



Certified Application Security Engineer

Course Description

The Certified Application Security Engineer (CASE) focuses on secure application software development processes. It is a, hands-on, comprehensive application security course that will help you create a secure application software. This course encompasses security activities involved in all phases of the Secure Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices to include secure requirement gathering, robust application design, and handling security issues in post development phases of application development.

The CASE certification exam and training program prepare application security engineers, analysts, testers, and anyone with exposure to any phase of SDLC to build secure applications that are robust enough to meet today's challenging operational environment by focusing not just on secure coding, but much more.

This makes CASE one of the most comprehensive certifications on the market today. It's desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Application Security: the Current and NEXT BIG THING

For most organizations, software and applications determine their success. However, expedition, duplication, and penny-pinching take centrestage with security taking a backseat or is not present at all. An insecure or vulnerable application places these businesses at risk.

1.8 Billion Active Websites
Managed by 21 Million Developers Globally
One of the Largest Economies - \$5.6 Trillion
by 2021

3.5 Billion Active Users
Making the Largest Platform For
Identity and Financial Theft

Average of 19 Vulnerabilities Found Per Day
Over 50% Termed Vulnerable
64% of Top 1 Million Alexa Websites Are Vulnerable

It is quite clear that application security still has a long way to go!

Do you belong to the pack that follows unsafe coding and deployment practices? Are you one of the 21 Million, putting the security of the software or web application at risk, resulting with a catastrophic loss?



Security Risk Not Limited to only Web Applications

Many globally recognizable retail outlets have dealt with enormous data breaches recently because they ignored application security.

Billion-dollar companies with global footprints have faced massive data leakage, including their customers' and employees' personal and financial information, because their applications were faulty.

Retail giants like Forever 21, GameStop, Panera Bread, Sonic, KMart, and Hudson Bay (Saks Fifth Avenue) are a few on the list of retailers with thousands of outlets that used POS machines or payment gateways that allegedly resulted in information theft. There are many more modern, digital platforms like Uber, Yahoo, Dropbox, Adobe, LinkedIn, and Tumblr who also faced similar breaches, owing to the same reason - lack of application security.

Application Security

How Secure Are You?

75%

of All Cyber
Attacks Target Web
Applications

90%

of Java Applications
Contain At Least One
Vulnerability

69%

Web Application
Attacks Rise

.NET

The Gap Between Patching Software and Security Is Vast!

The .Net framework has increased in popularity because of its open source nature, interoperability, language independence, library of codes and ease of deployment. It's become the preferred choice for application developers. However, there are not many classes that teach developers how to ensure their code is secure as well as correct. Moreover, any gap in the application development and deployment process can be damaging. .Net developers often learn security on the job. This is primarily because the basic education of programming does not usually cover or emphasize security concerns .

Java

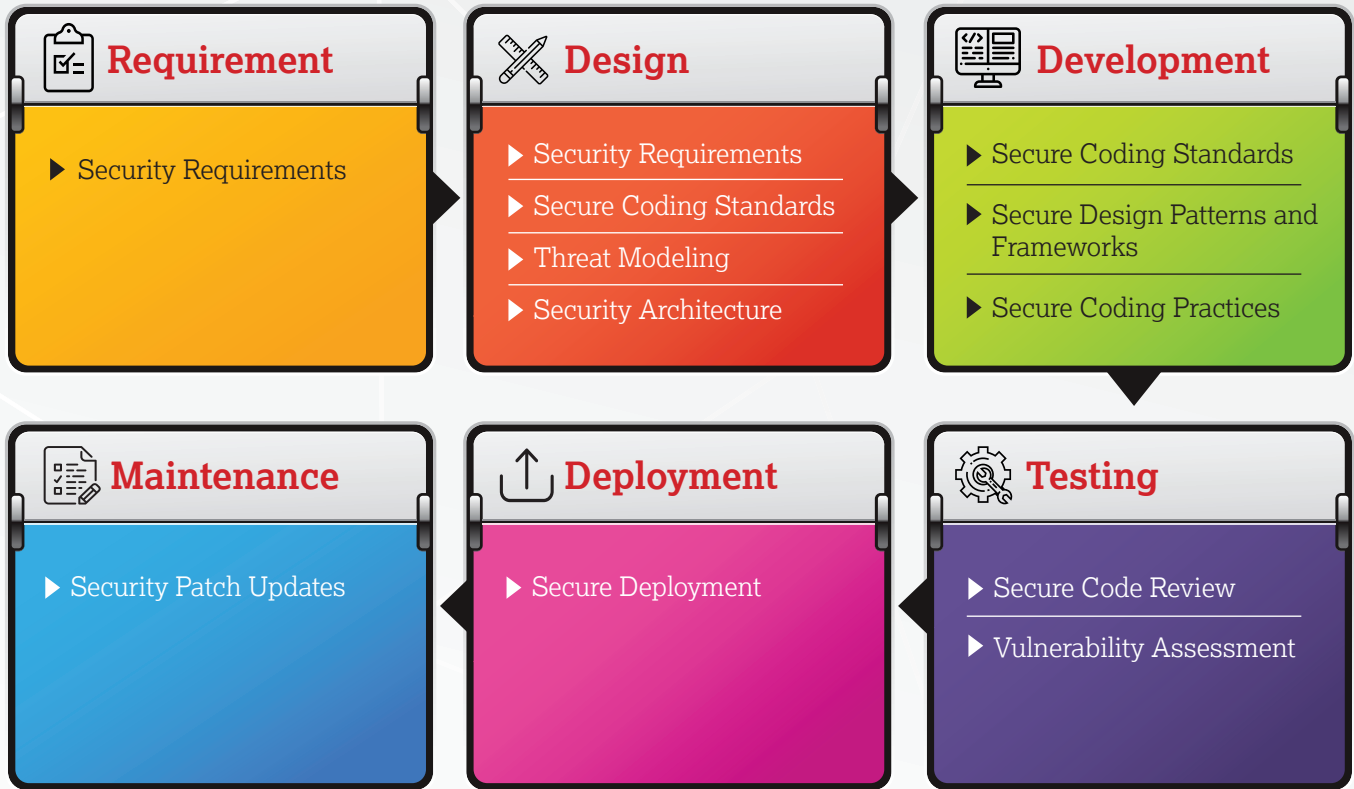
Java Based Applications: The Most Popular and Yet the Most Vulnerable?

According to the 2017 State of Software Security Report, nearly 90% of Java applications contain one or more vulnerable component, making them ideal breach points for hostile attackers.

Although Java has come a long way from its development in 1995, cyber crime has also spread, reaching epidemic levels, increasing the need for secure Java developers, regardless of whether they're creating a new program or upgrading an old one.

Secure Software Development Process

The Certified Application Security Engineer (CASE) program provides a comprehensive application security approach which encompasses security activities involved in all of the phases of Software Development Lifecycle (SDLC).



What You Will Learn

- ▶ In-depth understanding of secure SDLC and secure SDLC models
- ▶ Knowledge of OWASP Top 10, threat modelling, SAST and DAST
- ▶ Capturing security requirements of an application in development
- ▶ Defining, maintaining, and enforcing application security best practices
- ▶ Performing manual and automated code review of application
- ▶ Conducting application security testing for web applications to assess the vulnerabilities
- ▶ Driving development of a holistic application security program
- ▶ Rating the severity of defects and publishing comprehensive reports, detailing associated risks and mitigations
- ▶ Working in teams to improve security posture
- ▶ Application security scanning technologies such as AppScan, Fortify, WebInspect, static application security testing (SAST), dynamic application security testing (DAST), single sign-on, and encryption
- ▶ Following secure coding standards that are based on industry-accepted best practices such as OWASP Guide, or CERT Secure Coding to address common coding vulnerabilities.
- ▶ Creating a software source code review process that is a part of the development cycles (SDLC, Agile, CI/CD)



Course Outline of CASE

- ▶ Understanding Application Security, Threats, and Attacks

- ▶ Security Requirements Gathering

- ▶ Secure Application Design and Architecture

- ▶ Secure Coding Practices for Input Validation

- ▶ Secure Coding Practices for Authentication and Authorization

- ▶ Secure Coding Practices for Cryptography

- ▶ Secure Coding Practices for Session Management

- ▶ Secure Coding Practices for Error Handling

- ▶ Static and Dynamic Application Security Testing (SAST & DAST)

- ▶ Secure Deployment and Maintenance

“

100% of Web Applications are Vulnerable to Hackers.

- 2018 Global Security Report, Trustwave

Who Is CASE For?

.NET / Java Developers with a minimum of 2 years of experience and individuals who want to become application security engineers/analysts/testers.

Individuals involved in the role of developing, testing, managing, or protecting applications

Duration

Total Training Hours - 24

Certification

The CASE exam can be challenged after attending the official CASE training. Candidates that successfully pass the exam will receive their CASE certificate and membership privileges. Members are expected to adhere to the policies of EC-Council's Continuing Education Requirements.

Application Security Is No Longer An Afterthought But a Foremost One!

Attaining the Certified Application Security Engineer

CASE allows application developers and testers to demonstrate their mastery of the knowledge and skills required to handle common application software security vulnerabilities.

- ▶ **Exam Title:**
Certified Application Security Engineer

- ▶ **Number of Questions:** 50

- ▶ **Test Duration:** 2 Hours

- ▶ **Test Format:** Multiple Choice

- ▶ **Availability:** EC-Council Exam Portal



EC-Council



Eligibility Criteria

To be eligible to challenge the CASE Exam, the candidate must either:

- ▶ Complete the official EC-Council CASE training through an accredited EC-Council Partner (Accredited Training Centre/ iWeek/ iLearn) (All candidates are required to pay the USD100 application fee unless your training fee already includes this) or

- ▶ be an ECSP (.NET/ Java) member in good standing (you need not pay a duplicate application fee, as this fee has already been paid) or

- ▶ have a minimum of 2 years working experience in InfoSec/ Software domain (you will need to pay USD 100 as a non-refundable application fee) or

- ▶ have any other industry equivalent certifications such as GSSP .NET/Java (you will need to pay USD 100 as a non-refundable application fee)

The logo for EC-Council, featuring the text "EC-Council" in a bold, red, sans-serif font. The background of the entire page is a dark blue to black gradient with a complex, light blue circuit board pattern of lines and nodes.

EC-Council

www.eccouncil.org