تقرير شامل عن هجمات حقن □□□

حقن □□□ هو أسلوب حقن التعليمات البرمجية المستخدمة لمهاجمة التطبيقات المستندة إلى الب
عبارات □□□ الخبيثة في حقول الإدخال، وتجاوز التدابير الأمنية.

أنواع هجمات حقن □□□:

ويتراوح مقياس الخطورة من 1 إلى 5

1 هو الأدنى، 5 هو الأعلى

1. حقن □□□ داخل النطاق: النوع الأكثر شيوعًا حيث يستخدم المهاجمون نفس الشيء
قنوات الاتصال لشن الهجمات وجمع الإيرادات.

الشدة: 3

2. حقن □□□ على أساس الأخطاء: يستغل رسائل الخطأ التي تم إنشاؤها من قاعدة البيانات إلى
جمع المعلومات.

الشدة: 4

3. حقن □□□ الأعمى: يتضمن إرسال استعلامات □□□ إلى قاعدة البيانات وتحديدها
صلاحية الاستعلام بناءً على استجابة التطبيق.

الشدة: 5

4. حقن □□□ المستند إلى الاتحاد: معالجة نتيجة مشغل □□□□□ □□□ لتجميعها
المعلومات من قاعدة البيانات.

الشدة: 2

وقاية:

استخدم الاستعلامات ذات المعلمات أو البيانات المعدة.

التحقق من صحة مدخلات المستخدم وتعقيمها.

استخدم مبدأ الامتياز الأقل في حسابات قاعدة البيانات.

قم بتحديث وتصحيح البرامج الخاصة بك بانتظام.

تنفيذ التحقق من صحة الإدخال على كل من العميل والخادم.

استخدم جدار حماية تطبيق الويب □□□□□ لتصفية حركة المرور الواردة ومراقبتها.

استخدم الإجراءات المخزنة أو إطار عمل □□□.

تنفيذ المعالجة المناسبة للأخطاء لمنع الكشف عن المعلومات الحساسة.

استخدم ممارسات وأطر الترميز التي تركز على الأمان.

إجراء عمليات التدقيق الأمني واختبارات الاختراق بانتظام.

مدعوم من □□□□□ □□□□.□□□□□.□□□□