



Application Security Audit

Fault Injection Model, Fuzz Generators & Static Code Analysis

Training Brochure

Synopsis

This Four-day practical training is designed for Information Systems auditors, application developers, risk as well as compliance auditors who need to update their technical and operational knowledge to audit technologies relating to automated web based systems. We will discuss the audit and controls required when auditing Internet and Intranet based Web Applications. In addition, you will learn techniques for auditing payment gateways and performing static code analysis including manual and automated review methods. Then you will turn your attention to auditing the management of application transaction activity, controls, and procedures. You will master techniques that can be applied to web-based applications, distributed processing, and client/server-based applications during the audit training. You will gain field-tested auditing tools for testing, identifying, recording, assessing and evaluating web application controls effectively.

Various detailed web application audit case studies will provide step-by-step reinforcement of what you have learned, and you will leave this training with real-world examples of web application audit program, testing techniques, audit findings and methodologies.

Course Objectives

The course will

- Provide training on audit and security assessment testing practices of web applications
- Provide an overall description of the tools and methodologies used in web application audit and static code analysis (source code review)
- Explain and demonstrate the latest technologies used for audit and security assessment tests along with demonstrable and practical examples

Delivery

As with all of our audit and security assessment courses, this course makes extensive use of practical exercises and draws heavily on the company's experience in performing security assessment tests and security audits as well as implementing enterprise security solutions. This is an instructor led course. It is primarily designed as a publicly scheduled course for corporate organisations. It can also be delivered as in-house / onsite training for corporate groups.

Cost

Onsite: **N 1,500,000** (exclusive of 5% VAT) for any number of participants.

Course Description

PART I: Application Architectural Audit Using Fault Injection Model

Module 1: Web Application (In)security

explores the current state of security in web applications on the Internet today.

Module 2: Web Application Architecture Review

examines applications employed in a tiered architecture with the consequence that a failure to segregate different tiers properly often leaves an application vulnerable, enabling an attacker who has found a defect in one component to quickly compromise the entire application.

Module 3: Core Defense Mechanisms

describes the key security mechanisms that web applications employ to address the fundamental problem that all user input is untrusted.

Module 4: Web Application Technologies

provides a primer on the key technologies that you are likely to encounter when attacking / assessing web applications.

Module 5: Web Application Profiling

delves into attack surface mapping and application information gathering techniques and attack plan formulation.

Module 6: Bypassing Client-Side Controls

examines one of the first areas of actual web application vulnerability, which arises when an application relies upon controls implemented on the client side for its security.

Module 7: Auditing Authentication

examines the various functions by which applications gain assurance of the identity of their users. This includes the main login function and also the more peripheral authentication related functions such as user registration, password changing, and account recovery.

Module 8: Auditing Session Management

examines the mechanism by which most applications supplement the stateless HTTP protocol with the concept of a stateful session, enabling them to uniquely identify each user across several different requests.

Module 9: Auditing Access Controls

examines the ways in which applications actually enforce access controls and its relationship with authentication and session management mechanisms. This module also looks at ways in which these access controls can be broken and fixed.

Module 10: Web Application Logic Audit

examines a significant, and frequently overlooked area of every application's attack surface: the internal logic and design which it carries out to implement its functionality.

PART 2: Application Architectural Audit Using The Fuzzing Model (Fuzz Generators)

Module 11: Code Injection Audit

covers a large category of related vulnerabilities, which arise when applications embed user input into interpreted code in an unsafe way. SQLi, RFI and LFI are all covered.

Module 12: Path Traversal Audit

examines an all important category of vulnerabilities that arise when user input is passed to file system APIs in an unsafe way, enabling an attacker to retrieve or modify arbitrary files on the web server.

Module 13: Audit Users Related Vulnerabilities

investigates an area of related vulnerabilities which arise when defects within a web application can enable a malicious user of the application to attack other users and compromise them in various ways..Vulnerabilities such as XSS and Session Fixation and will be discussed.

Module 14: Web Server Audit

describes various ways in which you can target a web application by targeting the web server on which it is running.

Module 15: Web Application Audit Methodology

describes a comprehensive and structured collation of all the procedures and techniques described in the course and are organized and ordered according to the logical dependencies between tasks. This methodology can be used as a complete checklist and work plan when carrying out a web application security assessment.

PART 3: Software Security Review Using Static Code Analysis

Module 16: Introduction to Static Code Analysis

introduces basic static code analysis for auditors

Module 17: Methods of Static Analysis

describes a comprehensive approach and methods used in static code analysis

Module 18: The Code Review Process

delves into various steps involved in the code review process especially for large, monolithic and complex codebase

Module 19: Manual Methods of Code Review

covers various methods of manual source code audit including top down code analysis, control flow graphs and data flow analysis

Module 20: SDLC & Automated Code Review

examines the secure software development lifecycle as well as various tools used for white box automating code reviews. This section will include code entry point and candidate points as well as source to sink taint propagation method of code review

Module 21: Enterprise Security Application Programming Interface

provides a unique perspective to secure coding by examining the OWASP Enterprise Security API and its utilization in mitigating inherent risks in multiple language codebase.

Profile of Trainers

Adewale Obadare

Obadare Peter Adewale is a well recognized information security professional with numerous successful engagements to his credit in Nigeria. His skills and experience span Information Security, IT Governance, Risk Management, Compliance, Computer Forensics, and Business Continuity. He has worked as I.T Security auditor , vulnerability expert and system integrator at various organizations. His professional qualifications include:

- ❖ CHARTERED IT PROFESSIONAL (CITP)
- ❖ ISO 27001 LEAD IMPLEMENTER
- ❖ ISO 27001 LEAD AUDITOR
- ❖ BS 25999 LEAD AUDITOR
- ❖ LICENSED PENETRATION TESTER (LPT)
- ❖ EC- COUNCIL SECURITY ANALYST (ECSA)
- ❖ CERTIFIED ETHICAL HACKER (CEH)
- ❖ QUALYSGUARD CERTIFIED SPECIALIST (QCS)
- ❖ CISCO CERTIFIED INTERWORK EXPERT (CCIE WRITTEN)
- ❖ SECURING NETWORKS WITH ASA ADVANCE (SNAA)
- ❖ CISCO CERTIFIED DESIGN PROFESSIONAL (CCDP)
- ❖ CISCO CERTIFIED NETWORK PROFESSIONAL (CCNP)
- ❖ MICROSOFT CERTIFIED PROFESSIONAL (MCP)

Oluseyi Akindeinde

Olu has over 12 years experience working in the IT and information security arena, but has spent the better part of the last few years exploring the security issues faced by Electronic Funds Transfer (EFT) and Financial Transaction Systems (FTS). He has presented the outcome of his research work at several conferences; including the Information Security Society of Africa (ISS), the forum of the Committee of Chief Inspectors of Banks in Nigeria, the apex bank - Central Bank of Nigeria (CBN) as well as 15 of the 24 financial institutions in Nigeria. In his professional life, Seyi, as he is otherwise called, sits on the board of two companies. In addition to being the CTO, he holds a vital position as the Senior Information Security Analyst at Digital Encode Ltd an information security advisory and assurance company, not only performing various technical security assessments and digital forensics but also providing technical consulting in the field of security design and strategic technology reviews for top notch local clients. He has over the years developed an in-depth knowledge of security modeling which has hitherto improved his ability to initiate, perform and deliver world class enterprise security services that add veritable value to the corporate goals and objectives of organizations.

Olu is a research writer having written two books on Information Security Analytics. He is also the author of the Open Source Security Assessment Report (OSSAR) - a model framework for reporting and presenting enterprise security assessment findings. He is a speaker on matters bordering on information security, and has presented technical papers on a wide range of IT security and risk management topics for a number of high profile financial service providers at different retreats and forums. Furthermore, he has delivered several information security and ethical hacking training courses to delegates from diverse industries including finance, manufacturing, oil and gas, telecoms as well as State and Federal Government Agencies. He has administered security analysis and penetration testing courses to representatives of the National Assembly, Defense Intelligence Agency (DIA) and Office of the National Security Agency (NSA) through the annual Hacker Counterintelligence Program (HACOP) where he's been involved as a resident trainer and technical consultant for the last couple of years.

Olu graduated with a BSc in Civil Engineering from the University of Lagos in the year 2000.