COURSE TABLE OF CONTENTS

Security Issues and Performance Bottlenecks in AI-Generated Code

OEM: Koenig Original • Duration: 3 Days (24 hrs)

COURSE MODULES & TOPICS

Module 1: AI-Assisted Development and Risk Landscape

- Usage of code-generation tools
- Strengths and limitations of AI-generated code
- Hallucinated APIs and incorrect assumptions
- Outdated or insecure code patterns
- Generated-code provenance
- Human accountability and review responsibilities

Module 2: Secure Code Review Fundamentals

- Threat-modelling basics
- Assets, trust boundaries and attack surfaces
- Input validation and output encoding
- Authentication versus authorization
- Secrets and configuration handling
- Dependency and package risks

Module 3: Common Application and API Security Issues

- SQL injection and parameterized queries
- Cross-site scripting (XSS) and CSRF
- Broken authentication and authorization
- Insecure direct object references
- Sensitive-data exposure
- Unsafe file handling
- Deserialization risks
- Secure error handling
- OWASP Top 10 and API Security concepts

Module 4: Performance Bottlenecks in Generated Code

- Algorithmic complexity and inefficient loops
- N+1 database queries
- Missing indexes and inefficient SQL
- Unnecessary allocations and large object graphs
- Synchronous I/O and thread-pool starvation
- Caching misuse
- Excessive API calls and payload sizes
- Basic measurement and profiling concepts

Module 5: Verification and Engineering Guardrails

- Unit and integration tests
- Negative, boundary and regression testing

© Koenig Solutions

- Static analysis and linters
- Dependency and vulnerability scanning
- Code-review checklists
- Safe logging and telemetry
- CI quality gates
- Evidence-based acceptance criteria

Module 6: Hands-On Review and Remediation Lab

- Inspect flawed AI-generated code changes
- Identify and classify security and performance findings
- Prioritise risks and refactor selected issues
- Run tests and explain verification evidence