Day 1:
Introduction and Information Gathering

1. Why the Web
2. Application Assessment Methodologies
3. Course Logistics
4. Web Application Pen Tester's Toolkit
5. Interception Proxies
6. Exercise: Configuring Interception Proxies
7. HTTP Syntax and Messaging
8. Open Source Intelligence (OSINT)
9. Virtual Host Discovery
10. Exercise: Virtual Host Discovery
11. HTTP Semantics
12. HTTPS and Testing for Weak Ciphers
13. Exercise: Testing HTTPS
14. Target Profiling
15. Exercise: Gathering Server Information
16. Summary
17. Bonus Exercise: Testing and Exploiting Heartbleed

Day 2:
CONFIGURATION, IDENTITY, AND AUTHORIZATION TESTING

1. Insufficient Logging and Monitoring
2. Spidering Web Applications
3. Exercise: Web Spidering
4. Forced Browsing
5. Exercise: ZAP and ffuf Forced Browse
6. Fuzzing
7. Information Leakage
8. Authentication
9. Exercise: Authentication
10. Username Harvesting
11. Exercise: Username Harvesting
12. Burp Intruder
13. Exercise: Fuzzing with Burp Intruder
14. Session Management
15. Exercise: Burp Sequencer
16. Authentication and Authorization Bypass
17. Vulnerable Web Apps: Mutillidae
18. Exercise: Authentication Bypass
19. Summary
20. Appendix: Shellshock
21. Bonus Exercise: Exploiting Shellshock

Day 3:
INJECTION AND XXE

1. Command Injection
2. Exercise: Command Injection
3. File Inclusion and Directory Traversal
4. Exercise: Local/Remote File Inclusion
5. Insecure Deserialization
6: Exercise: Insecure Deserialization
7. SQL Injection Primer
8. Discovering SQLi
9. Exploiting SQLi
10. Exercise: Error-Based SQLi
11. SQLi Tools
12. Exercise: sqlmap + ZAP
13. XXE
14. Exercise: XXE
15. Summary

Day 4:
XXS:

1. Protecting Cookies
2. Document Object Model (DOM)
3. Cross-Site Scripting (XSS) Primer
4. Classes of XSS
5. Exercise: XSS
6. Discovering XSS
7. XSS Impacts
8. Exercise: HTML Injection
9. XSS Tools
10. BeEF
11. Exercise: BeEF
12. AJAX
13. Data Attacks
14. REST and SOAP
15. Exercise: DOM-Based XSS
16. Summary

Day 5:
CSRF, Logic Flaws and Advanced Tools

1. Cross-Site Request Forgery
2. Exercise: CSRF
3. Logic Attacks
4. Python for Web App Pen Testers
5. Exercise: Python

6. WPScan and ExploitDB
7. Exercise: WPScan and ExploitDB
8. Burp Scanner
9. Metasploit
10. Exercise: Metasploit
11. Exercise: Drupalgeddon2
12. When Tools Fail
13. Exercise: When Tools Fail
14. Business of Pentesting: Preparation
15. Business of Pentesting: Post Assessment
16. Summary
17. Bonus Exercise: Bonus Challenges
18. Preview: SEC642 and SEC552