

KAÏNA-COM

CATALOGUE DE FORMATION

Sécurité des applications Web



KSE002 – Sécurité des applications Web

Référence KSE002

Niveau

- Débutant
- Intermédiaire
- Expert

Nombre de jours Programme de formation :

- 24 heures (4 heures/jour)

Lieu de la formation

- I: i-learning, Formation individuelle (Formation en ligne)
- V: v-learning, classe virtuelle
- C: c-learning, cours présentiel

KAINA-COM

LE CARRÉ HAUSSMANN II,
6 Allée de la Connaissance
77127 Lieusaint - France

Prérequis Étant donné que les applications Web sont basées sur HTTP, HTML et JavaScript, il est recommandé :

- Une compréhension générale de HTTP, du concept de requête-réponse, des en-têtes HTTP, des cookies HTTP..

- Comprendre le HTML.

- Comprendre le JavaScript.

Les termes pertinents sont présentés dans ce cours, mais une connaissance préalable aidera le participant.

De plus, une connaissance préalable de l'architecture des applications Web et de l'infrastructure Web sera utile.

Un niveau d'anglais business moyen est requise car la formation sera dispensée en anglais.

Ce sujet continue à la page suivante



KSE002 – Sécurité des applications Web, Suite

Public

Les développeurs d'applications et tous ceux qui cherchent à mieux comprendre comment créer des applications sécurisées.

Objectifs

Lors de la gestion de la sécurité, l'accent a été mis principalement sur la sécurisation de l'infrastructure réseau et du système d'exploitation du serveur. Cependant, au cours des dernières années, l'attention s'est déplacée vers la couche application. En effet, la sécurité des infrastructures (réseau et OS) s'est considérablement améliorée tandis que les applications sont restées vulnérables. La couche application est devenue la principale cible des attaques. Cela est particulièrement vrai pour les applications Web qui sont plus vulnérables.

Le cours explique comment ses aspects tels que l'authentification, la confidentialité et l'intégrité des données s'appliquent aux applications Web. De plus, les participants apprendront en profondeur quelles sont les vulnérabilités des applications Web, quelles en sont les causes, comment les empêcher lors de la conception / codage et tester les perspectives d'attaques et quelles contre-mesures sont nécessaires pour empêcher l'exploitation de ces vulnérabilités.

Ce sujet continue à la page suivante



KSE002 – Sécurité des applications Web, Suite

Contenu du cours

Contenu du cours :

Table 1: KSE002 - Contenu du cours

Chapter	Description
Introduction	<ul style="list-style-type: none"> The unique security aspects and challenges of web applications Application layer logical vulnerabilities Application layer DoS and DDoS
Confidentiality and data integrity	<ul style="list-style-type: none"> Encryption and hashing SSL
HTTP Authentication and session management attacks and mitigation	<ul style="list-style-type: none"> HTTP basic and digest authentication Certificate based authentication Application layer authentication Web session management mechanisms Session hijacking Cookie poisoning
Non-validated input and related attacks	<ul style="list-style-type: none"> Direct object reference vulnerability and mitigation Input validation methodology Evasion techniques
Injection attacks and mitigation	<ul style="list-style-type: none"> SQL injection attack description and examples SQL injection evasion techniques Command (OS) injection LDAP Injection Buffer overflow

Ce sujet continue à la page suivante



KSE002 – Sécurité des applications Web, Suite

Contenu du cours, Suite

Chapter	Description
Cross site scripting attacks and mitigation	<ul style="list-style-type: none">• Reflected XSS• Stored XSS• DOM based XSS• XSS evasion techniques• XSS mitigation countermeasures
Cross site request forgery and mitigation	<ul style="list-style-type: none">• CSRF (XSRF) attack description• ISRF attack description• CSRF/ISRF mitigation countermeasures
Regulations and web application security	<ul style="list-style-type: none">• OpenID• OAuth• SAML• XCAML• Web application single sign on (SSO) and OpenID
Security of AJAX based web applications	<ul style="list-style-type: none">• Security of AJAX based web applications
The End	<ul style="list-style-type: none">• Summary• Q&A• Evaluation

