



API Security Bootcamp Hands-On OWASP Top 10 for APIs

Dr. Sunny Wear

2023

Burp Suite Cookbook

Practical recipes to help you master web penetration testing with Burp Suite



Packt
www.packtpub.com

Sunny Wear

Instructor: Sunny Wear, D.Sc.

- Doctor of Science in Cybersecurity
- Security Architect, Web App Pen Tester, Author, Teacher
- Website: <https://sunsolsec.com> for Sunshine Solutions, LLC
- Content is for educational purposes only
- Subscribe to YouTube Channel: <https://www.youtube.com/c/SunnyWear>
- Twitter **@SunnyWear**
- 3 Courses on Burp available on Pluralsight
- Books available on Amazon:
 - Burp Suite Cookbook, Secure Coding Field Manual
- Custom mobile app written as a Burp Suite reference - Burp Tool Buddy

Agenda

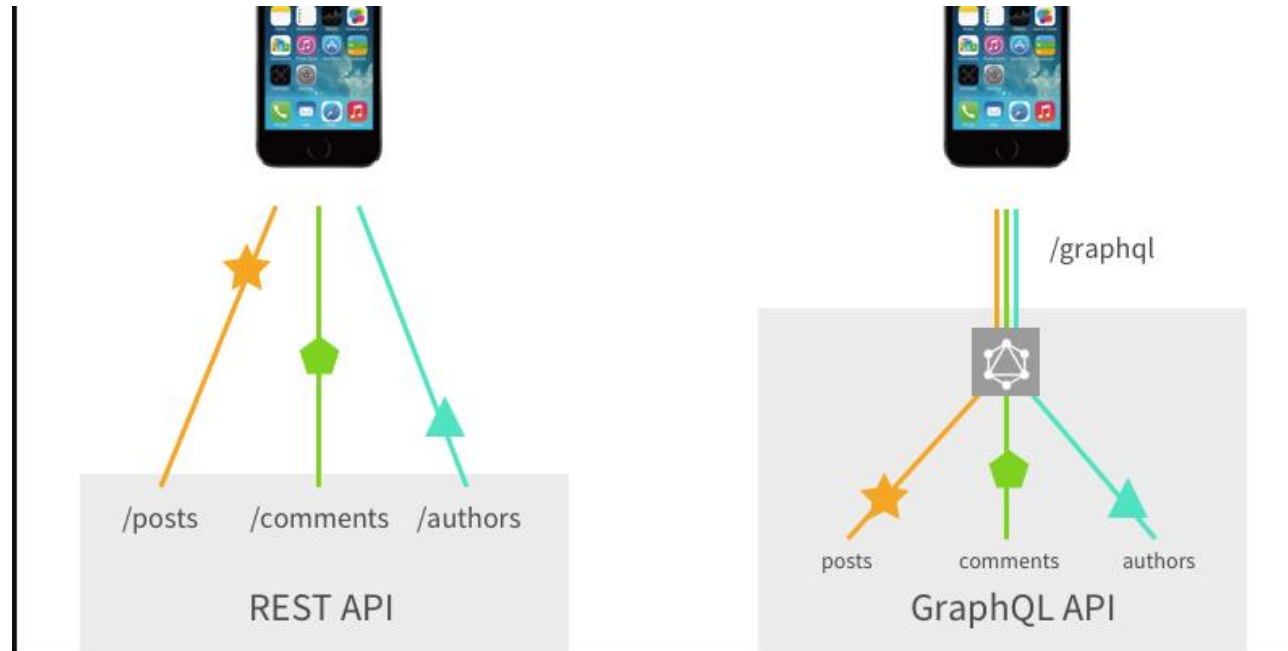
Day 1

- OAuth Attacks
- BOLA
- Excessive Data Exposure
- Hacking JWTs

Day 2

- Security Misconfigurations
- Hacking GraphQL
- Mass Assignment Attacks
- CORS

Types of APIs
to be
covered in
this
workshop

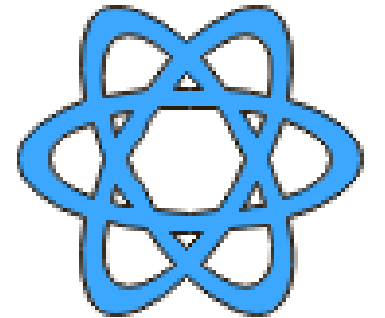


- REST API
- GraphQL

OWASP Top 10 for APIs

- 
- The infographic displays the OWASP Top 10 for APIs, organized into two columns. Each item is represented by a green circular icon with a white number, followed by a green arrow-shaped box containing the name of the vulnerability. The items are numbered 01 through 10.
- 01 Broken Object Level Authorization
 - 02 Broken User Authentication
 - 03 Excessive Data Exposure
 - 04 Lack of Resources & Rate Limiting
 - 05 Broken Function Level Authorization
 - 06 Mass Assignment
 - 07 Security Misconfiguration
 - 08 Injection
 - 09 Improper Asset Management
 - 10 Insufficient Logging & Monitoring

Getting Started



Let's setup your environment!

Environment Setup

Burp Community or Professional Edition

<https://portswigger.net/burp/communitydownload>

Burp Plugins: JWT Editor

Portswigger Account to access Labs

<https://portswigger.net/users/register>