DOCUMENTACIÓN DEL REPORTE DE RESULTADOS

Fecha de ejecución: 20/06/2025

Tester: Daniel Hervás Muñoz

Herramientas utilizadas: Node.js, Typescript y Playwright

ÍNDICE

1. Resumen

Se ejecutaron 46 casos de prueba manuales sobre el sistema, abarcando funcionalidades de login, registro de usuarios, validaciones de formularios, manejo de errores y aspectos básicos de seguridad. Durante la ejecución, se identificaron 11 casos que no cumplieron con el resultado esperado según los criterios definidos en el plan de pruebas.

2. Errores detectados

A continuación desgloso los errores detectados en el Test Plan dividiendolo en grupos y el número de errores, toda la información está en la excel de Test Cases.

2.1. Errores detectados durante el Test Plan:

- **Registro de usuarios (4 errores) :**

ID	Nombre del Caso	Pasos a seguir	Datos de entrada	Resultado esperado	Resultado real	Estado
TC-R04	Registro con contraseña corta	Llenar todos los campos y usar '123' como contraseña	PRUEBA / TC-R04 / user02 / 123	Rechazo si hay validación de longitud. Contraseña demasiado corta o poco segura.	Registro exitoso, se permite contraseña corta	FAIL
TC-R07	Campo Username con demasiados caracteres	Username con 300 letras	a...a / pass123	Rechazo por longitud excesiva	No muestra ningún mensaje y registra el usuario correctamente con los 300 caracteres.	FAIL
TC-R08	Campo Password con demasiados caracteres	Password con 300 letras	contra300 / a...a	Rechazo por longitud excesiva	mensaje y registra el usuario correctamente con los 300 caracteres de contraseña.	FAIL
TC-R11	Espacios en username	Registrar un usuario con espacios entre caracteres, 'mi usuario' como username	mi usuario / pass123	Rechazo o arreglo del input sin espacios.	Registra el usuario con el espacio entre caracteres	FAIL

- **Validaciones de formularios (5 errores) :**

ID	Nombre del Caso	Pasos a seguir	Datos de entrada	Resultado esperado	Resultado real	Estado
TC-V03	Espacios en username	Usar 'mi usuario' como username	mi usuario	Rechazo o arreglo del input sin espacios.	No hay validación; formulario acepta espacios	FAIL
TC-V05	Username con caracteres especiales	Usar 'user<script>' como username	user<script>	Escapar caracteres o rechazar input	Formulario permite caracteres especiales sin validación.	FAIL
TC-V09	Contraseña muy larga (300 caracteres)	Ingresar una contraseña de 300 caracteres al registrar.	a...a	Mensaje de error por longitud excesiva	Sin mensaje de restricción	FAIL
TC-V10	Username muy largo (300 caracteres)	Ingresar un username de 300 caracteres.	a...a	Mensaje de error por longitud excesiva	Sin mensaje de restricción	FAIL
TC-V11	Campos con espacios al final o al inicio	Escribir user10 con espacios antes y después	Marcos / Gil / user10 / pass123	Mensaje de error por espacios en el usuario	Sin mensaje de restricción	FAIL

- **Seguridad (2 errores) :**

ID	Nombre del Caso	Pasos a seguir	Datos de entrada	Resultado esperado	Resultado real	Estad
TC-S01	Inyección XSS en campo username	En el formulario register, Usar <script>alert(1)</script> como username	<script>alert(1)</script> / pass123	Campo escapa HTML o rechaza.	el <script>alert(1)</script> está siendo incrustado directamente en el HTML sin escapar, lo que muestra una vulnerabilidad XSS	FAIL
TC-S07	Autocompletado de contraseña	Observar atributo autocomplete		Autocomplete debe estar desactivado	El campo de contraseña no incluye el atributo autocomplete="off", pero el navegador no sugiere autocompletado.	FAIL

3. Conclusión

Durante la ejecución del plan de pruebas sobre el sistema de registro y autenticación de usuarios, se verificaron tanto funcionalidades básicas como aspectos de seguridad y validación de formularios.

3.1 Aspectos positivos

- **El flujo básico de registro y login funciona correctamente** cuando se utilizan datos válidos.
- El sistema **rechaza intentos básicos de SQL Injection**, incluyendo payloads clásicos y booleanos, demostrando protección a nivel backend.
- El **campo de contraseña** es del tipo adecuado (<input type="password">), lo que evita que se muestre el texto ingresado.

3.2 Fallos críticos detectados

Se identificaron varios errores graves que comprometen la **seguridad**, **integridad de datos** y **usabilidad** del sistema:

1. **Validaciones de formularios débiles o ausentes:**
    - El sistema permite el registro con **contraseñas demasiado cortas** (ej: "123"), lo cual no cumple estándares mínimos de seguridad.

- No hay límite ni restricción de longitud en campos como **username y password** (se aceptaron entradas de más de 300 caracteres sin errores).

- **No hay validación para espacios innecesarios** en campos ("mi usuario" fue aceptado como nombre de usuario sin limpieza o advertencia).

- Se aceptan **caracteres especiales** en el nombre de usuario (<script>), lo que representa un riesgo potencial.

2. **Vulnerabilidad XSS (Cross-Site Scripting):**

    - Se logró registrar un usuario con código HTML/JS embebido (<script>alert(1)</script>), el cual fue insertado sin escape en el DOM. Esto representa un **riesgo severo de ejecución de código malicioso**.

3. **Omisión de controles de autocompletado:**

    - El campo de contraseña **no especifica** autocomplete="off", lo que puede llevar a que navegadores recuerden credenciales en formularios inseguros, afectando la privacidad del usuario.

3.3 Recomendaciones

- Implementar **validaciones tanto en frontend como backend** para longitud, contenido y formato de los campos.

- Rechazar inputs que contengan **espacios innecesarios** o **caracteres especiales peligrosos**.

- Escapar correctamente cualquier entrada del usuario que se renderice en HTML, para prevenir XSS.

- Agregar el atributo autocomplete="off" en campos sensibles como contraseñas y datos personales.

- Aplicar políticas de seguridad más estrictas para contraseñas (mínima longitud, mezcla de caracteres, etc.).