Publicatiedatum : 11/07/2024

Opleiding : Beveiliging van Java-, .NET- en PHP-toepassingen

Praktijkcursus - 3d - 21u00 - Ref. ANP
Prijs : 2100 € V.B.

Deze zeer praktische cursus geeft je inzicht in de beveiligingsmechanismen die worden aangeboden door Java, .NET en PHP. Je leert hoe je beveiliging implementeert in de virtuele machine van Java en hoe je de beveiligingsmechanismen van de .NET- en PHP-platformen beheerst.

Pedagogische doelstellingen

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

- Veiligheid al in de ontwerpfase in de ontwikkeling integreren
- Identificeer potentiële ontwikkelingsfouten
- Veiligere applicaties ontwikkelen
- Beveiliging implementeren in de virtuele machine van Java
- Beheers de beveiligingsmechanismen van de .NET- en PHP-platforms

Doelgroep

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

Voorafgaande vereisten

De training "Beveiligde toepassingen ontwikkelen" hebben afgerond.

Opleidingsprogramma

DEELNEMERS

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

VOORAFGAANDE VEREISTEN

De training "Beveiligde toepassingen ontwikkelen" hebben afgerond.

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 Beveiliging van Java virtuele machine

- Klassen laden. Concept van "zandbak".
- SecurityManager, AccessController en definitie van permissies (.policy bestanden).
- Rechten maken met Java Beveiligingsrechten.
- Mechanismen om bytecode-integriteit, decompilatie en codeverduistering te beschermen.
- Beveiligingsfuncties voor applets.

Praktisch werk

Definitie van specifiek .beleid.

2 Java Authenticatie- en autorisatieservice

- JAAS-architectuur.
- Authenticatie via de PAM, notie van Subject en Principal.
- Toestemmingsbeheer, .policy-bestanden.
- JAAS gebruiken met Unix of Windows, JNDI, Kerberos en Keystore. Ondersteuning voor SSO.

Praktisch werk

Het toegangscontrolebeleid configureren, authenticatie implementeren.

3 Beveiligingsproblemen in .NET

- Definitie van veiligheid.
- Authenticatie, bescherming, encryptie.
- .NET-beveiligingstools.
- Uitvoerings-, authenticatie-, gegevens- en toegangsbeveiliging.
- Soorten bedreigingen, validatie van ingevoerde gegevens.

4 .NET Framework beveiliging

- Bescherming van montage-inhoud.
- Bescherming van de programma-uitvoering.
- Implementatie van een CLR-beveiligingsstrategie.
- Beveiligingsstrategie en inzet van applicaties. Principe van het gebruik van "bewijs".
- Uitvoeringsregels volgens de oorsprong van de applicaties.
- Nieuw in .NET4.
- Volledig/gedeeltelijk vertrouwen.

Praktisch werk

Het bewijsmateriaal van een assemblage ophalen. Een assemblage ondertekenen/wijzigen.

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.

5 .NET-codebeveiliging

- Transparante beveiligingscode, kritieke beveiligingscode en veilige kritieke code.
- Welke toegangsrechten heeft de code?
- Hoe code te verduisteren. Configuratie-informatie versleutelen.
- Declaratief/imperatief beheer van beveiligingsmechanismen implementeren.
- Uitvoeringsrechten van programma's beperken/verifiëren.
- Hoe rolgebaseerd beveiligingsbeheer implementeren.

Praktisch werk
Code toegangsautorisatie.

6 De juiste instellingen voor het beveiligen van PHP

- Het configuratiebestand PHP.ini. Identificeren van gevoelige directives, sessies en fouten.
- Hoe scriptbeveiliging instellen. Fysieke bescherming. Scripts op afstand of tijdens de uitvoering uitvoeren.
- Cookies en sessies.

7 Databasebeveiliging

- Wat zijn de mogelijke kwetsbaarheden die databases kunnen beïnvloeden? Beheer. Opslag.
- aanvallen van het type SQL-injectie". Principe en tegenmaatregelen. Opgeslagen procedures en geparametriseerde queries. Beperkingen.
- Wat zijn de toegangsbestanden? Organisatie en standaardwaarden. Anonieme toegang en protocollen.

8 Het gebruik van extensies in PHP beveiligen

- E-mail. Spam via een contactformulier: injecties en tegenmaatregelen.
- Hoe netwerktoegang implementeren met PHP. Sequentiële en recursieve aanroepen. Stealth aanvallen.

9 Kwetsbaarheden in webtoepassingen

- Waarom zijn webapplicaties meer blootgesteld? De grootste risico's voor webapplicaties volgens OWASP.
- Cross Site Scripting" of XSS-aanvallen. Waarom nemen ze toe? Hoe kunnen ze worden voorkomen?
- Injectieaanvallen (commando-injectie, SQL-injectie, LDAP-injectie, enz.). Aanvallen op sessies.
- Uitbuiten van kwetsbaarheden in het HTTP-front-end (Nimda-worm, Unicode-fout). Aanvallen op standaardconfiguraties
- Hoe te zoeken naar kwetsbaarheden.
- Onderzoek naar de meest voorkomende kwetsbaarheden. Cross-Site Scripting. SQL-injectie.
- Fouten in toepassingslogica. Buffer overloop. Uitvoering van willekeurige commando's.

10 Goede praktijken

- Wat zijn de verschillende soorten vermeldingen? Hoe valideer ik vermeldingen?
- Welke soorten bewerkingen kunnen worden uitgevoerd op numerieke types?
- Klassen en uitzonderingen.
- Multi-threading en synchronisatie.
- Input-output, serialisatie.
- Weten hoe je machtigingen beheert.

Praktisch werk

De praktische oefeningen zijn ontworpen om alle elementen van de taal te illustreren en de concepten systematisch te implementeren om de beveiligingsmechanismen onder de knie te krijgen.