Tecnológico de Monterrey

Integración de seguridad informática en redes y sistemas de software

Amenazas: vulnerabilidades, fallas en protocolos, falsificación de identidad y conexiones

Profesores:

José Oscar Hernández Pérez

Lizethe Pérez Fuentes

Alan Patricio González Bernal | **A01067546**

Fecha de entrega:
20 de octubre del 2023

Todos los conceptos aprendidos a lo largo del curso, e incluso de cursos anteriores, se aplican en gran medida al reto de varias formas, algunos se aplican para el backend como lo puede ser la SQL injection (claro, es algo que se debe cuidar en todas las vistas, pero su objetivo es el backend), otros como el phishing son externos a nosotros, pero sin duda debemos tomarlos en cuenta. El evitar prestar atención a estos detalles aumenta el riesgo existente en cualquier aplicación que maneje datos, ya sean sensibles o confidenciales.

El no tomar en cuenta estas vulnerabilidades y buscar soluciones o formas de evitar que existan es sumamente peligroso debido a que se espera que cientas de personas confíen su información a nuestra plataforma. El no protegerla significaría un gran fallo de nuestra parte, además de, como se ha comentado anteriormente en otras entregas, el detalle que nuestra aplicación tenga fallos de ese tipo puede repercutir de varias maneras.

Una de las formas en las que esto puede repercutir es en el aspecto legal. La filtración de esta información es ilegal y si nosotros no tomamos las medidas necesarias para protegerlas (y un poquito más) puede suponer en problemas para nosotros como desarrolladores, explícitamente de forma legal.

Además de esa forma, también afecta a nuestra reputación como desarrolladores, la fama que uno se hace en este mundo es de suma importancia porque en base a ella la gente juzga si un trabajo es de calidad o no, independientemente del proceso interno que conlleva al desarrollo de ese sistema.

Un aspecto más que me gustaría resaltar es el impacto en el ánimo del equipo que un problema de esos presentaría. Uno jamás termina de aprender y desarrollar sus habilidades como programador e ingeniero, pero sin duda una falta de ese tipo afectaría en gran medida a la moral de todo el equipo, causando que algo que de por sí no estamos muy seguros de cómo se debe hacer, decidamos tal vez jamás volver a hacerlo.

Una forma que podemos tener de prevenir que ese tipo de situaciones sucedan, es manteniendo siempre el control de lo que sucede, además de planes de contención y acción para siempre saber qué hacer en caso de que algo suceda. En todos los lugares donde se desarrollen sistemas o se tenga alguno, se debe tener siempre en cuenta el “que tal si pasa…?” Por cada posible (e incluso imposible) situación que uno pueda identificar, debe haber una forma de contrarrestarla. Todos los días hay personas que intentan atacar los sistemas, sistemas como Google, Facebook, Instagram, etc. Siempre y todos los días son tratadas de vulnerar, pero existen muchas medidas que permiten que este tipo de cosas no tengan éxito y en caso de tenerlo, tener una forma de detenerlo.

La ciberseguridad es un tema muy importante, y yo incluso diría que es algo que se debe tener en cuenta siempre, tanto al usar aplicaciones como a la hora de desarrollarlas. Esto siempre asegurará que el usuario y el developer siempre tengan una idea de cómo funcionan los ataques y poder tener una idea de contrarrestarlos.