Training Topic
Web Penetration Testing

Detail Training Syllabus for 2 Days:

Web Penetration Testing - The course will cover practical skills and knowledge to uncover 10 common, important vulnerabilities associated with web security, based on the OWASP Top 10 listing. The session will be packed with demos and hands-on sessions where participants gets to experience web hacking like black-hats do, all for the sake of understanding the true nature of the flaws and how they could affect your web application.

Day 1
A1-Injection
A2-Broken Authentication and Session Management
A3-Cross-Site Scripting (XSS)
A4-Insecure Direct Object References
A5-Security Misconfiguration

Day 2
A6-Sensitive Data Exposure
A7-Missing Function Level Access Control
A8-Cross-Site Request Forgery (CSRF)
A9-Using Components with Known Vulnerabilities
A10-Unvalidated Redirects and Forwards

About Trainer:

Dr Syed Zainudeen Mohd Shaid is a lecturer at Universiti Teknologi Malaysia (UTM) where he teaches subjects like Penetration Testing, Security Programming, OS Exploitation and other security related subjects. A member of the Information Assurance & Security Research Group (IASRG), he supervises students in doing research in computer security, specifically in Malware research. He also does training and consultancy on Web Security, Secure Coding, Android, and embedded systems. He loves gadgets and enjoys exploring new things related to security.