Certified Web Application Security Professional (CWASP)

16 hours of online training on Web Application Security

Batch 1: Asia & Middle East
Date : 5th – 7th June 2023
Timing: 6:00 am – 10:00 am GMT
Mode of training: Online

Batch 2: Americas & Europe
Date: 12th – 14th June 2023
Timing: 1:00 pm – 5:00 pm GMT
Mode of training: Online

Course Fee:

USD 200 for Regular Participants

USD 150 for ISACA/ISC2 Members

NETWORK INTELLIGENCE
The Digital Security Company

INTRODUCTION

Recent history has seen a rise in the popularity of web applications to carry 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. Penetration testing looks at vulnerabilities and will try and exploit them. Modern cyber defense requires a realistic and thorough understanding of web application security issues.

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.

In line with these objectives, we are pleased to announce a 3-day 4-hour online training on "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.

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

OBJECTIVES:

- 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

Course Content

Day1:

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
- A1-Broken Access Control

Day2:

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- A6-Vulnerable and Outdated Components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

Day3:

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

Beyond OWASP

- Unrestricted File Upload
- Understanding the vulnerability

Course Content

- 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

The CWASP training will provide participants with hands-on experience in implementing security measures for safeguarding web applications through case studies and examples.

Trainer Details

Gaurav Kumar,

Cybersecurity Consultant
Network Intelligence

Gaurav is a versatile IT and Cybersecurity expert with 8+ years of experience. His passion lies in securing web applications, conducting network and vulnerability assessments, and performing penetration testing. He's a tech wizard who can tackle various technologies, including operating systems, web apps and servers. Gaurav's specialized skills include Web application security, Network Security, Digital Forensics, and GRC. He has a string of impressive qualifications, such as CEH, CISC, CPFA, AWS CCP, CAP, and more. Gaurav has designed and delivered customized course outlines for NI's clientele.

Udit Pathak,

Head of Department– Compliance and Audit,
Network Intelligence

Udit has rich experience of 10+ Years in the field of information security and Audits., He has carried out PCI DSS audits, ISO27001, Vulnerability assessments, System and Server Audits, Web application security assessments, Secure code reviews, Technical security assessments, Vendor Audits, HIPAA Implementation & Audits, and SOC maturity assessments. Udit heads the Compliance & Audit Delivery channel at Network Intelligence. He has delivered excellent projects across the globe for the payment ecosystem, BFSI, the travel industry, health care, and defense services for both cloud and traditional on-prem solutions.

Registration link: https://forms.office.com/r/Affz0dUpy9