الدورة التدريبية: تطوير البرمجيات الآمنة: أفضل الممارسات للمبرمجين والفرق الهندسية



15 - 19 نوفمبر 2026
المنامة
4400 € (للشخص الواحد)
Ref: #CYB4024_397488

مقدمة الدورة التدريبية / لمحة عامة:

يمثل تطوير البرمجيات الآمنة حجر الزاوية في بناء أنظمة رقمية موثوقة ومقاومة للتهديدات. فمع تزايد تعقيد التطبيقات، تتصاعد المخاطر الأمنية التي تستهدف نقاط الضعف في الأكواد المصدرية، مما يستدعي نهجًا استباقيًا لتضمين الأمن في كل مرحلة من دورة حياة التطوير. تقدم هذه الدورة التدريبية المتخصصة للمبرمجين، مهندسي البرمجيات، ومديري المشاريع، المعرفة والمهارات اللازمة لبناء برمجيات حصينة من البداية. سنتناول في هذه الدورة مفاهيم الأمن في التصميم المعماري للبرمجيات، أفضل ممارسات الكود الآمن، وتقنيات اختبار الاختراق. سيكتسب المشاركون القدرة على تحديد الثغرات الأمنية، تطبيق ضوابط أمنية في الكود، والاستجابة الفعالة للحوادث الأمنية التي قد تحدث في التطبيقات. تهدف الدورة إلى بناء كوادر هندسية قادرة على كتابة كود آمن، مما يقلل من التكاليف والمخاطر الأمنية على المدى الطويل. يستند المحتوى إلى أحدث المعايير الصناعية وأفضل الممارسات في أمن التطبيقات، مع الاستفادة من إسهامات خبراء أكاديميين بارزين مثل البروفيسور غاري ماكغرو (Gary McGraw)، المعروف بأعماله الرائدة في هندسة الأمن واختبار أمن التطبيقات. يقدم BIG BEN Training Center هذه الدورة لتمكين الفرق الهندسية من بناء منتجات برمجية آمنة وموثوقة.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المبرمجون ومطورو البرمجيات.
- مهندسو الأمن.
- مديرو المشاريع التقنية.
- مهندسو البنية التحتية والأنظمة.
- فريق ضمان الجودة.
- الفرق الهندسية في الشركات الناشئة والتقنية.

القطاعات والصناعات المستهدفة:

- شركات تطوير البرمجيات.
- القطاع المالي والتكنولوجي.
- شركات التجارة الإلكترونية.
- القطاع الحكومي والجهات الأمنية.
- شركات الاتصالات.
- المؤسسات التي تعتمد على تطبيقات داخلية.

الأقسام المؤسسية المستهدفة:

- إدارة تطوير البرمجيات.
- إدارة الأمن السيبراني.
- أقسام ضمان الجودة.
- إدارة المنتجات.
- إدارة البنية التحتية.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم مبادئ تطوير البرمجيات الآمنة ودورة حياة التطوير الآمن (SDLC).
- القدرة على تحديد الثغرات الأمنية الشائعة في الكود.
- تطبيق أفضل الممارسات لكتابة كود آمن وموثوق.
- استخدام أدوات تحليل الكود الثابت والديناميكي (SAST/DAST).
- تأمين التطبيقات ضد هجمات الويب الشائعة (OWASP Top 10).
- إجراء اختبارات اختراق بسيطة على التطبيقات.
- الاستجابة للحوادث الأمنية في مرحلة التطوير والإنتاج.

منهجية الدورة التدريبية:

تعتمد هذه الدورة التدريبية منهجية عملية وتشاركية، مصممة لدمج مفاهيم الأمن السيبراني في عمل المبرمجين اليومي. سيتمكن المتدربون من خلال ورش العمل العملية، التي تتضمن تحليل كود ضعيف وإعادة كتابته بشكل آمن، ومحاكاة هجمات الاختراق، من اكتساب خبرة مباشرة في تطوير برمجيات آمنة. تتضمن المنهجية مناقشات متعمقة حول هجمات سيبرانية حقيقية وكيف كان يمكن تجنبها من خلال التصميم الآمن. سيتم التركيز على الجانب التطبيقي لأمن التطبيقات، من التشفير إلى إدارة الجلسات. يقدم BIG BEN Training Center هذه الدورة لتمكين الفرق الهندسية من بناء منتجات رقمية آمنة وموثوقة، مما يعزز الثقة في العلامة التجارية.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الأمن في دورة حياة تطوير البرمجيات (SDLC)

- مقدمة إلى دورة حياة تطوير البرمجيات الآمنة (SDLC).
- التصميم الأمني والنمذجة الأمنية للتهديدات (Threat Modeling).
- مفاهيم الأمن الأساسية (OWASP Top 10).
- أهمية الأمن الاستباقي بدلاً من التفاعلي.
- الفرق بين أمن التطبيقات وأمن البنية التحتية.
- التوعية الأمنية للمطورين.
- الامتثال للوائح الأمنية في التطوير.

الوحدة الثانية: كتابة الكود الآمن (Secure Coding)

- أفضل الممارسات في كتابة كود آمن.
- التحقق من صحة المدخلات (Input Validation).
- التعامل الآمن مع الأخطاء والاستثناءات.
- أمن المصادقة والجلسات.
- التعامل مع البيانات الحساسة (التشفير والتجزئة).
- الحماية من هجمات الحقن (SQL, Command Injection).
- منع هجمات XSS وCSRF.

الوحدة الثالثة: تأمين التطبيقات ضد هجمات الويب الشائعة

- هجمات الحقن (Injection Attacks).
- هجمات البرمجة عبر المواقع (Cross-Site Scripting - XSS).
- هجمات تزوير الطلبات عبر المواقع (Cross-Site Request Forgery - CSRF).
- الثغرات في المصادقة وإدارة الجلسات.
- التحكم في الوصول المعطل (Broken Access Control).
- تأمين خوادم التطبيقات والويب.
- الحماية من الثغرات في التكوين.

الوحدة الرابعة: اختبار أمن التطبيقات (Application Security Testing)

- أنواع اختبار أمن التطبيقات.
- تحليل الكود الثابت (Static Analysis Security Testing - SAST).
- تحليل الكود الديناميكي (Dynamic Analysis Security Testing - DAST).
- اختبار الاختراق اليدوي.
- أتمتة اختبارات الأمان في خطوط التطوير (CI/CD).
- إدارة الثغرات الأمنية المكتشفة.
- التحليل الأمني للمكتبات والتبعيات (Dependencies).

الوحدة الخامسة: الاستجابة للحوادث وبناء ثقافة الأمن

- وضع خطة للاستجابة للحوادث الأمنية على مستوى التطبيق.
- اكتشاف الاختراقات والاستجابة السريعة لها.
- التحقيق الجنائي الرقمي في حوادث التطبيقات.
- بناء ثقافة أمنية قوية ضمن الفريق الهندسي.
- التواصل مع الفرق الأخرى (Ops, Legal) بشأن الأمن.
- مراجعة الكود الأمنية الجماعية.
- مستقبل تطوير البرمجيات الآمنة.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور المتسارع للغات البرمجة وأطر العمل، كيف يمكن للمبرمجين والفرق الهندسية أن يبتكرون منهجيات تطوير برمجيات آمنة لا تقتصر على معالجة الثغرات المعروفة، بل تتوقع نقاط الضعف المستقبلية وتُنشئ بنية كود مرنة ومحصنة تضمن سلامة وأمان التطبيقات على المدى الطويل؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها المتخصص والعميق على تطوير البرمجيات الآمنة، مما يوفر محتوى مصممًا خصيصًا للمبرمجين والفرق الهندسية. بدلاً من تناول الأمن السيبراني بشكل عام، نغوص في التطبيق العملي لأمن التطبيقات، من تصميم الكود وحتى اختباره. تقدم الدورة ورش عمل عملية تتضمن تحليل كود ضعيف وكتابة كود آمن، مما يمنح المشاركين خبرة عملية مباشرة في حماية منتجاتهم. نركز على الدمج بين الأمن ودورة حياة التطوير (SDLC)، مما يضمن أن الأمن جزء لا يتجزأ من العملية الهندسية. إنها ليست مجرد دورة نظرية، بل هي برنامج تدريبي مكثف يهدف إلى بناء مطورين قادرين على بناء برمجيات آمنة، مما يقلل من المخاطر ويحمي سمعة المؤسسة.