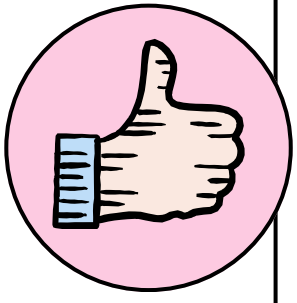
OWASP



A01: BROKEN ACCESS CONTROL

- Rutas expuestas sin requerir login
- Definidos fuera del middleware de autenticación
- /productos y /productos/tipos

A05: SECURITY MISCONFIGURATION

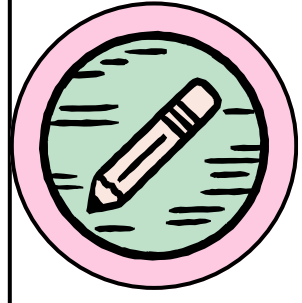
- El sistema permite subir cualquier archivo sin validar tipo ni extensión.
- Solo revisa que haya archivo y tamaño (5MB)
- Archivos guardados en disco público, accesibles por URL

A02: CRYPTOGRAPHIC FAILURES

- Datos personales y financieros en texto claro
- DPI, fechas de nacimiento, cuentas bancarias y salarios
- Base de datos sin cifrado de campos sensibles

A03: INJECTION, CROSS-SITE SCRIPTING

- Se inserta contenido dinámico en la interfaz sin escapado/sanitización, permitiendo JS malicioso
- Archivos subidos (HTML/JS) accesibles públicamente



A05: SECURITY MISCONFIGURATION

- Valores por defecto y ajustes inseguros que facilitan ataques sin no se cambian en producción
- Credenciales triviales en ejemplos (admin/secret)
- Ausencia de encabezados de seguridad HTTP