المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT I info@ainfct.com I www.ainfct.com

Secure Coding Practices Workshop

فكرة الدورة

أصبحت الثغرات البرمجية من أكثر مصادر المخاطر السيبرانية تأثيراً على التطبيقات والخدمات الرقمية، خصوصاً مع تسارع تطوير البرمجيات واعتماد الفرق على واجهات البرمجة والمكتبات مفتوحة المصدر وخطوط التكامل والنشر المستمر. لذلك لم تعد البرمجة الآمنة مسؤولية فريق الاختبار فقط، بل أصبحت ممارسة أساسية داخل دورة حياة التطوير.

تركز هذه الورشة التدريبية من AINFCT على بناء قدرة عملية لدى المشاركين على فهم مصادر الثغرات الشائعة، وتحويل المتطلبات الأمنية إلى ممارسات ترميز واضحة، وتطبيق مبادئ التحقق من المدخلات، وإدارة الجلسات، والتحكم بالوصول، والتشفير، والتعامل الآمن مع الأخطاء والسجلات. كما تربط الورشة بين ممارسات المطورين ومتطلبات الاختبار الأمني ومراجعة الكود.

توفر الورشة قيمة مهنية مباشرة من خلال أمثلة وسيناريوهات تطبيقية تساعد فرق التطوير على إنتاج برمجيات أكثر أماناً وقابلية للمراجعة والتحسين المستمر.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تطبيق مبادئ الترميز الآمن داخل دورة التطوير.
- اكتشاف أنماط الثغرات الشائعة في التطبيقات.
- تحسين التحقق من المدخلات ومعالجة المخرجات.
- تعزيز التحكم بالوصول وإدارة الجلسات.
- استخدام التشفير ومعالجة الأخطاء بصورة آمنة.
- دعم مراجعة الكود والاختبار الأمني التطبيقي.

منهجية الدورة

- شرح تفاعلي مدعوم بأمثلة من بيئات تطوير واقعية.
- تمارين تحليل كود وسيناريوهات ثغرات شائعة.
- نقاشات جماعية حول تصميم الضوابط والمعالجات.
- قوائم تحقق عملية قابلة للاستخدام داخل الفرق.
- مراجعات قصيرة لقياس الفهم بعد المحاور الرئيسية.

أثر الدورة على المنظمة

يمكن رفع جودة أمن البرمجيات المؤسسية من خلال:

- تقليل الثغرات الناتجة عن أخطاء الترميز.
- تحسين تكامل الأمن داخل فرق التطوير.
- رفع قابلية التطبيقات للمراجعة والاختبار.
- دعم الامتثال لمتطلبات أمن التطبيقات.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- كتابة كود أكثر أماناً وقابلية للصيانة.
- تحليل مخاطر الأمن داخل منطق التطبيق.
- استخدام قوائم تحقق عملية أثناء التطوير.
- التعاون بفعالية مع فرق الأمن والاختبار.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج المشاركين العاملين في تطوير البرمجيات أو اختبارها أو تأمينها، ممن يحتاجون إلى تحويل مفاهيم أمن التطبيقات إلى ممارسات ترميز يومية قابلة للتطبيق. كما يفيد الفرق التي تسعى إلى تحسين جودة البرمجيات وتقليل الثغرات قبل النشر.

- مطورو التطبيقات والبرمجيات.
- مختبرو الجودة والاختبار الأمني.
- مهندسو DevOps وDevSecOps.
- محللو أمن التطبيقات.
- قادة الفرق التقنية ومراجعو الكود.

موضوعات الدورة

اليوم الأول: مدخل إلى البرمجة الآمنة ودورة التطوير

- مفهوم البرمجة الآمنة ودورها في تقليل المخاطر.
- العلاقة بين المتطلبات الأمنية وتصميم البرمجيات.
- دمج الأمن داخل دورة حياة تطوير البرمجيات.
- أدوار المطورين والمختبرين وفرق الأمن.
- أخطاء الترميز الشائعة وأثرها التشغيلي.

اليوم الثاني: نمذجة التهديدات ومتطلبات الأمن

- تحديد الأصول ومسارات البيانات داخل التطبيق.
- تحليل الجهات المهددة وسيناريوهات إساءة الاستخدام.
- تحويل التهديدات إلى متطلبات أمنية قابلة للتنفيذ.
- ترتيب الضوابط حسب المخاطر والأولوية.
- توثيق افتراضات الأمن وحدود الثقة.

اليوم الثالث: التحقق من المدخلات ومعالجة المخرجات

- مبادئ قبول المدخلات والتحقق من صحتها.
- القوائم البيضاء والقيود المنطقية للبيانات.
- منع حقن الأوامر والاستعلامات النصية.
- ترميز المخرجات وفق سياق العرض والاستخدام.
- معالجة الملفات والبيانات غير الموثوقة.

اليوم الرابع: التحكم بالوصول وإدارة الصلاحيات

- الفرق بين المصادقة والتفويض والمحاسبية.
- تصميم ضوابط الوصول حسب الدور والسياق.
- منع تجاوز الصلاحيات الأفقية والعمودية.

- حماية الوظائف الحساسة من الاستخدام غير المصرح.
- مراجعة قرارات الوصول داخل منطق التطبيق.

اليوم الخامس: المصادقة وإدارة الجلسات

- مبادئ بناء آليات مصادقة آمنة.
- سياسات كلمات المرور والمصادقة متعددة العوامل.
- إدارة رموز الجلسات وحمايتها من الاختطاف.
- انتهاء الجلسات وتجديدها وإبطالها بأمان.
- حماية الحسابات من التخمين والإساءة الآلية.

اليوم السادس: ممارسات التشفير وحماية الأسرار

- استخدام التشفير المناسب لحماية البيانات الحساسة.
- إدارة المفاتيح والأسرار داخل التطبيقات.
- التخزين الآمن لكلمات المرور والقيم السرية.
- تجنب الخوارزميات والإعدادات الضعيفة.
- حماية البيانات أثناء النقل والتخزين.

اليوم السابع: التعامل الآمن مع الأخطاء والسجلات

- تصميم رسائل أخطاء لا تكشف معلومات حساسة.
- تسجيل الأحداث الأمنية بطريقة قابلة للتحليل.
- حماية السجلات من التلاعب والوصول غير المصرح.
- ربط السجلات بحالات التحقيق والاستجابة.
- موازنة التشخيص التشغيلي مع متطلبات السرية.

اليوم الثامن: أمن قواعد البيانات وواجهات البرمجة

- حماية الاستعلامات من الحقن والتلاعب.
- استخدام الاستعلامات المجهزة وربط المعاملات.
- تصميم واجهات برمجة آمنة وقابلة للتحكم.

- التحقق من الطلبات والردود وحدود الاستخدام.
- حماية المفاتيح والرموز الخاصة بواجهات البرمجة.

اليوم التاسع: أمن الويب والثغرات الشائعة

- فهم أهم أنماط ثغرات تطبيقات الويب.
- منع البرمجة العابرة للمواقع وتزوير الطلبات.
- حماية الملفات والتحميلات ومسارات الوصول.
- ضبط الرؤوس الأمنية وسياسات المتصفح.
- تحليل أمثلة تطبيقية على أخطاء أمنية شائعة.

اليوم العاشر: أمن المكونات والمكتبات وسلاسل التوريد

- مخاطر الاعتماد على المكونات الخارجية.
- إدارة الإصدارات والثغرات المعروفة في المكتبات.
- التحقق من مصادر الحزم وسلامة الاعتماديات.
- تقليل سطح الهجوم في المكونات غير المستخدمة.
- متابعة التنبيهات الأمنية وتحديثات المعالجة.

اليوم الحادي عشر: مراجعة الكود الآمن

- أهداف مراجعة الكود من منظور أمني.
- استخدام قوائم تحقق لمراجعة الأنماط الخطرة.
- مراجعة منطق الأعمال ومسارات الثقة.
- توثيق الملاحظات وربطها بمستويات المخاطر.
- تحسين جودة الكود من خلال التغذية الراجعة.

اليوم الثاني عشر: الاختبار الأمني أثناء التطوير

- الفرق بين الاختبار الوظيفي والاختبار الأمني.
- استخدام الاختبارات الثابتة والديناميكية بفعالية.
- بناء حالات اختبار للمدخلات والصلاحيات والجلسات.

- تفسير نتائج أدوات الفحص وتحديد الأولويات.
- إدارة النتائج الكاذبة وخطط المعالجة.

اليوم الثالث عشر: DevSecOps وأتمتة الضوابط

- إدراج الأمن داخل خطوط التكامل والنشر.
- فحص الكود والمكونات قبل النشر.
- إدارة الأسرار داخل بيئات التطوير والتشغيل.
- استخدام بوابات جودة أمنية قابلة للقياس.
- تحسين التعاون بين التطوير والعمليات والأمن.

اليوم الرابع عشر: إصلاح الثغرات وتحسين التصميم

- تحليل السبب الجذري للثغرات البرمجية.
- اختيار المعالجة المناسبة دون كسر الوظائف.
- إعادة تصميم المسارات عالية المخاطر.
- التحقق من فعالية الإصلاح بعد التطبيق.
- بناء دروس مستفادة قابلة لإعادة الاستخدام.

اليوم الخامس عشر: التطبيق العملي والمراجعة النهائية

- تحليل سيناريو تطبيقي شامل لثغرات متعددة.
- بناء قائمة تحقق للبرمجة الآمنة داخل الفريق.
- مراجعة المفاهيم الأساسية وربطها ببيئة العمل.
- مناقشة تحديات التطبيق داخل فرق التطوير.
- إعداد خطة تحسين شخصية بعد البرنامج.

course_daily_schedule

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة للمفاهيم السابقة، ثم عرض للمحور الرئيسي، يتبعه تمرين تطبيقي أو تحليل حالة عملية، وينتهي اليوم بخلاصة مركزة تربط الموضوعات بممارسات التطوير الآمن داخل بيئة العمل.

course_assessment

يعتمد التقييم على المشاركة الفعالة، وتمارين تحليل الكود، ومناقشة السيناريوهات التطبيقية، والمراجعات القصيرة المرتبطة بمحاور البرنامج. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course_key_competencies

- البرمجة الآمنة.
- أمن التطبيقات.
- نمذجة التهديدات.
- مراجعة الكود.
- اختبار أمن البرمجيات.
- DevSecOps.

مكتب القاهرة الرئيسي
القاهرة، جمهورية مصر العربية
7 شارع وهران، الطيران، مدينة نصر
+201152466358
info@ainfct.com
ainfct.com
رقم التسجيل الضريبي: 472920235
مكتب مدريد الفرعي
مدريد، إسبانيا

شارع الصحة 3، وسط المدينة، 28013 مدريد
training@ainfct.com
ainfct.com