UNIVERSIDAD TECNOLÓGICA DE SAN LUIS RIO COLORADO

GUÍA

MTRO. AURELIO FLORES

ALUMNO: VICTOR MANUEL GALVAN COVARRUBIAS

ING. EN DESARROLLO Y GESTIÓN DE SOFTWARE

San Luis Rio Colorado, Sonora Junio, 2022

UNCODING THE FUTURE

Static application security testing (SAST) is a set of technologies designed to analyze application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities. SAST solutions analyze an application from the “inside out” in a non-running state.

There are six simple steps needed to perform SAST efficiently in organizations that have a very large number of applications built with different languages, frameworks, and platforms.

1. **Finalize the tool.**
2. **Create the scanning infrastructure, and deploy the tool.**
3. **Customize the tool.**
4. **Prioritize and onboard applications.**
5. **Analyze scan results. Provide governance and training.**

Dynamic application security testing (DAST) is a program used by developers to analyze a web application (web app), while in runtime, and identify any security vulnerabilities or weaknesses. Using DAST, a tester examines an application while it’s working and attempts to attack it as a hacker would. DAST tools provide beneficial information to developers about how the app behaves, allowing them to identify where a hacker might be able to stage an attack, and eliminate the threat.

DAST is a **black box test**, meaning it is performed from the outside of the application, without a view into the internal source code or app architecture.

IAST shifts testing left in the SDLC. IAST generally takes place during the test/QA stage of the software development life cycle (SDLC). IAST effectively shifts testing left, so problems are caught earlier in the development cycle, reducing remediation costs and delays.

Key steps to run IAST effectively:

1. **Deploy DevOps.**
2. **Choose your tool.**
3. **Create the scanning infrastructure and deploy the tool.**
4. **Customize the tool.**
5. **Prioritize and add applications.**
6. **Analyze scan results.**
7. **Provide training.**

SAST	DAST
El tester tiene acceso al framework, diseño e implementación	El tester tiene conocimiento de en donde y como está construido el producto
Las pruebas son internas	Las pruebas son externas
Analiza mientras la aplicación no está siendo ejecutada	Analiza la aplicación mientras está siendo ejecutada
Sirve para todo tipos de software	Solo funciona para aplicaciones o servicios web.
Caja blanca	Caja negra
Las vulnerabilidades se encuentran antes del ciclo del software	Las vulnerabilidades se encuentran después del ciclo del software
No tan costoso de realizar	Costoso de realizar
No es posible encontrar errores al momento cuando el software está siendo utilizado	Es posible encontrar errores al momento cuando el software está siendo utilizado
El código es visible	El código no es visible
Fácil de llevar a cabo	No es fácil de llevar a cabo
Estático	Dinámico
Requiere el código fuente	No requiere el código fuente
El test es de adentro hacia a fuera	El test es de afuera hacia a adentro

Security log

A security log is used to track security-related information on a computer system.

Event log

It is necessary to create an event log that allows recording when an event has occurred, in such a way that it allows storing a data history and consulting the stored information of the event if required.

Error log

It is necessary to create an error log that allows you to control when an error has occurred, in such a way that it allows you to correct it and prevent it from happening again in the future.

Acciones para prevenir el carding y el pirateo de tarjetas incluyen:

- Implementar coincidencias AVS y CVV Funciones de detección de fraude en la pasarela de pago.
- Vigilancia de altos volúmenes de pedidos de pequeño importe, lo que podría ser una señal de carding.
- Observación de pedidos pequeños desde el extranjero con costes de envío superiores al producto.
- Creación de una lista negra de clientes para bloquear a aquellas personas que cometen fraudes de forma reincidente.
- Uso de herramientas automatizadas de prevención del fraude y protección antibots.