iGNITE Technologies

API PENTEST

Training Program by Ignite Technologies

API PENTEST TRAINING PROGRAM

ABOUT COURSE

What is API Pentest course?

The OWASP API Top 10 will be focused in the API Pentest course to create awareness about modern API security issues. If you're familiar with the OWASP Top 10 series, you'll notice the similarities: they are intended for readability and adoption. APIs play a very important role in modern applications' architecture and APIs handle a very high volume of sensitive data, ensuring their safety through persistent testing is critical.

Its purpose is to ascertain whether an API is vulnerable and then to suggest to the client what patches should be applied.

Who needs API Pentest?

API penetration testing should be conducted regularly for every company that uses mobile or web applications with an API backend. The security of APIs is crucial to the security of applications.

Ignite Training Objective

API Security Top 10

API Security Cheat Sheet

crAPI – Completely Ridiculous API, an intentionally vulnerable API project)

Prerequisites

Basic knowledge of Web Application Pentesting as per OWASP top 10, ethical hacking, Kali Linux and BurpSuite,

iGNITE Technologies

30 Hours (Tentative)

ABOUT

Well-Known Entity for Offensive Security

{Training and Services}

ABOUT US

With an outreach to over a million students and over thousand colleges, Ignite Technologies stood out to be a trusted brand in cyber security training and services

WHO CAN ?

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide realtime exposure.
- Get a training certificate of participation.

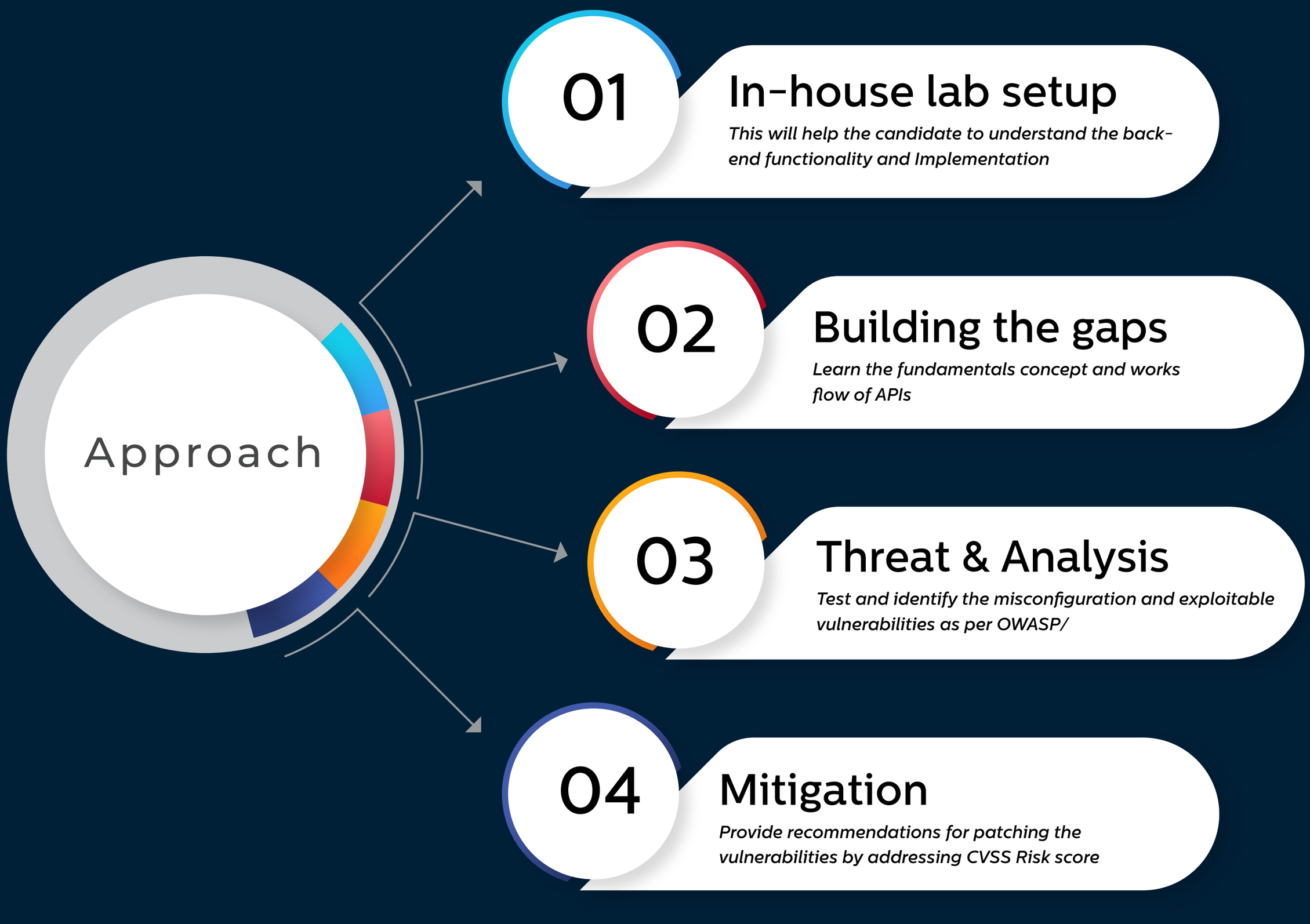
HOW WE FUNCTION

IGNITE TRAINERS

Ignite Trainers are well-experienced and have vast experience with real-time threats.

Had working exposure in Big Fours and MNCs and Fortune 500 companies and clients such as Tata, Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more.

Certified Trainers: CEH, OSCP, OSWP, Iso- Lead Auditor, ECSA, CHFI, CISM



iGNITE Technologies

Course Content

1. Course Introduction

2. How API works with Web application

3. Types of APIs and their advantages/ disadvantages

4. Analysing HTTP request and response headers

5. API Hacking methodologies

6. Enumerate web pages and analyse functionalities

7. API passive reconnaissance Strategies

8. API active reconnaissance (Kite runner)

9. Introduction to POSTMAN

10. Testing for the Excessive data exposure

11. Directory indexing /brute force

12. Password mutation

13. Password spray attacks against web application

14. Introduction to JSON Web Token

15. Hunting for JWT authentication vulnerabilities

16. Exploiting JWT unverified signature

17. Cracking JWT secret keys

18. Bypass JWT removing signature

19. Exploit jku header injection

20. Exploit KID in JSON web tokens

21. Attacking 0Auth 2.0

22. Introduction to OWASP TOP 10 API

23. Hunting and exploiting XXS in API

24. Testing for the ReDOS attack in the API web application

25. Exploiting XML vulnerabilities

26. WordPress XML-RPC attack

27. Exploiting WSDL/SOAP to RFI

28. API Automated Vulnerability scanning

29. Testing SQL/NoSQL Injection in an API

30. Exploiting object-level access control

31. Exploiting Function level access control

32. Testing in band SSRF vulnerabilities in an API

33. Testing out band SSRF vulnerabilities in an API

34. Testing OS Command Injection

35. Exploiting Java deserialization vulnerabilities

36. Testing for improper assets management

37. Testing for Mass assignment vulnerabilities

38. Bypass filter, space, and blacklisted characters

39. Bypass Captcha and MFA

40. Remediations and Reporting

iGNITE Technologies

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

WhatsApp

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/ignitetechnologies

iGNITE Technologies