Checkmarx

The world runs on code. We secure it.

Codebashing

AppSec Awareness and Secure Code Training

Give Developers What They Need

As DevOps becomes even more dominant, organizations are bringing development and security teams closer together to support more secure software releases and faster time to market. The benefits of moving security into the realm of the developer are clear: it saves time, money, and company resources.

However, only 60% of software developers say they're "very confident" in the security of their code.[1] This gap exists because most developers are underserved when it comes to security strategy. Although organizations now provide secure code training for their developers an average of six times per month—significantly more often than they did a few years ago—our research indicates that it leaves something to be desired: Not even a quarter of developers describe their training as "very effective." While most AppSec training may "check the box," it appears it really doesn't cultivate a sustained culture of security awareness. That's why we offer Checkmarx Codebashing™.

Unique Benefits

- **An approach honed over 15+ years:** Checkmarx Codebashing uses real-world examples and best practices gleaned from years of experience with more than 1,600 customers around the world.
- **Training and beyond:** Codebashing provides teams with the communication, engagement, training, and assessment tools they need to execute comprehensive AppSec awareness campaigns for developers throughout the year.
- **Developer-centric learning:** In bite-size lessons, developers wear the hacker's hat as they see all the moving parts of the application stack that are relevant to explain the specific vulnerability they're facing.
- **A solution built to scale:** Codebashing lets you easily manage and track large enterprise teams with drill-down dashboard analytics and built-in support for major SAML/SSO providers.
- **Just-in-time remediation support:** When used in conjunction with Codebashing, Checkmarx SAST™ includes an easy-to-follow link to the relevant Codebashing lesson the moment it detects vulnerabilities in your code.

Cultivate a Security Culture

Raising AppSec awareness shouldn't be one distinct step in the software development life cycle (SDLC). To fuel faster, more secure releases, it needs to be infused in every step of the SDLC. This is why Codebashing exists. Through open communication, ongoing engagement, gamified training, and on-the-spot remediation support, security managers can cultivate a culture of secure development that empowers developers to think and act securely in their day-to-day work.

Raise the AppSec Bar

Codebashing helps you raise the baseline AppSec knowledge across your entire development team in a fast, scalable, and positive manner. This empowers developers for the long term by teaching them how to think and act with a secure mindset, rather than how to solve specific issues. Security managers can create and sustain an open channel of communication, keeping developers up-to-date on AppSec news and activities. Managers have full control and visibility—they can easily assign specific programming language courses to their teams and continuously track their progress. Managers can also engage their developers in tournaments and other events, fostering learning through friendly competition.

[1] According to the results of a 2021 survey by Checkmarx and Censuswide.

Managers have full control and visibility—they can easily assign specific programming language courses to their teams and continuously track their progress. Managers can also engage their developers in tournaments and other events, fostering learning through friendly competition.

Learn While Coding

Unlike traditional classroom or video-based training, Codebashing is a fun, hands-on solution that fits into developers' daily routines. Instead of losing a day of development time learning about vulnerabilities with little or no context, developers get bite-size, on-demand sessions relevant to the specific challenges they're facing in their code.

Find and Fix in One Go

We offer a unique integration between Codebashing and our static code analysis solution, Checkmarx SAST. When it identifies vulnerabilities, Checkmarx SAST links to relevant training in Codebashing, providing quick and pointed remediation guidance. This teaches the developer what caused the problem, how to fix it, and how to avoid repeating the same mistake, all in less than five minutes per lesson.

Comply with Regulatory Standards

Codebashing satisfies regulatory standards, such as PCI DSS, that require "role-based security training" or "developer security training.".

Supported Languages

- Java
- Go
- Python
- Scala
- C
- Node.JS
- C++
- .NET
- PHP
- Swift UI
- Ruby on Rails
- Kotlin
- Android
- iOS

Vulnerability Coverage

- SQL Injection
- XXE Injection
- Command Injection
- Session Fixation
- Reflected XSS
- Click Jacking
- DOM XSS
- User Enumeration
- Directory (Path) Traversal
- Privileged Interface Exposure
- Authentication Credentials in URL
- Session Exposure Within URL
- Horizontal Privilege Escalation
- Vertical Privilege Escalation
- Cross-Site Request Forgery (POST)
- Cross-Site Request Forgery (GET)
- Insecure URL Redirect
- Persistent (Stored) XSS
- Insecure TLS Validation
- Leftover Debug Code
- Insecure Object Deserialization
- Components with Known Vulnerabilities
- Use of Insufficiently Random Values