Programme de la Formation
Sécurité des applications web

Référence : SSI_TR1

Description : Cette formation vous permettra d'identifier, de comprendre et de régler les failles de sécurité que l'on retrouve communément dans les applications web. Les travaux pratiques permettront de se mettre tantôt à la place de l'attaquant, tantôt à la place de la victime afin de mieux appréhender les vecteurs d'attaques et de comprendre comment protéger ses applications.

Durée : 2 jours.

Déroulé de la formation :

MATIN

MODULE 0 : Objectifs du cours

Journée 1

Introduction : Présentation des objectifs et du déroulement de la formation.

Tour de table : Présentation du groupe, des participants et de leurs attentes.

MODULE 1 : Introduction

Journée 1

Objectifs du module :

- Décrire les menaces qui pèsent sur les applications Web d'aujourd'hui.
- Identifier les organisations et ressources qui aident à identifier et corriger les vulnérabilités dans les applications.
- Décrire les techniques de test de sécurité applicative courantes.

ABlogiX – 2830, Route de Prévelles – 72110 Saint-Célerin
Tél : +33 2 85 29 43 43 – Web : www.ablogix.fr - SIREN : 494586399 – DREETS : 52720152772

MODULE 2 : Bases des applications Web

Journée 1

Objectifs du module :

- Décrire la structure habituelle des applications web.
- Comprendre et utiliser les bases de HTML et HTTP.

MODULE 3 : Les injections

Journée 1

Objectifs du module :

- Comprendre ce qu'est une attaque par injection.
- Réaliser une injection SQL.

APRÈS-MIDI

MODULE 4 : Contournement d'authentification

Journée 1

Objectifs du module :

- Lister les implications des mécanismes d'authentification faibles et des failles dans la gestion des sessions.
- Décrire comment les pirates réalisent des attaques de type :
  - *Session hijacking*
  - *Session fixation*
  - *Weak session management*
  - *Weak authentication management*
- Implémenter des mécanismes de mitigation :
  - Renforcement de la gestion des sessions.
  - Amélioration des mécanismes d'authentifications.
  - Prévenir le vol de session (*Session hijacking)*.

ABlogiX – 2830, Route de Prévelles – 72110 Saint-Célerin
Tél : +33 2 85 29 43 43 – Web : www.ablogix.fr - SIREN : 494586399 – DREETS : 52720152772

MODULE 5 : Exposition de données sensibles

Journée 1

Objectifs du module :

- Identifier les données sensibles.
- Comprendre et corriger les vulnérabilités courantes.
- Identifier les failles exposant des données sensibles.

-

MODULE 6 : Entités XML externes (*XXE*)

Journée 1

Objectifs du module :

- Décrire les effets possibles d'une attaque *XML External Entities (XXE) injections*.
- Protéger des ressources des injections *XXE*.

MATIN

MODULE 7 : Le contrôle d'accès au niveau des fonctions

Journée 2

Objectifs du module :

- Décrire les vulnérabilités de type *missing function-level access control*.
- Accès direct aux pages d'administration.
- Élévations de privilèges.
- Mise en œuvre du contrôle d'accès au niveau des fonctions.

MODULE 8 : Défauts de configuration

Journée 2

Objectifs du module :

- Répertorier les mauvaises pratiques de configuration.
- Mettre en œuvre les bonnes pratiques pour sécuriser ses configurations.

ABlogiX – 2830, Route de Prévelles – 72110 Saint-Célerin
Tél : +33 2 85 29 43 43 – Web : www.ablogix.fr - SIREN : 494586399 – DREETS : 52720152772

MODULE 9 : *Cross-site scripting (XSS)*

Journée 2

Objectifs du module :

- Décrire le principe d'une attaque par script inter-site (*cross-site scripting - XSS*).
- Comparaison des attaques XSS avancé et du *phishing*.
- Implémentation de techniques de protections contre les attaques XSS.

APRÈS-MIDI

MODULE 10 : Composants vulnérables.

Journée 2

Objectifs du module :

- Identifier les composants vulnérables.
- Implémentation de leur mise à jour.

MODULE 11 : Insuffisance de journalisation et de surveillance.

Journée 2

Objectifs du module :

- Décrire les effets possibles d'une journalisation et d'une surveillance insuffisantes.
- Implémentation d'une journalisation et d'une surveillance suffisantes.

MODULE 12 : Intégration de la sécurité dans le cycle de développement.

Journée 2

Objectifs du module :

- Mise en œuvre des tests de vulnérabilité pendant le cycle de développement.
- Présentation de la suite logicielle *HCL AppScan*.

ABlogiX – 2830, Route de Prévelles – 72110 Saint-Célerin
Tél : +33 2 85 29 43 43 – Web : www.ablogix.fr - SIREN : 494586399 – DREETS : 52720152772

Public concerné et prérequis

Ce cours est destiné aux développeurs, webmasters, architectes logiciel et chargés de projets souhaitant acquérir les bases de la sécurité applicative afin d'identifier les vulnérabilités des applications et service web.

- La maîtrise des bases du développement d'application Web est requise.
- La maîtrise des bases des réseaux TCP/IP et d'Internet est également requise.

Objectifs pédagogiques

Les objectifs de la formation sont les suivants :

- Obj.1 - Comprendre les menaces qui visent une application web.
- Obj.2 - Comprendre et appliquer les stratégies utilisées pour compromettre une application web.
- Obj.3 - Comprendre et corriger les problèmes de design et d'implémentation communes.
- Obj.4 - Comprendre et corriger les failles courantes (Injection SQL/XSS, défaut d'authentification, etc.)

Compétences visées

À l'issue de la formation le participant sera capable de :

- Reconnaître les vulnérabilités applicatives communes.
- Implémenter les correctifs appropriés.
- Identifier des données sensibles.
- Implémenter les mécanismes nécessaires à leur sécurisation.

Modalités et délais d'accès, accessibilité PSH[1]

Durée : 2 jours

Lieu : en entreprise (France entière) OU en Classe à distance

Dates : Pour tout souhait de formation, veuillez nous téléphoner au numéro indiqué en pied de page. Nous conviendrons avec vous d'une solution sur-mesure dans un délai co-élaboré d'un mois maximum.

Nombre minimum de stagiaires : 4 personnes.

Accessibilité personnes handicapées : Les salles que nous louons sont accessibles aux PMR[2]. Pour tout autre type de handicap, nous consulter au préalable pour co-construire une solution adaptée dans la mesure des ressources disponibles.

1 PSH : Personne en Situation de Handicape.

2 PMR : Personne à Mobilité Réduite.

ABlogiX – 2830, Route de Prévelles – 72110 Saint-Célerin
Tél : +33 2 85 29 43 43 – Web : www.ablogix.fr - SIREN : 494586399 – DREETS : 52720152772

Moyens pédagogiques, techniques et d'encadrement

La plus part des modules abordés font l'objet de travaux pratiques qui seront réalisés sur des cas concrets. Des questions de vérification des acquis seront posées. Chaque participant aura à disposition un ordinateur avec un navigateur Web.

Un support de formation sera fourni pour chaque module et sera présenté via un vidéoprojecteur ou grand écran. Un tableau blanc ou interactif devra être mis à disposition avec des stylos.

La formation est animée par un consultant-formateur ce qui permet aux participants de bénéficier de l'apport de retour d'expériences de terrain.

Modalité d'évaluation

Chaque participant aura à disposition un cahier d'exercice qui lui permettra de réaliser les exercices sur des cas pratiques depuis son ordinateur à la fin de chaque module de cours pour valider sa compréhension. Le formateur sera sollicité pour toute question et il pourra suivre l'avancement et corriger les exercices.

L'intervenant

ABLOGIX bénéficie d'une expertise de plus de 10ans en sécurité applicative et ses formateurs interviennent sur les différentes technologies WEB et sur les différentes catégories de vulnérabilités.

Validation de la formation

Certificat de réalisation.

Tarifs de la formation

À partir de 1100 euros HT par stagiaire, selon les besoins de construction de contenu sur-mesure. Hors frais de déplacement.

ABlogiX – 2830, Route de Prévelles – 72110 Saint-Célerin
Tél : +33 2 85 29 43 43 – Web : www.ablogix.fr - SIREN : 494586399 – DREETS : 52720152772