PROMPT ENGINEERING & SECURITY

BUILDING INJECTION-RESISTANT AI SYSTEMS

SECURE BY DESIGN | ROBUST PROMPTS | DETECT & PREVENT | MEASURE & IMPROVE

STEVE T.

Prompt Engineering & Security

Building Injection-Resistant AI Systems

Steve T.

This book is available at
https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems

This version was published on 2026-06-19

Contents

Prompt Engineering & Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Building Injection-Resistant AI Systems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

About This Book

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Table of Contents

Introduction: The New Attack Surface

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Attack Surface Has Changed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Why This Book Exists

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Who This Book Is For

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Central Thesis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

How This Book Is Organized

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

A Note on Scope and Limitations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Stakes Are Real

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 1. How LLMs Read Instructions: A Primer on Model Mechanics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Tokenization Layer: Where Text Becomes Numbers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Attention: How LLMs Contextualize Every Token

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Three Sources of Input in a Typical LLM Application

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Why This Is Not a "Bug": It's a Feature of the Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Historical Context: How We Got Here

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Competing Perspectives: Is the Risk Overstated?

The "Blast Radius" Argument: Capability Determines Risk

The Human-in-the-Loop Argument

The "Models Are Getting Better" Argument

The "It's Just Input Validation" Argument

Key Takeaway for Security Engineers

Chapter 2. The Principles of Prompt Engineering: Clarity, Reliability, and Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Core Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Security Dimension: Designing Secure Prompts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Design Patterns for Effective Prompts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Case Study: A Healthcare Chatbot That Hallucinated Because of Ambiguous Instructions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Trade-offs and Competing Perspectives

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Quantitative Data: What Actually Works?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Trade-offs and Competing Perspectives

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

A Deeper Dive. The Role-Playing Prompt: Security Implications

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Feedback Loop Risk: Why Multi-Hop Systems Are Inherently More Vulnerable

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Practical Walkthrough: Building a Secure RAG Prompt Template

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 3. Anatomy of Prompt Injection: Direct Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Direct Injection Mechanics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Real-World Examples: Documented Incidents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Prompt Leaking as Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Why Legacy Defenses Fail

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Fundamental Tension

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Remoteli.io Incident: A Deep Dive

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Bing/Sydney Leak: A Case Study in Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Prompt Leaking as Reconnaissance (Continued)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Why Legacy Defenses Fail (Expanded)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Fundamental Tension (Expanded)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 4. The Indirect Injection Threat: RAG, Web Content, and Data Poisoning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The RAG Trust Paradox

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Case Study: Slack AI (August 2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Case Study: ChatGPT Memory / SpAIware (September 2024)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

PoisonedRAG: Five Documents, 90% Success Rate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Vector Database Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Three-Layer Defense Architecture for RAG

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Slack AI Attack: A Full Technical Walkthrough

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Competing Perspectives: Is RAG Really That Vulnerable?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Three-Layer Defense Architecture for RAG (Expanded with Implementation)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 5. Jailbreaks: Social Engineering for Machines

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

What Jailbreaking Is (and Isn't)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Taxonomy of Jailbreak Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Characteristics of Jailbreak Prompts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Automated Jailbreak Discovery

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Consequences: Character.AI and Beyond

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The GOAT Framework: How Automated Red Teaming Works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

TAP: Tree of Attacks with Pruning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Defense Against Jailbreaks: A Practical Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Character.AI Case: A Cautionary Tale

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 6. AI Agents and Tool Use: When Prompts Become Shells

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

From Chatbots to Agents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Semantic Kernel RCE Vulnerabilities (May 2026)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Documented Incidents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Expanding Blast Radius

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Framework-Agnostic Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

CVE-2026-26030: A Step-by-Step Code Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Expanding Blast Radius: A Framework for Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

A Deeper Look: The Semantic Kernel RCE Vulnerabilities (CVE-2026-26030 and CVE-2026-25592)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Framework-Agnostic Vulnerabilities: The Deeper Truth

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 7. Defense-in-Depth Architecture: Layered Protections

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Three-Layer Model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Guardrails: The Runtime Enforcement Layer

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Trade-Off: Security vs. Usability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Trade-Off: Security vs. Usability (Expanded with Calibration Examples)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Competing Perspectives: Is Defense-in-Depth Overkill?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 8: Instruction Hierarchy and Isolation Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Core Principle: Instruction Hierarchy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Six Design Patterns for Injection-Resistant Agents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Architectural Isolation Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Case Study: Applying Patterns to a Customer Service Chatbot

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Pattern Selection: A Decision Framework

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Case Study: Applying Patterns to a Healthcare Data Analysis Platform

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Competing Perspectives: Are Design Patterns Enough?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 9. Enterprise Security Stacks: FIDES, LlamaFirewall, and Beyond

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Microsoft FIDES: Deterministic Defense Through Information Flow Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Meta LlamaFirewall: Open-Source Guardrail System

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Comparing Enterprise Options

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

OWASP Top 10 for LLM Applications 2025

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Choosing the Right Stack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

FIDES Implementation: A Practical Walkthrough

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

LlamaFirewall Deployment Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

LlamaFirewall's Agent Alignment Check: A Deeper Dive

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The TaskTracker Alternative: Detection Through Internal Activations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Comparing Enterprise Options (Expanded)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Competing Perspectives. Deterministic vs. Probabilistic: The Real Trade-Off

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 10. Red-Teaming AI Systems: Practical Security Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Why Red-Teaming Is Different

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Setting Up Automated Red Teams with Promptfoo

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

PyRIT and Garak: Alternative Frameworks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Building a Red-Team Playbook

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The LLMail-Inject Challenge: Lessons from 370,000+ Test Prompts

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

CI/CD Integration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

PyRIT: Multi-Turn Attack Walkthrough

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Garak: Comprehensive Vulnerability Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Garak: Comprehensive Vulnerability Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

CI/CD Integration: Making Red-Teaming Continuous

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The LLMail-Inject Challenge: Lessons from 370,000+ Test Prompts (Expanded)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Practical Red-Team Exercise: A Complete Walkthrough

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 11. Production Deployment: Monitoring, Incident Response, and Compliance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Runtime Monitoring and Anomaly Detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Data Governance in AI Systems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Incident Response Playbooks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Compliance Frameworks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Runtime Monitoring: A Practical Implementation Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Incident Response Playbook (Expanded Template)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Compliance Walkthrough: NIST AI RMF

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Compliance Walkthrough: EU AI Act

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Real-World Cost of Prompt Injection Incidents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Key Takeaway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Chapter 12. The Future of AI Security: Emerging Threats and Defenses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Multimodal Injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Supply Chain Attacks in AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Adaptive Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Deterministic vs. Probabilistic Defenses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Role of Regulation and Standardization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Adaptive Arms Race: Attack and Defense Evolution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Multimodal Injection: The Next Frontier

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Supply Chain Attack Surface: Beyond Code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Adaptive Arms Race: Attack and Defense Evolution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Regulatory Landscape: A Practical Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Supply Chain Security: Beyond Code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

The Regulatory Landscape: A Practical Guide

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Final Synthesis: Building a Security-First Culture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

Conclusion: Trust as a Design Principle

Glossary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.

References / Endnotes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/promptengineeringsecuritybuildinginjection-resistantaisystems.