

Reporte de errores de OrangeHRM

Proyecto: OrangeHRM

versión 1.0.0Historia de revisiones

| Versión | Autor(es) | Descripción | Fecha |
| --- | --- | --- | --- |
| 1.0.0 | Alejandra Kantun Chim | Creación del documento | 05/11/2023 |

# 

[**1 Uso del documento**](#_ijg79zk7n166) **3**

[**2 Descripción de errores**](#_lz7urnrgkl8l) **3**

[2.1 Errores de interfaces](#_woa5ea4a3mpy) 3

# 

# 1 Uso del documento

El documento se usará para poder hacer evidencia de los errores presentes dentro del portal web de OrangeHRM el cual cuenta con la siguiente dirección URL [https://opensource-demo.orangehrmlive.com/web/index.ph](https://opensource-demo.orangehrmlive.com/web/index.php)p, siendo este documento un análisis de los errores de los módulos funcionales.

# 2 Referencia documental

Este documento está basado en el uso de formato basado en los estándares planteados en el estándar de calidad ISO 9001.

# 3 Descripción de errores

## 3.1 Recuperar contraseña de usuario inexistente

**Id de error**: 1

**Id de caso de prueba**: 9

**Modulo:** Módulo de recuperación de contraseña

**URL del problema:** https://opensource-demo.orangehrmlive.com/web/index.php/auth/requestPasswordResetCode

**Gravedad:** Baja

**Prioridad:** media

**Reportado por:** Alejandra Kantun Chim

**Reportado en:** 05/11/2023

**Razon:** Defecto funcional

**Ambiente:** Sistema operativo Windows, navegador Google Chrome, Test.

**Descripción:**

En el módulo de resetear contraseña permite que se hagan solicitudes de reseteo de contraseña a usuarios inexistentes, esto genera un manejo de gasto de recursos de consultas de solicitudes HTTP.

**Pasos a reproducir:**

1. En el modulo de contraseña en el campo de username ingresar un usuario no existente en la plataforma.

**Resultado esperado:**

El módulo de resetear contraseña debería de validar si es que el usuario se encuentra en la plataforma debido a que esto podría generar que sí se permiten realizar peticiones al servidor con usuarios inexistentes hacer que el módulo sea usado como punto vulnerable de un ataque DoS o DDoS intentando resetear múltiples veces las contraseñas de usuarios inexistentes.

**Evidencia:**

Resetear\_contraseña\_fail.mp4