Práctica 2

CWE - COMMON WEAKNESS ENUMERATION

José Ángel Dorado González

Seguridad Informática

ÍNDICE

1º)Accede y adquiere una visión general de este proyecto y su estructura. Valora la importancia y el peso internacional del proyecto buscando información sobre él, sus patrocinadores, las empresas implicadas, etc.

CWE es una comunidad cuyo objetivo es crear un catálogo de vulnerabilidades software, el cual se ha ensamblado en tres niveles diferentes. El nivel superior divide las debilidades conocidas en unas pocas clases generales grandes para el debate entre la gente de gestión empresarial, investigadores, etc. El nivel intermedio consta de varias docenas de grupos de definiciones categorizadas para su uso por expertos en seguridad, administradores de sistemas y desarrolladores de software. El nivel inferior es la lista completa, destinada a personas de todos los niveles.

Actualmente, CWE tiene una gran importancia internacionalmente debido a que sirve de referencia para encontrar y mitigar las diferentes debilidades software. Esto sirve sobre todo a las organizaciones de desarrollo de software, hardware y a los profesionales de seguridad.

Se encuentra respaldado por los principales proveedores de sistemas operativos, proveedores de herramientas de seguridad de la información comercial, academias, agencias gubernamentales e instituciones de investigación.

CWE es mantenido por MITRE Corporation y su uso es gratuito para cualquier organización o persona con fines de investigación, desarrollo o comerciales.

2º)Enumera los principales capítulos de este proyecto. Adquiere una visión general de cada uno de sus proyectos y elabora una breve descripción de cada uno (responde en cada caso con una frase breve o máximo 1-2 párrafos de máximo 30-40 palabras cada uno).

Los principales capítulos de CWE se dividen en las siguientes tres áreas de vulnerabilidad:

- Desarrollo de software
    - Los conceptos se agrupan por frecuencia de encuentro o uso en el desarrollo de código fuente.
- Diseño de hardware
    - Se agrupan las debilidades más comunes en el diseño de hardware.
- Conceptos de investigación
    - Sirve para facilitar la investigación de problemas comunes, donde los elementos se agrupan por sus comportamientos.

3º)Accede y analiza el proyecto CWE Top 25 Most Dangerous Software Errors. ¿Qué es Rank, Score e ID en esa lista?

El proyecto CWE Top 25 Most Dangerous Software Errors es una lista de las 25 debilidades software más peligrosas de 2022.

Rank indica la posición en la lista de la debilidad identificada según la puntuación que tenga. ID es el identificador de cada una de las debilidades encontradas, registradas en CWE. Score es la puntuación general de cada debilidad, calculada en función de la prevalencia y gravedad de cada una.

4º)Clasifica los CWE Top 25 Most Dangerous Software Errors en las categorías que consideres de utilidad.

La clasificación se realizará con las tres áreas principales de vulnerabilidad: desarrollo de software, diseño de hardware y conceptos de investigación.

	Desarrollo de software	Diseño de hardware	Conceptos de investigación
CWE-787	X		
CWE-79			X
CWE-89			X
CWE-20		X	
CWE-125	X		
CWE-78			X
CWE-416			X
CWE-22	X		
CWE-352			X
CWE-434	X		
CWE-476		X	
CWE-502	X		
CWE-190		X	
CWE-287	X		
CWE-798	X		

CWE-862	X		
CWE-77	X		
CWE-306			X
CWE-119		X	
CWE-276	X		
CWE-918			X
CWE-362		X	
CWE-400	X		
CWE-611		X	
CWE-94	X		

5º)Elige una de estas vulnerabilidades y descríbela en más profundidad. Describe su origen, software al que afecta, investiga sobre casos, empresas o aplicaciones que se han visto afectadas. E informa de las contramedidas o soluciones que pueden adoptarse.

La vulnerabilidad elegida es la CWE-918 que trata de la falsificación de solicitud del lado del servidor (SSRF). Estas ocurren cuando una aplicación web está obteniendo un recurso remoto sin validar la URL proporcionada por el usuario, permitiendo que un atacante coaccione a la aplicación para que envíe una solicitud falsificada a un destino inesperado.

Esta vulnerabilidad ha sido descubierta por Microsoft que afecta a Microsoft Exchange Server 2013, 2016 y 2019, identificada como de día cero, es decir, ha sido descubierta por los cibercriminales antes que por el proveedor del servicio. Actualmente no existe corrección para la vulnerabilidad, aunque Microsoft está trabajando en ella.

Algunas de las prevenciones que se pueden tomar son las siguientes:

- Desde la capa de red
    - Segmentar la funcionalidad de acceso a recursos remotos en redes separadas para reducir el impacto de SSRF.
    - Cumplir las políticas de firewall "denegar por defecto" o las reglas de control de acceso a la red para bloquear todo el tráfico de la intranet excepto el esencial.
- Desde la capa de aplicación
    - Deshabilitar las redirecciones HTTP
    - Validar todos los datos de entrada proporcionados por el cliente

6º)¿Qué es CWE Compatibility y cuáles son los requisitos necesarios para que un producto sea etiquetado como CWE Compatible?

CWE Compatibility permite que un producto o servicio sea revisado y registrado oficialmente como “CWE Compatible” y “CWE Effective”, esto ayuda a las organizaciones en su selección y evaluación de herramientas o servicios para evaluar el software adquirido, para conocer las debilidades y su posible impacto.

Los productos y servicios compatibles con CWE deben cumplir con los primeros 4 requisitos, mientras que los productos y servicios con vigencia de CWE deben cumplir con todos los requisitos. Estos requisitos son los siguientes:

- CWE Searchable
- CWE Output
- Mapping Accuracy
- CWE Documentation
- CWE Coverage
- CWE Test Results

7º)Busca cualquier otro informe o proyecto de interés en CWE y descríbelo brevemente (2-3 párrafos).

El informe de debilidad elegido es el CWE-1389 sobre el análisis incorrecto de números con diferentes raíces. Esta vulnerabilidad provoca que se analice la entrada numérica asumiendo valores de base 10, sin tener en cuenta las entradas que usan un número base diferente.

Los modos de introducción pueden ser: que la aplicación cuente con un servicio que admita diferentes base numéricas o que la validación de entrada utilizada pueda asumir bases decimales durante las comprobaciones condicionales, cuando no siempre es el caso.

Esta vulnerabilidad puede llegar a provocar que un atacante use una base numérica inesperada para acceder a recursos de aplicaciones privadas o, para eludir o manipular los mecanismos de control de acceso.

8º)¿Por qué son interesantes en IT Security estas experiencias y esfuerzos comunes a nivel internacional?.

Como se comentó con anterioridad, la importancia de CWE en el ámbito internacional de la seguridad informática es inmensa, debido a que sirve de gran ayuda a las organizaciones para lograr identificar y poder solucionar diferentes debilidades que hayan sido publicadas.

Aunque es cierto que los ciberdelincuentes también pueden tener acceso a la información de estas debilidades, es mejor hacerlo público para que las organizaciones puedan saber cómo frenar dichas amenazas.

Además, CWE es apoyado por importantes empresas del sector tecnológico provocado principalmente por la gran ayuda que ofrecen.

9º)¿Existen comunidades similares? Busca y describe brevemente al menos una de ellas con su URL y una breve descripción de cada una (texto 1-2 párrafos).

CAPEC (Common Attack Pattern Enumeration and Classification) es un catálogo de patrones de ataque que se encarga de recolectar información sobre ellos. Estos patrones no son más que las descripciones de los métodos comunes utilizados para la explotación de vulnerabilidades.
URL: https://capec.mitre.org/

CVE (Common Vulnerabilities and Exposures) es una lista de información sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, versiones de software afectadas, posible solución al fallo o cómo mitigar el daño y referencias a publicaciones o entradas de foros donde se ha hecho pública la vulnerabilidad.
URL: https://cve.mitre.org/

NVD (National Vulnerability Database) es un proyecto del gobierno de EE.UU, creado para ayudar a las personas y a las empresas a investigar la automatización de la gestión de vulnerabilidades, junto con otros objetivos de seguridad. Esta base de datos incluye información sobre diferentes tipos de amenazas a la seguridad y otros factores en la ciberseguridad.
URL: https://nvd.nist.gov/

10º)Opcional. Investiga y comenta brevemente los proyectos.

FIRST CVSS - Common Vulnerability Scoring System. ¿Para qué sirve su servicio CVSS Calculator?

Este proyecto gratuito y abierto se utiliza para calificar la gravedad y el riesgo de las vulnerabilidades de seguridad en los sistemas informáticos. CVSS Calculator sirve para calcular mediante unos parámetros el impacto de una vulnerabilidad, compuesto de tres grupos principales de métricas:

- Base
    - Engloba cualidades intrínsecas de una vulnerabilidad y que son independientes del tiempo y el entorno.

- Temporal
    - Características de la vulnerabilidad que cambian con el tiempo.
- Entorno.
    - Características de las vulnerabilidades que están relacionadas con el entorno del usuario.

MITRE ATT&CK

MITRE ATT&CK describe y clasifica los comportamientos adversarios con base en observaciones reales. Básicamente es una lista de comportamientos conocidos de atacantes, recopilados en tácticas y técnicas, y expresados en varias matrices, así como a través de STIX y TAXII.

MITRE tiene ATT&CK distribuido en algunas matrices diferentes: Enterprise, Mobile y PRE-ATT&CK. Cada una de estas matrices contiene diversas tácticas y técnicas asociadas con el contenido de la matriz.

La matriz Enterprise se compone de técnicas y tácticas que se aplican a los sistemas Windows, Linux o MacOS. Mobile contiene tácticas y técnicas que se aplican a los dispositivos móviles. PRE-ATT&CK contiene tácticas y técnicas relacionadas con lo que los atacantes hacen antes de intentar vulnerar una red o un sistema en particular.

safecode.org y su proyecto "Fundamental Practices for Secure Software Development 2nd Edition".

SAFECode revela que existen prácticas de seguridad correspondientes para cada actividad en el ciclo de vida del desarrollo de software que pueden mejorar la seguridad del software y son aplicables en diversos entornos. El examen de estas prácticas de proveedores refuerza la afirmación de que la seguridad del software debe abordarse a lo largo del ciclo de vida del desarrollo del software para que sea eficaz y no se trate como un evento único.

Estos métodos de seguridad se encuentran actualmente en práctica entre los miembros de SAFECode, un testimonio de su capacidad para integrarse y adaptarse a entornos de desarrollo del mundo real.

OWASP y su proyecto "Top 10"

Es un documento de los diez riesgos de seguridad más importantes en aplicaciones web según la Fundación OWASP. Esta lista se publica y actualiza cada tres o cuatros años.

El último documento lanzado fue en 2021, incluye los siguientes diez riesgos:
- Pérdida de control de acceso
- Fallas criptográficas
- Inyección
- Diseño inseguro
- Configuración de seguridad incorrecta
- Componentes vulnerables y desactualizados
- Fallas de identificación y autenticación

- Fallas en el software y en la integridad de los datos
- Fallas en el registro y monitoreo
- Falsificación de solicitudes del lado del servidor (SSRF)

BIBLIOGRAFÍA

https://www.ultimahora.es/noticias/tecnologia-videojuegos/2022/09/30/1801999/microsoft-identifica-dos-vulnerabilidades-dia-cero-primera-activa-segunda-estan-siendo-explotadas.html

https://owasp.org/www-project-top-ten/

https://safecode.org/publication/SAFECode_Dev_Practices0211.pdf

https://attack.mitre.org/

https://www.first.org/cvss/calculator/3.0

https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System