NETWORK INTELLIGENCE
The Digital Security Company

Certified Web Application Security Professional (CWASP)

12 hours of training on Web Application Security

Batch : Global
Date: 12th – 14th May 2026
Timing: 1:00 pm – 5:00 pm GMT
Mode of training: Online

Course Fee: USD 199 **For ISACA/ISC2 members: USD 159** **For Client/Returning participants: USD 129**

Certified Web Application Security Professional(CWASP)

Introduction

- In recent history, there has been a rise in the popularity of web applications for carrying out multiple online activities. Since web applications usually store or send out sensitive data, it is crucial to keep these apps secure at all times, particularly those publicly exposed to the World Wide Web. Web applications play a vital role in every modern organization. Cyberattacks against web applications occur daily. Most breaches are caused by failure to update the software components known to be vulnerable for months or years. In Web application penetration testing, an assessment of the security of the code and the use of software on which the application runs takes place.

Importance Of Web Application Penetration Testing

- The way technology is advancing and how web applications are being incorporated into businesses have increased the popularity of web applications. This now has introduced another vector of attack that malicious third parties can exploit for their personal gains. It is more important than ever to conduct regular penetration activities to identify vulnerabilities and ensure that the cybersecurity controls are working. As a result, Web Application Penetration testing has emerged as one of the most significant tools in today's world.

- In addition to meeting regulatory requirements, ensuring the security of web applications is crucial for organizations. By doing so, they can effectively mitigate the risk of expensive incidents, compromise to their infrastructure, and potential damage to their reputation.

Certified Web Application Security Professional(CWASP)

Why CWASP?

In recent years, we have seen massive breaches at organizations such as Panama Papers and Equifax. In many cases, patches to the vulnerabilities in web applications were available but have not been updated.

The CWASP training course is focused on comprehensive coverage of web application security. It will present security guidelines and considerations in web application development. The participants will learn the basics of application security, how to enforce security on a web application, basics of Threat Modeling, Threat Profiling, OWASP Top Ten Testing, Black Box Testing, and Source Code Reviews.

Objective Of CWASP?

- Understanding the need for Security and various threats & countermeasures
- Building a framework for securing a web application
- Guidance to professionals for web applications
- Going beyond the traditional checklist-based approach for security
- Taking a risk-based approach to implementing security controls
- Winning end customer's trust

This Course Is Best For

- All web app developers, testers, designers who wish to improve their security skills.
- Developers and System Architects wishing to improve their security skills and awareness.
- Team Leaders and Project Managers.
- Security practitioners and managers.
- Auditors.
- Anyone interested in techniques for securing Web applications.
- QA analysts who want to learn the mechanics of Web applications for better testing

Course Contents

Day 1:

Introduction & Case Studies

- Introduction to Web Applications & Web Application Architecture.
- HTTP Protocol Basics.
- HTTP Attack Vectors
- Introduction to Application Security.
- Application Security Risks.
- Case Studies.

OWASP Top 10 2021

- What is OWASP
- OWASP Top 10
- The ‘OWASP Top 10’ for WebAppSec

Day 2:

- A1-Broken Access Control
- A2-Cryptographic Failures
- A3-Injection
- A4-Insecure Design
- A5-Security Misconfiguration
- A6-Vulnerable and Outdated Components
- A7-Identification and Authentication Failures

Day 3:

- A8-Software and Data Integrity Failures
- A9-Security Logging and Monitoring Failures
- A10- Server-Side Request Forgery
- Countermeasures of OWASP Top 10 2021

Course Contents

Beyond OWASP

- Unrestricted File Upload
- Understanding the vulnerability
- Discovering the vulnerability
- Attacking the Issue
- Impact & Countermeasure
- JWT Issues
- Understanding the Issue
- Discovering the Issue
- Attacking the Issue Impact & Countermeasure

API Security

- API Security
- Introduction to API & API Security
- SOAP vs REST
- Case Studies
- Common API Vulnerabilities
- API Assessment Approach
- How to stop API Attacks?

Practical Tips for Defending Web Applications & API

- Common Mistakes in Development
- Security Best Practices for Web Application & API Security
- Secure SDLC
- Threat Modelling
- Source Code Review
- VAPT

Trainer profile

Swapnil Khandekar,

Trainer and Cybersecurity Specialist,
Network Intelligence

Swapnil currently serves as a Senior Cybersecurity Analyst at NII and Senior trainer at IIS. His work mainly focuses on Security training, Vulnerability Assessment, and Penetration Testing for NII. His technical abilities span SOC, Networks, Web Apps, Databases, Digital Forensics, Cloud Security, Red teaming, and ISO Compliance. He has 6+ years of overall experience in the field of Information security and training on relevant topics.

Registration link: CWASP- Certified Web application Security Professional