COURSE TABLE OF CONTENTS

OWASP API Security Top 10

OEM: owasp • Duration: 2 Days (16 hrs)

COURSE MODULES & TOPICS

Module 1: API Fundamentals and Lab Setup
- Endpoints, HTTP methods, tokens, and API documentation
- Test accounts and mapping the training API
- Capture baseline requests (LAB)

Module 2: Broken Object Level Authorization
- Object ownership checks and unauthorized access
- Test access to records across user accounts (LAB)

Module 3: Broken Authentication
- Login, token validation, and session handling
- Authentication and token control weaknesses
- Test authentication and token controls (LAB)

Module 4: Broken Object Property Level Authorization
- Excessive field exposure and unauthorized property changes
- Inspect response fields and restricted property updates (LAB)

Module 5: Unrestricted Resource Consumption
- Request limits, pagination, and upload limits
- Resource budgets and consumption controls
- Check limits with controlled request budget (LAB)

Module 6: Broken Function Level Authorization
- Role restrictions and administrative endpoints
- Method-based authorization checks
- Compare actions for user and admin roles (LAB)

Module 7: Unrestricted Access to Sensitive Business Flows
- Abuse of valid actions: purchases, invitations, reservations
- Test business workflow for abuse controls (LAB)

Module 8: Server Side Request Forgery
- User-supplied URLs and server-initiated requests
- Destination controls and URL handling
- Validate URL handling with internal test service (LAB)

Module 9: Security Misconfiguration
- CORS, debug output, and error handling
- Insecure service settings and misconfigurations
- Inspect and verify misconfigurations (LAB)

© Koenig Solutions

Module 10: Improper Inventory Management

- API versions and undocumented endpoints
- Exposed test services and version comparison
- Find and compare API versions (LAB)

Module 11: Unsafe Consumption of APIs

- Trust in upstream responses and input validation
- Integration boundaries and crafted responses
- Test handling of mock upstream API response (LAB)

Module 12: Skills Assessment and Reporting

- Risk prioritisation and remediation
- Evidence quality and retesting
- Complete integrated API assessment and reporting (LAB)