

No. 116

CYBERSECURITY

Secure Coding Practices

Writing software that resists attack, in any language

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 116

Secure Coding Practices

Writing software that resists attack, in any language

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Secure Coding Practices
Writing software that resists attack, in any language

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, language and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why secure coding matters 5
2 Principles 6
3 Trust boundaries 8
4 Threat thinking 9
5 Secure by design 10
6 Common weakness lists 11
7 Security requirements and abuse cases 12

PART II · HANDLING DATA

8 Input validation 14
9 Output handling 15
10 Injection 16
11 Cross-site scripting 17
12 Files and paths 18
13 Deserialization 19
14 Server-side requests 20
15 Protecting data 21
16 Errors and logging 22
17 Limits and resource controls 23

PART III · IDENTITY AND SECRETS

18 Authentication 25
19 Storing passwords 26
20 Sessions 27
21 Authorization 28
22 Secrets 29
23 Cryptography 30

FREE SAMPLE · ojayo.com

24 Configuration and environments 31

PART IV · BUILDING AND SHIPPING

25 Dependencies 33
26 Memory safety 34
27 Concurrency and race conditions 35
28 Using framework security features 36
29 AI coding assistants 37
30 Code review 38
31 Tools 39
32 Security testing 40
33 Handling vulnerability reports 41
34 Team habits 42
35 A worked example 43
36 An improvement plan 44
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Most security vulnerabilities start as ordinary coding mistakes: a missing check, an unsafe query, a secret left in a file, an error handled the wrong way. **Secure coding** is the set of habits and techniques that prevent those mistakes, so software resists attack from the start rather than being patched afterwards.

This book explains secure coding practices for beginners in a language-neutral way, with short Python examples that were tested. The principles apply equally to JavaScript, Java, C#, Go and other languages. It is written for people who build software and want to do it safely.

What this book covers

- Core principles: distrust input, least privilege, fail closed, secure defaults.
- Input validation, output encoding and injection prevention.
- Authentication, sessions, authorization and password storage.
- Secrets, cryptography, errors, logging and file handling.
- Dependencies, memory safety, AI coding assistants, reviews and tools.

Who this book is for

- **Developers** in any language.
- **Students** learning to code.
- **Team leads** building secure development habits.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–7): why secure coding matters, principles, trust boundaries, threat thinking, secure by design, common weakness lists, and security requirements.
- **Part II — Handling data** (Chapters 8–17): input validation, output encoding, injection, cross-site scripting, files and paths, deserialization, server-side requests, data protection, errors and logging, and limits.
- **Part III — Identity and secrets** (Chapters 18–24): authentication, passwords, sessions, authorization, secrets, cryptography, and configuration.
- **Part IV — Building and shipping** (Chapters 25–36): dependencies, memory safety, concurrency, framework features, AI assistants, code review, tools, testing, vulnerability reports, team habits, a worked example, and a plan.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in real code.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on code

Code examples are short and were run to check they work. Use maintained libraries and your framework's security features in real projects.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why secure coding matters and the principles behind it.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why secure coding matters

Security starts with the code you write.

Code is the attack surface

Attackers exploit bugs in applications every day. Verizon's 2026 Data Breach Investigations Report found exploitation of vulnerabilities was the most common way into organizations.

Cheaper early



Figure 1.1 The later a flaw is found, the more it costs

Everyone's job

Security teams cannot review every line. Developers who write secure code by habit are the most effective defence.

KEY IDEA

A vulnerability prevented while coding never needs an incident response.

FREE SAMPLE · ojayo.com

CHAPTER 2

Principles

A few principles guide every decision.

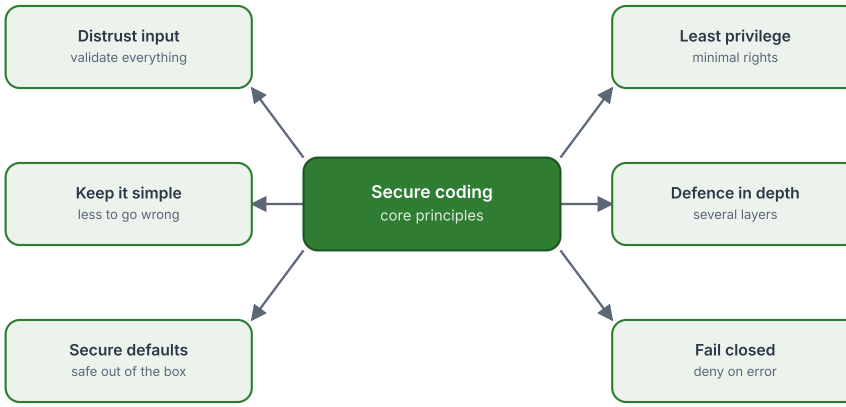


Figure 2.1 Principles of secure coding

Distrust input

Anything from outside your code, users, files, APIs, environment variables, other services, may be malicious.

Least privilege

Run with the minimum permissions: database accounts that can only read what they need, processes without admin rights.

Defence in depth

Use several layers, so one mistake does not lead to a breach.

FREE SAMPLE · ojayo.com

Fail closed

When something unexpected happens, deny rather than allow.

Secure defaults and simplicity

Make the safe option the default, and keep code simple enough to reason about.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices (you are reading this)
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Secure Coding Practices

Enjoyed it? The full book has 52 pages and 36 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.