

Opleiding : Applicatiebeveiliging, ontwikkelingsmethoden

Praktijkcursus - 2d - 14u00 - Ref. APD

Prijs : 1480 € V.B.

★★★★☆ 4,3 / 5

Met de explosie van digitale technologie, die de ontwikkelingsmogelijkheden heeft verveelvoudigd, is beveiliging bij softwareontwikkeling een belangrijk onderwerp geworden voor bedrijven. Deze uitgebreide cursus leert je de methoden en oplossingen die je nodig hebt om de veiligheid van je ontwikkelingen te garanderen en te testen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ Het OpenSAMM-volwassenheidsmodel beheersen voor de ontwikkeling van veilige toepassingen
- ✓ Een beveiligingsanalyse kunnen uitvoeren van de software die aan een audit wordt onderworpen
- ✓ Identificeer de essentiële delen van de broncode die gecontroleerd moeten worden
- ✓ Applicatiebeveiliging testen

Doelgroep

Ontwikkelaars, applicatie-architecten, projectmanagers die betrokken zijn bij het beveiligen van applicaties.

Voorafgaande vereisten

Bekend zijn met de ANSSI-gids voor veiligheidshygiëne. Afronding van de inleidende cursus in cyberbeveiliging. Kennis van een programmeertaal.

Opleidingsprogramma

DEELNEMERS

Ontwikkelaars, applicatie-architecten, projectmanagers die betrokken zijn bij het beveiligen van applicaties.

VOORAFGAANDE VEREISTEN

Bekend zijn met de ANSSI-gids voor veiligheidshygiëne. Afronding van de inleidende cursus in cyberbeveiliging. Kennis van een programmeertaal.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ... De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 Inleiding

- Wat is codebeveiliging?
- Beveiligingsspelers: CERT, OWASP, BSIMM, enz.
- Wat zijn de risico's bij het ontwikkelen van een applicatie?
- Sporen achtergelaten door ontwikkelaars: geheugen, logs, enz.
- Wat is veilige applicatiecodering?
- Soorten aanvallen.

2 Toepassingsbeveiliging met OpenSAMM

- Het volwassenheidsmodel voor de ontwikkeling van veilige toepassingen.
- De 4 niveaus van volwassenheid.
- Impliciet startniveau.
- Initiele kennis en implementatie van veiligheidspraktijken.
- De effectiviteit/efficiëntie van veiligheidspraktijken verbeteren.
- Volledige beheersing van veiligheidspraktijken.

3 OpenSAMM instellen

- Voorbereiden.
- Evalueren.
- Definieer het gewenste doel.
- Bepaal het plan.
- Opzetten.
- Beschikbaar stellen.

Praktisch werk

Het volwassenheidsniveau van een organisatie berekenen.

4 Inleiding tot BSIMM

- Wat is het BSIMM (Building Security In Maturity Model)?
- Bouw een solide basis voor applicatieontwikkeling.
- Beste praktijk.

5 Analyse van de beveiliging van de gecontroleerde toepassing.

- Identificeer de kritieke delen van je code.
- Bepaal de reikwijdte van de audit en beperk deze tot de kritieke onderdelen.

6 Essentiële delen van de broncode om te controleren

- Identificeer de essentiële delen van de broncode die gecontroleerd moeten worden.
- Authenticatie en cryptografische mechanismen.
- Gebruikersbeheer.
- Toegang tot bronnen beheren.
- Mechanismen voor interactie met andere applicaties.
- Toegang tot databases.
- Voldoen aan de veiligheidseisen die zijn vastgesteld voor de toepassing.

Praktisch werk

Voorbeeld van het identificeren van de essentiële delen van de broncode die gecontroleerd moeten worden.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

7 Applicatiebeveiliging testen

- Identificeer de essentiële delen van de broncode die gecontroleerd moeten worden.
- Projectprocessen en testen.
- De globale aanpak.
- Het testplan en zijn variaties. De teststrategie.
- De risicogebaseerde benadering. Schatting.

Praktisch werk

Voorbeeld van een applicatietest.

Data en plaats

KLAS OP AFSTAND

2026 : 12 maa., 28 mei, 15 okt., 19 nov.

PARIS LA DÉFENSE

2026 : 12 maa., 28 mei, 15 okt., 19 nov.