Instituto Tecnológico y de Estudios Superiores de Monterrey

Campus Santa Fe

Pruebas De Seguridad

29 de mayo de 2025

Objetivo

Describir el alcance, los criterios y la metodología de las pruebas de seguridad que se llevarán a cabo en la aplicación Visual Transformers, con el fin de identificar vulnerabilidades comunes, verificar controles y garantizar la protección de datos y la integridad del sistema.

Alcance

2.1 Módulos y funcionalidades a evaluar
– Autenticación y registro de usuarios
– Gestión de sesiones y cookies
– Endpoints de inferencia (/api/inference-jobs/)
– Carga y procesamiento de archivos (subida de imágenes)
– Gestión de errores y manejo de respuestas

2.2 Entornos
– Desarrollo (localhost)
– Preproducción
– Producción

2.3 Herramientas
– Navegadores: Google Chrome, Mozilla Firefox
– Cliente HTTP: Postman, cURL
– Escáneres de seguridad: OWASP ZAP, Nikto
– Análisis de dependencias: OWASP Dependency-Check

Normativa y herramientas

3.1 Normativa de referencia
– OWASP Top 10 (2021)
– OWASP ASVS v4 (niveles 1 y 2)
– Guías de seguridad de Django

3.2 Herramientas automáticas
– OWASP ZAP
– Nikto
– Burp Suite (Community Edition)

3.3 Herramientas manuales
– Revisión de cabeceras HTTP en DevTools
– Pruebas de inyección con Postman/cURL
– Comprobación de políticas CORS

Criterios de aceptación

– Todos los endpoints protegidos deben rechazar peticiones sin credenciales o con credenciales inválidas (401/403).
– Las contraseñas deben transmitirse y almacenarse de forma segura (HTTPS/TLS, hashing robusto).
– Cookies de sesión marcadas como Secure, HttpOnly y SameSite=strict.
– No debe existir vulnerabilidad de XSS ni CSRF.
– La aplicación debe ser resistente a inyección SQL.
– Carga de archivos restringida por tipo (png, jpg, jpeg) y tamaño máximo configurado.
– Presencia de cabeceras de seguridad HTTP: CSP, HSTS, X-Frame-Options, X-Content-Type-Options.
– Dependencias libres de vulnerabilidades críticas.

Plan de pruebas

5.1 Pruebas manuales

Caso de prueba: AUTENTICACIÓN NO AUTORIZADA
• Objetivo: Verificar que los endpoints privados rechacen accesos sin credenciales.
• Pasos:
a) Hacer petición GET a /api/inference-jobs/ sin token.
b) Repetir con token inválido o expirado.
• Resultado esperado: Respuesta 401 o 403 en ambos casos.

Caso de prueba: MANEJO DE SESIONES Y COOKIES
• Objetivo: Comprobar atributos de seguridad en las cookies de sesión.
• Pasos:
a) Iniciar sesión y revisar cookies en DevTools → Application > Cookies.
• Resultado esperado: Cookies con Secure, HttpOnly y SameSite=strict.

Caso de prueba: INYECCIÓN SQL
• Objetivo: Detectar vulnerabilidades de inyección SQL en formularios.
• Pasos:
a) Enviar payload `admin' OR '1'='1` en campo de usuario o contraseña.
• Resultado esperado: Acceso denegado (no returns datos sensibles ni éxito de autenticación).

Caso de prueba: CARGA DE ARCHIVOS NO PERMITIDOS
• Objetivo: Validar restricción de tipo y tamaño de ficheros.
• Pasos:
a) Intentar subir un archivo `.exe` o imagen > tamaño máximo (por ej. 10 MB).
• Resultado esperado: Rechazo de la carga con mensaje de error claro (413 o propio).

Caso de prueba: CABECERAS DE SEGURIDAD HTTP
• Objetivo: Verificar configuración de cabeceras de protección.
• Pasos:
a) Inspeccionar cabeceras en respuesta HTTPS via DevTools → Network.

• Resultado esperado: Presencia de CSP, HSTS, X-Frame-Options y X-Content-Type-Options con valores adecuados.

Registro de Resultados

Para cada caso de prueba se anotará:
– Fecha de ejecución
– Nombre del evaluador
– Estado
– Observaciones detalladas

Nombre de prueba	Fecha de ejecución	Nombre del evaluador	Estado	Observaciones
AUTENTICACIÓN NO AUTORIZADA	09/06/2025	Mauricio	Aprobado	El endpoint rechazó correctamente peticiones sin credenciales con código 401.
MANEJO DE SESIONES Y COOKIES	09/06/2025	Mauricio	Aprobado	Las cookies de sesión incluyen Secure, HttpOnly y SameSite=strict.
INYECCIÓN SQL	09/06/2025	Mauricio	Aprobado	La aplicación rechazó correctamente el payload sin exponer datos sensibles.
CARGA DE ARCHIVOS NO PERMITIDOS	09/06/2025	Mauricio	Fallido	El sistema permitió subir archivos no permitidos, indicando falta de validación de tipo.
CABECERAS DE SEGURIDAD HTTP	09/06/2025	Mauricio	Aprobado	Se encontraron las cabeceras CSP, HSTS, X-Frame-Options y X-Content-Type-Options configuradas

				correctamente.