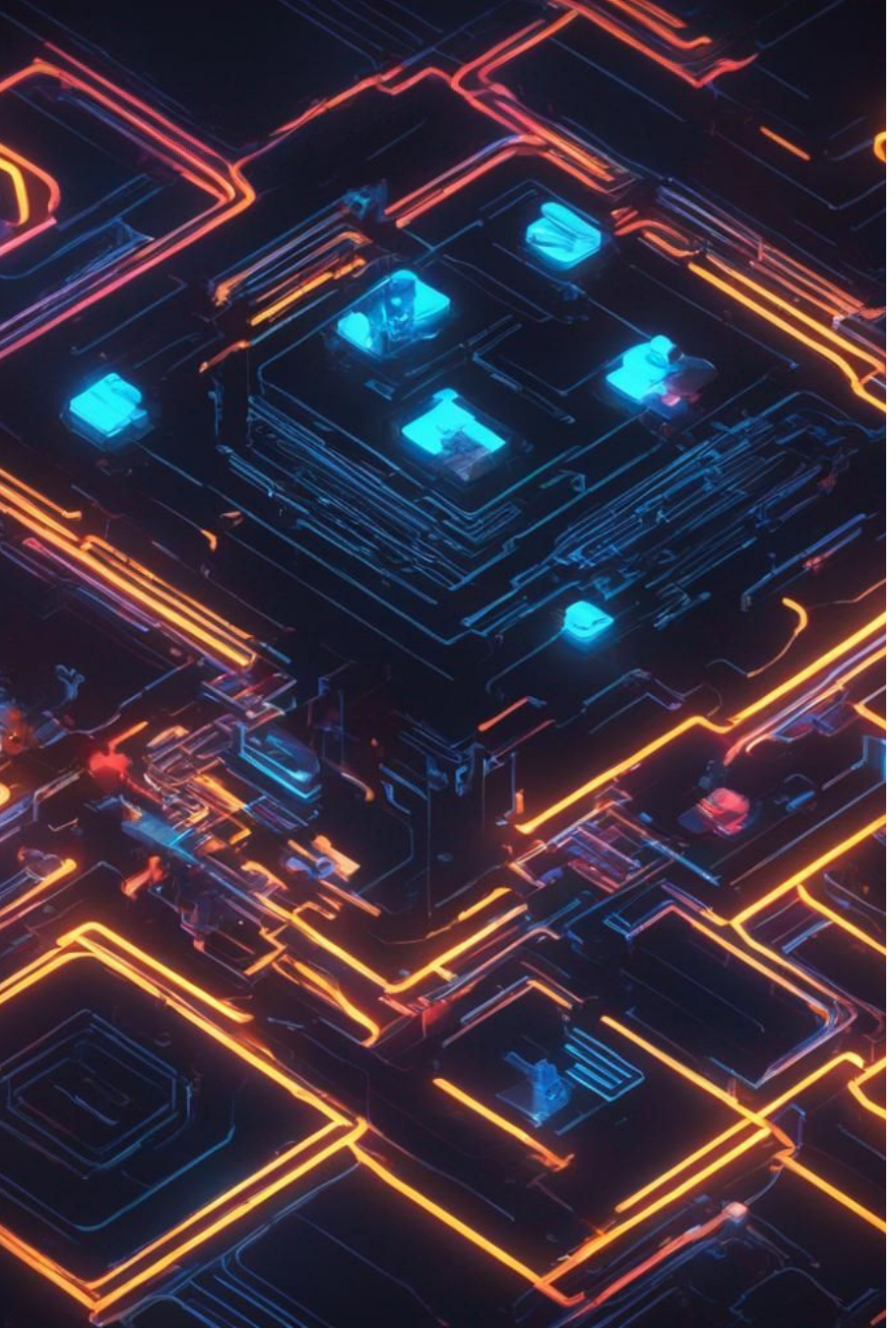

Securing the Code

A Comprehensive Guide to Software Development Security Practices and Principles

CISSP Study Guide - V

Introduction to Software Development Security

- Overview of Software Development Security
- Importance in protecting software life cycle
- Implementation of best practices and standards

System Development Life Cycle (SDLC)

- **Five Phases of SDLC:**
    a. Initiate
    b. Acquire/Develop
    c. Implement
    d. Operate/Maintain
    e. Dispose
- Iterative process to enhance security at each phase

Key Development Activities

- **Stages of Development:**
    a. Gather Requirements
    b. Design
    c. Develop
    d. Release/Maintain
- Focus on Change Management and Configuration Management for secure progression

Testing and Validation Techniques

Verification Testing: Confirm conformance to design specifications

Validation Testing: Ensure achievement of software purpose

Integration Testing: Verify module cooperation and adherence to security specifications

Acceptance Testing: Assess customer satisfaction with software functionality

Regression Testing: Confirm that code changes do not compromise functionality or security

Best Practices in Web Application Security

1. **WASC (Web Application Security Consortium):** Offers best practices for web applications

2. **OWASP (Open Web Application Security Project):** Monitors and reports on web attacks

3. **BSI (Build Security In):** Security recommendations across the development cycle

4. **IEC/ISO 27034:** Guidance for integrating security in software development and maintenance

Common Software Development Approaches

- **Overview of Development Models:**

> Build and Fix Model
>
> Waterfall Model
>
> V-Shaped Model
>
> Prototyping Model
>
> Incremental Model
>
> Spiral Model

- Emphasizes iterative development and feedback mechanisms

Agile Methodologies and Process Improvement

- RAD (Rapid Application Development) vs. Agile Model
- Agile vs. Waterfall Method Comparison
- **Capability Maturity Model Integration (CMMI) Levels:**

> Level 1: Initial
>
> Level 2: Managed
>
> Level 3: Defined
>
> Level 4: Quantitatively Managed
>
> Level 5: Optimizing

Programming Languages and Concepts

- **Types of Programming Languages:**

> Machine Languages
>
> Assembly Languages
>
> High-Level Languages
>
> Very High-Level Languages

- Object-Oriented Programming Features
- Polymorphism, Cohesion, and Coupling Concepts
- Data Structures and Distributed Systems

Database Architecture, Models, and Interfaces

Database Models: Relational, Hierarchical, Network, Object-Oriented, Object-Relational

Interface Languages: ODBC, JDBC, XML:DB API, OLE DB

Strategies: Data Warehousing and Data Mining

Database Security: Threats and Access Control Mechanisms

Software Threats and Countermeasures

- **Types of Software Threats:** Viruses, Worms, Trojan Horses, Botnets, Rootkits
- **Source Code Issues:** Buffer Overflows, Backdoors, Escalation of Privileges
- **Protection Mechanisms:** Antivirus, Antimalware, Security Policies
- **Software Security Effectiveness:** Certification and Accreditation Process

Information Security Buzz

Discover more at our InfoSec Knowledge Hub