GAQM®

Global Association for Quality Management

Certified Secure Application Professional (CSAP)™

www.gaqm.org

Certification Overview

The Certified Secure Application Professional (CSAP) certification is designed to equip IT professionals with advanced knowledge and practical skills in developing, deploying, and maintaining secure applications in today's digital landscape. With increasing cyber threats targeting applications, organizations require developers and security professionals who can integrate security principles into the software development lifecycle (SDLC), ensuring that applications are resilient against vulnerabilities and compliant with industry security standards. CSAP provides a comprehensive understanding of secure coding practices, threat modeling, risk assessment, and application security testing methodologies.

The CSAP certification validates an individual's ability to identify security risks, implement robust controls, and adopt best practices for secure application development. Candidates will gain expertise in security frameworks, authentication and authorization mechanisms, cryptography, secure API design, and vulnerability mitigation techniques. The certification emphasizes both theoretical knowledge and practical application, enabling professionals to proactively address security challenges and reduce the risk of breaches, data leaks, and non-compliance. Earning the CSAP credential demonstrates a commitment to delivering secure, reliable, and high-quality software solutions that meet organizational and regulatory requirements.

Target Audience

This certification is ideal for software developers, application architects, DevOps engineers, security analysts, and IT professionals who are responsible for designing, building, and maintaining secure software. It is also highly relevant for project managers and quality assurance professionals who need to ensure that security considerations are integrated into every phase of the application lifecycle. Organizations aiming to strengthen their application security posture can leverage CSAP-certified professionals to reduce vulnerabilities, enhance trust with clients, and achieve compliance with global security standards.

What Modules are covered?

Module 1- Introduction to Application Security

- Overview of application security concepts
- Common threats and vulnerabilities (OWASP Top 10)
- Secure software development lifecycle (SDLC)
- Security policies, standards, and compliance

Module 2: Secure Coding Practices

- Principles of secure coding
- Input validation and output encoding
- Error handling and logging securely
- Avoiding common coding vulnerabilities

Module 3: Authentication and Authorization

- Identity management and access control
- Multi-factor authentication
- Role-based and attribute-based access control
- Session management best practices

Module 4 - Cryptography and Data Protection

- Basics of encryption, hashing, and digital signatures
- Key management best practices
- Secure storage of sensitive data
- TLS/SSL implementation and secure communications

Module 5 - Application Threat Modeling

- Introduction to threat modeling
- Identifying threats using STRIDE and DREAD
- Risk assessment and mitigation strategies
- Security design reviews

Module 6 - Secure API and Web Services

- RESTful and SOAP API security
- OAuth, JWT, and token-based authentication
- Input validation for APIs
- Preventing common API attacks (parameter tampering, broken authentication)

Module 7 - Application Security Testing

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Interactive Application Security Testing (IAST)
- Penetration testing basics and reporting

Module 8 - DevSecOps and Secure Deployment

- Integrating security in CI/CD pipelines
- Automated security testing in DevOps
- Container security (Docker, Kubernetes)
- Secure configuration management

Module 9 - Incident Response and Compliance

- Application security incident response
- Monitoring, logging, and alerting for applications
- Regulatory standards (GDPR, PCI DSS, HIPAA)
- Continuous improvement and security audits