EDUCAQuest

Trabajo de Fin de Grado

Ingeniería Informática

VNiVERSiDAD
D SALAMANCA

Junio de 2025

4º curso

Autor:
Iker Botana Vázquez

Tutores:
María José Polo Martín
Jaime Rodríguez Moro
Enrique Prieto Conde

Anexo IV: Plan de Seguridad

ÍNDICE

LISTA DE FIGURAS

INTRODUCCIÓN

Este Plan de Seguridad describe las medidas técnicas, organizativas y legales adoptadas en el desarrollo del presente Trabajo Fin de Grado (TFG), con el objetivo de garantizar la protección de los datos, la integridad del sistema y la correcta gestión de accesos. Se detallan los elementos críticos, las metodologías aplicadas y las herramientas utilizadas para asegurar la fiabilidad del sistema ante posibles amenazas, todo ello conforme a la legislación vigente y las buenas prácticas de ciberseguridad.

OBJETIVOS DE SEGURIDAD

El plan persigue asegurar los siguientes principios fundamentales:

- Confidencialidad: Prevenir accesos no autorizados a la información.
- Integridad: Asegurar que los datos no sean alterados de forma indebida.
- Disponibilidad: Garantizar que el sistema esté operativo y accesible cuando sea necesario.

ELEMENTOS A PROTEGER

El sistema desarrollado en el presente proyecto implica la protección de diversas entidades y componentes críticos cuya seguridad es esencial tanto desde el punto de vista técnico como legal. A continuación se describen los principales elementos a proteger, junto con los riesgos asociados y las medidas implementadas para mitigarlos.

- Los usuarios registrados

  Constituyen un componente sensible, ya que el sistema almacena sus datos personales y credenciales. Para garantizar la confidencialidad de esta información,

se ha implementado un sistema de autenticación robusto y se han cifrado las contraseñas mediante algoritmos de hash seguros, como “bcrypt”, lo que impide su lectura incluso en caso de acceso no autorizado a la base de datos.

- La aplicación web

  Dispone de diferentes perfiles de usuario (administrador, profesor, etc.), cada uno con niveles de acceso diferenciados. Para impedir accesos indebidos entre roles, se han utilizado “guards” en el FrontEnd, que bloquean el acceso a rutas no autorizadas incluso si se intenta acceder directamente mediante la modificación de la URL. Esta gestión de roles y rutas asegura que cada usuario interactúe únicamente con las secciones correspondientes a su perfil, y, si intenta cambiar de pantalla mediante la modificación de la url, se le redirigirá a la pantalla de login.

- La base de datos

  Es uno de los puntos críticos del sistema, ya que en ella se almacena información sensible relativa a los usuarios y su actividad. Además del cifrado de contraseñas, se han aplicado medidas de validación de entradas y control de consultas para prevenir ataques de inyección SQL u otras amenazas comunes.

- El servidor de despliegue

  Representa un punto estratégico en términos de infraestructura. Para garantizar su seguridad, se ha alojado la aplicación en un servidor privado proporcionado por la Fundación Montemadrid, organización colaboradora de confianza. Esta elección no solo proporciona un entorno controlado y protegido, sino también la garantía de que la institución gestora no hará un uso indebido de los datos ni del sistema. Además, serán ellos los encargados de gestionarla a partir de ahora, ya que tienen más medios para garantizar su seguridad.

En conjunto, estas medidas permiten cubrir adecuadamente los principales vectores de ataque, reducir significativamente la superficie de exposición del sistema, y cumplir con los requisitos técnicos y legales aplicables a proyectos que manejan datos personales.

METODOLOGÍA Y NORMAS APLICADAS

Se ha seguido una estrategia basada en las buenas prácticas de seguridad establecidas por:

- OWASP Top 10, para la prevención de las vulnerabilidades más comunes en aplicaciones web.

- RGPD (Reglamento General de Protección de Datos) y LOPDGDD, para asegurar el correcto tratamiento de los datos personales de los usuarios.

- Referencias puntuales a la norma ISO/IEC 27001 como guía general de gestión de seguridad de la información.

HERRAMIENTAS Y TÉCNICAS DE SEGURIDAD IMPLEMENTADAS

- Cifrado de contraseñas mediante algoritmos como bcrypt para evitar su exposición.

  Como vemos en el siguiente código perteneciente a la parte de BackEnd, se recibe una contraseña del FrontEnd (la que ha introducido el usuario), y mediante la función bcrypt.hash (que sirve para generar un hash seguro a partir de una cadena de texto) obtenemos una nueva contraseña hasheada, es decir, no entendible para los seres humanos.

  El argumento “10” introducido en la función es el "salt rounds" o número de rondas de procesamiento para generar el hash. Cuanto mayor el número, más seguro, pero también más costoso computacionalmente. Un valor de 10 es un estándar bastante equilibrado entre seguridad y rendimiento, en el que se añade un valor aleatorio a la contraseña y hashea 10 veces, lo cuál es irreversible.

  Con esto lo que se consigue es que ningún humano vea la contraseña en ningún momento de este proceso, ya que la máquina directamente la guarda encriptada.

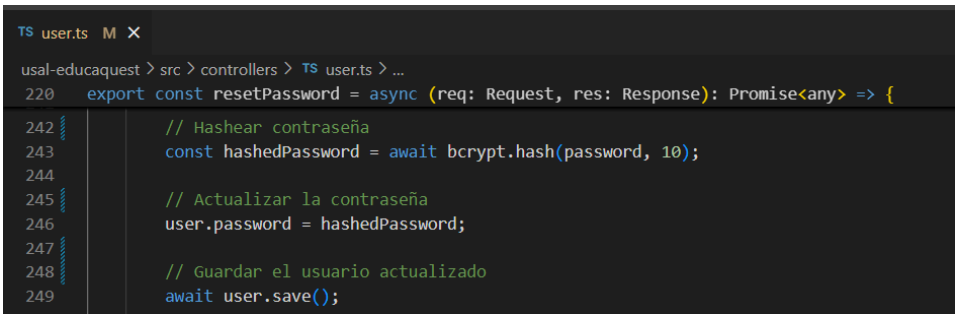

Figura 1. Código para hashear contraseña.

- Guards en el frontend que impiden el acceso a rutas no autorizadas aunque se modifique la URL directamente.

Para utilizar estos guards, primero hay que definirlos, en este caso usaremos uno para cada rol, y lo asociaremos a las urls que solo se puedan acceder desde dicho rol. Por ejemplo, en la siguiente imagen podemos ver la definición del guard para los usuarios con rol alumno.

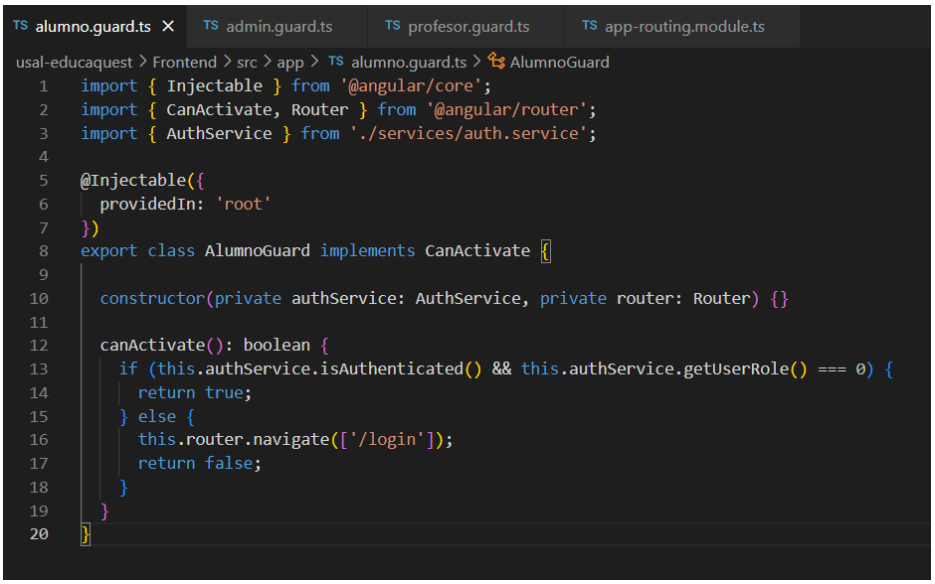

Figura 2. Guard para los alumnos.

Ahora, lo que habrá que hacer es ir a la sección de todas las rutas del sistema, y a cada una, aplicarle el guard que le corresponda, es decir, a todas las que sean para el administrador, por ejemplo, aplicarles el guard de administrador, y a las que sean comunes para todos los roles, aplicarle todos los guards.

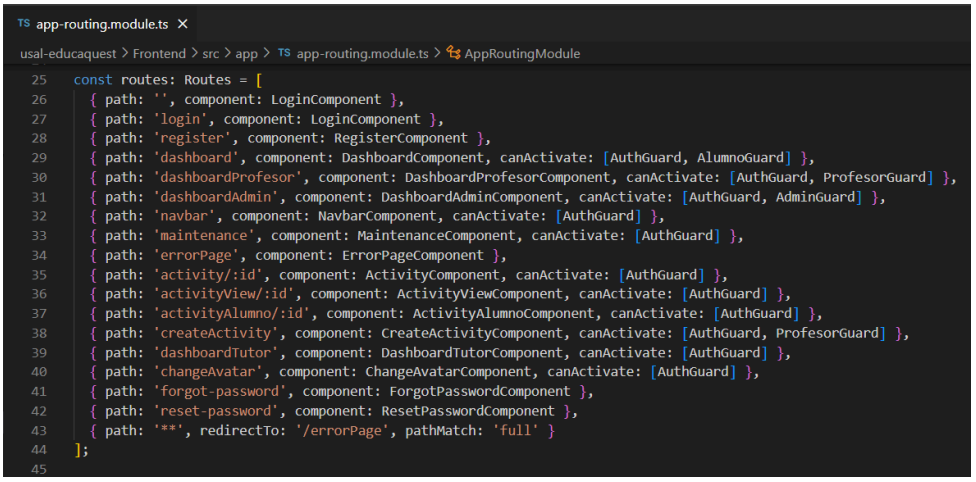

Figura 3. Rutas con guards aplicados.

- Roles de usuario claramente diferenciados (administrador, profesor, etc.), con comprobaciones tanto en el cliente como en el servidor.

- Servidor privado alojado en una infraestructura segura gestionada por la Fundación Montemadrid, lo que garantiza un entorno confiable y controlado.

  El acceso a la aplicación EDUCAQuest está garantizado como seguro porque solo podrán conectarse los usuarios autorizados por la Fundación Montemadrid. La aplicación está alojada en el servidor privado de la Fundación, que cuenta con una VPN protegida por credenciales específicas que ellos proporcionan. Esto implica que, para acceder a la aplicación, es necesario estar conectado a dicha VPN. Si un usuario no está dentro de esta red privada virtual, no podrá acceder a EDUCAQuest bajo ninguna circunstancia, lo que añade una capa adicional de seguridad y control al sistema. Así, el acceso queda restringido a un entorno controlado y confiable, minimizando riesgos de intrusiones externas.

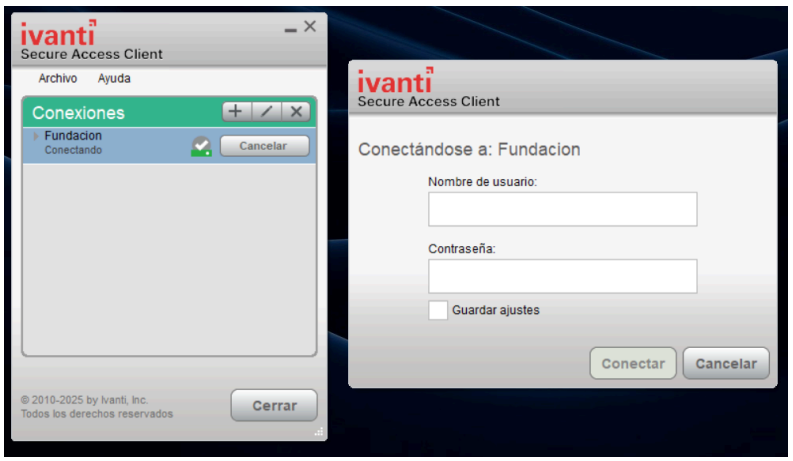

Figura 4. Conexión a VPN privada.

Tras conectarse a la VPN de la Fundación Montemadrid, ya si que se podrá acceder a la aplicación EDUCAQuest, con la siguiente ip privada:

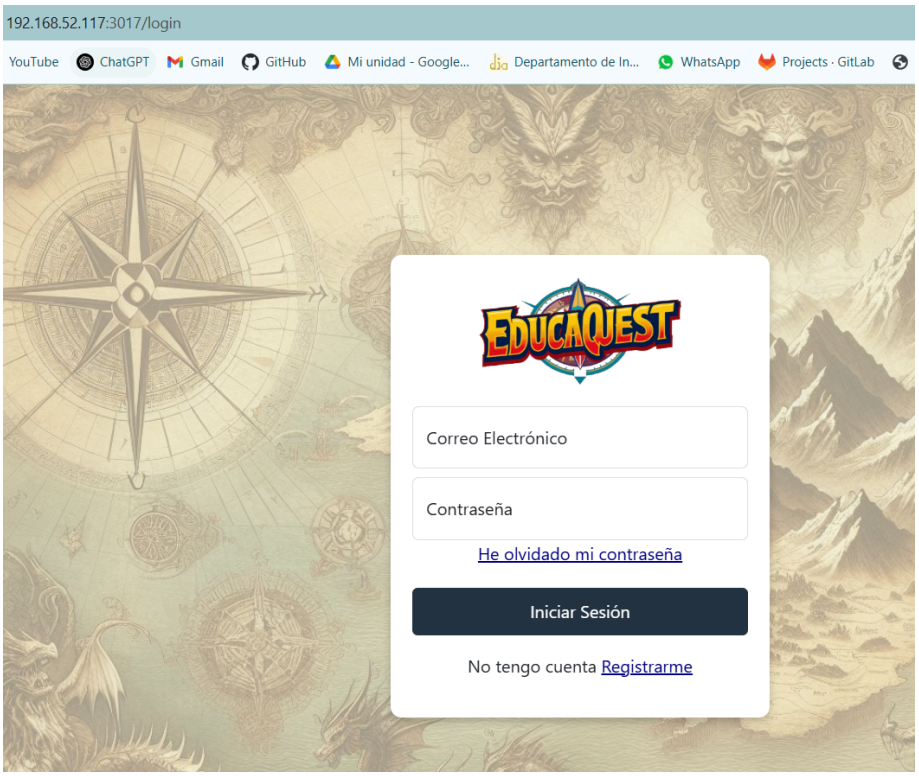

Figura 5. Acceso a EDUCAQuest mediante VPN.

- Control de acceso al BackEnd a través de autenticación segura y control de sesiones.

- Validación de inputs para prevenir inyecciones SQL, XSS y otras amenazas comunes.

CONCLUSIÓN

La seguridad ha sido tratada como un eje transversal en el desarrollo del proyecto, desde la fase de diseño hasta el despliegue final. Gracias a la combinación de buenas prácticas de desarrollo seguro, el uso de infraestructura confiable proporcionada por la Fundación Montemadrid, y la implementación de controles técnicos en base de datos, rutas y roles, el sistema alcanza un alto nivel de protección frente a amenazas comunes. Estas medidas permiten cumplir con los requisitos legales y técnicos necesarios para garantizar la seguridad y privacidad de los usuarios.