Formation sécurité web
4 jours

- ✔ Rappel sur les serveurs, langages et technologies du Web :
  - ✗ Serveurs Apache, IIS, JSP, MySQL, PosgreSQL, Oracle...
  - ✗ Langage ASP, JSP, PHP, SQL, Javascript, Flash....
  - ✗ Technologies HTTP, HTTPS, Ajax...
- ✔ Plan d'attaque d'un site Web
  - ✗ Récupération d'informations, cartographie du site web
  - ✗ Analyse du fonctionnement de l'application Web
  - ✗ Test des éléments du coté client
  - ✗ Test des mécanismes d'authentification
  - ✗ Test du mécanisme de session
  - ✗ Test des contrôles d'accès
  - ✗ Test d'injection
  - ✗ Test de vulnérabilité du serveur
- ✔ Serveur Apache, PHP, MySQL
  - ✗ Installation
  - ✗ Configuration de base
  - ✗ Implémentation des exercices

- ✔ Récupération d'informations, cartographie du site web
  - ✗ Observation
  - ✗ Outils
  - ✗ Google Hacking
- ✔ Passer les contrôles côté client
  - ✗ Champ caché de formulaire
  - ✗ Coookies
  - ✗ Paramètre de l'URL
  - ✗ Obfuscation Javascript
  - ✗ Contre mesure

- ✔ Attaques d'authentification
  - ✗ Attaque sur les mots de passe
  - ✗ Utilisation des fonctions du site (mot de passe oublié, mauvais mot de passe, …)
  - ✗ Contre mesure et bonnes pratiques
- ✔ Attaques de session
  - ✗ Fragilité des ID de session
  - ✗ Vol de session
    - – Reflected XSS
    - – Stored XSS
    - – XSRF (Cross-Site Request Forgery)
  - ✗ Contre mesure et bonnes pratiques
- ✔ Contrôle d'accès
  - ✗ Les fonctions non-protégées
  - ✗ Les fonctions protégées par une authentification
  - ✗ Accès aux fichiers

- ✗ Contre mesure

- ✔ Les injections
  - ✗ Injection de code interprété
  - ✗ Injection SQL
  - ✗ Inclusion de fichiers
  - ✗ Contre mesure et bonnes pratiques
- ✔ Exploiter Path Traversal
- ✔ Attaque du serveur Web
  - ✗ Failles dûes à une mauvaise configuration du serveur
  - ✗ Failles inhérentes à la version du serveur (exploit)
  - ✗ Une bonne configuration d'Apache, PHP, MySQL

- ✔ Entrainement : Découverte du Live CD OWASP