Exam Certification Objectives & Outcome Statements

The topic areas for each exam part follow:

Cross Site Request Forgery, Cross Site Scripting and Client Injection Attack
: The candidate will demonstrate an understanding of Cross Site Request Forgery, Cross Site Scripting and Client Injection attacks and the tools and techniques used to discover and exploit vulnerabilities.

Reconnaissance and Mapping
: The candidate will demonstrate an understanding of the techniques used to conduct discovery, exploration and investigation of a web site and web application features such as port scanning, identifying services and configurations, spidering, application flow charting and session analysis.

Web Application Authentication Attacks
: The candidate will demonstrate a familiarity with the process and mechanisms used to secure web applications by authentication, how to enumerate users and how to bypass and exploit weak authentication.

Web Application Configuration Testing
: The candidate will demonstrate a familiarity with the tools and techniques used to audit and identify flaws in the design or implementation in the configuration of a web site.

Web Application Overview
: The candidate will demonstrate an understanding of the technologies, programming languages and structures that are involved in the construction and implementation of a web site such as HTTP, HTTPS and AJAX within the context of security, vulnerabilities and basic operation.

Web Application Session Management
: The candidate will demonstrate an understanding of how a web application manages client sessions, tracks user activity and uses SSL/TLS in modern web communications as well as the attacks that can be leveraged against flaws in session state.

Web Application SQL Injection Attacks
: The candidate will demonstrate a familiarity with the techniques used to audit and test the security of web applications using SQL injection attacks and how to identify SQL injection vulnerabilities in applications.

Web Application Testing Tools

The candidate will demonstrate an understanding of the tools and techniques required to perform web application security testing on modern web-based languages such as JavaScript with AJAX including the use of proxies, fuzzing, scripting, and attacking application logic.