CybrigeSolutions
Cybersecurity Training

COURSE SYLLABUS

PHASE 3 · CCAP | LIVE INSTRUCTOR-LED | LAUNCHING SOON

CYBRIGE CERTIFIED API PENTESTER

(CCAP)

Hack REST and GraphQL APIs the way attackers do — OWASP API Top 10, broken auth, BOLA/IDOR, mass assignment and more.

LEVEL Basic To Advanced	LANGUAGE Hindi	MODE Live Instructor-led
ACCESS Lifetime	CERTIFICATE Yes, verifiable	SUPPORT WhatsApp

Kickstart your career in cybersecurity with Cybrige!

+91 88828 84212 · team@cybrigesolutions.com · cybrigesolutions.com

01 What you'll learn

- How modern REST and GraphQL APIs work under the hood
- OWASP API Security Top 10 with hands-on labs
- BOLA / IDOR, broken authentication, JWT attacks and mass assignment
- Testing with Postman, Burp Suite and automation scripts
- Writing API vulnerability reports that get accepted

02 Who this course is for

- Web pentesters and bug bounty hunters moving into APIs
- Developers who build APIs and want to secure them

03 Course Curriculum

3 modules · 12 topics

MODULE 01 API Fundamentals — 3 topics

- How REST & GraphQL APIs Work
- API Recon & Documentation Discovery
- Setting up Postman & Burp for APIs

MODULE 02 OWASP API Top 10 — 5 topics

- Broken Object Level Authorization (BOLA)
- Mass Assignment
- Rate Limiting & Resource Abuse
- Broken Authentication & JWT Attacks
- Excessive Data Exposure

MODULE 03 Advanced API Attacks — 4 topics

- GraphQL Introspection & Attacks
- Business Logic Flaws
- SSRF through APIs
- Reporting API Vulnerabilities

LAUNCHING SOON

Message us to reserve your seat

https://cybrigesolutions.com/courses/cybrige-certified-api-pentester

WhatsApp +91 88828 84212 · team@cybrigesolutions.com

Certificates issued by Cybrige Solutions can be verified at cybrigesolutions.com/verify