NETWORK INTELLIGENCE
Global cybersecurity provider

CERTIFIED WEB APPLICATION SECURITY PROFESSIONAL (CWASP)

A 12 Hours Web Application Security Training

Batch1 : America | Canada | Europe
Dates : December 13 – 15, 2021
Time : Time : 2.00 PM to 5.00 PM (GMT)
Mode : Online

Batch 2 : Asia | Middle East
Dates : December 20 -22, 2021
Time : Time : 6.00 AM to 10.00 PM (GMT)
Mode : Online

Course Fees:

- Non ISACA/ISC2 Members: USD 120
- ISC2 Members/Recurring : USD 80 (Christmas offer)

INTRODUCTION

Recent history has seen the rise in popularity of usage of web applications to carry out multiple activities over the internet. Since web applications usually store or send out sensitive data, it is crucial to keep these apps secure at all time, particularly those that are publicly exposed to the World Wide Web. Web applications play a vital role in every modern organization Cyberattacks against web applications occur every day. Most breaches are caused by failure to update the software components that are 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 defence requires a realistic and thorough understanding of web application security issues.

IMPORTANCE OF WEB APPLICATION PENETRATION TESTING

The Way technology is advancing, and the way web applications are being incorporated into the 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 before to conduct regular penetration activities to identify vulnerabilities and to 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. Apart from regulatory requirements, protecting the security of its web application, organizations reduce the risk of costly incidents, comptonization of its infrastructure and reputational harms as well.

Why CWASP ?

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

The CWASP training course is focused on a comprehensive coverage of web application security. It will present security guidelines and considerations in web applications 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

The CWASP training will provide participants a hands-on experience of implementing security measure for safeguarding web applications through case studies and examples.

OBJECTIVES

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

In line with these objectives, we are pleased to announce a 3-day 4-hour online training on “Certified Web Application Security Professional (CWASP) ”.

Course Contents:

PART 1:

Session 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.

Session 2: OWASP Top 10 2017 RC2

- What is OWASP
- OWASP Top 10
- The ‘OWASP Top 10’ for WebAppSec
- A1-Injection
- A2-Broken Authentication
- A3-Sensitive Data Exposure
- A4-XML External Entities (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 & Monitoring
- Countermeasures of OWASP Top 10 2017 RC2

Session 3: Beyond OWASP

CSRF

- Understanding the vulnerability
- Discovering the vulnerability
- Attacking the Issue
- Impact & Countermeasure
- SSRF
- Understanding the vulnerability
- Discovering the vulnerability
- Attacking the Issue
- Impact & Countermeasure

Session 4: API Insecurity

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

Examination – The participants would need to undergo an online examination after the training. On successfully clearing the examination, the participant would be awarded with the CWASP certificate

Session 5: Practical Tips for Defending Web Application & API

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

Remember….. you are the Centre of Security”

Trainer Details

Mufaddal Taskin

Training Specialist & Cyber Security Analyst,Network Intelligence

Mufaddal has over 25 years of diverse experience in technology solutions. He currently serves as a Security Analyst at NII and Training Specialist at NII. His work mainly focuses on Security Trainings, Vulnerability Assessment and Penetration Testing for NII. His technical abilities span across Networks, Web Apps, Incident Response, Cyber Threat Intelligence, SOC and ISO standards Compliance. Mufaddal has created custom course outlines as well as conducted the same for a variety of high technologies clients of NII.

Registration form : https://bit.ly/3wLYoiv