SEC542.1: Introduction and Information Gathering

• Overview of the web from a penetration tester's perspective
• Exploring the various servers and clients
• Discussion of the various web architectures
• Discovering how session state works
• Discussion of the different types of vulnerabilities
• WHOIS and DNS reconnaissance
• The HTTP protocol
• WebSocket
• Secure Sockets Layer (SSL) configurations and weaknesses
• Heartbleed exploitation
• Utilizing the Burp Suite in web app penetration testing

SEC542.2: Configuration, Identity, and Authentication Testing

• Scanning with Nmap
• Discovering the infrastructure within the application
• Identifying the machines and operating systems
• Exploring virtual hosting and its impact on testing
• Learning methods to identify load balancers
• Software configuration discovery
• Learning tools to spider a website
• Brute forcing unlinked files and directories
• Discovering and exploiting Shellshock
• Web authentication
• Username harvesting and password guessing
• Fuzzing
• Burp Intruder

SEC542.3: Injection

• Session tracking
• Authentication bypass flaws
• Mutillidae
• Command Injection
• Directory traversal
• Local File Inclusion (LFI)
• Remote File Inclusion (RFI)
• SQL injection
• Blind SQL injection
• Error-based SQL injection
• Exploiting SQL injection

• SQL injection tools
• sqlmap

SEC542.4: XXE and XSS

• XML External Entity (XXE)
• Cross-Site Scripting (XSS)
• Browser Exploitation Framework (BeEF)
• AJAX
• XML and JSON
• Document Object Model (DOM)
• Logic attacks
• API attacks
• Data attacks

SEC542.5: CSRF, Logic Flaws and Advanced Tools

• Cross-Site Request Forgery (CSRF)
• Python for web app penetration testing
• WPScan
• w3af
• Metasploit for web penetration testers
• Leveraging attacks to gain access to the system
• How to pivot our attacks through a web application
• Exploiting applications to steal cookies
• Executing commands through web application vulnerabilities
• When tools fail

SEC542.6: Capture the Flag