Présentiel/distanciel

Auditer et sécuriser un site Web

Cofinancé par l'Union européenne

Objectifs pédagogiques

- Auditer une application Web par un test de pénétration à l'aide d'outils automatiques mais aussi manuellement ;
- Mettre en place des contres mesures pour se prémunir des attaques.

Prérequis

- Notion de développement d'application Web ;
- Connaissances de base sur Apache, PHP et MySQL ;
- Bases d'utilisation de Linux.

Public concerné

Développeurs et administrateurs de sites et serveurs Web.

Présentiel/distanciel

Programme détaillé

Les technologies du Web
- Historique
- Les langages les plus utilisés
- Les Frameworks
- Les CMS

Tour d'horizon des attaques sur le Web
- Qui ? Pourquoi ? Comment ?
- Les cibles les plus courantes

Classification des attaques Web
- Présentation de l'OWASP
- Classification des dix attaques les plus courantes

Installation d'un serveur LAMP
- Installation
- Tour d'horizon des éléments de sécurité dans les fichiers de configuration
  - Fichiers de configuration d'apache
  - Fichier de configuration de PHP
  - Fichier de configuration de MySQL

Passage des contrôles côté client
- Les outils inclus dans les navigateurs
- Utilisation d'un proxy local (ZAP, BurpSuite)
- Utilisation d'addons (Tamper Data, Web developper, etc)
- Débogage de JavaScript (principe d'obfuscation)
- Bonne pratique et règle de sécurité pour les contrôles côté client
- Technique d'hameçonnage par injection dans l'URL

Les failles XSS
- Faille XSS reflétées
- Faille XSS stockées
- Exemple de récupération de session
- Se prémunir des failles XSS

Passage d'authentification
- Les bonnes pratiques
  - Gérer correctement les IDs de session
  - Politiques des mots de passe
- Les authentifications HTTP

Les injections SQL classiques
- Rappels sur les bases de données
- Principe des injections SQL
- Exemples et exercices pratiques

Les injections SQL en aveugle
- Principe
- Exploitation
- Exemples et exercices

Détection et exploitation des injections SQL
- Par des outils automatiques
- Manuellement
- Se prémunir des injections SQL

Cofinancé par l'Union européenne

La faille Include
- Exploitation d'une faille include
- Bonnes pratiques pour se prémunir des failles includes

La faille Upload
- Passage des extensions et types MME
- Mise en place d'un shell
- Saturation du serveur
- Contre mesure

Les outils d'audit automatiques
- ZAP
- W3AF
- Acunetix
- Burpsuite

Interprétation et vérification des résultats
- Interpréter les résultats d'un outil automatique
- Vérifier la véracité des alertes remontées

Synthèse des bonnes pratiques pour la réalisation d'une application Web

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

Jérôme HENNECART Enseignant à l'université de Valenciennes, commandant de gendarmerie réserviste et spécialiste de la lutte anti-cybercriminalité, il est expert en failles Web. Il est responsable du module Web de la licence professionnelle « ethical hacking » appelée CDAISI, la seule en France en sécurité dite offensive. Il est aussi responsable du module transversal Défense » de l'université de Valenciennes.
Il forme les ntech de la gendarmerie de la région Nord-Pas de Calais. Il réalise des audits pour des grandes entreprises Françaises et Africaines. Il est aussi membre du conseil d'administration de l'association ACISSI et organise chaque année les RSSIL et le challenge de hacking » Hacknowledge « .
Il donne des conférences en Europe et en Afrique sur le Web, les logiciels libres et la sécurité informatique. Il est également le co-auteur de plusieurs best-sellers sur la sécurité informatique parus aux Editions ENI.

Accessibilité de la formation