Hands on

Interactive

Advanced

Web focused

WEB APPLICATION SECURITY TRAINING

OVERVIEW

(Both intermediate and advanced classes)

This three day course on web application security is taught by our expert web app tester who has over eight years of experience in web app pentesting.

He has been a delivery team lead for all engagements relating to web application testing of commercial and retail customers and has several years of testing mobile applications for banking / financial sector clients.

You will also gain experience in testing cloud-based technologies and learn how to break in to Android and Apple phones.

WHO SHOULD ATTEND?

- Sys admins, SOC staff, security analysts consultants and those with some coding experience and anyone interested in information security.

FOUR DAY SYLLABUS

Day 1 web application basis

- Application architecture
- Web technologies and HTTP basics
- Current attack trend
- Application security overview
- Common pentest tools overview and Google hacking

Application test methodology

- Port scanning and web server assessment & SSL security
- Default configuration / common CMS exploitation techniques

Day 2 OWASP Top 10 / application vulnerabilities

- Authentication and authorisation vulnerabilities
- Session management security
- Business logic flaws
- SQL injection – blind, error based, time, outofband
- Cross site scripting – DOM, reflected, stored
- Insecure direct object references
- Broken access control
- Crosssite request forgery and unvalidated redirects and forwards
- Input validation and encoding, file inclusion – LFI, RFI privilege escalation opportunities and session fixation

Day 3 web services assesment

- Web services / XML attacks & web services overview
- XML security & SOAP/ WSDL/JSON/AJAX hacking

Advanced

- Clickjacking, Flash / Java application security
- Net remoting and advanced SQL injection

Capture the flag

- Challenges & quiz & hack lab access