Secure Code Training For Developers

Hands On Training

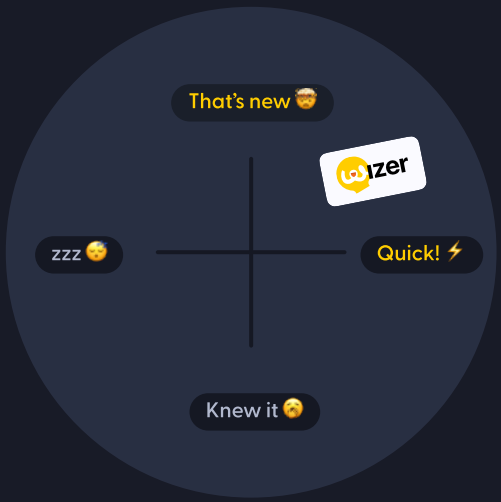
Rating 4.7

Time Wasted 0

Comply With Regulations

Small Bites

Why Wizer



The 4 Things We Don't Do

And why developers love us more for it 🤓

We Don't Teach You Things You Already Know

We teach you to think like a hacker

You will learn how to identify vulnerabilities, witness hacker maneuvers, and know how to mediate those threats

We Don't Waste Your Time

Just short, to-the-point videos

We deep dive on one subject each month, covering new vulnerabilities often exploited by hackers

We Don't Dwell On Theory

Only real-life examples!

We train you on a variety of topics beyond pure compliance and keep you consistently updated on the latest threats

We Don't Just Believe In Your Skills

We let Hands-On CTF Challenges prove them

Our Capture The Flag Challenges leverage live source code segments to sharpen your skills and encourage out-of-the-box thinking

What Does Secure Code Training Include?

Need Compliance?

Meet compliance requirements for PCI DSS, Third Party Vendor Assessments, and more. Plus, follow OWASP Top 10 with short, engaging content developers actually enjoy.

Full Video Library Access

Get full access to all 100+ bite-sized video training sessions - it's fast, simple, effective and fun!

Quizzes And Certificates

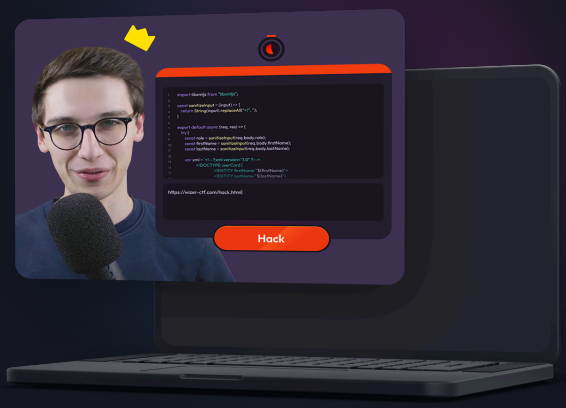
Check your team's knowledge with our interactive quizzes, spread throughout the training after each section. Once developers complete their training, they get a shiny certificate!

Assessing Your Dev Team's Secure Coding Skills

Gain actionable insights into your team's ability to identify vulnerabilities. Our detailed reports will reveal both easy-to-spot weaknesses and more challenging threats for your team.

Gamified, Hands-On Learning

Developers will face off in our exciting CTF challenges by identifying and exploiting vulnerabilities in short snippets of code, based on real-life scenarios.



Topics We Cover

- XSS (Cross-Site Scripting)
- IDOR (Insecure Direct Object Reference)
- SQL Injection
- SSRF (Server-Side Request Forgery)
- SSTI (Server-Side Template Injection)
- Insecure Deserialization
- Prototype Pollution
- Cryptographic Failure
- CSRF (Cross-Site Request Forgery)
- Authentication Forms
- OS Command Injection & Code Injection
- CSP
- Race Conditions
- Security Logging Failures
- Security Misconfiguration (Level 1)
- Vulnerable and Outdated Components
- JWT Tokens Risks
- File Upload Vulnerability
- And More...

Available Languages

Javascript ▶ Python ▶ JAVA ▶ Rust

.NET C# ▶ C/C++ ▶ Agnostic

wizer-training.com

Stay Wizer