

Secure Coding for Banking and Finance

Duration: 3 Days

Description

“Money makes the world go round....” – remember? And yes: it is your responsibility to secure all that. As a fintech company you have to take up the challenge, and beat the bad guys with bomb-proof, secure applications!

If there is a domain where security is critical, it is definitely fintech. Vulnerability is not an option if you want to stay a trusted and reliable vendor with systems and applications that certainly comply with PCI-DSS requirements. You need devoted secure coders with high-level professional attitude and developers eager to fight all coding problems: yes, you need a skilled team of software engineers.

Want to know why? Just for the record: even though IT security best practices are widely available, 90% of security incidents stem from common vulnerabilities as a result of ignorance and malpractice. So, you better keep loaded in all possible ways with up to date knowledge about secure coding – unless you wanna cry!

We offer a training program exclusively targeting engineers developing applications for the banking and finance sector. Our dedicated trainers share their experience and expertise through hands-on labs, and give real-life case studies from the banking industry – engaging participants in live hacking fun to reveal all consequences of insecure coding.

Delegates attending this course will

- Understand basic concepts of security, IT security and secure coding
- Understand special threats in the banking and finance sector
- Understand regulations and standards
- Learn Web vulnerabilities beyond OWASP Top Ten and know how to avoid them
- Learn about XML security
- Learn client-side vulnerabilities and secure coding practices
- Learn about JSON security
- Learn about denial of service attacks and protections
- Have a practical understanding of cryptography
- Understand essential security protocols
- Get sources and further readings on secure coding practices

Outline

IT security and secure coding

- Nature of security
- What is risk?
- IT security vs. secure coding
- From vulnerabilities to botnets and cybercrime
- Classification of security flaws

Special threats in the banking and finance sector

- Banking and finance threats – trends
- Banking and finance threats – some numbers
- Attacker profiles
- Most significant targets
- Attacker tools and vectors

Regulations and standards

- The fintech cybersecurity regulatory / compliance landscape
- Important organizations and regulations from an IT standpoint
- Data protection
- Breach disclosure obligations
- PCI DSS compliance

Web application security

- A1 - Injection
- A2 - Broken authentication
- A3 - Sensitive data exposure

Web application security

- A4 - XML external entity (XXE)
- A5 - Broken access control
- A6 - Security misconfiguration
- A7 - Cross-Site Scripting (XSS)
- A8 - Insecure deserialization
- A9 - Using components with known vulnerabilities
- A10 - Insufficient logging and monitoring

Client-side security

- JavaScript security

- Same Origin Policy
- Simple requests
- Preflight requests
- Exercise – Client-side authentication
- Client-side authentication and password management
- Protecting JavaScript code
- Clickjacking
- AJAX security
- HTML5 security

XML security

- Introduction
- XML parsing
- XML injection

JSON security

- Embedding JSON server-side
- JSON injection
- JSON hijacking
- Case study – XSS via spoofed JSON element

Denial of service

- DoS introduction
- Asymmetric DoS
- Case study – ReDos in Stack Exchange
- Hashtable collision attack

Practical cryptography

- Rule #1 of implementing cryptography
- Cryptosystems
- Symmetric-key cryptography
- Other cryptographic algorithms
- Asymmetric (public-key) cryptography
- Public Key Infrastructure (PKI)

Security protocols

- Secure network protocols
- Specific vs. general solutions
- SSL/TLS protocols

- Improper use of security features
- Input validation

Principles of security and secure coding

- Matt Bishop's principles of robust programming
- The security principles of Saltzer and Schroeder
- SEI Cert top 10 secure coding practices

Prerequisites

C# programming experience.