| **ITEM** | **CATEGORIA** | **CHEKLIST (Qué se verifica?** | **¿Cómo se verifica?** |
| --- | --- | --- | --- |
| A1 | Inyección | ¿Se puede acceder a los datos con seguridad?  ¿Están bien definidos los roles ? | Ingresar desde la ruta de login desde la aplicación y validar que esté activo el https desde el navegador y después de ingresar validar el network (consola de desarrollador) u otra herramienta que permita capturar la transmisión de datos (SELENIUM).  Verificar desde la cuenta del administrador de la aplicación si se puede crear usuarios con diferentes roles y autenticarse luego. (posteriormente pasar la verificación número 1) |
| A2 | Pérdida de autenticación y gestión de sesiones | ¿Las sesiones expiran correctamente?  ¿Se puede acceder sin login desde otra pestaña o equipo?  ¿Se puede forzar el login sin credenciales? | Iniciar sesión en WordPress y cierra el navegador. Luego, vuelve a abrir y revisa si la sesión sigue activa.  Usar Selenium para automatizar el cierre y reapertura de sesión.  Verificar si puedes copiar cookies de sesión (con extensiones del navegador o dev tools) y usarlas en otro navegador para simular robo de sesión. |
| A3 | Datos sensibles accesibles | ¿Se están transmitiendo datos sensibles (contraseñas, tarjetas) en texto plano?  ¿Hay datos personales visibles sin login? | Usar la consola del navegador (Network) y JMeter para interceptar peticiones con credenciales y ver si están encriptadas.  Navegar a URLs sensibles sin autenticar (por ejemplo: /wp-admin/, /cart, /checkout) y revisa si se muestran datos. |
| A4 | Entidad externa de XML (XXE) | ¿Se usan entradas XML que puedan ser manipuladas para acceder a archivos o servicios internos? | Nuestra tienda MiniShop no permite importar productos vía XML, pero si lo hiciera se debe revisar si se puede subir un XML modificado con una entidad externa.  Usar JMeter o una herramienta como Burp Suite para probar cargas maliciosas si hay carga de archivos XML. |
| A5 | Control de acceso inseguro | ¿Los usuarios pueden acceder a páginas o funciones restringidas (como /wp-admin/)?  ¿Pueden realizar acciones como modificar productos sin ser administradores? | Acceder como usuario normal y prueba entrar a rutas administrativas directamente.  Usar Selenium para automatizar el acceso a menús o acciones que deberían estar ocultas (como editar productos o ver reportes de ventas). |
| A6 | Configuración de seguridad incorrecta | ¿Están activos plugins innecesarios?  ¿Está activo el modo debug en producción?  ¿Se muestran errores detallados? | En el archivo wp-config.php, revisa si hay líneas como define( 'WP\_DEBUG', true ); (debe estar en false).  Visitar URLs erróneas y revisar si se muestran mensajes de error con detalles del sistema.  Usar JMeter o navegador para probar endpoints no documentados como /phpinfo.php. |
| A7 | Cross site scripting (XSS) | ¿Es posible inyectar scripts (por ejemplo, en formularios, comentarios o campos de productos)? | Ingresar <script>alert("XSS")</script> en formularios como el de contacto, búsqueda, comentarios o reseñas de productos.  Usar Selenium para automatizar la inyección y ver si aparece la alerta al cargar la página. |
| A8 | Decodificación insegura | ¿Hay campos que acepten objetos codificados que puedan ser modificados para ejecutar código? | Revisar si hay cookies codificadas en Base64 o JSON y prueba a modificarlas.  Usar JMeter para interceptar una cookie o parámetro y alterarlo (por ejemplo, cambiar el rol a admin en una cookie serializada). |
| A9 | Componentes con vulnerabilidades | ¿Se usan plugins o temas con vulnerabilidades conocidas? | Usar un escáner como [WPScan](https://wpscan.com/) para analizar el sitio y ver qué plugins y versiones tienen vulnerabilidades.  También puedes revisar manualmente la lista de plugins desde /wp-admin/plugins.php y buscar sus versiones en sitios como CVE Details. |
| A10 | Insuficiente monitorización y registro | ¿Se registran los accesos fallidos, cambios importantes o acciones críticas?  ¿Hay alertas ante múltiples accesos erróneos? | Realiza múltiples intentos de login fallidos y observa si el sistema los bloquea o registra.  Accede al panel de administración y revisa si hay un log o plugin instalado para auditoría como **WP Security Audit Log**. |