Seguridad de aplicaciones

Lorenzo Elguea

Tema 2

2. Tecnologías de Seguridad de aplicaciones

    2.1 Pruebas inteligentes de software (Fuzzing)

    2.2 Sistemas Criptográficos para aplicaciones

        2.2.1 Algoritmos de cifrado

        2.2.2 Sistemas de Firmas y autenticación

        2.2.3 Intercambio de llaves públicas y privadas

            2.2.4 Protocolos para Transacciones monetarias

    2.3 Pruebas de penetración a aplicaciones

    2.4 Análisis de Vulnerabilidades.

2.1 Pruebas inteligentes de software (Fuzzing)

La prueba de software es el **proceso de evaluación y verificación de un producto o aplicación de software para saber si hace lo que se supone que debe hacer**.

- Pruebas de aceptación: Verificar si todo el sistema funciona según lo previsto.
- Pruebas de integración: Se asegura de que los componentes o funciones del software operen juntos.
- Examen de la unidad: Valida que cada unidad de software funcione como se esperaba. Una unidad es el componente comprobable más pequeño de una aplicación.
- Pruebas funcionales: Verifica las funciones simulando escenarios comerciales, basados en requisitos funcionales. Las pruebas de caja negra son una forma común de verificar funciones.

2.1 Pruebas inteligentes de software (Fuzzing)

- Las pruebas de caja negra son una forma común de verificar funciones.
- Pruebas de rendimiento: Prueba el rendimiento del software en diferentes cargas de trabajo. Las pruebas de carga, por ejemplo, se utilizan para evaluar el rendimiento en condiciones de carga reales.
- Pruebas de regresión: Verifica si las nuevas funciones rompen o degradan la funcionalidad. Las pruebas de cordura se pueden utilizar para verificar menús, funciones y comandos a nivel de superficie, cuando no hay tiempo para una prueba de regresión completa.
- Pruebas de estrés: Prueba cuánta tensión puede soportar el sistema antes de que falle. Está considerada como un tipo de prueba no funcional.
- Pruebas de usabilidad: Valida qué tan bien un cliente puede usar un sistema o una aplicación web para completar una tarea.

2.1 Pruebas inteligentes de software (Fuzzing)

IA en la automatización de pruebas de software

El uso de la IA en el desarrollo de software aún está evolucionando, pero el nivel en el que se usa actualmente en las pruebas automatizadas de software es más bajo en comparación con áreas de trabajo más avanzadas, como los sistemas autónomos o el control asistido por voz, la traducción automática y la robótica.

La aplicación de IA en herramientas de prueba de software se centra en facilitar el ciclo de vida del desarrollo de software (SDLC). Mediante la aplicación del razonamiento, la resolución de problemas y, en algunos casos, el aprendizaje automático, la IA se puede utilizar para ayudar a automatizar y reducir la cantidad de tareas mundanas y tediosas en el desarrollo y las pruebas.

2.2 Sistemas Criptográficos para aplicaciones

Las herramientas Criptográficas se pueden usar en diferentes partes de las aplicaciones:

- Bases de Datos
- Algoritmos propietarios
- Sistemas de Comunicación
- Auditoría
- Registro y Seguimiento de transacciones

Herramientas Criptográficas: Base de Datos

Existen varias bases de datos, ellas implementan diferentes herramientas de seguridad.

Nos centraremos en la autenticación y autorización en una Base de Datos Open Source en Java llamada Derby

https://es.wikipedia.org/wiki/Apache_Derby

https://db.apache.org/derby/derby_downloads.html

Derby, permite implementar un mecanismo de autenticación instanciando UserAuthenticator

2.3 Pruebas de penetración a aplicaciones

Las principales pruebas de penetración es por métodos de “fuerza bruta”

Existen herramientas como:

John the Ripper password cracker: https://www.openwall.com/john/

esp8266_deauther: https://github.com/SpacehuhnTech/esp8266_deauther

Aircrack-ng: https://www.aircrack-ng.org/

y Bases de datos como:

https://github.com/hackingyseguridad/diccionarios

https://haveibeenpwned.com/

2.4 Análisis de Vulnerabilidades.

Existe una base de datos pública para registrar, identificar y clasificar cada vulnerabilidad. Dicho sistema se conoce como CVE (Common Vulnerabilities and Exposures) y es una lista donde se especifican las versiones y la criticidad de las vulnerabilidades.

Se puede consultar en:

https://cve.mitre.org/

https://www.cvedetails.com/

https://www.cve.org/

https://nvd.nist.gov/vuln

MITRE Corporation se encarga de supervisar los CVE con la financiación de la Agencia de Ciberseguridad y Seguridad de la Infraestructura, que forma parte del Departamento de Seguridad Nacional de Estados Unidos.

2.4 Análisis de Vulnerabilidades.

El formato es CVE es CVE-YYYY-#####

Ejemplo de CVEs famosos:

CVE-2021-44228

CVE-2021-40539

CVE-2017-11882

CVE-2021-26084

Hay muchas formas de evaluar la gravedad de un punto vulnerable. Una de ellas es el Sistema común de calificación de los puntos vulnerables (CVSS)

https://nvd.nist.gov/vuln-metrics/

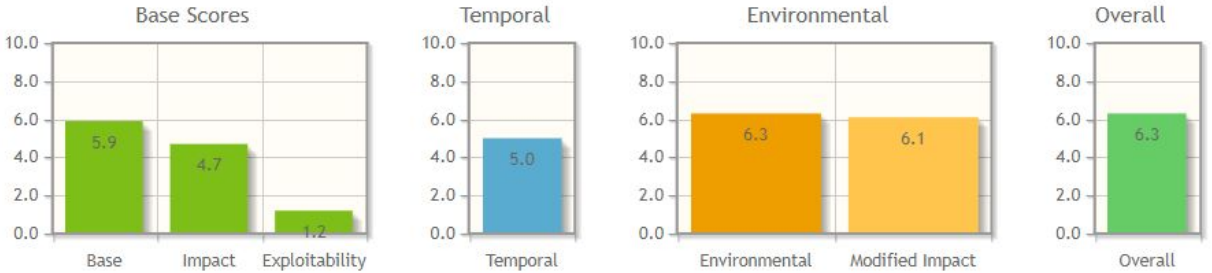
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Mitre ATT&CK

2.4 Análisis de Vulnerabilidades.

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 5.9
Impact Subscore: 4.7
Exploitability Subscore: 1.2
CVSS Temporal Score: 5.0
CVSS Environmental Score: 6.3
Modified Impact Subscore: 6.1
Overall CVSS Score: 6.3

Show Equations

CVSS v3.1 Vector

AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:H/E:U/RL:T/RC:R/CR:M/IR:H/AR:M/MAV:A/MAC:H/MPR:H/MUI:R/MS:C/MC:H/MI:H/MA:H

2.4 Análisis de Vulnerabilidades

NVD Vulnerability Severity Ratings

NVD provides qualitative severity ratings of "Low", "Medium", and "High" for CVSS v2.0 base score ranges in addition to the severity ratings for CVSS v3.0 as they are defined in the CVSS v3.0 specification.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Mitre ATT&CK

MITRE ATT&CK® es una base de conocimiento accesible a nivel mundial de tácticas y técnicas del adversario basadas en observaciones del mundo real. La base de conocimientos de ATT&CK se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad.

El marco es una base de conocimiento accesible a nivel mundial de tácticas y técnicas de los adversarios que pueden describirse como un inventario de indicadores de compromiso (IOC por sus siglas en inglés) estáticos basados en la reputación que cambian con el tiempo, expiran y solo tienen un valor en un punto en el tiempo.
https://www.mitre.org/news-insights/publication/finding-cyber-threats-attck-based-analytics

Mitre ATT&CK

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.

https://attack.mitre.org/

Más detalles en:
https://www.ibm.com/docs/es/qradar-common?topic=app-mitre-attck-mapping-visualization