EDUCACIÓN CON RESPONSABILIDAD SOCIAL

UNIVERSIDAD DE COLIMA

Facultad de Telemática

Ingeniería de Software

Desarrollo de software seguro

Ramírez Morfín José Nabor

Actividad 13.- MVP (Minimum Viable Product) Seguro - REPORTE ESCRITO

09 de junio del 2021

Samanta Vianey Rubio García 6K

Marian Fernanda Palacios García 6J

ÍNDICE

INTRODUCCIÓN

La seguridad es un factor importante a la hora de lanzar al mercado algún producto, ya que esto es parte fundamental para que los usuarios se sientan cómodos a la hora de usarlo así como siendo un factor decisivo a la hora de adquirirlo.

Existen varios elementos que tomar en cuenta a la hora de buscar la seguridad, así como un sin fin de factores que pondrán en duda nuestra seguridad.

Por esta razón es que elaboramos un minimum viable product basadoe en un videojuego donde aplicaremos la metodología SecDevOps para así tener una solución a los posibles riesgos de seguridad que podamos tener en un futuro, utilizando diversos elementos de seguridad correspondientes a cada etapa.

Dentro del desarrollo del proyecto se tiene contemplado desarrollar un total de dos iteraciones siendo estas un sistema de autenticación de usuarios e implementación de reglas de seguridad firebase para el llenado y obtención de datos de una base de datos.

A continuación se mostrará el proceso a seguir para cada una de las iteraciones.

DESARROLLO

Roles con acceso permitido

1. Baby User: Este usuario se encuentra en el rango de 7 - 9 años de edad y se le mostrará contenido conforme a su edad.
2. Junior User: Este usuario se encuentra en el rango de 10 - 12 años de edad y se le mostrará contenido conforme a su edad.
3. Senior User: Este usuario se encuentra en el rango de +13 años de edad y se le mostrará contenido conforme a su edad.

Etapas y elementos de seguridad

La metodología que se utilizará para este proyecto será en base a SecDevOps en donde se implementarán las siguientes etapas con sus respectivos elementos de seguridad:

1. *Planificación:*
    a. Matriz de activos de información: Se utiliza para poder desarrollar los posibles daños que se pueden sufrir así como desarrollar la manera en la que se resolvería cada uno de ellos.
    b. Arquitectura de seguridad: Se utiliza para identificar las áreas que podrían ser vulnerables y el como darles seguridad, así como se relacionan con ellas.
    c. Árbol de ataque: Se utiliza para desarrollar los ataques, de una manera que se pueda pensar más allá de un solo ataque, todo en base a una misma situación.
2. *Codificación:*
    a. Godot engine: Se utiliza el programa de desarrollo de Godot para una correcta codificación, compilación y depuración del código.
    b. Visual estudio code: Se utiliza esta IDE para mejorar el código fuente y verificar que se apliquen buenas prácticas de programación.

3. *Control de versiones*:
    a. Github: Se utilizan los repositorios de github para almacenar las iteraciones del proyecto y tener el control de manipulación de cada versión que se genere.
    b. Documentación: Se documenta cada iteración así como sus respectivos procedimientos, resultados, problemas y soluciones obtenidos en cada etapa.
4. *Pruebas:*
    a. Validación de reglas firebase: Se utiliza la misma plataforma o prototipo para las pruebas en las reglas implementadas en la base de datos.
    b. Validación de entradas y salidas: Se testea las validaciones codificadas para evitar ataques e intrusiones en el proyecto.
5. *Pruebas de aceptación:*
    a. Usuarios reales autorizados: Se utilizan usuarios reales para realizar pruebas y asegurarse que el software funcione correctamente y sea fácil de usar.
6. Producción:
    a. Servidor de alojamiento: Se utiliza un servidor gratis y seguro como Itch.io para alojar el videojuego y que este pueda ser utilizado por los usuarios finales quienes podrán darnos su retroalimentación acerca del funcionamiento y/o vulnerabilidades que pudiesen presentarse sin haberlas contemplado con anterioridad.

Herramientas de trabajo a distancia

Gracias a la situación actual que se vive es que tuvimos que hacer uso de un mayor número de herramientas para poder organizarnos y ponernos en contacto, por lo que a continuación se presenta una lista de ellas.

- ☐ Google Meet
- ☐ WhatsApp
- ☐ Google Docs
- ☐ Draw.io
- ☐ Gmail
- ☐ Github
- ☐ Godot engine
- ☐ Firebase
- ☐ Itch.io

CONCLUSIONES

Como conclusión considero que la implementación de seguridad en cada etapa del desarrollo de software (como lo hace SecDevOps) es una de las partes más importantes para aplicar a nuestros proyectos. Ya que en la actualidad las TICs se han visto con un mayor grado de vulnerabilidades y es necesario poseer el conocimiento para reducir los riesgos de ataques hacia nuestros sistemas.

- **Rubio García Samanta Vianey**

Actualmente la ciberseguridad se volvió una necesidad, ya no es tiempo de tomarnos a la ligera la existencia de vulnerabilidades, es hora de hacer algo para defendernos de los ataques sin antes de ser atacados, por lo que considero que es de suma importancia que se implementen métodos de seguridad en cada etapa del desarrollo de software, tal como lo hace SecDevOps.

- **Palacios García Marian Fernanda**

REFERENCIAS

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

Haber, M. J. (2020). Secured DevOps (SecDevOps). In Privileged Attack Vectors (pp. 251-255). Apress, Berkeley, CA.