Plantilla para escenario específico de atributo de calidad

Requerimiento no funcional asociado: Almacenamiento seguro de las contraseñas

Categoría: Seguridad

Fuente del estímulo: Un atacante que pretende obtener la contraseña de un usuario

Estímulo: Un ataque dirigido a obtener la contraseña de algún usuario.

Ambiente o contexto: Es un ataque desde fuera del sistema. El ataque permitió al atacante obtener un acceso de solo lectura a la base de datos.

Artefacto: Afecta a la base de datos que guarda las contraseñas.

Respuesta: El atacante logró acceder a los registros deseados de la base de datos.

Medición de la respuesta: Los datos privados como contraseñas deben ser inaccesibles de todos modos para el atacante. Además, otros datos críticos (como tarjetas de crédito) deben seguir siendo innaccesibles directamente para el atacante (posiblemente encriptados).

Este escenario se logrará mediante las siguientes tácticas:

1. Empleo de funciones hash seguras para el almacenamiento de las contraseñas, como b2crypt.
2. Los datos críticos del usuario deben estar encriptados, ya sea con la clave del usuario o si esto no fuera posible con una clave almacenada en la aplicación/servidor, de modo que al menos se dificulte el acceso a la información.
3. El uso de sistemas de autenticación de terceros (como Facebook)