AI Vibe Coding & Security: ChatGPT, Cursor & TDD

Vibe coding with ChatGPT and Cursor can empower everyday users to build helpful applications, but only if it’s done safely. This course equips product owners, analysts, and developers with practical strategies to use vibe coding tools effectively while protecting data and reducing risk. You’ll learn how to write prompts that avoid exposing PII, apply context-aware prompt engineering, spot and defend against prompt injection, and validate AI-generated outputs. Finally, you’ll see how to hand off reproducible code steps that engineers can trust, turning quick ideas into secure, usable solutions.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Explore the AI Behind Vibe Coding Tools

What is AI?

Understanding Karpathy’s Software Evolution Framework

Software 1.0

Software 2.0

Software 3.0

Challenge

Explore Essential Prompt Engineering Techniques

Introduction

Context, Role, and Expectation (CRE)

Dev Team CRE Example

Zero Shot

One Shot

Few Shot

ASK-2 & Safety

 Challenge

Explore HTML, CSS & JS Foundations with CodePen

Introduction

Understanding HTML Structure

CSS Fundamentals Overview

JavaScript Basics

Challenge

Move From VS Code to Agentic Coding with Cursor

Introduction

Setting Up Visual Studio Code

Linking CSS and JavaScript in VS Code

WEEK 2

Vibe Coding a Click Counter Game with AI

Exploring Cursor AI for Vibe Coding

Vibe Coding a Rock Paper Scissors Game with Cursor AI

Challenge

Apply Test Driven Development with Agentic Coding

Introduction

TDD with Assertions and the Plan-Act-Check (PAC) Method

JavaScript Assertions and Equality

Simplifying Assertions with Functions

Tokenizing PII in AI Workflows

Context Windows & Prompt Injections

Challenge

Deploy an HTML, CSS, & JS Website to GitHub Pages

Introduction

Create and Clone our GitHub Website Repo

Creating the Boilerplate

Deploy Website To GitHub Pages

Challenge

Last updated 10.10.2025