

140, bd Haussmann  
75008 Paris  
T. +33 (0) 1 45 63 19 89  
magento@academy-ecommerce.com  
[magento.academy-ecommerce.com](mailto:magento.academy-ecommerce.com)

## Formation **Développeur Sécurité**

*Développeur indépendant ou en agence, vous souhaitez enrichir vos connaissances en sécurité de la programmation et ainsi renforcer la robustesse de vos développements.*

*Manager ou dirigeant, vous souhaitez sensibiliser vos collaborateurs à la sécurité et ainsi valoriser cet aspect critique du E-commerce auprès de vos clients.*

### **Description**

*La formation Développeur Sécurité permet de maîtriser les différents risques de sécurité pouvant être rencontrés au cours d'un développement. La formation Développeur Sécurité valorise ainsi un autre aspect du métier de développeur, auprès des clients finaux et au sein de l'entreprise. Toutes les grandes familles de vulnérabilités du web sont travaillées en détail, par la théorie et la pratique : prévention, détection, correction, au travers d'exemples concrets. Certaines spécificités liées à la configuration de l'environnement de développement sont également couverts, tels que la configuration de PHP. La formation Développeur Sécurité est indispensable à tout développeur expert dans sa technologie.*

*D'une durée de 2 jours et en constante adéquation avec la réalité des vulnérabilités du web, la formation Développeur Sécurité est accompagnée d'un support de formation riche, pouvant notamment servir de mémo technique pour les futurs développements.*

### **À l'issue de la formation**

*Une assistance professionnelle d'une durée de deux heures est assurée par les experts de l'Académie dans les six mois suivant la formation.*

### **Prérequis**

*Vous avez de solides connaissances en développement PHP et vous connaissez les couches base de données.*

### **Objectifs**

*Maîtriser les problématiques de sécurité liées aux technologies web.*

*Maîtriser l'ensemble des vulnérabilités « web » : savoir comment les éviter, les détecter, les corriger.*

*Acquérir les bonnes pratiques de développement sécurisé.*

# Plan de formation

## Jour 1

### Introduction à la sécurité applicative

- Introduction à la sécurité web : injections SQL, XSS, CSRF, etc.
- L'écosystème de la sécurité web
- Quels sont les risques de vos clients ? Sachez y répondre !

### La sécurité dès la conception

- Appliquer un modèle de sécurité.
- Identifier & minimiser la surface d'attaque.
- Gérer les erreurs de manière sécurisée.
- Limiter les privilèges (CGI, backoffice, etc.).
- Faire reposer la sécurité sur des principes, frameworks et algorithmes éprouvés.
- Garder les mécanismes de sécurité simples.
- Détecter les intrusions (journaux d'événements intelligents, détecter les comportements « anormaux »).
- Connaître les limites de sécurité de l'infrastructure et des services, savoir effectuer une analyse objective du niveau de sécurité de ces éléments.

### Paramètres à prendre en compte lors d'une auto-évaluation

- Savoir analyser son propre niveau de sécurité en partant du principe que les attaquants possèdent le code source.
- Gérer les entrées et actions utilisateur pour éviter les malveillances.
- Séparation des tâches dans l'application afin d'éviter les incohérences.
- Comment évaluer et « calibrer » le niveau de sécurité cible dans ces conditions ?

### Les grandes familles de vulnérabilités récurrentes :

- XSS (Cross Site Scripting)
  - Qu'est ce qu'un XSS ? Dans quel contexte se produit-il et quels sont les impacts potentiels ?
  - Les différents types de XSS : XSS éphémères, XSS stockés, XSS dans les logs, XSS dans le backoffice.
  - Les vecteurs d'injections.
  - Prévention des XSS.
- Injection SQL
  - Qu'est ce qu'une injection SQL ? Dans quel contexte se produit-elle ? Quels sont les impacts potentiels ?
  - Différents types d'injections SQL.
  - Prévention des injections SQL.
- CSRF (Cross Site Request Forgery)
  - Qu'est ce qu'un CSRF ?
  - Dans quel contexte se produit-il ?
  - Comment se produit-il et quels sont les impacts ?
- Gestion des fichiers :
  - File Upload :

- Risques et Bonnes pratiques liés aux fonctionnalités d'upload de fichiers.
- File download :
  - Risques et bonnes pratiques liés aux fonctionnalités de téléchargement de fichiers.
- Autres vulnérabilités moins courantes : Directory Traversal, URL redirection abuse, http response splitting, etc.

## Jour 2

### Problématiques liées à l'authentification

- Sessions
  - Problèmes d'entropie.
  - Session guessing.
  - Session fixation.
- Cookies
  - Présence d'informations confidentielles dans les cookies.
  - Transmission des cookies en http.
- Mots de passe
  - Génération des mots de passe.
  - Stockage des mots de passe (chiffrement).
  - Vérification de robustesse des mots de passe.
  - Gestion des questions de type « Mot de passe perdu ».
  - Accepter des mots de passe en http.
  - Problématique du blocage des comptes (Déni de service).
  - Faire reposer l'information sur des briques existantes : LDAP, domaine windows, etc.
- Gestion des privilèges
  - Les bonnes pratiques pour assurer la sécurité du système de privilèges.

### Risques liés au spam et à l'utilisation « automatisée » d'un site :

- Prévenir l'utilisation automatisée du site ou d'une de ses fonctionnalités lorsque nécessaire.
- Acquérir les bonnes méthodes pour lutter contre l'utilisation automatisée : Captcha et autres tests de Turing.

### Webservices

- Risques de sécurité liés aux WebServices.

### Problèmes de configuration serveur :

- Configuration PHP, ASP, etc.
- Configuration Apache, IIS, etc.
- Gérer Flash.

### Présentation des outils de sécurité à utiliser dans le cadre d'un projet de développement :

- Outils de tests automatisés.
- Outils d'analyse statique de code source.
- Les méthodes de test manuel : test en 'boite noire'.
- Les méthodes d'audit manuel : apprendre à auditer du code.

## **Présentation des frameworks permettant de renforcer efficacement la sécurité d'un développement**

### **Cas pratique :**

- Mettre en place rapidement et efficacement des correctifs génériques sur un développement existant.
- Analyse de code vulnérable et mise en place de correctifs : Injections SQL, XSS, CSRF, Directory traversal, remote file include, etc.

### **Les limites des fonctions de sécurité :**

- Clauses order by.
- Les XSS 'browser dependant'.
- Appliquer le concept de liste blanche

# L'Académie *s'engage*

## **Centre Magento de référence**

*Centre Magento de référence, l'Académie s'engage à proposer des formations Magento garantissant le meilleur retour sur investissement possible. Une méthodologie de travail rigoureuse, une constante adaptation à la réalité des projets, un investissement communautaire constant, garantit un haut niveau d'expertise en formation, conseil et audit.*

## **Professionnalisme et expertise**

*Certifiés et reconnus par l'éditeur et fortement investis dans la Communauté Francophone, les experts de l'Académie sont en mesure de garantir un niveau d'expertise sans équivalent. Cette expertise, combinée à leurs valeurs de rigueur et d'exigence, est transmise sans aucune rétention d'information dans le cadre des formations. Ainsi, les stagiaires bénéficient des conseils issus des différentes expériences des experts formateurs.*

## **Retour sur investissement**

*Grâce à des formations adaptées, complètes et en phase avec la réalité des projets Magento, l'Académie est en mesure de garantir un retour sur investissement rapide : une semaine de formation permet ainsi d'économiser 3 à 4 mois d'apprentissage autodidacte. Le support de formation, riche et complété des conseils avisés des experts de l'Académie, permet de retrouver par écrit les points travaillés pendant la formation. De plus, toutes les formations sont accompagnées de deux heures d'assistance professionnelle, dans les six mois suivant la formation.*

## **Indépendance et transparence**

*Centre de formation uniquement, l'Académie n'a aucunement vocation à réaliser des prestations de développement ou d'intégration. L'Académie s'engage donc sur un principe de non-concurrence, et garantit la confidentialité des informations stratégiques qui lui sont communiquées. Centre Magento de référence, l'indépendance de l'Académie vis-à-vis de Magento Inc. garantit des formations, du conseil et des audits transparents, sans complaisance.*