CERTIFIED SECURE DEVELOPER

CSD

Duration: 3 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

A recent study compared the cost implementing security into applications at various stages of the development life cycle. Some of the interesting findings from that study include:

- Adding security during coding costs 6.5 times more than architecting it during the upfront software design process
- Implementing security after deployment costs 15 times more than architecting it during the upfront software design process
- Fixing security holes after deployment costs 100 times more than architecting it during the upfront software design process
- On average, every 1,000 lines of code has at least 5 to 15 defects (United States Department of Defense and the Software Engineering Institute).

Developers want to Write Secure Code, they just Don't know how. This course transforms a developer into a secure developer irrespective of the language they use.

OBJECTIVES

- Understand the cost savings of implementing security during the software design process compared to after deployment or fixing security holes
- Learn the basics of web application security and why traditional security measures such as anti-virus and firewalls are not enough to stop application hacking
- Understand the principles of secure development and how to apply them in software development to prevent vulnerabilities
- Learn about the OWASP and SANS top web application vulnerabilities and how to defend against them through hands-on labs
- Learn about various tools and techniques for application security testing, including vulnerability scanning and exploiting web vulnerabilities
- Understand how to perform vulnerability assessment and reporting with remediations and mitigations
- Understand the basic principles of secure coding and how to write secure code
- Learn how to apply threat modeling to identify and prioritize threats to an application
- Understand how to identify and mitigate the common security issues in the protocol structures of web.
- Understand the basics of web services and its security
- Understand the basics of web server and database and its security
- Understand the importance of a holistic approach to security
- Learn the basics of Network, Host & Application security
- Understand the importance of RACI matrix in security.

PREREQUISITES

Current and Future Software Developers

COURSE CONTENTS

Module 1: Web Application – Security Basics

- What is Security?
- What is Secure Coding ?
- Why Anti-virus, Firewall, IPS, IDS is not enough to stop application hacking?
- Why do you need a Web Application Firewall?
- Protocol Basics of HTTP and HTTPS
- What is a Stateless protocol,
- Why Cookies and/or Sessions are an integral part of web applications?
- What is a Web Server?
- Database and its language basics
- Issues in the protocol structures of web
- A Holistic approach to Security
- Secure the Network, Host & Application
- Threat Modelling : Stride and Dread
- RACI Matrix
- Web Services

Module 2: Principles of Secure Development

The 8 Principles of Secure Development are basic foundation blocks for Secure Programming. Generally, these 8 principles are not followed during the Software Development process resulting in applications with tons of vulnerabilities that are easily exploited by hackers/intruders

- Input Validation,
- Output Validation,
- Error Handling,
- Authentication and Authorization,
- Session Management,
- Secure Communications,
- Secure Storage and
- Secure Resource Access

Module 3: OWASP & SANS Top Web Application Vulnerabilities – Attacks & Defenses

Attacks with Hands-on Labs on :

- SQL Injection,
- Cross Site Scripting,

- Cross Site Request Forgery,
- LDAP Injection,
- Command Injection,
- Parameter/Form Tampering,
- Payment Gateway hacking
- Improper Error Handling,
- unvalidated Input,
- Directory Traversal,
- Cookie Poisoning,
- Insecure storage,
- Information Leakage,
- Broken Account Management,
- Denial of Service,
- Buffer Overflow,
- Log Tampering,
- Broken Access Control,
- Broken Session Management,
- Session Fixation,
- Security Misconfiguration.
- File Upload and Download and many more

Module 4: Application Security Testing

- Automatic and Manual Vulnerability Scanning with W3af, Wapiti, Nikto, BurpSuite
- Vulnerability Scanning with Acunetix & Other Commercial Scanners
- Vulnerability Scanning with NeXpose Community
- SSL Strip & Man-in-the-Middle Attacks
- Password Cracking
- HTTP DOS
- Automated and Manual Exploitation of Web Vulnerabilities using tons of Scripts
- Vulnerability Assessment reporting with Remediations and Mitigations