

No. 55

ABAP CODE SECURITY

ABAP Custom Code Security

Finding injection, missing authority checks and backdoors with the Code Vulnerability Analyzer, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 55

ABAP Custom Code Security

Finding injection, missing authority checks and backdoors with the Code Vulnerability Analyzer, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

ABAP Custom Code Security
Finding injection, missing authority checks and backdoors with the Code Vulnerability Analyzer, explained for beginners

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. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP 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 custom code matters 5
2 Common weaknesses 7
3 Secure development principles 9

PART II · SECURE CODING

4 Authorization checks 11
5 CALL TRANSACTION 13
6 SQL injection 14
7 Code injection and backdoors 16
8 File access and directory traversal 17
9 Securing RFC function modules 18
10 Web and Fiori back ends 20

PART III · CODE VULNERABILITY ANALYZER

11 The Code Vulnerability Analyzer 22
12 ATC landscapes 24
13 Licensing and the cloud 26
14 Handling findings 28
15 Exemptions 30
16 Transport gates 32

PART IV · GOVERNANCE

17 Clean core and security 34
18 Developer access 36
19 Third-party and partner code 38
20 AI-generated code 39
21 Worked example: first CVA scan 40

Checklists 42

FREE SAMPLE · ojayo.com

Glossary 44
Further reading 45

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.

Almost every SAP customer has **custom ABAP code**: reports, function modules, interfaces, enhancements and Fiori back ends. This code runs with the full power of the SAP system. If a developer forgets an authorization check, builds SQL from user input or leaves a hard-coded password, attackers and curious users can bypass every role the security team designed.

This book explains, for beginners, **how to secure ABAP custom code**: the most common weaknesses, how to write correct authorization checks, how to avoid injection, how to secure RFC function modules, and how to use the **SAP Code Vulnerability Analyzer (CVA)** in the **ABAP Test Cockpit (ATC)**, on premise and in the cloud. It also covers governance: exemptions, transport gates, developer access and clean core.

Which versions this book covers

- **SAP S/4HANA** (on-premise and Private Edition) and **SAP ECC**, with classic ABAP.
- **ABAP Cloud** in the **SAP BTP ABAP environment** and **S/4HANA Cloud Public Edition**.
- **CVA** through local ATC, remote ATC and **ATC in the cloud**, which SAP describes as the recommended tool for static code quality assurance of private cloud and on-premise landscapes.

Who this book is for

- **ABAP developers** who want to write secure code.

FREE SAMPLE · ojayo.com

- **Development leads and architects**.
- **SAP security teams** who review custom code.
- **Auditors** assessing custom code risk.

How the book is organized

- **Part I — Foundations** (Chapters 1–3): why custom code matters, common weaknesses, and secure development principles.
- **Part II — Secure coding** (Chapters 4–10): authorization checks, CALL TRANSACTION, SQL injection, code injection, file access, RFC, and web and Fiori back ends.
- **Part III — Code Vulnerability Analyzer** (Chapters 11–16): CVA, ATC landscapes, licensing and the cloud, handling findings, exemptions, and transport gates.
- **Part IV — Governance** (Chapters 17–21): clean core, developer access, third-party code, AI-generated code, and a worked example.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN SAP

Product-specific details and names.

WATCH OUT

Common misunderstandings.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on code and screens

Code examples are **short original illustrations** for learning, not production code. Screens are **simplified illustrations**, not copies of SAP screens. Check syntax against your release.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why custom code is a security risk, list common weaknesses, and introduce secure development principles.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why custom code matters

Custom code runs with the system's power. Its security is the developer's responsibility.

Roles are not enough

SAP roles control which transactions and authorization objects a user has. But a custom program decides for itself **whether** to check authorizations. If it does not check, the user's roles are irrelevant once they can start it.

Where custom code lives

- **Reports** and transactions.
- **Function modules**, especially **remote-enabled** ones.
- **Enhancements** and user exits.
- **OData services** behind Fiori apps.
- **Interfaces** and batch jobs.

How it goes wrong

- Developers focus on **function**, not abuse.
- Code is **copied** from old programs with old weaknesses.
- Tests check that authorized users **can** do things, not that unauthorized users **cannot**.
- Code reviews skip **security**.

FREE SAMPLE · ojayo.com

KEY IDEA

Every custom program is a small security system of its own. If it skips a check, no role can fix it.

FREE SAMPLE · ojayo.com

CHAPTER 2

Common weaknesses

A handful of weaknesses cause most ABAP security problems.

Weakness	Example impact
Missing authority check	anyone can run a sensitive report
SQL injection	read or change any table
Code injection	attacker-defined ABAP runs
Directory traversal	read server files
Hard-coded credentials	backdoor user or password
Unsafe RFC	remote access without checks

Figure 2.1 Common ABAP security weaknesses and their impact.

The main categories

SAP's community overview of CVA groups its checks, inspired by the OWASP Top 10, into categories such as:

- **Missing or incorrect authorization checks**, including in RFC function modules and before CALL TRANSACTION.
- **SQL injection** in dynamic Open SQL, native SQL and ADBC.
- **Code injection** through dynamic code generation.
- **Directory traversal** in file access.
- **Hard-coded** user names, passwords, system IDs and clients, which can act as **backdoors**.
- **Web weaknesses** in BSPs, such as missing XSRF protection and unvalidated redirects.

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 (you are reading t…
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
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

ABAP Custom Code Security

Enjoyed it? The full book has 51 pages and 21 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.