CONCEPT

إدارة واجهات برمجة التطبيقات API وأمنها: التصميم والبوابات والاختبار ودورة الحياة

إدارة واجهات برمجة التطبيقات API وأمنها: التصميم والبوابات والاختبار ودورة الحياة

مقدمة:

تحدد إدارة واجهات برمجة التطبيقات API ما إذا كانت واجهات المنظمة تعمل كمنتجات موثوقة أم تتحول إلى نقاط وصول غير موثقة وإصدارات خفية وقواعد وصول متضاربة. عندها يتكامل الشركاء والفرق الداخلية مع عقود تتغير دون إشعار، ويستغل المهاجمون ضعف التفويض على مستوى الكائن أو نقاط وصول منسية. تدرب هذه الدورة من كور كونسبت الممارسين على تصميم الواجهات بمنهج العقد أولا وفق مواصفة OpenAPI، ونشرها عبر بوابة تفرض السياسات، وحمايتها باستخدام OAuth 2.0 وJWT، واختبارها وحوكمة دورة حياتها. ويعد المشاركون مخطط إدارة منتجات واجهات برمجة التطبيقات وأمنها.

أهداف الدورة:

- تعريف منتجات الواجهات والمستهلكين ونموذج تشغيل يقوم على الواجهة أولا مع سجل لنقاط الوصول القائمة ومالكيها
- كتابة وصف OpenAPI لواجهة REST يطبق قواعد تسمية الموارد ورموز الحالة وتقسيم النتائج ونموذج الأخطاء
- إعداد سياسات البوابة لتحديد المعدل والحصص والتخزين المؤقت وتحويل الطلبات والتحقق من الرموز على واجهة منشورة
- تطبيق اختيار منح OAuth 2.0 وآلية PKCE والنطاقات والتحقق من رموز JWT لحماية عمليات الواجهة من مخاطر Top 10 OWASP API Security
- بناء حزم اختبار وظيفية واختبار عقود واختبار أداء للواجهة وربطها بخط الإصدار
- إعداد مخطط إدارة منتجات واجهات برمجة التطبيقات وأمنها يغطي بوابة المطورين والإصدارات والإيقاف والمراقبة وقواعد الحوكمة

الفئة المستهدفة:

- المطورون الذين يبنون خدمات REST ويصونونها ويطورون التكاملات التي تستهلكها
- معماريو الحلول والتكامل المسؤولون عن تصميم الواجهات بين التطبيقات والشركاء
- مالكو منتجات الواجهات المسؤولون عن المستهلكين وتهيئتهم وخارطة الطريق
- مهندسو المنصات والبرمجيات الوسيطة الذين يشغلون بوابات الواجهات وبوابات المطورين
- العاملون في أمن التطبيقات الذين يراجعون تفويض الواجهات وانكشافها ويختبرونه

محاور الدورة:

اليوم 1: استراتيجية الواجهة أولا ومنتجات الواجهات والوضع الحالي لها

- مكونات إدارة الواجهات: البوابة وبوابة المطورين والتحليلات ودورة الحياة وتحقيق الإيرادات
- نموذج التشغيل القائم على الواجهة أولا ومسار العمل بالعقد قبل البرمجة
- لوحة منتج الواجهة: المستهلكون والقيمة ومستويات الخدمة وفئات الوصول
- نماذج إتاحة الواجهات الخاصة وواجهات الشركاء والواجهات العامة
- سجل جرد الواجهات وملكيتها في بيئة المشاركين

اليوم 2: تصميم REST ومواصفة OpenAPI وخيارات أنماط الواجهات

- نمذجة موارد REST وطرق HTTP ورموز الحالة وقابلية التكرار دون أثر جانبي
- بنية مواصفة OpenAPI لوصف الواجهات: المعلومات والخوادم والمسارات والمكونات ومخططات الأمان
- قواعد تقسيم النتائج والتصفية وحمولة الأخطاء والتسمية في دليل أسلوب الواجهات
- نظرة عامة على GraphQL وgRPC والواجهات القائمة على الأحداث: متى لا يناسب REST
- مختبر: كتابة وصف OpenAPI لخدمة نموذجية وفحصه آليا

اليوم 3: سياسات بوابة الواجهات وOAuth 2.0 وJWT تطبيقيا

- مسار الطلب في بوابة الواجهات: التوجيه وترتيب السياسات والوساطة مع الخدمات الخلفية
- مختبر: سياسات تحديد المعدل والحصص وكبح الذروة حسب فئة المستهلك
- مختبر: سياسات التخزين المؤقت للاستجابات وإعادة كتابة الترويسات وتحويل الحمولة
- أنواع منح OAuth 2.0 والنطاقات وآلية PKCE وفق أفضل الممارسات الأمنية في RFC 9700
- مختبر: التحقق من توقيع رمز JWT ومصدره وجمهوره وانتهاء صلاحيته في البوابة

اليوم 4: مخاطر OWASP API Security Top 10 واختبار الواجهات وضبط العقود

- ضعف التفويض على مستوى الكائن وعلى مستوى الوظيفة: مسارات الهجوم والضوابط
- ضوابط الاستهلاك غير المقيد للموارد وتزوير الطلبات من جهة الخادم وأخطاء إعدادات الأمان
- ضعف إدارة جرد الواجهات والاستهلاك غير الآمن لواجهات الأطراف الخارجية
- مختبر: مجموعات اختبار وظيفية وسلبية باستخدام أدوات اختبار الواجهات الشائعة
- اختبارات العقود التي يقودها المستهلك واختبارات الحمل ضمن خط الإصدار

اليوم 5: بوابة المطورين والإصدارات والمراقبة والحوكمة وإعداد المخطط

- مسار تهيئة المطورين في البوابة: التوثيق وبيئة التجربة والمفاتيح والدعم
- نظام ترقيم الإصدارات وقواعد التغييرات الكاسرة وخطة إشعار الإيقاف
- لوحة تحليلات الواجهات: حجم الحركة وزمن الاستجابة ومعدل الأخطاء ومؤشرات تبني المستهلكين
- مجلس مراجعة حوكمة الواجهات وقواعد الفحص الآلي للتصميم وقائمة التحقق قبل النشر
- إعداد مخطط إدارة منتجات واجهات برمجة التطبيقات وأمنها ومراجعته من الزملاء

المهارات التي ستكتسبها:

- تعريف منتجات الواجهات
- كتابة عقود OpenAPI
- إعداد سياسات البوابة
- التفويض بالرموز للواجهات
- تقييم تهديدات الواجهات
- اختبار العقود والحمل
- ضبط دورة حياة الإصدارات
- حوكمة تصميم الواجهات

لماذا تحضر هذه الدورة:

- العودة بمخطط إدارة منتجات واجهات برمجة التطبيقات وأمنها مبني على واجهات تنشرها فرقك أو تستهلكها
- التوقف عن كسر تكاملات المستهلكين بالانتقال إلى التصميم بالعقد أولا والعقود المختبرة والإيقاف المخطط
- سد ثغرات التفويض والجرد التي تقف وراء أكثر اختراقات الواجهات شيوعا قبل أن يكتشفها المهاجم
- إعداد البوابة والرموز والاختبارات عمليا في المختبرات ومقارنة ممارسات الواجهات مع زملاء من المصارف والاتصالات والتجزئة والخدمات اللوجستية والخدمات العامة

الخاتمة:

باتت الواجهات تحمل المعاملات والبيانات وتكاملات الشركاء التي تعتمد عليها المنظمات، لذا تحتاج إلى انضباط المنتج وضوابط الحدود الأمنية معا. تنتقل الدورة من منتجات الواجهات ووضعها الحالي، إلى تصميم REST ومواصفة OpenAPI، ثم سياسات البوابة وOAuth 2.0 وJWT، ومنها إلى مخاطر OWASP API Security Top 10 والاختبار الوظيفي واختبار العقود والأداء. ويتناول اليوم الأخير بوابة المطورين والإصدارات والمراقبة والحوكمة، ويخرج المشاركون بمخطط إدارة منتجات الواجهات وأمنها.