

**Carrera de Computación**

**Título:**

Evaluación de vulnerabilidades al proyecto de titulación

**Asignatura:**

Seguridad de la información

**Estudiantes:**

Bryam Barrera

Pedro Illaisaca

**Docente:**

Ing. Jennifer Yepez

**Cuenca, 25 de enero 2022**

**1. Describir las características de su proyecto de titulación.**

El trabajo de titulación del presente grupo tiene como título Desarrollo de un aplicación móvil y web para la inspección de juntas de agua potable usando servicios de geolocalización y almacenamiento en la nube, consta en desarrollar dos aplicaciones una web y la otra una aplicación móvil, ambas aplicaciones compartirán una misma base de datos no relacional que reside en la nube, adicional a esto las aplicaciones cuentan con servicios de almacenamiento de imágenes y servicios de geolocalización, la aplicación web estará desplegada en un servidor en la nube que permitirá acceder desde internet, en cuanto a la aplicación móvil está disponible solamente para la plataforma Android, con el objetivo de reutilizar el mismo código que se usó para el desarrollo de la aplicación web y aprovechando las posibilidades que nos brinda el framework usado, se compilo en una versión móvil considerando la interacción con sensores, servicios y permisos que necesita la plataforma.

**2. Enumerar y describir 5 debilidades que considera existe en su proyecto de titulación, detallando qué amenaza se podría aprovechar de cada vulnerabilidad y lo que implicaría para la seguridad de la información.**

* Acceso a internet ilimitado: ausencia de configuración de filtros de un firewall que limite el tráfico, implica que haya mayor probabilidad de sufrir un ataque desde internet.
* Transmisiones mediante Wifi: este tipo de comunicación no siempre está cifrado, por lo que cualquiera que esté auditando el tráfico de red tendrá a información comprometida especialmente en dispositivos móviles, implicando que la información que circula por este medio pueda ser interceptada.
* Calidad de código fuente: una calidad de código pobre puede ocasionar que nuestra aplicación sea ineficiente, esto implica que haya la posibilidad de un desbordamiento de buffer o ataques que permitan acceder a información sensible ocasionado por una mala codificación
* Ausencia de certificado SSL: en el caso de la aplicación web no se contempló este tipo de seguridad al momento de ponerla en producción, por lo cual un atacante puede acceder a la información entre el cliente y el servidor, esto ocasiona que los usuarios desconfíen de la aplicación.
* Debilidad XSS: esta vulnerabilidad ataca a datos guardados en Storage y variables globales que estén presentes en la aplicación, como es el caso de la aplicación web, este ataque inserta código malicioso que puede robar información de los usuarios.

**3. Presentar una medida de protección para cada debilidad descrita previamente. Se deberá justificar por qué se seleccionó la medida de protección y detallar cómo la medida de protección evitará que una amenaza se aproveche de la vulnerabilidad. No se podrá repetir las medidas planteadas; es decir, para cada vulnerabilidad debe presentarse una medida diferente.**

Acceso a internet ilimitado: Para esta vulnerabilidad se aplicarán reglas de firewall en nuestro caso en la plataforma de Google Cloud con el fin de definir las rutas de acceso para instancias salientes, al aplicar reglas de firewall esto permitirá que se filtren cierto tipo de tráfico no deseado, denegar el acceso a direcciones IP no deseadas, con el objetivo de controlar el tráfico procedente de internet al equipo o viceversa.

Transmisiones mediante Wifi: para mitigar esta vulnerabilidad es recomendable hacer uso de vpn´s de este modo el tráfico ya no va a poder ser legible por un atacante.

Calidad de Código fuente: una medida de protección para esta vulnerabilidad se podría aplicar diferentes metodologías como código único, es decir no considerar el hecho de reutilizar código o mantenerlo como código abierto, ya que esto podría facilitar a que otros puedan detectar fallos, pero también mayor exposición y riesgo a que manos ajenas con intenciones malignas tengan a su alcance al código de nuestra aplicación. Al aplicar este tipo de protección estaríamos fomentando una buena higiene del código al integrarse directamente en el desarrollo, además de realizar prácticas de desarrollo seguro.

Ausencia de certificado SSL: para que la aplicación web este considerada como sitio seguro por los navegadores tendremos realizar gastos para adquirir dicho certificado de seguridad a una entidad certificadora, de este modo tendremos una comunicación segura entre cliente y servidor.

Vulnerabilidad XSS: para evitar este tipo de vulnerabilidad debemos configurar en el servidor donde reside la nuestra aplicación web y configurar la Política de Seguridad de Contenido (CSP), de este modo todos los ataques de este tipo no tendrán efecto.