Informe de Avance RF2

Datacript Equipo 1 10/10/2023

Integrantes

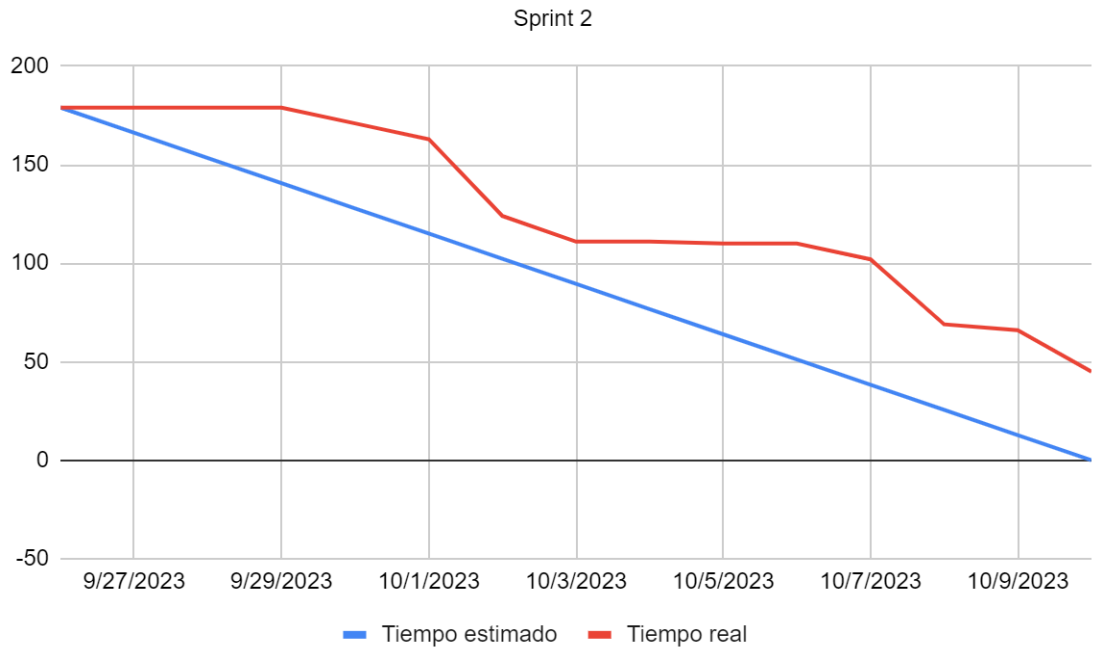
Apellido y Nombre	Rol
Dikenstein, Leandro	Product Owner
Perez, Giannina	Scrum Master
Prieto, Lucas	Líder Técnico
Benitez, Micaela	Desarrolladora
Benitez, Yamila	Desarrolladora
Clauser, Nahuel	Desarrollador
Torrico, Franco	Desarrollador
Gómez, Federico	Tester

Funcionalidad Comprometida

Requerimientos prometidos	Completo	Responsable
Clasificación de Datos Maestros	Si	Giannina Perez
Definición de Estrategia de Seguridad de la Información (ESI)	Si	Yamila Benitez
Definición de Prueba de Penetración	No	Federico Gómez
Diseño de Base de Datos	Si	Nahuel Clauser
Implementación de Base de datos para pruebas	Si	Lucas Prieto
Definición de comunicación entre APIs	No	Lucas Prieto
Modificación API REST para Pruebas	Si	Franco Torrico

Get de Historial para API	Si	Micaela Benitez
Get y Post de Diagnóstico para API	Si	Franco Torrico
Test API REST	No	Federico Gómez
Definición de Roles y Permisos	Si	Micaela Benitez
Definición de políticas para contraseñas	Si	Yamila Benitez
Construcción Guía de Buenas prácticas de ciberseguridad	Si	Giannina Perez
Prueba de integración para conexión con modelos	No	Lucas Prieto

Burndown Chart



Actividades realizadas

1. **Estrategia de Seguridad de la información (ESI):** Se definió la estrategia de seguridad teniendo en cuenta los siguientes pasos: clasificación de activos, identificación de amenazas y vulnerabilidades, perfil de riesgo y tratamiento de riesgos.

2. **Clasificación de datos personales según Ley 25326: Protección de datos personales:** Los datos personales se clasificaron con el fin de priorizar y determinar qué datos necesitarán cifrado u otra política de seguridad.

3. **Diseño e Implementación de Base de Datos:** Se implementó una base de datos relacional para almacenar datos de pruebas que posteriormente van a ser levantados con API's.

4. **Actualizaciones en la API de pruebas:** Se agregaron endpoints para continuar con las pruebas de integración con los demás equipos.

5. **Definición de roles y permisos:** Junto a los demás equipos, se definieron los roles y permisos de usuario de la plataforma.

6. **Evaluación de Vulnerabilidades en el Sistema:** Se utilizará la herramienta OWASP ZAP (Zed Attack Proxy) para probar y evaluar las vulnerabilidades en el sistema.

7. **Definición de políticas de seguridad para contraseñas:** Se establecieron políticas de seguridad para la creación de contraseñas para garantizar la seguridad de las cuentas y la integridad de los datos

Problemas o inconvenientes detectados

- La base de datos está hosteada a través de Ngrok, por lo que cada vez que se reinicia el servidor el puerto asignado cambia.

Propuesta próximo ciclo

En nuestro próximo Sprint, nos enfocaremos en la implementación de los diversos aspectos que hemos definido hasta este punto. Estas implementaciones abarcan el cifrado con AES, la prueba de penetración y las políticas para contraseñas. Además, nos ocuparemos de la gestión de roles y permisos para diferentes tipos de usuarios, incluyendo administradores/auditores, administradores, profesionales de la salud y médicos.

Por otro lado, continuaremos trabajando en la definición de aspectos cruciales de ciberseguridad que serán implementados en fases posteriores. Esto incluye la planificación para implementar actualizaciones de software y un backup para la base de datos.