الدورة التدريبية: أمن تطبيقات الويب المتقدم والامتثال لمعايير الصناعة



01 - 05 نوفمبر 2026
عمان
3800 € (للشخص الواحد)
Ref: #IT4663_411005

مقدمة الدورة التدريبية / لمحة عامة:

تُعد تطبيقات الويب العصب الحيوي للعديد من المؤسسات في العصر الرقمي الحالي، حيث تُشكل واجهة تفاعل أساسية مع العملاء والشركاء. ومع تزايد الاعتماد على هذه التطبيقات، تتصاعد كذلك التهديدات الأمنية التي تستهدفها، مما يستدعي فهمًا عميقًا لمفاهيم أمن تطبيقات الويب ومعايير الامتثال الصناعية. تقدم هذه الدورة التدريبية الشاملة من BIG BEN Training Center رؤى متعمقة حول أحدث الممارسات والتقنيات في تأمين تطبيقات الويب، بدءًا من اكتشاف الثغرات الأمنية الشائعة مثل حقن SQL والبرمجة النصية عبر المواقع (XSS)، وصولًا إلى آليات الحماية المتقدمة وتطبيق أفضل المعايير الأمنية العالمية. سيتعلم المشاركون كيفية تحليل نقاط الضعف، وتطبيق التشفير الآمن، وإدارة الهوية والوصول، بالإضافة إلى فهم المتطلبات التنظيمية والامتثال لمعايير الصناعة مثل OWASP Top 10 وPCI DSS. تركز الدورة على الجانب العملي والتطبيقي، مستلهمة من أفكار خبراء الأمن السيبراني مثل البروفيسور دانييل جرينبيرغ (Daniel J. Greenwood) من جامعة هارفارد، الذي يُعد رائدًا في مجال أمن المعلومات والقانون، مما يضمن حصول المتدربين على معرفة شاملة ومتكاملة تمكنهم من بناء تطبيقات ويب آمنة وموثوقة. يهدف BIG BEN Training Center إلى تزويد المشاركين بالأدوات والمهارات اللازمة لمواجهة تحديات الأمن السيبراني المعاصرة بفعالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- مهندسو تطوير الويب ومبرمجو التطبيقات.
- متخصصو الأمن السيبراني ومديرو أمن المعلومات.
- مدققو الأنظمة والمخاطر.
- مسؤولو البنية التحتية لتكنولوجيا المعلومات.
- محللو ضمان الجودة واختبار الاختراق.
- مديرو المنتجات التقنية.
- مستشارو الامتثال التنظيمي.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي.
- قطاع التكنولوجيا والاتصالات.
- القطاع الحكومي والهيئات التنظيمية.
- قطاع الرعاية الصحية.
- قطاع التجارة الإلكترونية والتجزئة.
- قطاع الطاقة والمرافق.
- شركات تطوير البرمجيات والاستشارات التقنية.

الأقسام المؤسسية المستهدفة:

- أقسام تطوير البرمجيات.
- أقسام الأمن السيبراني وامن المعلومات.
- أقسام الامتثال والمخاطر.
- أقسام تكنولوجيا المعلومات والبنية التحتية.
- أقسام التدقيق الداخلي والخارجي.
- أقسام إدارة المشاريع التقنية.

أهداف الدورة التدريبية:

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

- فهم التهديدات الأمنية الشائعة لتطبيقات الويب وكيفية استغلالها.
- تطبيق أفضل الممارسات لتأمين الشيفرة المصدرية لتطبيقات الويب.
- التعرف على آليات التشفير وإدارة المفاتيح وتطبيقها بفعالية.
- إدارة الهوية والوصول وتكوين أنظمة المصادقة والتفويض الآمنة.
- تحديد نقاط الضعف في تطبيقات الويب باستخدام أدوات وتقنيات متقدمة.
- تطوير استراتيجيات الاستجابة للحوادث الأمنية والتعافي من الكوارث.
- الالتزام بمعايير الامتثال الدولية مثل OWASP Top 10 وPCI DSS وGDPR.
- تقييم أمان تطبيقات الويب وتحليل الثغرات الأمنية المحتملة.
- بناء تطبيقات ويب مرنة ومقاومة للهجمات السيبرانية.

منهجية الدورة التدريبية:

تتبع هذه الدورة التدريبية منهجية تفاعلية وشاملة، تجمع بين الشرح النظري المتعمق والتطبيقات العملية المكثفة، لضمان استيعاب المتدربين للمفاهيم المعقدة وتحويلها إلى مهارات قابلة للتطبيق. يتميز أسلوب التدريب في BIG BEN Training Center بالتركيز على دراسات الحالة الواقعية، التي تُقدم سيناريوهات حقيقية للهجمات الأمنية وكيفية معالجتها، مما يمنح المشاركين فرصة لتحليل المشكلات واقتراح الحلول. تُشجع ورش العمل الجماعية المتدربين على التعاون وتبادل الأفكار، مما يعزز الفهم الجماعي ويكشف عن وجهات نظر متعددة في مواجهة التحديات الأمنية. تُعد الجلسات التفاعلية جزءًا أساسيًا من المنهجية، حيث تتيح طرح الأسئلة، والمناقشات المفتوحة، وتلقي التغذية الراجعة الفورية من المدربين الخبراء. يتم استخدام أدوات محاكاة بيئة الاختراق الأخلاقي، مما يمكن المتدربين من ممارسة تقنيات الدفاع والهجوم بطريقة آمنة ومتحكم بها. هذا النهج الشامل يُجهز المتدربين بالمعرفة النظرية والخبرة العملية اللازمة لبناء وتأمين تطبيقات ويب قوية ضد التهديدات السيبرانية المتجددة، مع الالتزام بمعايير الصناعة وأفضل الممارسات.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات أمن تطبيقات الويب.

- فهم تحديات الأمن السيبراني لتطبيقات الويب.
- نموذج OWASP Top 10 والمخاطر الشائعة.
- مفاهيم المصادقة والتفويض وإدارة الجلسات.
- مبادئ البرمجة الآمنة والتشفير.
- أدوات وتقنيات اختبار أمان الويب.
- مقدمة عن معايير الامتثال الصناعي.
- بناء بيئة عمل آمنة لتطوير التطبيقات.

الوحدة الثانية: هجمات الويب الشائعة وتقنيات الدفاع.

- حقن SQL وهجمات قواعد البيانات.
- البرمجة النصية عبر المواقع (XSS) والحماية منها.
- التزوير عبر طلبات المواقع (CSRF) ووسائل المنع.
- هجمات الاختراق وكسر المصادقة.
- هجمات التحميل والتلاعب بالملفات.
- الحماية من هجمات DDoS ورفض الخدمة.
- أفضل الممارسات لتكوين الخوادم الآمنة.

الوحدة الثالثة: التشفير وإدارة المفاتيح وأمن البيانات.

- مبادئ التشفير المتماثل وغير المتماثل.
- التوقيعات الرقمية والشهادات الرقمية.
- إدارة مفاتيح التشفير وتخزينها الآمن.
- تأمين البيانات في أثناء النقل والتخزين.
- التعامل مع البيانات الحساسة وحمايتها.
- مفاهيم أمن السحابة لتطبيقات الويب.
- تأمين واجهات برمجة التطبيقات (APIs).

الوحدة الرابعة: الامتثال التنظيمي والمعايير الصناعية.

- معيار أمان بيانات صناعة بطاقات الدفع (PCI DSS).
- اللائحة العامة لحماية البيانات (GDPR).
- قانون نقل التأمين الصحي والمساءلة (HIPAA).
- معايير أيزو 27001 لنظم إدارة أمن المعلومات.
- إجراء عمليات التدقيق الأمني والامتثال.
- وضع سياسات وإجراءات أمن المعلومات.
- الاستجابة للحوادث الأمنية والتعافي.

الوحدة الخامسة: تقييم أمان تطبيقات الويب ومستقبلها.

- اختبار الاختراق (Penetration Testing) لأمان الويب.
- تحليل الثغرات الأمنية وأدوات الفحص الآلي.
- تقييم المخاطر الأمنية ووضع خطط التخفيف.
- أمن تطبيقات الويب في بيئات DevOps.
- الذكاء الاصطناعي وتعلم الآلة في أمن الويب.
- مستقبل أمن تطبيقات الويب والتهديدات الناشئة.
- بناء ثقافة أمنية قوية داخل المؤسسة.

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:

كيف يمكن للمنظمات تحقيق التوازن بين الابتكار السريع في تطوير تطبيقات الويب، وضرورة تطبيق أعلى معايير الأمن والامتثال دون إعاقة عملية النشر؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة التدريبية بمنهجها الشامل والعميق، حيث لا تقتصر على تقديم المفاهيم النظرية فحسب، بل تُركز بشكل مكثف على التطبيق العملي والرؤى المستنيرة المستقاة من أفضل الممارسات العالمية في مجال أمن تطبيقات الويب. يقدم BIG BEN Training Center محتوى أكاديميًا متطورًا يتجاوز التغطية السطحية للمواضيع، ليغوص في تفاصيل الهجمات السيبرانية المعقدة وأساليب الدفاع المتقدمة. تعتمد الدورة على أمثلة عملية من واقع الصناعة، مما يساعد المتدربين على ربط المفاهيم النظرية بالتحديات الحقيقية التي يواجهونها في بيئات العمل. بدلاً من مجرد سرد الأدوات، تُركز الدورة على فهم فلسفة الأمن وراء كل تقنية، مما يُمكّن المشاركين من اتخاذ قرارات مستنيرة وتطوير حلول أمنية مبتكرة ومستدامة. يضمن هذا النهج حصول المتدربين على فهم معمق لكيفية بناء تطبيقات ويب مرنة وآمنة، مع القدرة على تلبية المتطلبات التنظيمية الصارمة ومعايير الامتثال الصناعي، مما يجعلهم خبراء في مجال حماية الأصول الرقمية لمؤسساتهم.