Informe de Desarrollo

Proyecto: Inventario de Motos | Desarrollador: Sebastian Ibarra | Fecha: 27/11/2025

1. Descripción del Desarrollo

El proyecto **Inventario de Motos** es un sistema web de gestión desarrollado en PHP 8 y MySQL. Su objetivo principal es administrar el inventario de un taller o concesionario de motocicletas.

Características Principales:

- **Gestión de Inventario (CRUD):** Funcionalidad completa para Crear, Leer, Actualizar y Eliminar registros de motocicletas y categorías.
- **Panel de Administración:** Dashboard con estadísticas en tiempo real sobre el stock y valor del inventario.
- **Seguridad:** Sistema de autenticación robusto y protección contra vulnerabilidades web comunes.
- **Diseño:** Interfaz moderna y responsiva con una paleta de colores personalizada (Naranja/Gris Oscuro).

2. Resultados del Análisis de Calidad

Se realizó una auditoría de seguridad y calidad del código, identificando áreas críticas que requerían intervención para garantizar la integridad y seguridad de la aplicación.

Hallazgos Principales:

- **Vulnerabilidad a SQL Injection:** El código original concatenaba variables directamente en las consultas SQL.
- **Riesgo de XSS (Cross-Site Scripting):** Los datos de entrada no se sanitizaban adecuadamente antes de mostrarse.
- **Falta de Protección CSRF:** Los formularios no contaban con tokens de verificación, permitiendo ataques de falsificación de solicitudes.
- **Gestión de Sesiones:** La verificación de sesión estaba dispersa y era inconsistente en varios archivos.

3. Tabla Comparativa de Errores Corregidos

Vulnerabilidad / Error	Estado Anterior	Estado Actual (Corregido)
SQL Injection	Consultas directas vulnerables (ej. `"SELECT * FROM t WHERE id = $id"`)	Uso de **Prepared Statements** con PDO y validación estricta de IDs.

Vulnerabilidad / Error	Estado Anterior	Estado Actual (Corregido)
Cross-Site Scripting (XSS)	Impresión directa de variables (ej. `echo $_POST['nombre']`)	Sanitización de entradas y escape de salidas mediante funciones `htmlspecialchars` centralizadas.
CSRF	Formularios sin protección	Implementación de **Tokens Anti-CSRF** en todos los formularios de escritura (POST).
Seguridad de Sesión	Checks manuales repetitivos	Función centralizada `require_login()` y regeneración de IDs de sesión.
Mantenibilidad	Código de seguridad duplicado en cada archivo	Creación de `includes/security.php` para centralizar toda la lógica de seguridad.

4. Conclusiones Personales

> El proceso de refactorización y aseguramiento del proyecto "Inventario de Motos" ha transformado una aplicación funcional pero vulnerable en un sistema robusto y seguro.
>
> La implementación de una capa de seguridad centralizada (`security.php`) no solo corrige las vulnerabilidades críticas actuales, sino que establece un estándar para el desarrollo futuro, facilitando el mantenimiento y reduciendo la deuda técnica. La adopción de buenas prácticas como el uso de PDO y tokens CSRF asegura que el sistema cumpla con los estándares modernos de desarrollo web.
