**Malas practicas y fugas de información en los sistemas de Rappi.**

En primera instancia cabe resaltar que los hallazgos por parte de los investigadores de seguridad en el sistema de Rappi eran bastante delicados, teniendo en cuenta que un sitio web o aplicación móvil que quiera recolectar información de las tarjetas de crédito de sus usuarios debe cumplir con los estándares mas altos de seguridad definidos por la alianza PCI DSS que fue creado por los mayores emisores de tarjetas de crédito como lo son Visa, MasterCard etc, estos estándares definen las buenas practicas y requisitos que se deben tener en cuenta a la hora de diseñar sistemas que recolectan información de tarjetas de crédito de sus usuarios y así prevenir fraudes electrónicos o fugas de información sensible relacionados con las mismas.

La solución mas sencilla y rápida es implementar una pasarela de pagos o gateway que ya cumple con los mas altos estándares de calidad para recolectar los datos relacionados con tarjetas de crédito de manera segura, de esta manera el formulario para la recolección, el procesamiento y almacenamiento de la información es llevada a cabo por la pasarela, eliminando así toda responsabilidad u administración por parte del sitio que realiza el comercio. Realizando las transacciones a través de estas pasarelas la probabilidad ante un ataque remoto o fraude digital son mínimas, ya que sus creadores se han basado en los estándares definidos por el PCI DSS, el cual básicamente lo que busca es tokenizar cada transacción y procesarla en servidores que contemplen las buenas practicas de hardening y mitigar estos posibles ataques externos. En esta parte es donde estaba fallando Rappi, ya que para tratar de mejorar la experiencia de usuario la recolección de los datos de las tarjetas de crédito lo hacían a través de sus formularios y los enviaban a un compartimento seguro del gateway el cual generaba un token asociado a la información de una tarjeta de crédito, tales como fecha de expiración, nombre del propietario, CVV etc… La pasarela que estaban usando en Rappi para este fin es conocida como Spreedly, en la documentación oficial de Spreedly dice claramente que las llaves de acceso a este compartimento deben hacerse desde servidores con altos estándares de seguridad, cosa que los desarrolladores del sistema de Rappi no tuvieron en cuenta, exponiendo estas claves sin ningún algoritmo de encriptación en scripts que eran cargados en el cliente o el navegador del usuario, de esta manera un atacante que se lograra hacer con estas claves de acceso al compartimento seguro podía extraer información parcial de las tarjetas de crédito almacenadas allí e incluso vincular tarjetas de crédito a cuentas de usuario diferentes, otra falla grave de seguridad fue encontrada en el login, ya que las llaves de acceso al API para autenticación con Facebook también se encontraban quemadas allí, facilitando de esta manera la suplantación de identidades en el sistema y dando entrada ataques del tipo Cross site request forgery, conociendo todo esto y teniendo en cuenta que la información de las tarjetas de crédito están vinculadas a un usuario, de esta manera también se podían generan cargos a las tarjetas de los usuarios por medio de suplantación de identidades derivados de la vulnerabilidad en los inicios de sesión.

Tomando como base estos antecedentes, se debe tener presente que las llaves de acceso a estas API que almacenan información sensible de los usuarios de un sistema, no deberían quemarse en el cliente, deben almacenarse y procesarse de manera segura (con algoritmos de encriptación por e.g) en el servidor el cual también debe estar configurado de tal manera que minimice al máximo posibles fugas de esta información, además de esto tener en cuenta todos los estándares y buenas practicas definidas por el PCI DSS para garantizar la integridad y seguridad de los datos financieros de los usuarios de determinado sistema.