



Ejercicio Práctico

 **Título:** Identificación de Buenas Prácticas en la Seguridad de una API RESTful

Objetivo:

Identificar errores comunes en una API RESTful y proponer buenas prácticas básicas para reforzar su seguridad y monitoreo.

Escenario:

Estás revisando la configuración de seguridad de una API RESTful utilizada por una aplicación web. En el análisis inicial, detectas los siguientes aspectos:

1. La API muestra mensajes de error completos al usuario, incluyendo detalles técnicos y trazas.
 2. No hay sistema implementado para revisar logs de acceso o errores.
 3. No se usan tokens de autenticación para acceder a los endpoints protegidos.
 4. Los errores 401 y 403 no se diferencian correctamente en las respuestas.
-

Actividades:

1. **Identifica el riesgo o mala práctica presente en cada uno de los 4 puntos.**
 2. **Propón una medida básica de mitigación o mejora para cada punto.**
 3. **Justifica brevemente por qué la medida sugerida mejora la seguridad.**
-

Formato sugerido para la respuesta:

Problema Detectado	Medida Correctiva Propuesta	Justificación
Mensajes de error con trazas visibles		
Ausencia de revisión de logs		
Falta de tokens de autenticación		
Respuestas de error poco diferenciadas entre 401 y 403		

Recomendaciones:

- Considera el uso de mensajes de error genéricos, tokens JWT, herramientas SIEM o auditoría básica de logs.
 - No se requiere configuración avanzada, solo **buenas prácticas básicas** de seguridad.
-

Solución Modelo – Ejercicio Práctico


 **Escenario:** Evaluación básica de una API RESTful expuesta sin controles de seguridad adecuados.

Tabla de Respuesta

Problema Detectado	Medida Correctiva Propuesta	Justificación
Mensajes de error con trazas visibles	Mostrar mensajes de error genéricos	Evita divulgar detalles internos que puedan ser aprovechados por atacantes.
Ausencia de revisión de logs	Implementar auditoría básica de logs (accesos y errores)	Permite detectar accesos no autorizados o comportamientos anómalos.
Falta de tokens de autenticación	Usar tokens JWT o API Keys en endpoints protegidos	Asegura que solo usuarios autenticados puedan acceder a recursos sensibles.

Respuestas de error poco diferenciadas entre 401 y 403

Configurar correctamente los códigos de respuesta HTTP

Ayuda a identificar si el fallo es por falta de autenticación (401) o permisos (403), facilitando la administración y el monitoreo.

Comentario Final

Estas prácticas permiten establecer una **base mínima de seguridad para cualquier API RESTful**, facilitando el monitoreo, evitando fugas de información y reforzando el control de accesos. Son pasos sencillos pero fundamentales en una estrategia de **mejora continua en ciberseguridad**.
