

Análisis de Seguridad y Mejoras para el Proyecto

Puntos Críticos de Seguridad Identificados

1. Inyección SQL

Uso de `mysqli_query()` sin consultas preparadas

Concatenación directa de variables en consultas SQL

Necesidad de usar `mysqli_real_escape_string()` o mejor aún, consultas preparadas

2. Autenticación y Autorización

Almacenamiento de contraseñas sin encriptar

Falta de validación de sesiones

Control de acceso a `admin.php` sin verificación de roles

3. Manejo de Archivos

Subida de imágenes sin validación de tipo/seguridad

Posible ejecución de archivos maliciosos

Rutas de archivos expuestas

4. Validación de Entrada

Falta de validación en formularios (registro, login, votos)

No verificación de tipos de datos

Posible XSS en visualización de datos

5. Gestión de Sesiones

Falta de regeneración de ID de sesión

Timeout de sesión no configurado

Datos sensibles en sesiones