Juan David Cardona
Melisa Meneses

Informe de Defectos

➔ **Defecto N°1:**

Identificador: DEF001

Título y resumen del defecto: Creación de usuarios a través del servicio web al enviar un JSON vacío.
Fecha del informe: 28 de febrero de 2023
Organización: Aliexpress.
Emisora: Equipo de Pruebas Sofka U
Autor: Juan David Cardona
Elemento de configuración: Servicio web de creación de usuarios
Entorno: Postman
Paso a paso que permite replicar el defecto:

- Crear la nueva solicitud de tipo POST.
- Ingresar la ruta del endpoint a users.
- Ingresar en el body un json vacío.
- Hacer click en Send.

Fase del ciclo de vida en la que se observó el defecto: Pruebas de sistema.
Resultados esperados: El servicio web debe rechazar una solicitud con un JSON vacío y devolver un mensaje de error.
Resultados reales: Se muestra el mensaje 201 Created que crea un nuevo registro únicamente con un id.
Alcance o grado de impacto del defecto en los intereses de las partes interesadas: El defecto tiene un impacto medio ya que puede afectar en la capacidad de almacenamiento de datos del servidor guardando registros vacíos.
Impacto absoluto en el desarrollo: El defecto requiere la corrección del código en el servicio web de creación de usuarios y la realización de pruebas adicionales para asegurar que no se hayan introducido otros problemas.
Urgencia/Prioridad para arreglar: El defecto tiene una prioridad media y debe ser corregido en la siguiente versión del software.

➔ **Defecto N°2:**

Identificador: DEF002

Título y resumen del defecto: Creación de nuevos usuarios con caracteres numéricos en el campo name.
Fecha del informe: 28 de febrero de 2023
Organización: AliExpress.
Emisora: Equipo de Pruebas Sofka U.
Autor: Melissa Meneses Acevedo
Elemento de Configuración: Servicio web de creación de usuarios
Entorno: Postman.
Paso a paso para replicar el defecto:

- Abrir Postman.
- Crear la nueva solicitud de tipo POST
- Ingresar la ruta del endpoint a users.
- Ingresar en el Body un json con caracteres numéricos en el campo name
- Hacer click en Send.

.

Fase del ciclo de vida en la que se observó el defecto: Pruebas de integración de componentes.
Resultados esperados:
Se espera un mensaje de error indicando que el campo name no puede contener caracteres numéricos.
Resultados Reales: Se muestra el mensaje 201 Created que crea un nuevo registro de usuario con el campo name numérico.
Alcance o grado de impacto del defecto en los intereses de las partes interesadas:
El defecto tiene un alcance moderado,ya que podría afectar las funcionalidades del sistema en un futuro al querer filtrar a un usuario mediante un nombre que fue almacenado con caracteres inválidos.
I**mpacto absoluto en el desarrollo**:
El impacto absoluto en el desarrollo es bajo, ya que el problema está limitado al campo de validación de entrada de nombre de usuario y puede ser resuelto con una actualización del software.
Urgencia/Prioridad para arreglar:
El defecto tiene una prioridad baja, pero puede generar complicaciones a la hora de solicitar la información de nombre de un usuario , por lo que se recomienda corregirlo a la brevedad.

➔ **Defecto N°3:**

Identificador: DEF003
Título y resumen del defecto que se informa: Actualización de información de usuario con ID inválido permitida en el servicio
Fecha del informe: 28 de febrero de 2023
Organización: AliExpress.
Emisora: Equipo de Pruebas Sofka U.
Autor: Juan David Cardona
Elemento de Configuración: Servicio web de creación de usuarios
Entorno: Postman.
Paso a paso que permita replicar el defecto:

- Abrir Postman.
- Crear la nueva solicitud de tipo PUT
- Ingresar la ruta del endpoint a usuarios con el id de usuario invalido.
- Ingresar en el Body un json con los datos a actualizar.
- Hacer click en Send.

Fase del ciclo de vida en la que se observó el defecto: Pruebas de sistema.
Resultados esperados: Si se envía una solicitud de actualización de información de usuario con un ID inválido, el servicio debería mostrar un mensaje de error y no permitir la actualización de la información de usuario.
Resultados reales: El servicio acepta la solicitud y no muestra ningún mensaje de error, y actualiza la información como si existiera un usuario con este id.

Alcance o grado de impacto del defecto en los intereses de las partes interesadas:
El defecto puede tener un impacto alto en la integridad de los datos de los usuarios porque podría estar actualizando la información de otro usuario.
Impacto absoluto en el desarrollo:
El defecto requiere una corrección en el código del servicio para asegurar que las solicitudes con IDs inválidos sean rechazadas correctamente.
Urgencia/prioridad para arreglar:
La corrección del defecto debe tener una prioridad alta debido a su impacto en la integridad de los datos del usuario y en la satisfacción del usuario por lo que debería ser solucionado antes de la siguiente versión del software.

➔ **Defecto N°4**:

Identificador: DEF004
Título y resumen del defecto que se informa: Actualización de un id de usuario existente , al que ya se le ha asignado un id anteriormente.
Fecha del informe: 28 de febrero de 2023
Organización: AliExpress.
Emisora: Equipo de Pruebas Sofka U.
Autor: Melissa Meneses Acevedo.
Elemento de configuración: Servicio web de creación de usuarios
Entorno: Postman.
Paso a paso para replicar el defecto:

- Abrir Postman.
- Crear la nueva solicitud de tipo PUT
- Ingresar la ruta del endpoint a usuarios con el id del usuario existente.
- Ingresar en el Body un json con los datos a actualizar, especificando el id al que se desea cambiar.
- Hacer click en Send.

Fase del ciclo de vida: Pruebas de Sistema.
Resultados esperados: El servicio debería mostrar un mensaje de error indicando que el ID proporcionado no es posible actualizarlo porque a ese usuario ya tenía un id asociado .
Resultados reales: El servicio muestra el mensaje 201 Created que actualiza el id que se le había asignado antes a ese usuario .
Alcance o grado de impacto del defecto en los intereses de las partes interesadas: Este defecto tiene un alto impacto, ya que puede provocar la pérdida de datos del usuario y afectar la integridad de la base de datos.
Impacto absoluto en el desarrollo: El impacto en el desarrollo es alto, este defecto requiere una corrección en el código del servicio web para que no permita actualizar el id de un usuario que ya tiene un id asociado .
Urgencia/prioridad para arreglar: Este defecto tiene una prioridad alta y se recomienda que sea solucionado en la próxima versión del software, ya que puede afectar la integridad de los datos asociados al usuario existente

➔ **Defecto N°5**:

Identificador: DEF004
Título y resumen del defecto: Creación de contraseñas inseguras en el módulo de registro de Aliexpress.
Fecha del informe: 28 de febrero de 2023
Organización: AliExpress.
Emisora: Equipo de Pruebas Sofka U.
Autor: Melissa Meneses Acevedo.
Elemento de configuración: Servicio web de creación de usuarios
Entorno: Postman.
Paso a paso que permita replicar el defecto:

- Acceder al módulo de registro de Aliexpress
- Ingresar información requerida para el registro, incluyendo la contraseña
- Crear una contraseña insegura (por ejemplo, "password" o "123456")
- Completar el registro y verificar que la contraseña insegura es aceptada y almacenada en el sistema

Fase del ciclo de vida en la que se observó el defecto: Pruebas de sistema.
Resultados esperados: Se espera que el sistema no permita la creación de contraseñas inseguras y muestre un mensaje de error al usuario si intenta hacerlo.
Resultados reales: El sistema permite la creación de contraseñas inseguras sin mostrar ningún mensaje de error.
Alcance o grado de impacto del defecto en los intereses de las partes interesadas: Este defecto puede poner en riesgo la seguridad de la información de los usuarios de Aliexpress, ya que las contraseñas inseguras son fáciles de adivinar o hackear. Por lo tanto, el impacto en los intereses de los clientes y de la empresa es alto.
Impacto absoluto en el desarrollo: El defecto requerirá la implementación de medidas de seguridad adicionales en el módulo de registro de Aliexpress, lo que puede implicar cambios significativos en el código y un aumento en el tiempo de desarrollo.
Urgencia/prioridad para arreglar: Este defecto tiene una alta urgencia y prioridad, ya que afecta la seguridad de los datos de los usuarios. Se debe corregir lo antes posible para minimizar el riesgo de violación de datos.