Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias y Sistemas
Software Avanzado
Primer Semestre 2025
Catedrático:
Ing. Everest Medinilla
Tutor Académico:
Julio Roberto Vasquez Santiago

Autorización y Autenticación

PONDERACIÓN: 1.5

Horas Aproximadas: 16

Práctica 2

Contenido

Objetivos Generales 2

Objetivos Específicos 2

Descripción 2

Documentación 2

Entregables: 2

Requerimientos mínimos 2

Restricciones: 3

Cronograma 4

Valores 5

Rubrica 5

Fecha de entrega: 6

Referencia 6

Objetivos Generales

- Aplicar los conocimientos adquiridos a lo largo de la carrera de Ingeniería en Ciencias y Sistemas para generar software de alta calidad y escalable, a través de diferentes técnicas de desarrollo y utilizando las últimas tecnologías.

Objetivos Específicos

- Que el estudiante elija un lenguaje y framework de desarrollo que crean sea útil para la tarea asignada
- Familiarizarse con los métodos de autenticación utilizados

Descripción

En el corazón de nuestro proyecto, se ha ordenado la creación de un **Módulo de Registro y Login**. Esta no es una simple tarea, es una **el inicio de toda su plataforma.** Usted, como el ingeniero a cargo de la tarea, tiene la libertad de utilizar las herramientas que mejor se adecuen a la resolucion del problema.

Sin embargo, para garantizar que este código se mantenga puro y reutilizable a lo largo del tiempo, se han impuesto una serie de requisitos en el diseño de la solucion. El incumplimiento de estas normas podria generar problemas de dificil solucion en el futuro.

Las restricciones:

- **La comunicación entre las capas:** El frontend y el backend deben comunicarse a través de un **API REST**. Ninguna otra forma de comunicación será tolerada.
- **Autenticación:** El método de autenticación se hará a través del uso de **JWT (JSON Web Token)**. Este token, una especie de llave con un sello mágico, será la única prueba de la identidad del usuario. El JWT debera de estar almacenado en un Cookie accesible unicamente por el servidor del backend (Cookie del tipo HTTPS).
- **El Tiempo de Vida del JWT:** El tiempo de existencia de cada sello JWT no será eterno. Su tiempo de vida será definido por una **variable de entorno**.
- **Renovación:** Si el tiempo de vida del JWT expira, este no será olvidado inmediatamente. Se le concederá un **periodo de gracia** (definido por otra variable de entorno) para su renovación. Si el usuario desea mantenerse dentro del sistema durante este tiempo, se renovará automáticamente el token.
- **El Resguardo de la Información:** Todos los datos, incluyendo nombres, correos y contraseñas, deben ser almacenados en un **estado de cifrado absoluto**. Para esto se recomienda el uso del algoritmo de encriptacion AES, sin embargo, si usted tiene una mejor solucion para la encriptacion, es libre de utilizarla.
- **Implementacion de 2FA:** Debe de exisitr una opcion para el usuario en el cual pueda implementar y usar un sistema de 2FA (Se le recomienda utilizar alguna app para esto, como lo puede ser Google Authenticator)
- **Limitación de intentos de login:** Para prevenir ataques de fuerza bruta, debera agregar un sitema de bloqueo temporal a un usuario después de un número

determinado de intentos fallidos de login. El tiempo de bloqueo queda a su discrecion.

- **Confirmación de correo electrónico:** Después de que un usuario se registre, su cuenta no debería estar activa de inmediato. Se le enviaría un correo electrónico con un enlace único y temporal. El usuario debe hacer clic en este enlace para verificar su identidad y activar su cuenta.

Por último, el líder del proyecto nos recuerda la importancia de las **buenas prácticas de programación**. El código debe ser tan **reutilizable** y **robusto** capaz de resistir el paso del tiempo. El Módulo de Registro y Login es solo el principio.

Documentación

En un archivo de tipo MARKDOWN deberá incluir las instrucciones para poder ejecutar su solución. En el mismo archivo deberá de colocar una explicación breve sobre las siguientes tecnologías y herramientas utilizadas:

1. Herramientas de backend y frontend utilizadas, incluyendo la base de datos, así como las ventajas y desventajas de estas.
2. Que son los algoritmos de encriptación simétrica y asimétrica
3. Que es y cómo funciona el algoritmo de encriptación AES
4. Qué son las cookies del tipo HTTP/HTTPS y el algoritmo de encriptación AES.
5. Una explicación sobre qué es JWT y su uso para autenticación.
6. Deberá realizar un diagrama de secuencia sobre cómo se comporta su sistema de autenticación utilizando JWT e incluirlo dentro de la documentación.

Entregables:

- Subir a UEDI el enlace del repositorio. (Si aún no hay acceso a UEDI se habilitara entregable en classroom)

Requerimientos mínimos

Documentación completa

- Último commit subido antes de la hora y fecha de entrega.
- Debe de crear un repositorio privado con el siguiente formato de nombre:
    - Practicas-SA-<<SECCIÓN>>-<<CARNE>>
    - Manejar una rama separada con el nombre de feature/P2
    - Crear carpeta dentro del repositorio con el nombre **P2** e incluir los archivos a entregar

- Agregar al auxiliar al repositorio, con el rol Developer:
    - Sección A: **GitLab: @jrvasquez, GitHub: hkjvasquez**
    - Sección B: **di3gini (ambas plataformas)**

Restricciones:

- Se debe hacer uso de un repositorio en la nube para realizar la entrega de su proyecto (Gitlab, Github, Bitbucket, etc.)
- Los lenguajes de programación a utilizar son de elección libre según lo requiera el estudiante.
- El estudiante será libre de elegir el tipo y motor de base de datos que prefiera. Recuerde que deberá justificar su decisión en la calificación.
- Se trabajará de manera individual.
- Las copias completas/parciales serán merecedoras de una nota de 0 puntos, los responsables serán reportados al catedrático de la sección y a la Escuela de Ciencias y Sistemas.

Cronograma

Tarea	Fecha
Asignación practica	09/08/2025
Fecha de entrega	16/08/2025
Fecha de calificación	16/08/2025

Valores

En el desarrollo de la práctica, se espera que cada estudiante demuestre honestidad académica y profesionalismo. Por lo tanto, se establecen los siguientes principios:

1. **Originalidad del Trabajo**

    - Cada estudiante o equipo debe desarrollar su propio código y/o documentación, aplicando los conocimientos adquiridos en el curso.
2. **Prohibición de Copias y Plagio**
    - Si se detecta la copia total o parcial del código, documentación o cualquier otro entregable, la calificación será de **0 puntos**.
    - Esto incluye la reproducción de código entre compañeros, la reutilización de proyectos de semestres anteriores o el uso de código externo sin la debida referencia.
3. **Uso Responsable de Recursos Externos**
    - El uso de bibliotecas, frameworks y ejemplos de código externos está permitido, siempre y cuando se referencian correctamente y se comprendan plenamente. (Consultar con el catedrático su política)
4. **Revisión y Detección de Plagio**
    - Se podrán utilizar herramientas automatizadas y revisiones manuales para identificar similitudes en los proyectos.
    - En caso de sospecha, el estudiante deberá justificar su código y demostrar su desarrollo individual o en equipo. Si este extremo no es comprobable la calificación será de **0 puntos**.

Al detectarse estos aspectos se informará al catedrático del curso quien realizará las acciones que considere oportunas.

Rúbrica de Calificación

La evaluación de la práctica busca medir el cumplimiento de los objetivos planteados, así como la correcta aplicación de los conocimientos técnicos y habilidades.

Se debe agregar una tabla con los aspectos a calificar con su respectiva puntuación.

Descripción	Valor
Módulo de registro y login	**65**
Implementación correcta del modelo API REST	7.5
Autenticación con JWT	7.5
Almacenamiento seguro del token usando Cookies HTTP/HTTPS	10
Configuración del tiempo de vida y renovación del token	5

Encriptación de datos	5
Funcionamiento del registro y login	10
Implementación de 2FA	10
Confirmación de correo	5
Buenas practicas de programacion	5
Documentación	**25**
Explicación de las tecnologías utilizadas	2.5
Descripción de cookies del tipo HTTP/HTTPS	5
Encriptacion simetrica y asimetrica	2.5
Que es y cómo funciona AES	5
Que es JWT y su uso para autenticación	5
Diagrama de secuencia	5
Preguntas	**10**
Pregunta 1	5
Pregunta 2	5
Total	**100**

Fecha de entrega:

Día 16 de agosto de 2025 antes de las 07:00 hrs, la entrega se realizará por medio de UEDI, en caso exista algún problema, se estará habilitando un medio alterno por medio del auxiliar del laboratorio

Referencias

JWT Auth - Box Developer Documentation