Training Catalogue
22/05/2020

KAÏNA-COM
TRAINING CATALOGUE

Web Application Security

Nos locaux
KAÏNA-COM France
LE CARRÉ HAUSSMANN II
6 Allée de la Connaissance
77 127 Lieusaint

Contact
+33(0)9 50 20 91 64

E-mail
info@kaina-com.fr

Site Internet
www.kaina-com.fr

KSE002 – Web Application Security

Reference	KSE002
Experience	☒ Beginner ☒ Intermediate ☐ Advanced
Duration	Training Program: • 3 days
Training Method	☐ I: i-learning, individual training (web-based training) ☒ V: v-learning, virtual class ☐ C: c-learning, classroom training **KAÏNA-COM** LE CARRÉ HAUSSMANN II, 6 Allée de la Connaissance 77127 Lieusaint - France
Price	2.049,00 € HT
Prerequisite	Since web applications are based on HTTP, HTML and JavaScript, the following is recommended: • A general understanding of HTTP, the request-response concept, HTTP headers, HTTP cookies. • Understanding HTML. • Understanding JavaScript. The relevant terms are presented in the course, but prior knowledge will help the participant. Additionally, prior knowledge on web application architecture and in the web infrastructure will help.

Continued on next page

KSE002 – Web Application Security, Continued

Audience

Application developers and Everyone who seeks to better understand how to build Secure Applications.

Objective

Most of the focus when dealing with security has been on securing the network infrastructure and the server OS. However, during the last few years the focus has shifted to the application layer. This is because infrastructure (network and OS) security has improved significantly while applications have remained vulnerable. The application layer has become the main target of attack. This is particularly true for web applications which are more vulnerable.
The course discusses how application aspects such as authentication, confidentiality and data integrity apply to web applications. In addition, participants will learn in depth what web application vulnerabilities are, what causes them, how to prevent them from design/coding and testing perspectives and what countermeasure are required to prevent exploitation of these vulnerabilities.

Continued on next page

KSE002 – Web Application Security, Continued

Course Contents

Course Contents :

Table 1: KSE002 - Course Contents

Chapter	Description
Introduction	• The unique security aspects and challenges of web applications • Application layer logical vulnerabilities • Application layer DoS and DDoS
Confidentiality and data integrity	• Encryption and hashing • SSL
HTTP Authentication and session management attacks and mitigation	• 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	• Direct object reference vulnerability and mitigation • Input validation methodology • Evasion techniques
Injection attacks and mitigation	• SQL injection attack description and examples • SQL injection evasion techniques • Command (OS) injection • LDAP Injection • Buffer overflow

Continued on next page

KSE002 – Web Application Security, Continued

Course Contents, continued

Chapter	Description
Cross site scripting attacks and mitigation	• Reflected XSS • Stored XSS • DOM based XSS • XSS evasion techniques • XSS mitigation countermeasures
Cross site request forgery and mitigation	• CSRF (XSRF) attack description • ISRF attack description • CSRF/ISRF mitigation countermeasures
Regulations and web application security	• OpenID • OAuth • SAML • XCAML • Web application single sign on (SSO) and OpenID
Security of AJAX based web applications	• Security of AJAX based web applications
The End	• Summary • Q&A • Couse's Evaluation