Secure Software Development Life Cycle (Secure SDLC)

Online Lab Access | 32+ Hours | Hack2Secure's "SWADLP" Exam Attempt

Aligned with Industry Security Standards and Best Practices

Secure Software Development Life Cycle or Secure SDLC is a systematic and structured concept to integrate Security at every phase of Software Development Life Cycle. Ensuring security in a product from scratch, not only helps in ensuring all compliances and basic security requirements but can also assist in implementing Security Controls at Low Cost.

Hack2Secure's Workshop on Secure Software Development Life Cycle provides hands-on exposure and relevant Case Studies to assist in analysing, evaluating, implementing and ensuring Security requirements across SDLC phases.

Key Take Away

- Security requirements across SDLC phases
- Secure SDLC Compliances and Framework requirements
- Software Security Standards and Assurance Methodologies
- OWASP Top 10 Web Security Risk
- Gathering Security Requirements
- Establishing Security Baseline, Checkpoints and Quality Gates
- Software Security Risk Management
- Threat Modeling: Process and Use Cases
- Secure Coding Practices and Review Guidelines
- Web Application Security Testing Tools, Techniques and Methodologies
- Building and Evaluating Final Security Review Plan
- Incident Handling Process
- Supply Chain Risk Management
- Security Patch Management
- Handling 3rd party Library upgrades

For more details

www.hack2secure.com/securesdlc

Get Aligned

Get Aligned with Industry Security Standards and Best Practices

- BSIMM7 & OpenSAMM Framework
- NIST SP 800-64 Secure SDLC requirements
- PCI DSS, NIST and FIPS recommended Software Security practices
- OWASP Web Security Testing Practices
- OWASP and CERT recommended Secure Coding Practices
- Common Vulnerability Scoring System

How It Helps?

- Early Identification and Mitigation of Security Vulnerabilities
- Reduced Control Implementation Cost
- Awareness on Potential Engineering Challenges
- Measurable and Comprehensive Security Risk Management
- Security Assurance and Industry Compliant Software
- Adoption of Security Standards, Best Practices and Methodologies

Online Lab Access | 32+ Hours | Hack2Secure's "SWADLP" Exam Attempt

Aligned with Industry Security Standards and Best Practices

What You Will Receive

- **Instructor-Led Sessions**
  - Live online | Classroom
- **Soft Deliverables**
- **Online Lab Access**
  - Cloud Based | 30 Days
- **SWADLP Cert Attempt Voucher**
  - 1 Attempt, 6 months Validity
  - Globally Proctored by Pearson VUE
- **Training Completion Certificate**
- Access to **Self-Paced Online Sessions**

Pre-Requisites

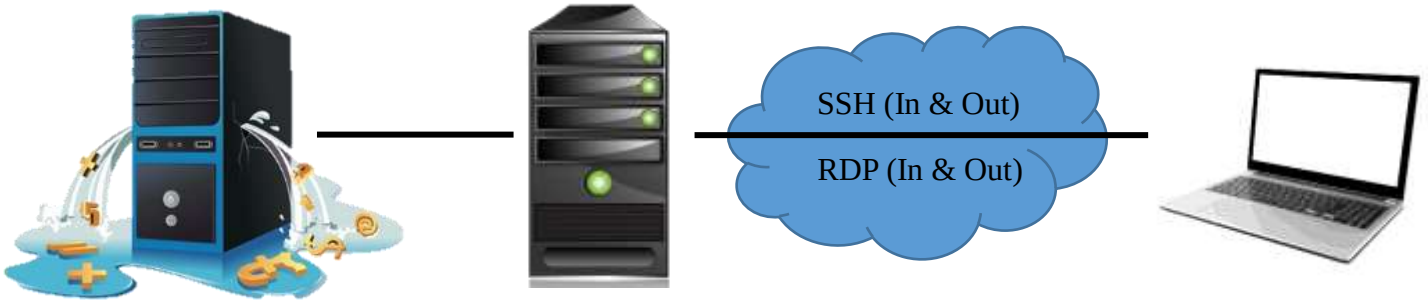
- Awareness on Software/Application Development Methodologies
- Knowledge of Web Technologies
- Basic Protocol functionality of Protocols especially HTTP

Who Should Attend

- **Management Team**
  - Software Development Managers
  - Software Program Managers
  - Project Assurance Team
  - Team Leads, Senior Consultants
  - CxO, Directors, VPs
- **Research & Development Team**
  - Architects, Developers
  - Software Testing Team (QA)
  - Software Analyst, Consultants
  - Research Engineers
- **Product Security Team/Office**
  - CISO, Security Managers
  - Assurance and Compliance Officer
  - Security Consultants
  - Auditors, Security Engineers, Testers and Analyst
- **Students**, Looking to pursue career in Secure Software Development and Management
- **Anyone**, Who is interested in exploring Secure SDLC process and practices

Online Lab Layout

Cloud Based | Independent Setup for Each Participant | Accessible for 30 Days



Vulnerable Web Server (Target Machine)

Linux Machine (Client/Attacker)

Candidate Machine

Detailed Curriculum

Secure SDLC Phase#1: Security Awareness

- About Secure SDLC
- Process, Requirements & Methodologies
- Secure SDLC in Agile
- Case Studies
- Information Security Concepts
- Core Security Concepts
  - C.I.A. Triad, A.A.A. Concept
- Security Design Principles
- Threats, Risk & Vulnerabilities
- Software Security Standards, Regulations & Compliances
- Secure SDLC Standards & Frameworks
- NIST SP 800-64
- BSIMM7 Framework
- Security Assurance Methodologies
- STRIDE, DREAD
- Common Vulnerability Scoring System (CVSS)
- Risk Management: Overview
- OWASP Top10 Web Application Security Risk

Secure SDLC Phase#2: Building Security Requirements

- Defining Security Quality Gates
- Building Security Requirement Checklist
  - Core Security Requirements
    - Ensure C.I.A. and A.A.A.
  - General Security Requirements
    - Ensure Secure Session, Error and Configuration Management
  - Operational Security Requirements
    - Related with Secure Deployment Environment, Archiving and Anti-Piracy
  - Other
    - Related with International Laws, Procurement & Time Sequencing concerns

Secure SDLC Phase#3: Ensuring Secure Design

- About STRIDE
- Attack Surface Analysis
- Threat Modeling
  - Process, Benefits & Use Cases
  - Workshop: Design, Define & Analyze Threat Model

Secure SDLC Phase#4: Secure Implementation (Coding)

- Application Coding: Common Security Myths
- CWE Top 25 Programming Errors
- Implementation Level Controls against
  - OWASP Top10 Web Security Risk
  - Buffer Overflow
  - Insecure Cryptographic Storage
  - Information Leakage
  - Improper Error Handling
- Defensive Coding Practices
  - Input Validation
  - Canonicalization
  - CAS
  - Declarative vs Programmatic Security
  - Exception Management
- Security Code Review process and Best Practices

Secure SDLC Phase#5: Web Application Security Testing

- Application Security Testing Tools, Techniques and Methodologies
  - Testing for Core Security Concepts
  - Testing for OWASP Top10 Web Application Security Risk
- Handling Security Defects

Secure SDLC Phase#6: Security Review & Response

- Building Final Security Review Plan
- Handling Auditing
- Handling VA-PT Process
- Incident Handling Process
- Threats to Supply Chain Software
- Software Deployment and Procurement Risk

Secure SDLC Phase#7: Securing Maintenance Cycle

- Security Patch Management
- Handling 3rd Party Library Upgrades
- Application Disposal Policy

Secure Web Application Development Lifecycle Practitioner

Evaluate your Skills in Secure Application Development

Hack2Secure

Secure Web Application Development Lifecycle Practitioner

Globally Available | Proctored | 150 mins. | 90 MCQ | Passing Grade: 60% | Exam Language: English

Secure Web Application Development Lifecycle Practitioner (SWADLP) Certificate program evaluates individual's implementation level skills in Security practices required to ensure Secure Application Development. This program ensures candidate's awareness on Application Security Challenges, Threats, Standards, Best Practices and assurance methodologies along with hands-on implementation level knowledge and skill-sets.

SWADLP is based on globally recognized Standards and Industry best practices to ensure knowledge and Understanding of Secure Application Development requirements. It walks through phases of Software Development and provide required strategies and processes to integrate Security at every level.

Benefits

- Validates your expertise and knowledge in Secure Application Development Process
- Get Global Recognition and Credibility
- Ensures Real Time skills required to handle Web Application Security Risk
- Demonstrate Knowledge of Industry Standards and Best Practices
- Ensures effective skills to measure and implement Security Controls

Attempt to SWADLP Exam is **included** as part of Secure SDLC Training Program from Hack2Secure

1 Attempt | 6 months Voucher Validity

Delivered globally at Pearson VUE Authorized Test Centres

Pearson | VUE

To Schedule SWADLP Exam,
www.pearsonvue.com/hack2secure

For more details, visit **www.hack2secure.com/swadlp**

www.hack2secure.com | **certificate@hack2secure.com**

About Hack2Secure

Hack2Secure excels in "Information Security" Domain and offers customised IT Security programs, including Training, Services and Solutions. Our programs are designed by industry experts and tailored as per specific needs. We help students, professionals and companies with knowledge, tools and guidance required to be at forefront of a vital and rapidly changing IT industry.

Hack2Secure
INSPIRE • INDUCE • INNOVATE

Security Training

Vendor Independent, Customizable, Across Domains

Hack2Secure excels in delivering intensive, immersion security training sessions designed to master practical steps necessary for defending systems against the dangerous security threats. Our wide range of fully customizable training courses allow individual to master different aspects of Information Security as per their industry requirement and convenience.

- Delivered Training to more than 15k+ Professionals Globally
- Vendor Independent programs aligned with Industry Security Practices and Requirements

Security Certification

- Globally delivered and Proctored Security Certification programs with **PearsonVUE**
- Vendor Independent Programs based on Industry Security Standards and Practices

End-to-End Security Services

Hack2Secure offers IT Security Professional Services to provide ways to stay ahead of Security Threats through adaptive and proactive Security methods like

- Secure Software Development Lifecycle.
- Secure Application Design & Threat Modeling.
- Application Security Testing.
- Network/Infrastructure Risk Assessment.
- Consulting

skype **hack2secure**

+91 900 81 78676
+91 900 83 78676

Hack2Secure featured as:

25 FASTEST GROWING CYBER SECURITY COMPANIES IN INDIA
Source: The CEO Magazine, India

10 BEST SECURITY COMPANIES in INDIA: 2017
Source: Silicon Review Magazine, India

EXCELLENCE IN SECURITY TRAINING PROGRAMMES
Source: GDS Review Magazine