Sans Sec 542 Syllabus

Introduction and Information Gathering

01-Why the Web

02-Understanding the Web

03-Web App. Pen Tester's Toolkit

04-Interception Proxies

05-WHOIS and DNS

06-Open Source Information

07-The HTTP Protocol

08-HTTP Methods

09-HTTP Status Codes

010-WebSocket

011-HTTPS

Configuration, Identity, and Authentication Testing

01-Nmap

02-Testing Software Configuration

03-Spidering Web Applications

04-Analyzing Spidering Results

05-Fuzzing

06-Authentication

07-Username Harvesting

Injection

01-Session Tracking

02-Session Fixation

03-Bypass Flaws

04-Vulnerable Web Apps

05-Command Injection

06-File Inclusion-Directory Traversal

07-SQL Injection Primer

08-Discovering SQLi

09-Exploiting SQLi

010-SQL Tools

XXE and XSS

01-Cross Site Scripting

02-XSS Fuzzing

03-XSS Exploitation

04-BeEF

05-XXE

CSRF, Logic Flaws

01-Cross Site Request Forgery

02-Logic Attacks

03-WPScan and Other Tools

04-Pen Testing Methods

05-Reporting