Secure Coding Training That Changes How Developers Actually Build Software

Practical, engaging, real-world application security training for modern development teams.

Tanya Janca
Founder, She Hacks Purple Consulting

Why Teams Choose She Hacks Purple?

Most secure coding training teaches rules, vulnerabilities, or tools in isolation.

Developers leave knowing what is wrong, but not how to consistently build software more securely in real production environments.

She Hacks Purple training is different.

We focus on:

- How developers actually work
- The technologies teams are actually using
- Practical patterns that fit real constraints

Training emphasizes secure defaults, realistic code review, and decision-making skills developers can apply immediately.

The goal is not **fear, compliance, or checklists.**

The goal is **better software.**

Meet Tanya Janca

Tanya Janca, also known as **SheHacksPurple**, is an internationally recognized authority on **secure software development** and **application security.**

She is the **best-selling author** of *Alice and Bob Learn Secure Coding*, *Alice and Bob Learn Application Security,* and *Cards Against AppSec*. Over her 28-year career in IT and security, Tanya has **trained** thousands of developers and security professionals **worldwide.**

Her background includes **securing national-scale systems**, **leading application security programs**, and **advising organizations** across finance, healthcare, government, and technology.

Tanya's training blends deep **technical expertise** with engaging delivery, practical examples, and an emphasis on **long-term behaviour change** rather than **short-term awareness.**

- She Hacks -
PURPLE

Training Designed for Real Teams

She Hacks Purple training is:

- Deeply technical, without being overwhelming
- Grounded in real code and real systems
- Adaptable to your stack, maturity, and goals

Sessions combine clear explanations of security concepts, extensive “Bad, Better, Best” code review, group discussion, and practical examples. Optional hands-on exercises and tooling demos are available.

Learning is reinforced using proven techniques such as spaced repetition, recall exercises, micro breaks, and opportunities to immediately apply new ideas.

The result is training that *sticks*.

HOW CUSTOM TRAINING WORKS

Design your own training. All training is modular and built collaboratively with your team.

Programs are assembled from three layers:

1. Core Foundations

- Choose one primary foundation based on your audience and goals

2. Focused Modules

- Add short modules to target specific risks, technologies, or skills.

3. Optional Deep Dives

- Go deeper into specific languages, frameworks, or platforms

This approach keeps training relevant, efficient, and aligned with how your organization builds software right now.

Core Training Options (Choose One)

Secure Coding Foundations

- 1 day
- For software developers writing production code.
- Focuses on building safer code by default and understanding common failure patterns.

Application Security Foundations

- 1 to 2 days
- For security teams, technical leaders, and security champions.
- Covers how application security programs work and how to scale them effectively.

API Security Foundations

- Half day or full day
- For teams designing, building, or maintaining APIs.
- Based on the OWASP API Security Top Ten with practical hardening guidance.

FOCUSED MODULES (MIX AND MATCH)

Add Focused Modules (30 to 90 minutes each)

Secure Development Practices

- Input validation and output encoding
- Authentication and authorization
- Password and credential management
- Secure error handling, logging, and monitoring
- Reviewing AI code for security
- Secure defaults and safe configurations

Architecture and Design

- Securing the software supply chain and build process
- Threat modelling with a live example
- Secure design concepts
- Trust boundaries and data flows
- Least privilege and fail-closed design

Platform and Environment

- Cloud and SaaS security best practices
- Containers and Kubernetes fundamentals
- Secrets management
- Incident response for developers
- Secure SDLC fundamentals

LANGUAGE AND FRAMEWORK DEEP DIVES

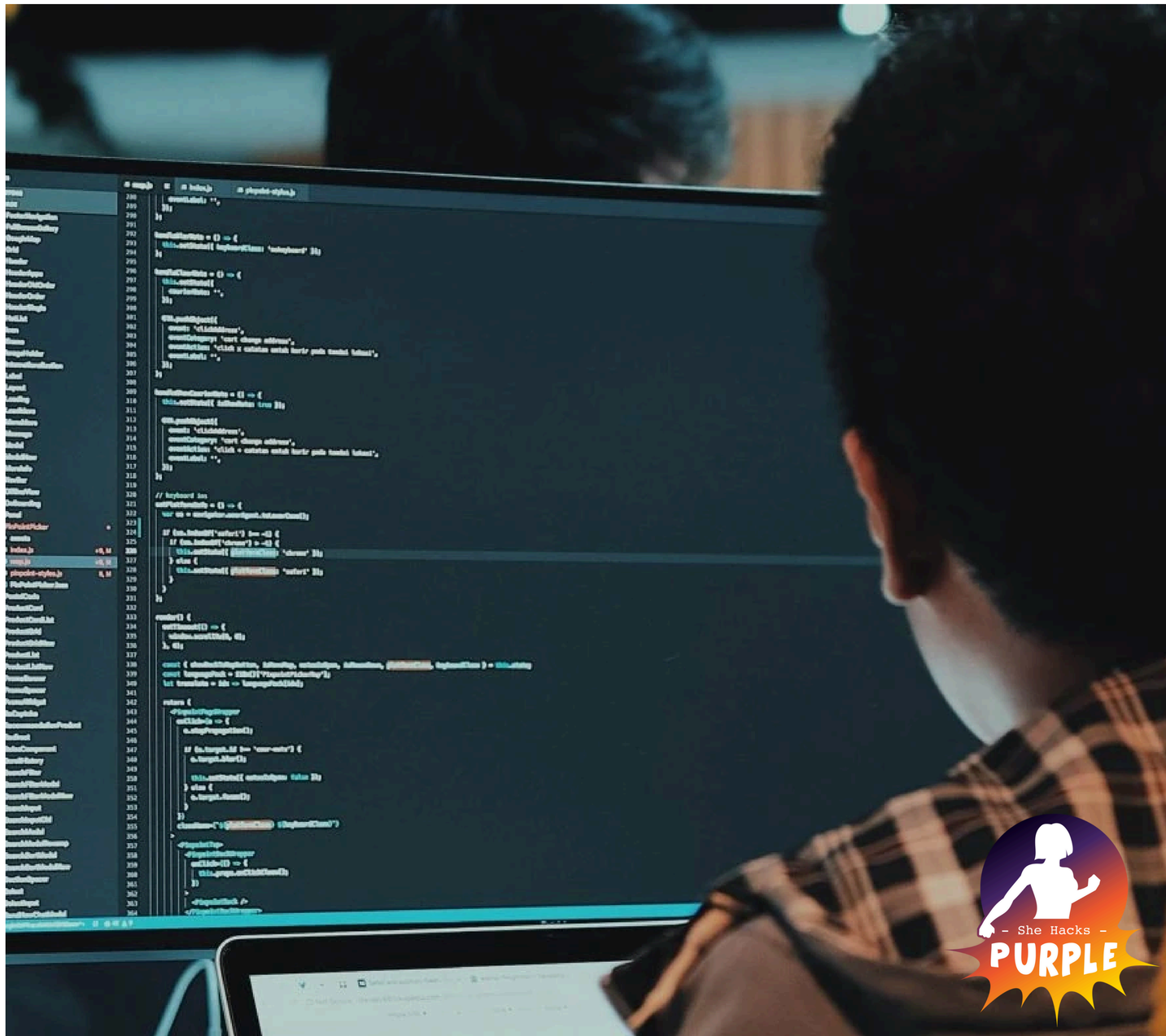
Deep dives focus on real vulnerabilities, real fixes, and practical code review in your environment.

Languages

- JavaScript and TypeScript
- Python
- Java
- C# and .NET
- C and C++

Frameworks and Technologies

- React, Vue, Angular
- Express, Spring, Flask
- APIs
- Embedded and IoT systems
- Serverless architectures



WHAT CLIENTS SAY

What Teams Experience After Training

“Tanya's training went well beyond filling secure coding knowledge gaps on our team. Her responsive and engaging approach built on our developers' natural curiosity and passion for building great software and inspired them to learn more. Now they're sharing their knowledge, asking great questions, proactively finding problems and solutions, and collaborating more effectively with our cybersecurity team. The momentum we've gained in advancing our app sec program is going to pay forward for a long time.”

-Melissa

“Tanya Janca’s Application Security and Secure Coding courses do a great job of breaking down complex security concepts into practical, easy-to-follow lessons. The ‘Bad, Better, Best’ technique was especially helpful. The sessions are engaging, and Tanya brings real-world context that keeps the material relevant.”

-Pascale Morin

- She Hacks -

PURPLE

LET’S DESIGN THE RIGHT TRAINING FOR YOUR TEAM

Training is available in half-day, full-day, and multi-day formats. Content is customized in advance to reflect your technologies, team roles, and goals.

To start the conversation, contact:
Training@SheHacksPurple.ca