API Hacking | Security Testing Training for DevOps | InfoSec Startups

Online Training 24x7 Availability

API Security Testing Training

for Pentester | Bug Hunters | DevOps and InfoSec

Bug Bounty

WANTED:

Contact Anytime Call | WhatsApp: +91 96809 81337

Training Fee: 6000 inr | 100 usd

The Hacktivists

Information Security Training Providing Company

Call us : 96809 81337

Syllabus: API Hacking and Security Testing Training

Requisite: Web Application Pentesting | Knowledge of OWASP Top 10 Security Risks

Level: Intermediate -> Advanced **Fee : 6000 INR | 100 USD**

Training Level: Live API Hacking | Security | Bug Bounty | Development

Why you Join us :
01. 100% #vulnerability #Practical on #Live Secure | Unsecure Web & Mobile APIs
02. Covered Bugs & Vulnerabilities with two-time practicals with Challenges
03. InfoSec Employer? We got something special for you too. Contact us!
04. Cover each Bugs according to Bug Bounty Platforms like HackerOne and Bugcrowd
05. We provide training in Hindi, English, Spanish and in Portuguese too.

An Introduction to APIs for the Security Testing

- What An API Is and Why It's Valuable
- Different Approach of API Security Testing
- Real-time Challenges of API Security Testing
- Tools and Frameworks for API Security Testing
- Types of Bugs that API Security testing detects
- Difference between Common API testing and API Security testing

Rethink Governance in an API-First World

- Primary Goal of API Governance
- So Why Implement API Governance?
- What Should API Governance Include?
- Implementing an API Governance Approach
- Modern APIs Are Different Than Integration
- how governance can enable security and compliance
- All WebApp and MobileApp development is API development
- best practices to help organizations scale their API program
- API governance : A key element for security and scaling API programs

- how to execute API governance throughout design, implementation & runtime operations

Setup of API Security Testing environment

- Installation of API Security Testing tools
- Installation of API Security Testing Frameworks
- Configuration and Testing builds of Live Test Cases

Testing APIs Code Quality and Build Settings

- First, let’s look at the APIs Documentations
- API Documentation Made Easy Security Testing
- Security Review of APIs Documentations
- Understanding API-Based Platforms

Getting Started with API Security Testing

- Setup API Live Test Case Environment
- API Penetration Testing Methodologies
- API Security testing Checklists for Pentesters
- API Security testing Checklists for Developers
- API Security testing Checklists for Bug Hunters
- API Security testing according to API governance

MobileApp and WebApp APIs Security Testing

- Complete Security testing of Web API Applications
- Complete Security testing of Mobile API Applications
- Covering Security Audit of MobileApp API and WebApp API

Discovering Leaky APIs | Hidden APIs – Reconnaissance

- Configure Fiddler to find Sensitive and leaky APIs
- Configure Burpsuite to Security test of Hidden APIs
- Proxying Device Traffic Through Fiddler | Burpsuite
- Discovering More About Mobile Apps via Fiddler
- Discovering Hidden APIs via Documentation Pages
- Discovering Hidden APIs via Search Engine
- Discovering Hidden APIs via robots.txt

- Discovering Leaky APIs - UserID Endpoint
- Discovering Leaky APIs - User Input Endpoint
- Discovering Leaky APIs - User Interaction Endpoint
- Personally Identifiable Information (PII) Disclosure

API Authentication and Authorization Vulnerabilities

- A Practical Approach to Test: Various OAuth Misconfiguration
- A Practical Approach to Test: OAuth Authorization Bypass
- A Practical Approach to Test: Account takeover Issues
- Improper Restriction of Unprotected APIs Endpoint
- Transporting API Auth tokens as Cleartext Allowed
- Improper Restriction of Misconfigured API
- Insufficient Entropy For Random Values
- Leakage of API Authentication Tokens
- Improper Access Control

API Manipulation and Parameter Tampering

- A Practical Approach to Test: XML External Entity (XXE) Processing
- A Practical Approach to Test: HTTP Parameter Pollution Attacks
- A Practical Approach to Test: Cross-site Scripting (XSS)
- A Practical Approach to Test: Common Injection Attacks
- A Practical Approach to Test: Command Injection
- A Practical Approach to Test: SQL injection
- Manipulating App Logic by Request Tampering
- Response Tampering

API Security Top 10 according to OWASP

- OWASP API Security Vulnerabilities - Practicals
- Testing for Broken Function Level Authorization
- Testing for Broken Object Level Authorization
- Testing for Lack of Resources & Rate Limiting
- Testing for Broken User Authentication
- Testing for Improper Assets Management
- Testing for Security Misconfiguration
- Testing for Excessive Data Exposure
- Testing for Mass Assignment

Modern APIs Vulnerabilities and Bug Bounty - Introduction

- Why APIs Security Testing Important in Bug Bounty Hunting
- Why APIs Security Testing Important in WebApp Security Auditing
- Why APIs Security Testing Important in MobileApp Security Auditing

Modern APIs Vulnerabilities and Bug Bounty - Practicals

- A Practical Approach to Test: Insecure Direct Object Reference(IDOR)
- A Practical Approach to Test: Cross-Origin Resource Sharing (CORS)
- A Practical Approach to Test: Cross-Site Request Forgery (CSRF)
- A Practical Approach to Test: Open Redirection Vulnerability
- A Practical Approach to Test: Privilege escalation Issues
- A Practical Approach to Test: Local File Inclusion (LFI)
- A Practical Approach to Test: Remote File Inclusion(RFI)
- A Practical Approach to Test: Input validation Issues

*Contact us :

- Need technical assistance? Speak with a support representative by calling +91-9680-981-337