Beveiliging van webapplicaties

Praktijkcursus van 3 dagen - 21u
Ref : SER - Prijs 2024 : € 2 390 excl. BTW

Inbraak op de servers van de onderneming vormt een groot risico. Het is van essentieel belang de technologieën en producten te begrijpen en toe te passen waarmee de ingezette toepassingen, en met name risicotoepassingen zoals extranet-diensten en e-mail, doeltreffend kunnen worden beveiligd. Deze buitengewoon pragmatische opleiding zal u inwijden in de geheimen van de beveiliging van een online dienst, aan de hand van concrete voorbeelden van aanvallen en gepaste verdedigingen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De meest voorkomende zwakke plekken in webapplicaties identificeren

Het verloop van een aanval begrijpen

Eenvoudige beveiligingsmaatregelen voor webapplicaties implementeren

Een webserver configureren om het webverkeer te versleutelen met HTTPS

De beveiliging van uw webapplicaties testen

HANDS-ON WORK

Hierbij zullen beveiligde en beschermde online sites (multi-DMZ firewall) worden ingezet, SSL acceleratie, een analyse-proxy van het HTTP-protocol, een HTTP(S) flow injector, een sterke authenticatie met certificaat, aanvalstools op HTTPS-stromen...

HET PROGRAMMA

laatste update: 11/2021

1) Inleiding

- Statistieken en evolutie van web-gerelateerde zwakke plekken volgens IBM X-Force en OWASP.
- Evolutie van protocol- en applicatieaanvallen.
- De wereld van hackers: wie zijn ze? Wat zijn hun motieven, hun middelen?

2) Componenten van een webapplicatie

- De elementen van een N-tier applicatie.
- De HTTP front-end server, zijn rol en zwakke punten.
- De intrinsieke risico's van deze componenten.
- De belangrijkste spelers op de markt.

3) Het HTTP-protocol in detail

- Herhalingen TCP, HTTP, persistance en pipelining.
- De PDU's GET, POST, PUT, DELETE, HEAD en TRACE.
- Headervelden, statuscodes 1xx tot 5xx.
- Redirection, virtual host, proxy cache en tunneling.
- Cookies, attributen, bijbehorende opties.
- Authenticaties (Basic, Improved Digest...).
- HTTP-versnelling, proxy, web balancing.
- Protocolaanvallen HTTP Request Smuggling en HTTP Response splitting.

Installatie en gebruik van de Wireshark netwerk analyzer. Gebruik van een specifieke HTTP analyse-proxy.

DEELNEMERS

Netwerk- en systeembeheerders, webmasters.

VOORAFGAANDE VEREISTEN

Basiskennis van systemen, netwerken en internet.

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.

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.

4) Zwakke plekken van webapplicaties

- Waarom lopen webapplicaties meer gevaar?
- De voornaamste risico's van webapplicaties volgens OWASP (Top Ten 2017).
- "Cross Site Scripting"- of XSS-aanvallen - Waarom zijn ze in opmars? Hoe kun je ze vermijden?
- Injectie-aanvallen (commando-injectie, SQL-injectie, LDAP-injectie...).
- Aanvallen op sessies (cookie poisoning, session hijacking...).
- Misbruik van zwakke plekken in de HTTP front-end (Nimda-worm, Unicode-fout...).
- Aanvallen op de standaardconfiguraties (Default Password, Directory Transversal...).

Cross Site Scripting aanval. Misbruik van een zwakke plek in de http front-end. Omzeiling van een authenticatie door injectie van SQL query.

5) De netwerkfirewall in de bescherming van HTTP-toepassingen

- De netwerk-firewall, zijn rol en functies.
- Hoeveel DMZ's voor een N-Tier architectuur?
- Waarom is een netwerkfirewall niet in staat een webapplicatie te beschermen?

6) Beveiliging van de stromen met SSL/TLS

- Herhaling van de cryptografische technieken die in SSL en TLS worden gebruikt.
- Uw servercertificaten beheren, de X509-standaard.
- Wat brengt het nieuwe X509 EV-certificaat bij?
- Welke certificeringsinstantie moet ik kiezen?
- Technieken voor het vastleggen en analyseren van SSL-stromen.
- De belangrijkste gebreken van X509-certificaten.
- Gebruik van een reverse proxy voor de SSL-acceleratie.
- Het belang van HSM crypto hardwarekaarten.

Implementatie van SSL onder IIS en Apache. Aanvallen op HTTPS-stromen met sslstrip en sslsnif.

7) Systeem- en softwareconfiguratie

- De standaardconfiguratie, het grootste risico.
- Regels voor het installeren van een besturingssysteem.
- Linux of Windows. Apache of IIS?
- Hoe Apache en IIS configureren voor een optimale beveiliging?
- Middleware en de database. V.D.S. (Vulnerability Detection System).

Beveiligingsprocedure voor de web front-end (Apache of IIS).

8) Principe van beveiligde ontwikkeling

- Beveiliging van de ontwikkeling, welk budget?
- Beveiliging in de ontwikkelingscyclus.
- De rol van client-side code, beveiliging of ergonomie?
- Controle van door de client verzonden gegevens.
- Bestrijding van "Buffer Overflow" aanvallen.
- De ontwikkelingsregels die moeten worden nageleefd.
- Hoe de restrisico's aanpakken: Headers, misvormde URL, Cookie Poisoning... ?

9) Authenticatie van de gebruikers

- Authenticatie via HTTP: Basic Authentication en Digest Authentication of door de applicatie (HTML form).
- Sterke authenticatie: X509 client certificaat, Token SecurID, ADN digital Mobilegov...
- Andere software-authenticatietechnieken: CAPTCHA, Keypass, enz.
- Aanval op wachtwoorden: sniffing, brute force, phishing, keylogger.
- Aanval op sessienummers (session hijacking) of op cookies (cookie poisoning).
- Aanval op HTTPS-authenticatie (fake server, sslsniff, X509 certificate exploit...).

"Man in the Middle"-aanval op de gebruikersauthenticatie en overname van de sessie (session hijacking).

10) De "applicatiefirewall"

- Reverse proxy en applicatiefirewall, details van de functies.
- Wat zijn de voordelen van de applicatiefirewall voor de beveiliging van websites?
- Een applicatiefirewall invoegen op een systeem in productie. De marktspelers.

Toepassing van een applicatiefirewall. Beheer van het beveiligingsbeleid Aanvallen en resultaten.

DATA

KLAS OP AFSTAND
2024 : 23 sep, 11 dec

BRUSSEL
2024 : 23 sep, 11 dec