**CASO 2**

José Leonardo Patarroyo Devia

Juan Diego Trujillo

**PARTE A**

1.

* **Datos de acceso de cada usuario (usuario y contraseña):** Ya que es un sistema financiero, los usuarios son altamente sensibles a usos y accesos inadecuados de sus datos, por lo que si no se protegen los datos de los usuarios el sistema pierde confiabilidad y los usuarios dejan de ser parte de este sistema. Además, obteniendo los datos de los usuarios es posible realizar transacciones.
* **Transacciones realizadas por los usuarios:** Como se mencionó anteriormente, los usuarios desean que todos sus datos transaccionales sean confidenciales puesto que son datos de alta sensibilidad. Al poder acceder de forma indebida a la información transaccional de un usuario es posible tener problemas legales por manejo de la información, pérdida de confiabilidad y se puede realizar seguimiento a las acciones de un usuario, lo cual puede comprometer su seguridad física.
* **Archivo de configuración de usuarios:** Si se accede a este archivo se podrá suplantar cualquier actor del sistema, desde un usuario común y corriente hasta un administrador, y a través de esto realizar acciones indebidas a datos o transacciones de alto nivel.

2.

a) Hay una vulnerabilidad al no poseer un componente que se encargue de verificar la identidad del usuario en la comunicación de todo el sistema, puesto que si se logra vulnerar uno de los servidores y suplantar una identidad desde allí, desde ese punto el atacante puede manipular acciones en otros servidores de los otros servicios.

b) Hay una vulnerabilidad al utilizar un servicio de correo propio que no esté regulado por un tercero puesto que a través de este sistema de comunicación se puede llegar a suplantar identidades y generar datos o procesos no deseados.

c) El hecho de que cada aplicación tenga su propio archivo de configuraciones puede generar que un usuario obtenga acceso a un servicio a través del archivo y como el resto de servicios no conocen cómo ese usuario se relaciona con los demás servicios, puede permitirle realizar acciones indebidas.

d) Tener toda la información financiera guardada en un solo servidor permite que si un atacante obtiene acceso a ese servidor y decide borrar la información de allí, todo el sistema financiero se verá comprometido y así mismo la empresa.

**PARTE B**

Para mitigar las vulnerabilidades se debe:

1. Tener un componente dentro del sistema que esté constantemente verificando la identidad de los usuarios que están realizando acciones entre servicios
2. Para tener un canal de comunicación seguro se debe utilizar una verificación de un tercero para el correo electrónico
3. A través del componente propuesto en (a) se puede también revisar la configuración global de permisos de los usuarios
4. Se deben tener varias copias de los datos en diferentes servidores para tener una recuperación exitosa en caso de pérdida de los datos