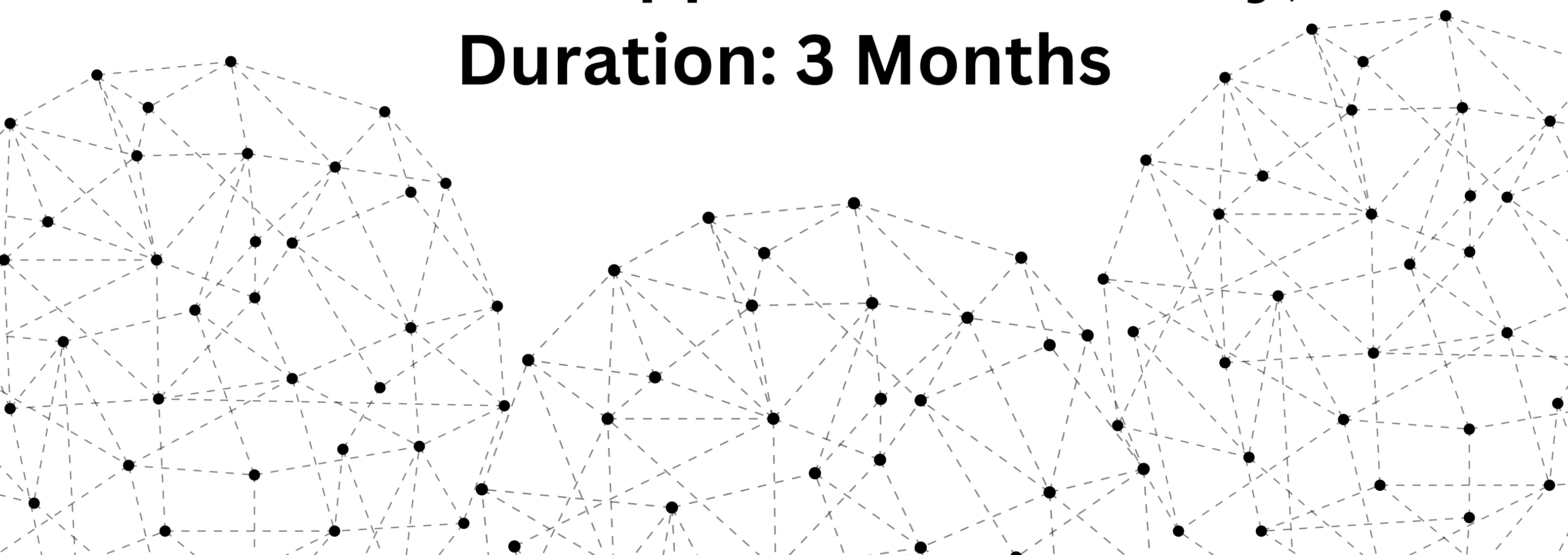


NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY, PATNA

SUVIKSAN TECHNOLOGIES PRIVATE LIMITED

Syllabus

Course : Application Security,
Duration: 3 Months



Module 1: Introduction to Application Security

- o What is Application Security?
- o Why Apps Get Hacked (Real-World Breaches)
- o Secure SDLC vs. Traditional SDLC
- o OWASP Overview: OWASP Top 10 (Web + API)

Module 2: Secure Coding Principles

- o Common Coding Flaws & Fixes
 - ▢ Input Validation & Sanitization
 - ▢ Authentication & Session Management
 - ▢ Secure Password Handling
 - ▢ Cryptography Basics (Hashing, Encryption)
- o Language-Specific Secure Coding:
 - ▢ Java, Python, PHP, JavaScript (overview)
- o Lab: Identify & fix vulnerabilities in code snippets

Module 3: Web Application Security

- o OWASP Top 10 (Deep Dive):
 - ▢ SQL Injection, XSS, CSRF
 - ▢ Insecure Deserialization
 - ▢ Security Misconfigurations
 - ▢ Broken Authentication/Authorization
- o Tools: Burp Suite, OWASP ZAP, Postman
- o Lab: Exploit & patch vulnerabilities in DVWA / Juice Shop

Module 4: API & Mobile Application Security

- o API Security
 - ▢ OWASP API Top 10
 - ▢ Authentication & Rate Limiting
 - ▢ Example attacks: BOLA (Broken Object Level Authorization)
- o Mobile Security (Intro)
 - ▢ Android & iOS App Risks (MASVS)
 - ▢ Reverse Engineering Basics
- o Tools: Postman, MobSF
- o Lab: Test insecure APIs & mobile APKs

Module 5: Application Security Testing

- o Testing Approaches:
 - ▢ SAST (Static Analysis)
 - ▢ DAST (Dynamic Testing)
 - ▢ IAST (Interactive Testing)
- o Tools: SonarQube, Dependency-Check, Burp Suite Pro
- o Secure Code Review Basics
- o CI/CD Pipeline Security (DevSecOps)
- o Lab: Add SAST/DAST to a CI/CD pipeline

Module 6: Governance, Risk & Compliance

- o Application Security Policies
- o Secure Coding Standards (CERT, CWE, OWASP ASVS)
- o Regulatory Needs: PCI DSS, HIPAA, GDPR
- o Security Documentation & Reporting

Module 7: Capstone Project & Final Assessment

- o Project Examples:
 - ▢ Secure a vulnerable web app (OWASP Juice Shop)
 - ▢ Perform API pentest & fix issues
 - ▢ Implement a DevSecOps mini pipeline with SAST/DAST
- o Final Assessment: Theory + Hands-On

(Note: Points mentioned are just short summary, but they consist of a lot of subtopics and detailed structure with practical scenarios)