10: MISHANDLING OF EXCEPTIONAL CONDITIONS (MANEJO INCORRECTO DE EXCEPCIONES)

CRISTIAN MATEOS VEGA

DESCRIPCIÓN GENERAL

La gestión inadecuada de condiciones excepcionales en el software ocurre cuando los programas no logran prevenir, detectar ni responder a situaciones inusuales e impredecibles, lo que provoca fallos, comportamientos inesperados y, en ocasiones, vulnerabilidades. Esto puede implicar una o más de las siguientes tres fallas:

- la aplicación no previene la ocurrencia de una situación inusual
- no la identifica en el momento en que ocurre
- responde de forma deficiente o nula a la situación posteriormente.

COMO NOS PUEDE HACER DAÑO

El manejo incorrecto de excepciones puede ser explotado por atacantes de varias formas:

Tipo de daño	Ejemplo práctico
Exposición de información sensible	Mostrar stack trace revela nombres de archivos, rutas del servidor, versiones de librerías.
Facilitar ataques posteriores	Un atacante puede usar la información para planear SQL Injection, RCE o ataques de directorio traversal.
Caída del sistema o DoS	Errores no controlados pueden hacer que la app deje de responder, afectando disponibilidad.
Escalada de privilegios	Errores mal manejados pueden permitir que un usuario obtenga permisos que no debería.

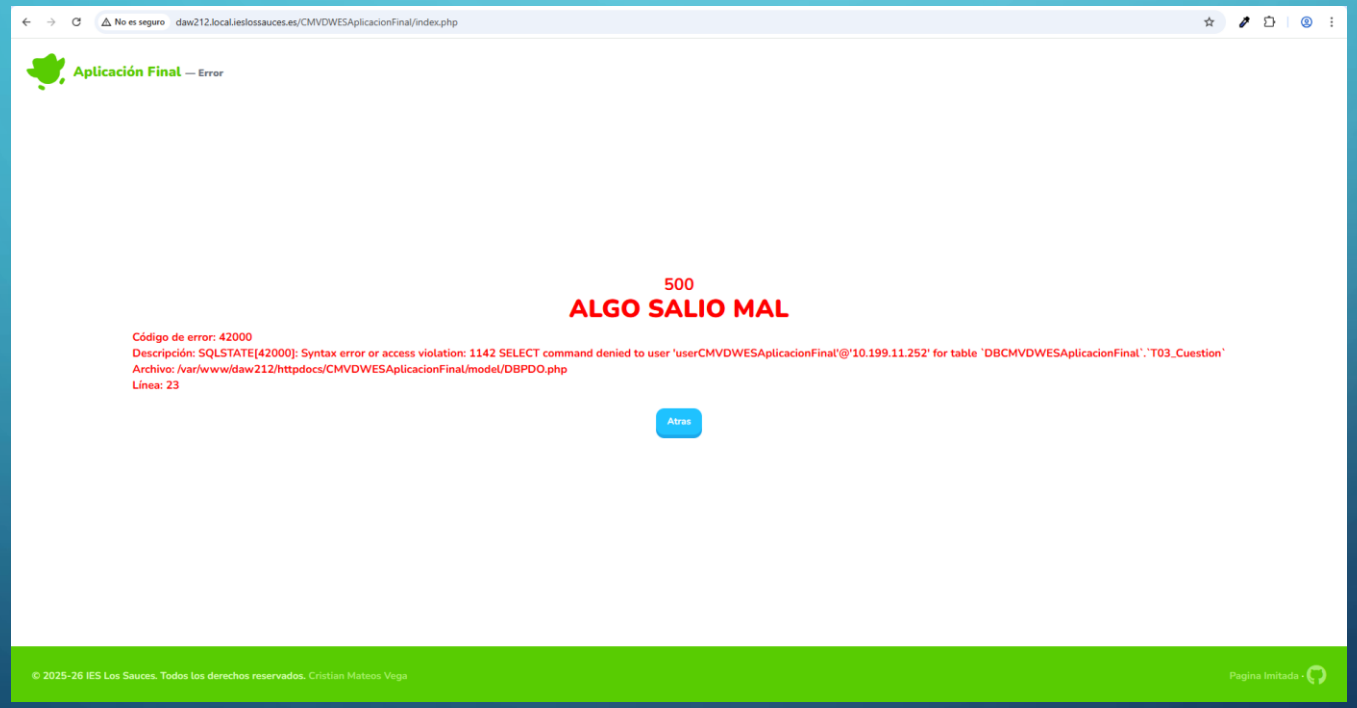
COMO SOLUCIONARLO

La prevención y solución se basa en controlar errores correctamente, proteger información sensible y auditar eventos críticos.

Estrategia	Cómo aplicarla
Mensajes de error genéricos al usuario	Mostrar mensajes simples como “Ocurrió un error. Inténtelo más tarde.”
Registro seguro de errores	Guardar los detalles del error en un log seguro, accesible solo para administradores.
Validación y manejo de excepciones	Usar bloques try/catch y prever errores comunes (conexión a DB, entrada de usuario, API externas).
No exponer información interna	Nunca mostrar stack traces, rutas de archivos, contraseñas o claves en el frontend.
Auditoría y monitoreo	Revisar logs regularmente y alertar ante errores críticos o patrones repetitivos.
Pruebas de estrés y manejo de errores	Simular errores y verificar que la app no falle de manera insegura.

COMO ESTÁ NUESTRA APP EN ESTE ASPECTO?

En nuestra app tenemos una página de error que se muestra cuando hay un error con la base de datos, pero está mal hecho porque da la información a todo el mundo sobre el problema y esa información se puede utilizar para atacar la app. Además, otro tipo de excepciones, no están controladas, rompiendo la aplicación.



GRACIAS POR SU ATENCIÓN!