testuj.pl

Testy bezpieczeństwa API - 2 dni

Korzyści dla uczestników:

- Zrozumienie działania API
- Poznanie podstawowych mechanizmów komunikacji API
- Poznanie typowych słabości bezpieczeństwa API poprzez wykonywanie ataków
- Zyskanie świadomości i znajomości istniejących metod defensywnych

- Jak działa API?
  - Architektura
  - Określanie słabości architektury
  - Schemat działania API
- Metody komunikacji z API
  - POST, GET, PUT, DELETE
- Konfigurowanie komunikacji z API poprzez Postman
  - Importowanie API calls
  - Proxowanie komunikacji między Postmanem a Burpem
  - Wyszukiwanie endpointów
- OWASP API Top 10
  - Broken Object Level Authorization
  - Broken Authentication
  - Broken Object Property Level Authorization
  - Unrestricted Resource Consumption
  - Broken Function Level Authorization
  - Unrestricted Access to Sensitive Business Flows
  - Server Side Request Forgery
  - Security Misconfiguration
  - Improper Inventory Management
  - Unsafe Consumption of APIs
- Wykonywanie testów penetracyjnych
  - Przeprowadzanie ataków na każdy z elementów OWASP API Top 10
- Określanie mechanizmów bezpieczeństwa
  - Definiowanie przykładowych mechanizmów bezpieczeństwa na bazie wykonanych ataków