CONCEPT

البرمجة الآمنة وفق OWASP Top 10: نمذجة التهديدات ومراجعة الشيفرة وخطوط DevSecOps

البرمجة الآمنة وفق OWASP Top 10: نمذجة التهديدات ومراجعة الشيفرة وخطوط DevSecOps

مقدمة:

تعود معظم اختراقات تطبيقات الويب إلى ثغرات كتبت في الشيفرة أو تسللت عبر عملية البناء: تحقق من الصلاحيات غائب في الخادم، واستعلامات تركب بدمج النصوص، وإدارة جلسات ضعيفة، ومكتبات قديمة، وخطوط نشر تطلق كل ما يجتاز الترجمة. وتحدد قائمة OWASP Top 10 هذه المخاطر المتكررة، لكن الفرق تحتاج إلى عادات برمجة وبوابات فحص تمنع وصولها إلى بيئة الإنتاج. تدرب هذه الدورة من كور كونسبت المطورين وقادة أمن التطبيقات على البرمجة الآمنة وفق OWASP Top 10 بما يمنع كل خطر في الشيفرة، ونمذجة التهديدات بطريقة STRIDE، والمراجعة الأمنية لطلبات الدمج، وتشغيل فحوص SAST وDAST وSCA وكشف الأسرار في خط النشر. ويعد المشاركون دليل البرمجة الآمنة لتطبيقات الويب.

أهداف الدورة:

- ربط فئات مخاطر OWASP Top 10 بنقاط الدخول وحدود الثقة ومسارات البيانات في تطبيق ويب يتولى الفريق صيانته
- بناء نموذج تهديدات لميزة جديدة باستخدام أسئلة OWASP الأربعة وطريقة STRIDE وتحويله إلى متطلبات أمنية
- تطبيق أنماط البرمجة الآمنة التي تمنع خلل التحكم في الوصول والحقن وإخفاقات التشفير وإخفاقات المصادقة في شيفرة التطبيق
- إعداد بوابات أمنية في خط النشر لفحوص SAST وDAST وSCA وكشف الأسرار مع توليد قائمة مكونات البرمجيات SBOM وقواعد فرز التبعيات
- إجراء مراجعة أمنية لشيفرة طلب دمج وتصنيف الملاحظات حسب الخطورة وإحالتها للمعالجة
- إعداد دليل البرمجة الآمنة لتطبيقات الويب متوافقا مع مجموعات ممارسات NIST SSDF

الفئة المستهدفة:

- المطورون الذين يكتبون شيفرة الخادم والواجهة الأمامية لتطبيقات الويب ويتولون صيانتها
- القادة التقنيون الذين يعتمدون طلبات الدمج ويضعون معايير كتابة الشيفرة لفريق التطوير
- موظفو أمن التطبيقات الذين يحددون متطلبات التطوير الآمن ويفرزون نتائج أدوات الفحص
- مهندسو DevOps والبناء المسؤولون عن خطوط CI/CD ومستودعات الحزم وبوابات الإصدار
- مهندسو ضمان الجودة والاختبار الذين يضيفون حالات اختبار أمنية إلى حزم الاختبار الوظيفي واختبار الانحدار

محاور الدورة:

اليوم 1: مشهد مخاطر تطبيقات الويب وقائمة OWASP Top 10 وخط الأساس لدورة حياة التطوير الآمن

- هدف قائمة OWASP Top 10 وفئات المخاطر فيها واستخدامها معيارا لتوعية المطورين
- خريطة سطح الهجوم لتطبيق الويب: نقاط الدخول وحدود الثقة ومسارات البيانات
- مراحل دورة حياة تطوير البرمجيات الآمنة وربط الأنشطة الأمنية بكل مرحلة
- مجموعات ممارسات NIST SSDF إطار تطوير البرمجيات الآمنة: الإعداد والحماية والإنتاج والاستجابة
- تقييم الوضع الحالي للتطوير الآمن باستخدام ممارسات OWASP SAMM نموذج نضج ضمان البرمجيات

اليوم 2: نمذجة التهديدات والمتطلبات الأمنية والتصميم الآمن

- طريقة OWASP للأسئلة الأربعة في نمذجة التهديدات مطبقة على ميزة ويب
- فئات تهديدات STRIDE على مخطط تدفق البيانات مع حدود الثقة
- الوقاية من التصميم غير الآمن: حالات إساءة الاستخدام وأنماط التصميم الآمن وبوابات مراجعة التصميم
- مستويات التحقق في OWASP ASVS معيار التحقق من أمن التطبيقات مصدرا لمتطلبات أمنية قابلة للاختبار
- مختبر: نموذج تهديدات وسجل إجراءات التخفيف لتطبيق ويب تجريبي

اليوم 3: أنماط البرمجة الآمنة للتحكم في الوصول والحقن والتشفير والمصادقة

- الوقاية من خلل التحكم في الوصول: الرفض الافتراضي والتحقق من الصلاحيات في الخادم وقوائم السماح لمنع SSRF
- الوقاية من الحقن: الاستعلامات المهيأة بالمعاملات وترميز المخرجات حسب السياق والتحقق من المدخلات بقوائم السماح
- الوقاية من إخفاقات التشفير: تصنيف البيانات وإعداد TLS والتعامل مع المفاتيح وتجزئة كلمات المرور
- الوقاية من إخفاقات المصادقة: المصادقة متعددة العوامل ودورة حياة الجلسة وتخزين بيانات الاعتماد
- مختبر: إعادة هيكلة عينات شيفرة معيبة إلى بدائل آمنة مع اختبارات الوحدة

اليوم 4: سلسلة التوريد والإعدادات والسلامة والتسجيل وخط DevSecOps

- ضوابط أخطاء الإعدادات الأمنية: الإعدادات الافتراضية المحصنة لأطر العمل وترويسات الأمان وتطابق البيئات
- إخفاقات سلسلة توريد البرمجيات: جرد التبعيات وتوليد SBOM وفرز المكونات المعرضة للثغرات
- إخفاقات سلامة البرمجيات أو البيانات: الحزم الموقعة وخطوط البناء المحمية وإلغاء التسلسل الآمن
- إخفاقات التسجيل الأمني والتنبيه وسوء التعامل مع الحالات الاستثنائية: أحداث التدقيق ومعالجة الأخطاء الآمنة عند الفشل
- مختبر: بوابات خط النشر لفحوص SAST وDAST وSCA وكشف الأسرار مع قواعد إيقاف البناء

اليوم 5: المراجعة الأمنية للشيفرة والاختبار الدفاعي ودليل البرمجة الآمنة

- قائمة تدقيق المراجعة الأمنية للشيفرة مرتبطة بفئات OWASP Top 10
- مختبر: مراجعة أمنية من الأقران لطلب دمج مع ملاحظات مصنفة حسب الخطورة
- أساسيات الاختبار الأمني الدفاعي: اختبارات الوحدة الأمنية وحالات اختبار مبنية على ASVS وفحوص DAST الأساسية
- ترتيب أولويات المعالجة والتحقق من الإصلاح ومسار التعامل مع الثغرات لفرق التطوير
- إعداد دليل البرمجة الآمنة لتطبيقات الويب ومراجعته من الأقران

المهارات التي ستكتسبها:

- اختيار أنماط البرمجة الآمنة
- نمذجة التهديدات بطريقة STRIDE
- تحديد المتطلبات الأمنية
- المراجعة الأمنية للشيفرة
- إعداد البوابات الأمنية في خط النشر
- إدارة التبعيات وقوائم SBOM
- فرز نتائج أدوات الفحص
- المعالجة الآمنة للأخطاء والتسجيل

لماذا تحضر هذه الدورة:

- العودة بدليل البرمجة الآمنة لتطبيقات الويب يضم معيار شيفرة للفريق ونموذج نمذجة تهديدات وإعدادات بوابات خط النشر وقائمة تدقيق للمراجعة
- خفض إعادة العمل التي تكشفها اختبارات الاختراق متأخرة، عبر اكتشاف ثغرات التحكم في الوصول والحقن والتبعيات عند طلب الدمج ومرحلة البناء
- التدرب عمليا في المختبرات على إعادة هيكلة عينات شيفرة حقيقية ومراجعتها وفحصها بدل الاكتفاء بالعروض النظرية عن المخاطر
- مقارنة ممارسات التطوير الآمن مع مطورين وقادة أمن تطبيقات من فرق التمويل والخدمات الحكومية والتجزئة والتقنية

الخاتمة:

لا تنتج تطبيقات الويب الآمنة عن اختبار واحد قبل الإطلاق، بل عن عادات هندسية متكررة. تبدأ الدورة بفئات مخاطر OWASP Top 10 وسطح الهجوم ودورة حياة التطوير الآمن، ثم تنتقل إلى نمذجة التهديدات بطريقة STRIDE والمتطلبات الأمنية، فأنماط البرمجة الآمنة للتحكم في الوصول والحقن والتشفير والمصادقة. بعد ذلك تتناول الإعدادات وسلسلة التوريد والسلامة والتسجيل وفحوص خط النشر، وتختتم بالمراجعة الأمنية للشيفرة والاختبار الدفاعي وإعداد دليل البرمجة الآمنة لكل فريق.