que una aplicación maliciosa permanezca oculta en el sistema operativo o que la misma no pueda ser eliminada normalmente.
- **Backdoors**: Son programas que habilitan un acceso alternativo al sistema permitiendo evitar el método de autenticación principal.
- **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.

OWASP Riesgos de seguridad en aplicaciones

Top Ten Web Application Security Risks 2021

- **AOI - Pérdida de Control de Acceso**
  Muchas aplicaciones Web verifican el nivel de acceso a las funciones justo antes de hacer estas funcionalidades y/o datos visibles en la interfaz gráfica. Sin embargo, las aplicaciones necesitan realizar el mismo control de acceso del lado del servidor al momento que cada función y/o dato es accedido. Si las solicitudes no son verificadas, los atacantes serán capaces de forzar peticiones con la finalidad de acceder a la funcionalidad sin la autorización apropiada.
- **A02 - Fallas Criptográficas**
  La información sensible demanda protección adicional como la encriptación en su almacenamiento y tránsito, al igual que precauciones especiales cuando es intercambiada con el cliente o navegador.
- **A03 – Inyección**
  Las fallas de inyección, tales como SQL, NoSQL, Object-Relational Mapping (ORM), OS, y LDAP, X-PATH ocurren cuando datos no confiables son enviados a

un intérprete como parte de un comando o consulta. Los datos hostiles del atacante pueden engañar al intérprete en ejecutar comandos no intencionados o acceder datos no autorizados.

Medidas de prevención

- Uso de APIs con manejo parametrizado de intérpretes o una herramienta de mapeo relacional de objetos (ORMs)
- Codificación de los caracteres especiales en función del interprete a utilizar
- Validación de entradas positiva o de "lista blanca"
- Utilice LIMIT y otros controles SQL dentro de las consultas para evitar la divulgación masiva de registros

- **A04 - Diseño Inseguro**
  Se centra en los riesgos relacionados con el diseño y las fallas arquitectónicas, con un llamado a un mayor uso del modelado de amenazas, patrones de diseño seguros y arquitecturas de referencia.
- **A05 - Configuración de Seguridad Incorrecta**
  Una buena seguridad requiere tener definida e implementada una configuración segura para la aplicación, marcos de trabajo, servidor de aplicación, servidor web, base de datos, y plataforma. Todas estas configuraciones deben ser definidas, implementadas, y mantenidas ya que por lo general no son seguras por defecto. Esto incluye mantener todo el software actualizado, incluidas las librerías de código utilizadas por la aplicación.

Referencia: Entidad externa de XML (XXE)

Muchos procesadores XML antiguos o mal configurados evalúan referencias de entidades externas en documentos XML. Las entidades externas se pueden utilizarse para revelar archivos internos utilizando el gestor de archivos URI, compartir archivos SMB internos en servidores Windows no actualizados, escanear de puertos internos, ejecución remota de código y ataques de denegación de servicio, como lo es el ataque Billion Laughs.

- **A06 - Componentes Vulnerables y Desactualizados**
  Componentes, como librerías, frameworks, y otros módulos de software, son siempre ejecutados con privilegios completos.
  Las aplicaciones que utilizan componentes con vulnerabilidades conocidas deberían determinar las defensas de la aplicación para el caso y habilitar un rango de posibles ataques e impacto de los mismos.
- **A07 - Fallas de Identificación y Autenticación**
  Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son frecuentemente implementadas incorrectamente, permitiendo a los atacantes comprometer contraseñas, claves, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios
- **A08 - Fallas en el Software y en la Integridad de los Datos**

Los fallos de integridad del software y de los datos están relacionados con código e infraestructura no protegidos contra alteraciones (integridad). Incluiremos la dependencia en plugins, bibliotecas o módulos de fuentes, repositorios o redes de entrega de contenidos (CDN) no confiables. Así como también actualizaciones automáticas adulteradas o alteraciones de objetos o datos serializados.

Referencia: Deserialización insegura

Defectos de deserialización insegura ocurren cuando una aplicación recibe objetos serializados hostiles. Deserialización insegura conduce a la ejecución remota del código. Incluso si el defecto de deserialización no resultara en la ejecución remota del código, los objetos serializados pueden ser reproducidos, manipulados o borrados por el atacante, realizar ataques de inyecciones o elevar sus privilegios.

- **A09 - Fallas en el Registro y Monitoreo**
  El registro y monitoreo insuficiente, junto con la falta o integración inefectiva de respuesta de incidentes permiten a los atacantes persistir en el tiempo el ataque al sistema, pivotear a más sistemas y manipular, extraer o destruir datos. La mayoría de los estudios muestran que el tiempo de detección de una violación de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de procesos internos o monitoreo.
- **AIO - Falsificación de Solicitudes del Lado del Servidor (SSRF)**
  Las fallas de SSRF ocurren cuando una aplicación web está obteniendo un recurso remoto sin validar la URL proporcionada por el usuario. Permite que un atacante coaccione a la aplicación para que envíe una solicitud falsificada a un destino inesperado, incluso cuando está protegido por un firewall, VPN u otro tipo de lista de control de acceso a la red (ACL).

Controles Pro-activos 2018

- Cl: Definir Requisitos de Seguridad
- C2: Hacer Uso De Librerías y Marcos de Trabajo de Seguridad
- C3: Acceso Seguro a Bases de Datos
- C4: Encodear y Escapar Datos
- C5: Validar todas las Entradas de Datos
- C6: Implementar Identidad Digital
- C7: Implementar Controles de Acceso Adecuados
- C8: Proteger los Datos

Referencia: CSRF (Falsificación de Peticiones en Sitios Cruzados)

La aplicación permite que usuarios envíen peticiones de cambio de estado, que no incluyen nada secreto. El atacante podrá insertar su ataque dentro de una etiqueta de imagen en un sitio web, o iframe, que este bajo su control y al que la víctima se podrá dirigir.

Secuencia de comandos en sitios cruzados (XSS-Cross site scripting)

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 secuencias 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.

- **XSS Reflejado**: La aplicación o API utiliza datos suministrados por un usuario sin ser validados o codificados apropiadamente como parte del HTML de salida o cuando no existe un cabezal que establezca la política de seguridad de contenido (CSP). Típicamente el usuario deberá interactuar con un enlace, o alguna otra página controlada por el atacante, como un ataque del tipo pozo de agua, publicidad maliciosa, o similar.
- **XSS Almacenado**: La aplicación o API almacena datos proporcionados por el usuario sin validar ni sanear, la que posteriormente es entregada a otro usuario o un administrador. XSS Almacenado es usualmente considerado como de riesgo de nivel alto o crítico.
- **XSS Basados en DOM**: Frameworks en JavaScript, aplicaciones de página única o APIS que dinámicamente incluyen datos controlables por un atacante son vulnerables al DOM XSS. Idealmente, se debe evitar enviar datos controlables por el atacante a APIs no seguras.

Medidas de prevención

- Codificar los datos no confiables basados en el contexto HTML donde serán ubicados
- Validación de entrada positiva o de “lista blanca”
- Para formato enriquecido considere utilizar APIs de auto-sanitización
- Considerar el uso de políticas de seguridad de contenido CSP