Séminaire de formation

« Sécurité WEB »

« Maitriser la sécurité de vos applications WEB »

L'objectif de la formation

L'objectif de cette formation est :

- Maitriser les vulnérabilités des applications WEB
- Etre capable de détecter les failles relatives aux applications WEB
- Maitriser le processus d'audit applicatif

Public cible

Cette formation s'adresse :

- Développeurs web.
- Architectes d'applications web.
- Architectes d'applications web souhaitant renforcer ou actualiser leurs connaissances dans la sécurité des applications web.
- Experts en sécurité informatique.
- Chefs de projets ou responsables sécurité voulant mieux comprendre les techniques des attaquants pour mieux sécuriser leurs applications.

Les participants doivent avoir de bonnes connaissances des protocoles et des archtectures web classiques.

Une bonne connaissance des notions réseaux, les systèmes d'exploitation Windows et Linux, les technologies web.

Organisation et logistique

La formation sera assurée dans un hôtel de la place du 13 au 17 Avril 2015

Les participants sont invités à ramener leur ordinateur portable pour la réalisation des différents travaux pratiques. Les ordinateurs portables doivent avoir une bonne performance à savoir 4 Go de RAM au minimum avec un espace libre sur le disque dur d'une taille de 20 Go au minimum et doivent disposer d'un lecteur DvD, d'une carte réseau Ethernet et d'une carte Wifi.

Formateur

L'animateur**, Anis Fourati,** certifié CEH et ISO27001 LA est consultant sénior en sécurité des systèmes d'informations et a plusieurs références dans l'audit de la sécurité de l'information et particulièrement l'audit des applications web en Tunisie et à l'étranger.

Programme de la formation

Cette formation traite des aspects purement techniques pour permettre aux participants de toucher aux aspects pratiques de la sécurité WEB et de voir les risques réels encourus par la présence d'éventuelles failles dans les systèmes et applications.

La formation sera répartie comme suit :

- 40% du temps sera alloué aux aspects théoriques et méthodiques quant à la gestion de la mission d'audit et à la compréhension des notions de base.
- 60% du temps sera alloué à des exercices pratiques et à des études de cas.

Le programme de la formation se présente comme suit :

1. **Introduction** :
    a. Statistiques et évolution des failles – Evolution des attaques applicatives ;
    b. Présentation du TOP10 de l'OWASP
    c. Qui sont les hackers ?
2. **La technologie Web** :
    a. Architecture d'une application WEB – le protocole http ;
    b. L'application web : porte pour les hackers ;
    c. Les WebShells ;
    d. Terminologies essentielles ;
    e. Typologie et classification des attaques (Injection / redirection / session / authentification / manipulation de fichier / …)
3. **PARTIE 1 : Aspects pratiques des attaques WEB** :
    a. Les **attaques Cross site scripting**/Cross-Site Request Forgery/HTTP Response Splitting/ Cross-User Defacement ;
    b. Les **attaques par injection** (SQL Injection /command Injection/OS injection/Xpath injection/….) ;
    c. Les **attaques sur les sessions** (Cache Poisoning/Hijacking/ Mauvaise gestion des sessions et de l'authentification….) ;
    d. Les vulnérabilités **d'authentification et l'autorisation** (Brute force/ insuffisance d'authentification / insuffisance d'autorisation/ Escalation de

privilège/ Référence directe non sécurisée à un objet .....) ;

e. La **manipulation des fichiers** (Remote File Include /Remote File upload/Path Manipulation/Directory traversal/Directory indexing....);
f. Les **attaques logiques** (déni de service/Abus de fonctionnalité/ insuffisance anti-automation...) ;
g. **Attaques sur la configuration standard** (Mauvaise configuration/configuration par défaut/mot de passe par défaut...) ;
h. L'attaque de **Phishing** ;
i. Les attaques **réseaux** (DOS/DDOS/DNS cache poisonning) ;
j. Les **Bonnes pratiques** du développement sécurisé et d'administration de plate forme d'hébergement :
   i. Bonnes pratiques pour le développement sécurisé ;
   ii. Bonnes pratiques pour l'administration des sites web ;
   iii. Bonnes pratiques pour la sécurité des plateformes web ;
   iv. Travaux pratiques : correction de certaines vulnérabilités.
k. **Travaux pratiques**
   i. Webshell
   ii. Attaques par injection
   iii. Attaque sur certains CMS : Word Press
   iv. Attaques XSS
   v. Attaque XSS (Stored, Reflected, redirection, vol de session)
   vi. Attaque sur les sessions
   vii. Attaque par brute force
   viii. Attaque sur certains CMS : Joomla / Twiki / Vitiger CRM
   ix. Exemple d'attaque DoS
   x. Exemples de correction des vulnérabilités WEB : SQL Injection, XSS, Remote File Inclusion, remote command execution, ...

4. **PARTIE 2 : Comment détecter les failles applicatives** :

a. Les **Types d'audit** (Dynamique / Statique, Boite noire / boite Blanche, ...) ;
b. Démarche d'audit (TOP10 de l'OWASP, Approche du CEH, outils d'audit, référentiels d'audit applicatifs, ...) ;
c. Approche de l'OWASP pour la validation des applications (approche e test par niveau, OWASP ASVS 2009 et 2014, ...);
d. Audit dynamique (outils, démarches, ...) ;
e. Audit statique (outils, démarches, ...) ;
f. Analyse des risques
   i. Approches d'analyse des risques techniques ;
   ii. OWASP Risk Rating;

g. Travaux pratiques

i. Recherche de vulnérabilités sur un CRM
ii. Audit d'un formulaire d'authentification : préparation d'une check-list et déroulement des tests
iii. Scan des vulnérabilités dynamiques (Acunetix, Tamper Data, ...) et interprétation des résultats;
iv. Analyse des résultats de scan et Exploitation des vulnérabilités SQL Injection ;
v. Scan des vulnérabilités statiques
    1. préparation de signature de détection d'une faille ;
    2. Scan d'une application;
    3. Exemple d'exploitation suite à une analyse statique;
vi. Analyse des risques conformément à l'OWASP Risk Rating;