Análisis de Seguridad e Implementación de Autenticación

Proyecto: TRANSPUBLI CALI
Curso: Desarrollo de Software I
Versión: 1.0
Integrantes:Juan Camilo Minota Peña

Karen Jhulieth Lucumi Mosquera

1. Objetivo del Análisis

El objetivo de este documento es exponer los riesgos de seguridad identificados durante el desarrollo de TRANSPUBLI CALI y presentar las medidas adoptadas para mitigar vulnerabilidades, conforme a las recomendaciones de la fundación OWASP. También se detalla la implementación del sistema de autenticación y pruebas realizadas mediante Postman.

2. Evaluación de Riesgos (OWASP Top 10)

Riesgo Identificado	Descripción	Estado
A01: Control de acceso roto	Verificación de roles en rutas protegidas	Mitigado
A02: Fallas criptográficas	Almacenamiento de contraseñas con bcrypt	Mitigado
A05: Configuraciones de seguridad erróneas	Headers HTTP seguros, protección de CORS	Mitigado
A07: Fallos en control de acceso	Middleware para rutas privadas	Mitigado
A09: Logging y monitoreo insuficientes	Registro de eventos relevantes en consola y logs locales	En proceso

3. Sistema de Autenticación Implementado

- Se utilizó **JWT (JSON Web Token)** para gestionar sesiones de usuario de manera segura.
- Las contraseñas se almacenan con **bcrypt**, aplicando salting para proteger contra ataques de diccionario.
- Las rutas protegidas del backend requieren validación de token válido mediante middleware personalizado.

Flujo de Autenticación:

1. El usuario envía sus credenciales a `POST /api/login`.
2. El servidor valida la información y genera un token JWT.
3. El cliente almacena el token localmente y lo adjunta en futuras peticiones.
4. El middleware `verifyToken` comprueba el token en rutas privadas como `/api/usuarios` o `/api/emergencias`.

4. Pruebas Realizadas con Postman

Escenario	Endpoint	Resultado esperado	Estado
Login exitoso	POST /api/login	Token JWT, status 200	Aprobado
Acceso sin token	GET /api/usuarios	Error 401 (Unauthorized)	Aprobado
Acceso con token inválido	GET /api/usuarios	Error 403 (Forbidden)	Aprobado
Acceso con token válido	GET /api/usuarios	Lista de usuarios, status 200	Aprobado

5. Conclusión

El sistema TRANSPUBLI CALI integra mecanismos de seguridad alineados con los estándares actuales del desarrollo web, mitigando los riesgos más comunes según OWASP. La autenticación mediante JWT y el uso de bcrypt fortalecen la privacidad y protección de los datos del usuario. Las pruebas realizadas con Postman confirman el correcto funcionamiento del sistema de acceso seguro.