EduGroupe
Accompagner pour réussir

Sécurité du Web

Référence : **SECWEB** Durée : **3 jours (21 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances de base en systèmes, réseaux et d'Internet

Profil des stagiaires

- Cette formation Sécurité du Web s'adresse aux Administrateurs réseaux, systèmes et aux Webmasters

Objectifs

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque
- Mettre en place des mesures de sécurisation simples pour les applications Web
- Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
- Tester la sécurité de ses applications Web

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-Formateur expert Sécurité défensive

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Introduction

- Statistiques et évolution des failles liées au Web selon IBM X-Force et OWASP
- Evolution des attaques protocolaires et applicatives
- Le monde des hackers : qui sont-ils ? Quels sont leurs motivations, leurs moyens ?

2. Constituants d'une application Web

- Les éléments d'une application N-tiers
- Le serveur frontal HTTP, son rôle et ses faiblesses
- Les risques intrinsèques de ces composants
- Les acteurs majeurs du marché

3. Le protocole HTTP en détail

- Rappels TCP, HTTP, persistance et pipelining
- Les PDU GET, POST, PUT, DELETE, HEAD et TRACE
- Champs de l'en-tête, codes de status 1xx à 5xx
- Redirection, hôte virtuel, proxy cache et tunneling
- Les cookies, les attributs, les options associées
- Les authentifications (Basic, Improved Digest...)
- L'accélération HTTP, proxy, le Web balancing
- Attaques protocolaires HTTP Request Smuggling et HTTP Response splitting
- Travaux pratiques : Installation et utilisation de l'analyseur réseau Wireshark. Utilisation d'un proxy d'analyse HTTP spécifique

4. Les vulnérabilités des applications Web

- Pourquoi les applications Web sont-elles plus exposées ?
- Les risques majeurs des applications Web selon l'OWASP (Top Ten 2017)
- Les attaques "Cross Site Scripting" ou XSS - Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
- Les attaques en injection (Commandes injection, SQL Injection, LDAP injection...)
- Les attaques sur les sessions (cookie poisonning, session hijacking...)
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode...)
- Attaques sur les configurations standard (Default Password, Directory Transversal...)
- Travaux pratiques : Attaque Cross Site Scripting. Exploitation d'une faille sur le frontal http. Contournement d'une authentification par injection de requête SQL

5. Le firewall réseau dans la protection d'applications HTTP

- Le firewall réseau, son rôle et ses fonctions
- Combien de DMZ pour une architecture N-Tiers ?
- Pourquoi le firewall réseau n'est pas apte à assurer la protection d'une application Web ?

6. Sécurisation des flux avec SSL/TLS

- Rappels des techniques cryptographiques utilisées dans SSL et TLS
- Gérer ses certificats serveurs, le standard X509
- Qu'apporte le nouveau certificat X509 EV ?
- Quelle autorité de certification choisir ?
- Les techniques de capture et d'analyse des flux SSL
- Les principales failles des certificats X509
- Utilisation d'un reverse proxy pour l'accélération SSL
- L'intérêt des cartes crypto hardware HSM
- Travaux pratiques : Mise en œuvre de SSL sous IIS et Apache. Attaques sur les flux HTTPS avec sslstrip et sslsnif

7. Configuration du système et des logiciels

- La configuration par défaut, le risque majeur
- Règles à respecter lors de l'installation d'un système d'exploitation
- Linux ou Windows. Apache ou IIS ?
- Comment configurer Apache et IIS pour une sécurité optimale ?
- Le cas du Middleware et de la base de données. Les V.D.S. (Vulnerability Detection System)

8. Principe du développement sécurisé

- Sécurité du développement, quel budget ?
- La sécurité dans le cycle de développement
- Le rôle du code côté client, sécurité ou ergonomie ?
- Le contrôle des données envoyées par le client
- Lutter contre les attaques de type "Buffer Overflow"
- Les règles de développement à respecter
- Comment lutter contre les risques résiduels : Headers, URL malformée, Cookie Poisoning... ?

9. L'authentification des utilisateurs

- L'authentification via HTTP : Basic Authentication et Digest Authentication ou par l'application (HTML form)
- L'authentification forte : certificat X509 client, Token SecurID, ADN digital Mobilegov...
- Autres techniques d'authentification par logiciel : CAPTCHA, Keypass, etc.
- Attaque sur les mots de passe : sniffing, brute force, phishing, keylogger
- Attaque sur les numéros de session (session hijacking) ou sur les cookies (cookie poisoning)
- Attaque sur les authentifications HTTPS (fake server, sslsniff, X509 certificate exploit...)
- Travaux pratiques : Attaque "Man in the Middle" sur l'authentification d'un utilisateur et vol de session (session hijacking)

10. Le firewall "applicatif"

- Reverse proxy et firewall applicatif, détails des fonctionnalités
- Quels sont les apports du firewall applicatif sur la sécurité des sites Web ?
- Insérer un firewall applicatif sur un système en production. Les acteurs du marché
- Travaux pratiques : Mise en œuvre d'un firewall applicatif. Gestion de la politique de sécurité. Attaques et résultats

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.