EC - COUNCIL CERTIFIED SECURE PROGRAMMER

DURATION: 5 DAYS

COURSE OVERVIEW

Software defects, bugs, and flaws in the logic of the program are consistently the cause for software vulnerabilities.

Analysis by software security professionals has proven that most vulnerabilities are due to errors in programming.

Hence, it has become a must for organizations to educate their software developers about secure coding practices.

Attackers try to find security vulnerabilities in the applications or servers and then try to use these vulnerabilities
to steal secrets, corrupt programs and data, and gain control of computer systems and networks.

Sound programming techniques and best practices can be used to develop high quality code to prevent web application
attacks. Secure programming is a defensive measure against attacks targeted towards application systems.

TARGET AUDIENCE

This course will be invaluable to software developers and programmers alike to code and develop highly secure applications and web applications. This is done throughout the software life cycle that involves designing, implementing and deployment of applications.

.Net is widely used by almost all organizations as the leading framework to build web applications.

The course teaches developers how to identify security flaws and implement security countermeasures throughout the software development lifecycle to improve the overall quality of products and applications.

EC-Council Certified Secure Programmer lays the foundation required by all application developers and development organizations to produce applications with greater stability and fewer security risks to the consumer.

The Certified Secure Application Developer standardizes the knowledge base for application development by incorporating the best practices followed by experienced experts in the various domains.

This course is purposefully built with tons of labs peppered throughout the three days of training, offering participants critical hands on time to fully grasp the new techniques and strategies in secure programming.

COURSE OBJECTIVES

Familiarize you with .Net Application Security, ASP.Net Security Architecture and help you understand the need for application security and common security threats to .Net framework

Discuss security attacks on .Net framework and explain the secure software development lifecycle

Help you to understand common threats to .Net assemblies and familiarize you with stack walking processes

Discuss the need for input validation, various input validation approaches, common input validation attacks, validation control vulnerabilities and best practices for input validation

Familiarize you with authorization and authentication processes and common threats to authorization and authentication

Discuss various security principles for session management tokens, common threats to session management, ASP.Net session management techniques and various session attacks

Cover the importance of cryptography in .Net, different types of cryptographic attacks in .Net and various .Net cryptography namespaces

Explain symmetric and asymmetric encryption, hashing concepts, digital certificates, digital and XML signatures

Describe the principles of secure error handling, different levels of exception handling and various .Net logging tools

Examine file handling concepts, file handling security concerns, path traversal attacks on file handling and defensive techniques against path traversal attack

COURSE CONTENT

1. Net framework security features and various secure coding principles
2. Net framework runtime security model, role-based security, code access security (CAS), and class libraries security
3. Various validation controls, mitigation techniques for validation control vulnerabilities, defensive techniques for SQL injection attacks, and output encoding to prevent input validation attacks

4. Defensive techniques against session attacks, cookie security, and View State security
5. Mitigating vulnerabilities in class level exception handling, managing unhandled errors and implementing windows log security against various attacks
6. Defensive techniques against path traversal attacks and defensive techniques against canonicalization
attack and file ACLs
7. Mitigating vulnerabilities in machine config files, mitigating the vulnerabilities in app config files and security code review approaches
8. The importance of secure programmers and certified secure programmers, the career path of secure
programmers, and the essential skillset of secure programmers

COURSE PREREQUISITES

You must be well-versed with .NET programming language.

TEST CERTIFICATION

The ECSP .NET 312-93 exam will be conducted on the last day of training. Students need to pass the online exam to receive the ECSP certification.