incusdata (pty) ltd. 1995/04149/07
Coding · Matters
PO Box 94
Raslouw, 0109
tel : +27 12 666 2020
info@incusdata.com
www.incusdata.co.za

Price: R5,200.00 excl. VAT
Duration: 2 days
Code: WBSEC

Web Application Security

Description

This course gives you an overview of the most important security concerns in web applications, and how to deal with them. You will learn how and why web apps are vulnerable. The course will cover the top 10 vulnerabilities, based on the Open Web Application Security Project. You will learn what each vulnerability is, and the best approach to counter the risk. This course does not focus on any particular programming language.

Objectives

After you have completed the Web Application Security overview, you will:

- Understand the concepts and terminology used in web security.
- Be aware of the global organisations and standards that focus on web application security.
- Know what the most important vulnerabilities are, and what countermeasures to take.
- Know what is required to implement a secure development approach.
- Be aware of best practices and secure design principles for development.

Intended Audience

You should attend the web security overview course if:

- You are a web application developer, and you need to write secure applications.
- You are a manager and you want to reduce your organisation's vulnerability to security attacks.
- You are a network or server engineer, and you are responsible for application security.

Prerequisites

Before you attend the web security overview course:

- You should have some technical background and a basic understanding of web applications.

Course Contents

Introduction

- Case studies and statistics.
- Introduction to web applications.
- Basics of web application architecture.
- Application security risks.
- Attack vectors.
- Threat agents.

HTTP Protocol

- HTTP protocol basics.
- HTTP response headers.
- HTTP versus HTTPS.
- HTTP Strict Transport Security (HSTS).
- X-Frame-Options.
- X-XSS-Protection.
- X-Content-Type-Options.
- Content-Security-Policy.

- Referrer-Policy.
- Expect-CT.

Vulnerability Assessment and Penetration Testing

- What is VAPT?
- Steps involved in VAPT.
- Black box vs grey box vs white box testing.

Global Organisations, Standards and Frameworks

- The Web Application Security Consortium (WASC).
- The Open Web Application Security Project (OWASP).
- The National Institute of Standards and Technology (NIST).
- The Common Weakness Enumeration (CWE) category system.
- The SysAdm, Audit, Network, Security (SANS) Institute.

Fundamentals of a Secure Environment

- CIA: Confidentiality, integrity, availability.
- Policies and standards.
- Acquiring secure software.
- Training.
- Secure architecture.
- Physical security.
- Introduction to secure SDLC.

Common Attack Categories

- Insecure interaction between components.
- Risky resource management.
- Poroous defences.

OWASP Top 10 Web Application Vulerabilities

- Injection.
- Broken authentication and session management.
- Sensitive data exposure.
- XML external entity (XXE).
- Broken access control.
- Security misconfiguration.
- Cross-site xcripting (XSS).
- Insecure deserialization.
- Using components with known vulnerabilities.
- Insufficient logging & monitoring.
- Definitions, explanations and examples.
- Countermeasures.

Other Common Vulnerabilities

- Clickjacking.
- Cross-Site Request Forgery (CSRF).
- Server Side Request Forgerty (SSRF).
- Definitions, explanations and examples.

- Countermeasures.

Secure Development Approach

- The secure SDLC.
- Threat modelling.
- Source code review.
- Common dangerous programming practices.
- Common development mistakes.

Secure Design Principles and Best Practices

- Defense in depth.
- Fail safe.
- Least privilege.
- Separation of duties.
- Economy of mechanism.
- Complete mediation.
- Open design.
- Least common mechanism.
- Psychological acceptability.
- Weakest link.
- Leveraging existing components.

******* *The lecturer reserves the right to modify the contents of the course to suit the needs of the delegates.*