As DevOps becomes even more dominant, organizations are bringing development and security teams closer together to support even more secure software releases and faster time-to-market. The needs and benefits of moving security into the realm of the developer are clear – it saves time, money and company resources. However, roughly 60% of developers* don't have confidence in the security of their own applications. This gap exists because most developers are underserved when it comes to security strategy. Organizations normally put developers through secure code training once a year, or at best once a quarter, and hope that from then onwards developers will be able to get on the same page as security teams. While this approach "checks the training box", it really doesn't cultivate a sustained culture of software awareness.

Raising AppSec awareness shouldn't be thought of as a distinct step in the SDLC. It's all about inserting awareness into every step of the SDLC in a manner that actually fuels faster releases. CxCodebashing was designed specifically for this reason. Through the use of open communication, ongoing engagement, gamified training, and on-the-spot remediation support, security managers can cultivate a culture that empowers developers to think and act securely in their day-to-day work.

CxCodebashing's unique value:

Leveraging Over 13 years of AppSec Experience
An integral part of Checkmarx, CxCodebashing makes use of real-world examples and best practices gleaned from years of experience with over 1400 customers around the globe

Training and Beyond
Providing security teams with the communication, engagement, training, and assessment tools they need to execute comprehensive AppSec awareness campaigns for developers throughout the year

Developer-Centric
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 in an interactive lesson

Built to Scale
Easily manage and track large enterprise teams in CxCodebashing with drill-down dashboard analytics and built-in support for major SAML/SSO providers
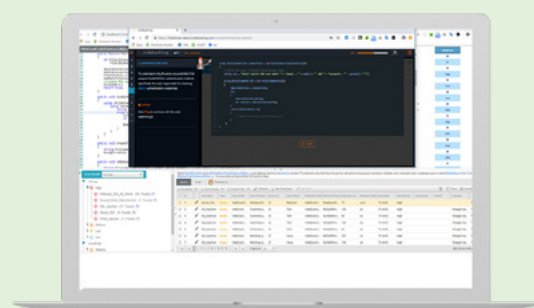
Just-in-Time Remediation Support
Vulnerabilities detected in Checkmarx Static Application Security Testing (CxSAST) include an easy-to-follow link to the relevant CxCodebashing lesson

Interactive Bite-Sized Code Walkthrough

CxCodebashing and CxSAST integration

Raise the AppSec bar

CxCodebashing allows you to 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.

Learn while coding

Unlike traditional classroom or video-based training, CxCodebashing is a is a fun, hands-on, interactive solution that fits into your developers' daily routines. Rather than losing a day of development learning about security vulnerabilities with little or no context, your developers receive bite-size, on-demand sessions that are relevant to the specific challenges they are facing in their code.

Find and Fix in one go

Checkmarx offers a unique integration between our Static Application Security Testing (CxSAST) solution and our secure coding education solution. Vulnerabilities identified by static analysis are linked to relevant, practical training lessons providing quick and pointed remediation guidance. This teaches the developer why the problem happened, how to fix it, and more importantly, how to prevent making the same mistake again in less than 5 minutes per lesson.

Comply with regulatory standards

CxCodebashing is compatible with regulatory standards like PCI-DSS that require either "role based security training" or, more specifically, "developer security training".

Supported Languages and Frameworks

Vulnerability Coverage

- SQL Injection
- XXE Injection
- Command Injection
- Session Fixation
- Use of Insufficiently Random Values
- Reflected XSS
- Persistent (Stored) XSS
- DOM XSS

- Directory (Path) Traversal
- Privileged Interface Exposure
- Leftover Debug Code
- Authentication Credentials In URL
- Session Exposure within URL
- User Enumeration
- Horizontal Privilege Escalation
- Vertical Privilege Escalation

- Cross Site Request Forgery (POST)
- Cross Site Request Forgery (GET)
- Click Jacking
- Insecure URL Redirect
- Insecure TLS Validation
- Insecure Object Deserialization
- Components with Known Vulnerabilities

Checkmarx

About Checkmarx

Checkmarx is the global leader in software security solutions for modern enterprise software development. Checkmarx delivers the industry's most comprehensive Software Security Platform that unifies with DevOps and provides static and interactive application security testing, software composition analysis, and developer AppSec awareness and training programs to reduce and remediate risk from software vulnerabilities. Checkmarx is trusted by more than 40 of the Fortune 100 companies and half of the Fortune 50, including leading organizations such as SAP, Samsung, and Salesforce.com. Learn more at **Checkmarx.com.**