! DEVELOPER SECURITY

AI Security for Developers

Protecting Code in the Age of Agents

Prompt injection · Data leakage · OWASP LLM

Attack patterns, defenses, and compliance

prompt injection | data leakage | OWASP | MCP security | sandboxing | compliance

Caio Incau

v1.0 // 2026

AI Security for Developers

Protecting Code in the Age of Agents

CAIO INCAU

This book is available at https://leanpub.com/ai-security-for-developers

This version was published on 2026-05-25

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Contents

Getting Started

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Unsure How to Get Started? Try our Book Workshop!

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

How to Write on Leanpub

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Previewing and publishing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Basic formatting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Markdown and Markua

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Generate a preview version of your book

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Either read a tutorial, or just go for it!

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Read the tutorial...

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

...or just go for it!

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Thanks for being a Leanpub author!

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Writing in Markua

Writing in Markua is easy! You can learn most of what you need to know with just a few examples.

To make *italic text* you surround it with single asterisks. To make **bold text** you surround it with double asterisks.

Section One

You can start new sections by starting a line with two # signs and a space, and then typing your section title.

Sub-Section One

You can start new sub-sections by starting a line with three # signs and a space, and then typing your sub-section title.

Including a Chapter in the Sample Book

At the top of this file, you will also see a line at the top:

```
1  {sample: true}
```

Leanpub has the ability to make a sample book, which interested readers can download or read online. If you add this line above a chapter heading, then when you publish your book, this chapter will be included in a separate sample book for these interested readers.

Links

You can add web links easily.

Here's a link to the Leanpub homepage.

Images

You can add an image to your book in a similar way.

First, add the image to the “Resources” folder for your book. You will find the “Resources” folder under the “Manuscript” menu to the left.

If you look in your book’s “Resources” folder right now, you will see that there is an example image there with the file name “palm-trees.jpg”. Here’s how you can add this image to your book:

If you want to add a figure title, you put it in quotes:

Figure 1. Palm Trees

If you want to add descriptive alt text, which is good for accessibility, you put it between the square brackets:

Figure 2. Palm Trees

You can also set the alt text and/or the figure title in an attribute list:

Figure 3. Palm Trees

Finally, if no title is provided, and the `alt-title` document setting is the default of `all`, the alt text will be used as the figure title instead of as alt text.

Figure 4. Palm Trees

You can set the important document settings at Settings > Generation Settings.

Lists

Numbered Lists

You make a numbered list like this:

1. kale
2. carrot
3. ginger

Bulleted Lists

You make a bulleted list like this:

- kale

- carrot
- ginger

Definition Lists

You can even have definition lists!

term 1
: definition 1a

: definition 1b

term 2
: definition 2

Page Breaks

We don't recommend that you manually break pages, since that is brittle and can lead to unexpected formatting if you edit text earlier in your chapter and forget about the manual page breaks. But if you really want to add a page break, you use the `{pagebreak}` directive on a line by itself, with blank lines above it and below it.

Code Samples

You can add code samples really easily. Code can be in separate files (a "local" resource) or in the manuscript itself (an "inline" resource).

Local Code Samples

Here's a local code resource:

Figure 5. Hello World in Ruby

```ruby
require 'time'

# This is just some pointless code so you can see the syntax highlighting...
def display_info
  pi = Math::PI.round(10)
  time_last_year = (Time.now - 365 * 24 * 60 * 60).getlocal("-08:00")
  formatted_time = time_last_year.strftime("%Y-%m-%d %H:%M:%S")
  puts "Pi to 10 decimal places: #{pi}"
  puts "The time 1 year ago in Pacific Time: #{formatted_time}"
end
```

Inline Code Samples

Inline code samples can either be spans or figures.

A span looks like `puts "hello world"` this.

A figure looks like this:

```ruby
require 'time'

# This is just some pointless code so you can see the syntax highlighting...
def display_info
  pi = Math::PI.round(10)
  time_last_year = (Time.now - 365 * 24 * 60 * 60).getlocal("-08:00")
  formatted_time = time_last_year.strftime("%Y-%m-%d %H:%M:%S")
  puts "Pi to 10 decimal places: #{pi}"
  puts "The time 1 year ago in Pacific Time: #{formatted_time}"
end
```

You can also add a figure title using the title attribute:

Figure 6. Hello World in Ruby

```ruby
require 'time'

# This is just some pointless code so you can see the syntax highlighting...
def display_info
  pi = Math::PI.round(10)
  time_last_year = (Time.now - 365 * 24 * 60 * 60).getlocal("-08:00")
  formatted_time = time_last_year.strftime("%Y-%m-%d %H:%M:%S")
  puts "Pi to 10 decimal places: #{pi}"
  puts "The time 1 year ago in Pacific Time: #{formatted_time}"
end
```

Tables

You can insert tables easily inline, using the GitHub Flavored Markdown (GFM) table syntax:

Header 1	Header 2
Content 1	Content 2
Content 3	Content 4 Can be Different Length

Tables work best for numeric tabular data involving a small number of columns containing small numbers:

Central Bank	Rate
JPY	-0.10%
EUR	0.00%
USD	0.00%
CAD	0.25%

Definition lists are preferred to tables for most use cases, since reading a large table with many columns is terrible on phones and since typing text in a table quickly gets annoying.

Math

You can easily insert math equations inline using either spans or figures.

Here's one of the kinematic equations $d = v_i t + \frac{1}{2}at^2$ inserted as a span inside a sentence.

Here's some math inserted as a figure.

$$\left|\sum_{i=1}^{n} a_i b_i\right| \le \left(\sum_{i=1}^{n} a_i^2\right)^{1/2} \left(\sum_{i=1}^{n} b_i^2\right)^{1/2}$$

Figure 7. Something Involving Sums

Headings

Markua supports both of Markdown's heading styles.

The preferred style, called atx headers, has the following meaning in Markua:

```
{class: part}
# Part

This is a paragraph.

# Chapter

This is a paragraph.

## Section

This is a paragraph.

### Sub-section

This is a paragraph.

#### Sub-sub-section

This is a paragraph.

##### Sub-sub-sub-section

```

```
This is a paragraph.

###### Sub-sub-sub-sub-section

This is a paragraph.
```

Note the use of three backticks in the above example, to treat the Markua like inline code (instead of actually like headers).

The other style of headers, called Setext headers, has the following headings:

```
{class: part}
Part
====

This is a paragraph.

Chapter
=======

This is a paragraph.

Section
-------

This is a paragraph.
```

Setext headers look nice, but only if you're only using chapters and sections. If you want to add sub-sections (or lower), you'll be using atx headers for at least some of your headers. My advice is to just use atx headers all the time. (The `{class: part}` attribute list on a chapter header to make a part header does actually work with Setext headers, but it's really ugly.)

Note that while it is confusing and ugly to mix and match using atx and Setext headers for chapters and sections in the same document, you can do it. However, please don't.

Block quotes, Asides and Blurbs

> Block quotes are really easy too.
>
> —Peter Armstrong, *Markua Spec*

A> Asides are useful for longer text.
A>
A> But typing them like this isn't fun.

A> Asides can be written this way, since adding a bunch of A> stuff at the beginning of each line can get annoying with longer asides.

B> Blurbs are useful

B> Blurbs are useful

There are many types of blurbs, which will be familiar to you if you've ever read a computer programming book.

This is a discussion.

You can also specify them this way:

This is a discussion

This is an error.

This is information.

This is a question. (Not a question in a Markua course; those are done differently!)

This is a tip.

This is a warning.

This is an exercise. (Not an exercise in a Markua course; those are done differently!)

Good luck, have fun!

If you've read this far, you're definitely the right type of person to be here!

Our last piece of advice is simple: once you have a couple chapters completed, publish your book in-progress!

This approach is called Lean Publishing. It's why Leanpub is called Leanpub.

If you want to learn more about Lean Publishing, read this or watch this.

* * *

author: Caio Incau date: "2026-05-25T13:41:16Z" identifier: "urn:uuid:9224380c-44fa-4fba-a29b-526741c89a23" language: en title: AI Security for Developers

[]{#title_page.xhtml}

[]{#ch001.xhtml}

Preface

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

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/ai-security-for-developers.

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/ai-security-for-developers.

What you need

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 1 —- The New Attack Surface

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The pre-AI security model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

What AI changes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The new threat categories

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Why traditional AppSec is not enough

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

A defense-in-depth model for AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 2 —- How AI-Generated Code Introduces Vulnerabilities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Why AI writes insecure code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The vulnerability taxonomy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

SQL injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Cross-site scripting (XSS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Hardcoded credentials and secrets

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Insecure cryptographic practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Path traversal

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Measuring your exposure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The trust calibration problem

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 3 —- Prompt Injection: The SQL Injection of AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

How prompt injection works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The attack taxonomy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Direct prompt injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Indirect prompt injection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Why there is no parameterized query equivalent

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Building layered defenses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Layer 1: Input filtering

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Layer 2: Prompt hardening

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Layer 3: Output validation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Layer 4: Structural separation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 4 —- Data Leakage and Model Extraction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Training data memorization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

How memorization works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

What gets memorized

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Context window exposure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

System prompt extraction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Conversation history leakage

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Model extraction attacks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The economics of model theft

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

How extraction works

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Defending against model extraction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Practical data loss prevention for AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 5 —- Securing AI-Generated Code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Static analysis for AI-generated code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Bandit: Python security linter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Semgrep: pattern-based analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Building the CI/CD security gate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

GitHub Actions integration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Automated fix suggestions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 6 —- Secure Coding with AI Assistants

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Security-aware prompting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The security prompt template

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The security review checklist for AI code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Configuring AI assistants for security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Project-level security instructions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Pre-commit hooks for AI code

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The review workflow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 7 —- Input Validation for AI Systems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Input validation architecture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Pre-model input filters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Length and format validation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Injection pattern detection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Content policy enforcement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Runtime guardrails

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Output sanitization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Putting it all together

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 8 —- Authentication and Authorization with AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The agent authentication problem

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

OAuth 2.0 for AI agents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

API key management for AI services

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The principle of least privilege for AI agents

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Middleware for AI endpoint protection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 9 —- Securing MCP Servers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The MCP security model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Server hardening

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Restricting tool exposure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Parameter sanitization for dangerous tools

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Transport security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Production deployment patterns

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The gateway pattern

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 10 —- Securing AI Agents in Production

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The agent threat model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Sandboxing agent execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Network isolation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Resource limits and quotas

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Comprehensive audit trails

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Putting it all together: the secure agent runtime

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 11 —- Supply Chain Security for AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Model provenance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Dependency risk management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Third-party model evaluation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

AI Software Bill of Materials (AI-SBOM)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 12 —- Monitoring and Incident Response

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

What to monitor

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Building the monitoring pipeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Detection rules

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Incident response playbooks

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Forensic analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 13 —- Compliance and Regulatory Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

OWASP Top 10 for LLM Applications

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

EU AI Act security requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

SOC 2 implications for AI

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Automated compliance evidence collection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next chapter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Chapter 14 —- Building a Security-First AI Practice

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The DevSecAI workflow

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Threat modeling for AI systems

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Security training program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

The security champion model

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Security metrics and reporting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Common mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Exercises

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.

Next steps

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/ai-security-for-developers.