Burp Suite Community Edition, Part 2 of 4: Dashboard and Live Task

page 1

Meet the expert: Atul has been involved in information security, IT auditing, and penetration testing web apps in the field of information security training for over 8 years.

Prerequisites: Web application development and HTML knowledge are required

Runtime: 02:32:15

Course description: Burp Suite is a set of tools to test web applications for penetration testing. Burp suite community edition gives tools and strategy to assist in hunting and finding bugs on the target platforms. This course covers: Burp Dashboard, Repeater module, Attack Types, and payloads and hidden form fields.

Course outline:

Burp Dashboard and Live Task
- Introduction
- Burp Dashboard and live task
- New Live Passive Scan
- Individual Tasks
- Burp UserOptions and ProjectOptions customisations
- User Options
- Reload Options
- Preserve User Options
- Override User Options
- Summary

Repeater Module Testing
- Introduction
- Repeater module testings
- Searching
- Request Tips
- Burp intruder Configurations
- Intruder Options
- Attack Types Overview
- Summary

Burp Intruder Attack Types
- Introduction
- Burp Intruder attack types - Attacks
- Battering Ram and Pitchfork
- Cluster Bomb
- Payload processing and bruteforcer
- Payload Processing Rules
- Summary

Grep-extract with Cluster Bomb
- Introduction
- Grep-Match _ Grep-extract with clustor bomb
- Match Unique Value
- Valid User
- SQL Injection Ninja
- Match Expressions for SQL Injection
- Summary

Payload Types and Hidden Form Fields
- Introduction
- Some Best payloads type used and hidden form fiel
- Null Payload and Other Types
- Username Request and Response
- User names generator
- Summary