SEC522.1: Web Fundamentals and Security Configurations

- Introduction to HTTP protocol
- Overview of web authentication technologies
- Web application architecture
- Recent attack trends
- Web infrastructure security/Web application firewalls
- Managing configurations for web apps

SEC522.2: Defense Against Input Related Threats

- Input-related vulnerabilities in web applications
- SQL injection
- Cross-site request forgery
- Cross-site scripting vulnerability and defenses
- Unicode handling strategy
- File upload handling
- Business logic and concurrency

SEC522.3: Web Application Authentication and Authorization

- Authentication vulnerabilities and defense
- Multifactor authentication
- Session vulnerabilities and testing
- Authorization vulnerabilities and defense
- SSL vulnerabilities and testing
- Proper encryption use in web application

SEC522.4: Web Services and Front-End Security

- Honeytoken
- Web services overview
- Security in parsing of XML
- XML security
- AJAX technologies overview
- AJAX attack trends and common attacks
- REST security
- Browser-based defense such as Content Security Policy

SEC522.5: Cutting-Edge Web Security

- Serialization security
- Clickjacking
- DNS rebinding
- HTML5 security
- Logging collection and analysis for web apps
- Security testing
- IPv6 impact on web security

SEC522.6: Capture-and-Defend-the-Flag Exercise

- Mitigating server configuration errors
- Discovering and mitigating coding problems
- Testing business logic issues and fixing problems
- Testing web services and mitigating security problems
- Reinforcing key topics discussed throughout the course through comprehensive exercises