Publicatiedatum : 24/07/2024

Opleiding : Beveiliging van webtoepassingen, samenvatting

seminarie - 2d - 14u00 - Ref. SEW
Prijs : 1850 € V.B.

Dit seminar biedt een overzicht van webbedreigingen. Kwetsbaarheden in browsers, sociale netwerken, SSL/TLS- en X509-certificaten en Java EE-, .NET- en PHP-toepassingen komen uitgebreid aan bod. Er worden oplossingen gepresenteerd voor het beschermen en controleren van de beveiliging van toepassingen.

Pedagogische doelstellingen

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

- Beveiligingsbedreigingen voor webapplicaties identificeren
- Webbeveiligingsprotocollen
- Typologieën van aanvallen begrijpen
- Webapplicaties beveiligen

Doelgroep

CIO's, CISO's, beveiligingsmanagers, ontwikkelaars, ontwerpers, projectmanagers die beveiligingsbeperkingen integreren, netwerk-, IT- en systeemmanagers of -beheerders.

Voorafgaande vereisten

Basisvaardigheden op het gebied van computer en netwerk.

Opleidingsprogramma

1 Bedreigingen en kwetsbaarheden van webtoepassingen

- Belangrijkste risico's voor webtoepassingen volgens IBM X-Force en OWASP.
- Cross Site Scripting (XSS), injectie en sessieaanvallen.
- Foutverspreiding met een webworm.
- Aanvallen op standaard configuraties.

DEELNEMERS

CIO's, CISO's, beveiligingsmanagers, ontwikkelaars, ontwerpers, projectmanagers die beveiligingsbeperkingen integreren, netwerk-, IT- en systeemmanagers of -beheerders.

VOORAFGAANDE VEREISTEN

Basisvaardigheden op het gebied van computer en netwerk.

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.

2 SSL- en TLS-beveiligingsprotocollen

- SSL v2/v3 en TLS, PKI, X509-certificaten, certificeringsinstantie.
- Invloed van SSL op de beveiliging van UTM en IDS/IPS firewalls.
- SSL/TLS kwetsbaarheden en aanvallen. Technieken voor het vastleggen en analyseren van SSL stromen.
- HTTPS-strippingaanval op beveiligde links.
- Aanvallen op X509-certificaten, OCSP-protocol.
- SSL en prestaties van webtoepassingen.

3 Aanvallen gericht op de gebruiker en de browser

- Aanvallen op webbrowsers, Rootkit.
- Smartphonebeveiliging voor surfen op het internet.
- Kwaadaardige code en sociale netwerken.
- Technieken voor social engineering.

4 Gerichte aanvallen op verificatie

- Authenticatie via HTTP, SSL met X509-certificaat van client.
- Implementeer sterke authenticatie met behulp van software.
- Niet opdringerige (agentless) Web SSO oplossing.
- Belangrijkste aanvallen op authenticatie.

5 Beveiliging van webservices

- Protocollen, beveiligingsstandaarden XML-encryptie, XML-handtekening, WS-beveiliging/betrouwbaarheid.
- Injectieaanvallen (XML-injectie, enz.), brute kracht of replay-aanvallen.
- Toepassingsfirewalls voor webservices.
- Belangrijkste spelers en producten op de markt.

6 Efficiënte beveiliging van webapplicaties

- Hardening: het beveiligen van het systeem en de HTTP-server.
- Virtualisatie en beveiliging van webapplicaties.
- .NET-, PHP- en Java-omgevingen. De 5 fasen van SDL.
- Fuzzing-technieken. Je toepassing kwalificeren met ASVS.
- WAF: welke efficiëntie, welke prestaties?

7 De beveiliging van webapplicaties beheren

- Pentest, beveiligingsaudit, kwetsbaarheidsscanners.
- Organiseer een effectieve technologiebewaking.
- Beveiligingsincidenten melden.

Demonstratie

Implementatie van een webserver met een X509 EV-certificaat: analyse van protocoluitwisselingen. Exploitatie van een kritieke beveiligingsfout in het HTTP front-end. HTTPS Stripping aanval.

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.

Data en plaats

KLAS OP AFSTAND
2026 : 17 maa., 28 mei, 8 sep., 26 nov.

PARIS LA DÉFENSE
2026 : 17 maa., 28 mei, 8 sep., 26 nov.