Certified Secure Web Application Engineer (CSWAE) (OWASP)

In de training: “Certified Secure Web Application Engineer (CSWAE) (OWASP)” van Mile2 krijg jij uitgebreide kennis en praktische vaardigheden waarmee jij leert hoe jij webapplicaties kunt beveiligen.

Algemene omschrijving

In de training: “Certified Secure Web Application Engineer (CSWAE) (OWASP)” van Mile2 krijg jij uitgebreide kennis en praktische vaardigheden waarmee jij leert hoe jij webapplicaties kunt beveiligen. Leer de belangrijkste beveiligingsrisico's, de basisprincipes van een beveiligde webontwikkeling en het belang van het volgen van beste werkwijzen zoals gedefinieerd door OWASP (Open Worldwide Application Security Project), een non-profitorganisatie voor het verbeteren van de beveiliging van software.

Verdiep je in “OWASP Top 10”, een standaard voor de belangrijkste beveiligingsrisico’s van webapplicaties. Deze training behandelt elk van de top 10 risico's in detail, inclusief de oorzaken, gevolgen, en hoe jij de beveiligingsrisico’s kunt beperken. Leer hoe jij voor veilige code kunt zorgen en veelvoorkomende beveiligingsfouten in webapplicaties kunt voorkomen. Door deze training krijg jij praktische technieken en strategieën aangereikt voor het ontwikkelen van robuuste en veilige webapplicaties.

Verken geavanceerde essentiële beveiligingstechnieken en -hulpmiddelen voor het beveiligen van webapplicaties, waaronder inputvalidatie, authenticatie, autorisatie, sessiebeheer, en meer. Verkrijg praktische kennis en vaardigheden in het testen en auditen van webapplicaties om beveiligingslekken op te sporen. Leer hoe je penetratietesten en beveiligingsaudits uit kunt voeren, en leer hoe je kwetsbaarheden effectief kunt rapporteren en hoe je iemand aan kunt spreken.

Doelgroep

De training: “Certified Secure Web Application Engineer (CSWAE) (OWASP)” is geschikt voor de volgende mensen:

- **Softwareontwikkelaars die webapplicaties creëren**
  - Ontwikkelaars die webapplicaties creëren en hun vaardigheden uit willen breiden met geavanceerde kennis in het beveiligen van webapplicaties tegen veelvoorkomende en geavanceerde beveiligingsrisico's.

- **ICT-beveiligingsspecialisten**
  - ICT-professionals die gespecialiseerd zijn in systeembeveiliging en specifieke kennis en vaardigheden willen verkrijgen van webapplicatiebeveiliging, in overeenstemming met de richtlijnen van OWASP.
- **Penetratietesters en beveiligingsauditors**
  - Professionals die gespecialiseerd zijn in het testen van de beveiliging van webapplicaties en die hun kennis willen verdiepen met betrekking tot de specifieke kwetsbaarheden en beveiligingsstrategieën van webapplicaties.
- **Projectmanagers en teamleiders**
  - Leidinggevenden die betrokken zijn bij projecten en die hun organisatie willen leiden in het ontwikkelen van veiligere en robuustere webapplicaties.

Leerdoelen

Door de training: “Certified Secure Web Application Engineer (CSWAE) (OWASP)” te volgen krijg je de volgende kennis en vaardigheden:

- **Begrip van beveiligingsrisico’s van webapplicaties**
  - Verkrijg diepgaande kennis van de meest voorkomende beveiligingsrisico's voor webapplicaties, zoals gedefinieerd in de OWASP Top 10.
- **Het ontwikkelen van veilige webapplicaties**
  - Leer hoe jij veilige webapplicaties kunt ontwikkelen door het toepassen van de beste werkwijzen in het ontwerpen en programmeren om kwetsbaarheden te voorkomen.
- **Beveiligingsstrategieën en -methoden**
  - Leer hoe jij geavanceerde beveiligingsstrategieën en -methoden toe kunt passen waarmee jij webapplicaties optimaal kunt beschermen, inclusief:
    - Authenticatie.
    - Autorisatie.
    - Sessiebeheer.
- **Penetratietesten en kwetsbaarheidsbeoordeling**
  - Ontwikkel vaardigheden in penetratietesten en kwetsbaarheidsbeoordelingen om beveiligingslekken in webapplicaties op te sporen en te verhelpen.
- **Gebruik van beveiligingshulpmiddelen en -technieken**
  - Leer de verschillende beveiligingshulpmiddelen en -technieken kennen die worden gebruikt voor het testen en beveiligen van webapplicaties.

Voorkennis

Voordat jij deelneemt aan deze training raden wij aan dat jij over de volgende voorkennis beschikt:

- Twee jaar programmeerervaring met een specifieke focus op beveiligingsaspecten.
- Een grondige kennis van computernetwerken.
- Ervaring met ten minste één programmeertaal.
- Kennis van Linux.
- Ervaring met CLI-omgevingen (Command Line Interface).

Onderwerpen

Modules

- Module 1: Web Application Security.

- Module 2: Secure Software Development Lifecycle.
- Module 3: Risk Management.
- Module 4: Threat Modeling.
- Module 5: Secure Architecture Design and Analysis.
- Module 6: Application Mapping.
- Module 7: Application Attacks.
- Module 8: Input Validation and Data Sanitization.
- Module 9: Securing Web Applications.
- Module 10: Web Application Penetration Testing.
- Module 11: Code Review and Security Testing.
- Module 12: Secure Back-End Components.
- Module 13: AJAX Security.
- Module 14: Mobile Security.
- Module 15: Content Management Systems Security.

Labs

- Lab 1a: Environment Setup and Architecture.
- Lab 1b: OWASP TOP 10.
- Lab 2: Threat Modeling.
- Lab 3: Application Mapping & Analysis.
- Lab 4: Application Attacks.
- Lab 5: Securing Web Applications.
- Lab 6: Web Application Penetration Testing.
- Lab 7: Code Review and Security Test Scripts.
- Lab 8: AJAX Attacks.
- Lab 9: Code Review and Security Testing.