

No. 69

SAP PENETRATION TESTING

SAP Penetration Testing

Planning, scoping and acting on security tests of SAP systems, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 69

SAP Penetration Testing

Planning, scoping and acting on security tests of SAP systems, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

SAP Penetration Testing

Planning, scoping and acting on security tests of SAP systems, 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 test SAP 5
2 Kinds of security testing 6
3 What makes SAP different 8
4 Legal and ethical basics 9

PART II · PLANNING

5 Goals and scope 11
6 Testing perspectives 13
7 Rules of engagement 15
8 Test or production 17
9 Testing SAP cloud and RISE 18
10 Choosing a provider 20
11 Preparing your team 22

PART III · WHAT GETS TESTED

12 The SAP attack surface 24
13 Gateway, message server and SAProuter 26
14 Web, Fiori and OData 28
15 Authentication and users 29
16 Authorizations 30
17 Custom code 31
18 Patch level and known vulnerabilities 32

PART IV · AFTER THE TEST

19 Reading the report 35
20 Judging severity 37
21 Remediation 39
22 Retesting 41

FREE SAMPLE · ojayo.com

23 Did we detect it? 42
24 Continuous testing 43
25 Worked example: Bayview Logistics 44
Checklists 46
Glossary 47
Further reading 48

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.

Configuration checks and audits tell you whether SAP settings match a policy. A **penetration test** answers a harder question: could someone actually break in, and how far could they get? For SAP, that question matters because the system holds money, personal data and production plans.

SAP penetration testing is a specialist field. Security firms point out that SAP uses its own protocols, such as RFC, DIAG and the message server protocol, which generic web and network tests do not cover well. And in SAP's cloud offerings, customers cannot test freely: SAP requires a formal approval process.

This book is written for the **people who plan, buy, support and act on** SAP penetration tests: security managers, SAP security and Basis teams, and auditors. It explains goals, scope, rules of engagement, cloud approvals, choosing a provider, what areas are tested, how to read results, and how to fix and retest. It describes testing areas at a level suitable for defenders; it is not an attack manual.

Which versions this book covers

- **SAP S/4HANA** and **SAP NetWeaver ABAP and Java**, on-premise and in RISE with SAP.
- **SAP cloud services** that follow SAP's customer penetration test request process (SAP KBA 3080379).
- Vulnerability examples from public reporting through 2026.

FREE SAMPLE · ojayo.com

Who this book is for

- **CISOs and security managers** who commission tests.
- **SAP security and Basis teams** who support testers and fix findings.
- **Auditors and risk teams** who rely on test results.
- **Junior testers** who want to understand SAP-specific scope.

How the book is organized

- **Part I — Foundations** (Chapters 1–4): why test, kinds of testing, what makes SAP different, and legal and ethical basics.
- **Part II — Planning** (Chapters 5–11): goals and scope, perspectives, rules of engagement, environments, SAP cloud approvals, choosing a provider and preparing your team.
- **Part III — What gets tested** (Chapters 12–18): attack surface, network services, web and Fiori, authentication, authorizations, custom code and patch level.
- **Part IV — After the test** (Chapters 19–25): reports, severity, remediation, retesting, detection, continuous testing 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.

FREE SAMPLE · ojayo.com

KEY IDEA

The one thing to remember from a section.

A note on screens and examples

Screens are **simplified illustrations**, not copies of real tools or reports. Company names, systems and findings in the examples are invented.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why SAP needs penetration testing, the different kinds of security testing, what makes SAP different and the legal and ethical basics.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why test SAP

Testing shows what an attacker could really do.

Reasons to test

- **Real-world proof**: checks show settings; tests show impact.
- **Attackers target SAP**: public reporting in 2025 and 2026 described active exploitation of SAP NetWeaver vulnerabilities.
- **Regulation**: frameworks such as DORA expect resilience testing, including threat-led penetration testing for significant financial entities.
- **Audit and customers**: many audits and customer questionnaires ask for regular penetration tests.
- **Change**: new Fiori apps, interfaces and cloud services add new exposure.

What testing does not do

- It does not prove a system is **secure**; it shows what was found in a limited time.
- It does not replace **patching**, **hardening** or **monitoring**.
- It does not fix anything by itself; remediation is the real work.

KEY IDEA

A penetration test is valuable only if its findings are fixed and the fixes are verified.

FREE SAMPLE · ojayo.com

CHAPTER 2

Kinds of security testing

Several kinds of testing answer different questions.

Assessment type	What it answers
Configuration review	are settings as they should be?
Vulnerability scan	which known weaknesses exist?
Penetration test	can weaknesses be exploited, and how far?
Authorization review	can users do more than intended?
Red team	can a goal be reached undetected?

Figure 2.1 Different kinds of SAP security testing and the questions they answer.

Configuration review

Compares settings to a baseline, often with tools. Fast and repeatable.

Vulnerability scanning

Finds known weaknesses, such as missing Security Notes. Broad but shallow.

Penetration testing

A tester tries to **exploit** weaknesses in a controlled way to show real impact, such as reaching sensitive data or administrator access.

FREE SAMPLE · ojayo.com

Authorization testing

Checks whether users can perform actions their roles should not allow. Security firms describe chaining authorizations that each look harmless into a real exploit path.

Red teaming

A goal-driven exercise, often over weeks, that also tests whether the SOC **detects** the activity.

> **TIP**
> Combine methods: continuous configuration checks and scanning, plus periodic penetration tests for depth.

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 (you are reading this)
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
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

SAP Penetration Testing

Enjoyed it? The full book has 53 pages and 25 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.