مهمة تصميم الأمان لنظام إدارة المخزون

1. الهدف:

تصميم وتنفيذ آليات الأمان لحماية البيانات والمستخدمين من التهديدات والهجمات الإلكترونية.

2. المكونات:

أ. حماية البيانات:

تشفير البيانات: تشفير البيانات المخزنة والمرسلة باستخدام تقنيات مثل AES-256 وSSL/TLS.

حماية كلمات المرور: تخزين كلمات المرور بشكل مشفر باستخدام تقنيات مثل bcrypt أو Argon2.

ب. إدارة الوصول:

التوثيق (Authentication): استخدام MFA (التحقق متعدد العوامل) وOAuth 2.0 للتحقق من هوية المستخدمين.

التحكم في الصلاحيات (Authorization): تحديد أدوار وصلاحيات دقيقة للمستخدمين لضمان الوصول المناسب.

ج. حماية التطبيق:

الوقاية من SQL Injection: استخدام استعلامات محضرة (Prepared Statements).

الوقاية من XSS وCSRF: تعقيم المدخلات وتوليد رموز CSRF.

د. حماية الشبكة:

جدران الحماية (Firewall): تكوين جدران حماية لحماية النظام من الهجمات.

كشف التسلل (IDS/IPS): استخدام أدوات لمراقبة الأنشطة المشبوهة.

هـ. اختبار الأمان:

اختبارات اختراق (Penetration Testing): اختبار النظام بحثًا عن ثغرات أمنية.

تحليل الكود: استخدام أدوات مثل SonarQube لاكتشاف الثغرات البرمجية.

3. خطوات التنفيذ:

1. تحليل التهديدات: تحديد المخاطر الأمنية المحتملة.

2. تنفيذ الأمان: تطبيق تدابير التشفير، إدارة الوصول، والتحقق من المدخلات.

3. اختبار الأمان: إجراء اختبارات اختراق وتحليل الكود.

4. المراقبة المستمرة: متابعة النظام واكتشاف أي تهديدات جديدة.

4. الأدوات المستخدمة:

OWASP ZAP وBurp Suite لاختبار الأمان.

Nessus للكشف عن الثغرات.

النتيجة:

ضمان حماية البيانات والمستخدمين من الهجمات وتوفير بيئة آمنة لنظام إدارة المخزون.