Blandskron

Informe de Auditoría de Seguridad – `auth-service`

1. Hallazgos Críticos (Alta Prioridad)

Autenticación insegura

- El endpoint `/login` compara directamente `email` y `password` contra MongoDB sin ningún hash.
- Riesgo: **Violación de confidencialidad** si hay acceso a la base de datos, ya que las contraseñas están en texto plano.

Mejora recomendada (OWASP A2 - Broken Authentication):

- Utilizar **hashing con sal** mediante `bcrypt` o `argon2` para almacenar y verificar contraseñas.

```
const bcrypt = require('bcrypt');

const user = await db.collection('users').findOne({ email });

if (user && bcrypt.compareSync(password, user.password)) {

  ...

}
```

Conexión a MongoDB expone credenciales

- Archivo `db.js` contiene la URI: `'mongodb://admin:admin123@localhost:27017'`.

Mejora recomendada (ISO 27001 A.9.2):

- Usar variables de entorno y `.env` para credenciales.
- Implementar control de acceso por roles en MongoDB.

Sin validación de entrada en el login

- No se validan los campos `email` y `password` antes de procesarlos.

Mejora recomendada (OWASP A1 - Injection):

- Agregar validaciones con `Joi`, `express-validator` o `zod` para evitar inyecciones y garantizar estructura.

No se usa HTTPS

- Los endpoints están definidos como `http://localhost:3000` en Postman y Swagger.

Mejora recomendada (OWASP A6 - Sensitive Data Exposure):

- Implementar TLS/SSL para cifrado en tránsito.

2. Hallazgos Moderados

Logout sin manejo real de sesión

- El endpoint `/logout` devuelve una respuesta estática sin invalidar tokens ni sesiones.

Mejora recomendada:

- Integrar manejo de sesiones o tokens JWT e invalidarlos con listas negras o expiraciones.

CORS abierto sin restricciones

- El uso de `app.use(cors())` permite todos los orígenes.

Mejora recomendada (OWASP API6 - Mass Assignment):

- Restringir orígenes confiables en producción.

```
app.use(cors({
  origin: ['https://tusitio.com'],
  methods: ['GET', 'POST']
}));
```

No hay control de rate limit ni bloqueo de fuerza bruta

- El login está abierto a pruebas masivas sin limitación.

Mejora recomendada (OWASP A7 - Identification and Authentication Failures):

- Añadir `express-rate-limit` y/o `helmet` para prevenir ataques de fuerza bruta.

Dependencias desactualizadas o sin verificación de seguridad

- Aunque actualizadas, no se audita la seguridad de paquetes `npm`.

Mejora recomendada (ISO 27001 A.12.6.1):

- Usar `npm audit`, `snyk`, `OWASP Dependency-Check` regularmente en CI/CD.

3. Hallazgos Menores

Falta logging seguro

- No se registran intentos fallidos de login ni se almacena IP de origen.

Mejora recomendada:

- Añadir un sistema de logging con rotación y ofuscación de información sensible.

4. Conformidad con Estándares

Estándar	Cumplimiento Actual	Recomendación
OWASP Top 10	❌ Parcial/Inseguro	Abordar A1, A2, A6, A7
ISO/IEC 27001:2013	❌ Bajo cumplimiento	Aplicar controles A.9 (acceso), A.12, A.14
GDPR (si aplica)	❌ Riesgo alto	No hay consentimiento ni cifrado

Recomendaciones Finales

1. **Hash de contraseñas y autenticación segura**
2. **Uso de variables de entorno**
3. **HTTPS obligatorio**
4. **Rate limit + CSRF protection + CORS restringido**
5. **Auditoría de dependencias periódica**
6. **Documentación actualizada de seguridad en Swagger (añadir seguridad a los endpoints)**