Checkmarx AppSec Awareness Solution (CxCodebashing)

datasheet

As DevOps continues along its path of domination, organizations are seeking to bring development and security teams closer together to support the release of secure software 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, the reality is that around 60% of developers* don't have confidence in the security of their own applications. This gap exists as developers are often 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 doesn't not truly cultivate a sustained culture of software awareness.

Raising AppSec awareness cannot 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 exactly 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 of software security 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
Being an integral part of Checkmarx, CxCodebashing makes use of real-world examples and best practices gained from years of experience with over 1400 customers around the globe

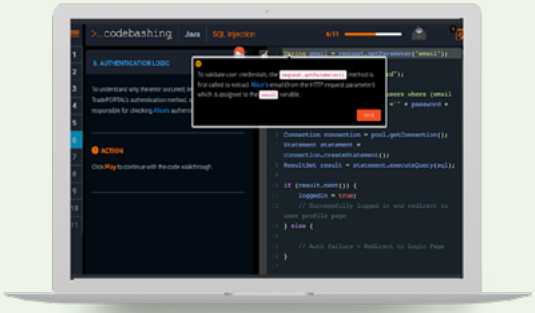
Training and Beyond
Providing security teams with the communication, engagement, training, and assessment tools they need to execute comprehensive AppSec Awareness campaigns for developers throughout the year

Developer-Centric
Developers "wear the hacker's hat" as they see all the moving parts of the application stack that are relevant to explaining the vulnerability

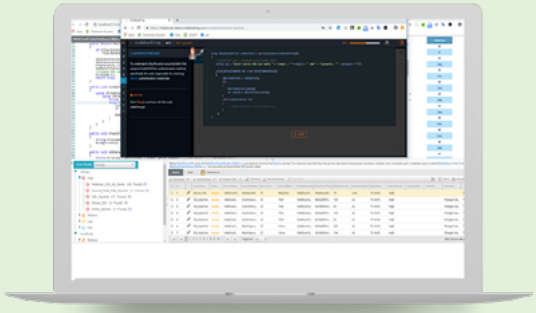
Built to Scale
Large enterprise teams are easily be managed and tracked in CxCodebashing with drill-down dashboard analytics and built-in support for major SAML/SSO providers

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 organization to raise the baseline AppSec knowledge across their entire development team in a fast, scalable, and positive manner. The philosophy behind the solution is to empower developers 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.

Learn while coding

Unlike traditional classroom or video-based training, CxCodebashing is a hands-on, interactive solution that fits into developers' daily routine. Rather than spending a whole day learning about security vulnerabilities out-of-context, 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 its Static Application Security Testing (CxSAST) solution and secure coding education solution. Vulnerabilities identified by static analysis are linked to 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.

Comply with regulatory standards

CxCodebashing is compatible with regulatory standards such as the PCI-DSS that requires either "role based security training" or more specifically "developer security training".

Supported Languages and Frameworks

Vulnerability Coverage

CxIAST detects input related and application vulnerabilities, including the OWASP Top Ten and more.

- 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

Software = Security

About Checkmarx

Checkmarx makes software security essential infrastructure, setting a new standard that's powerful enough to address today's and tomorrow's cyber risks. Checkmarx delivers the industry's only comprehensive, unified software security platform that tightly integrates SAST, SCA, IAST and AppSec Awareness to embed security into every stage of the CI/CD pipeline and minimize software exposure. Over 1,400 organizations around the globe trust Checkmarx to accelerate secure software delivery, including more than 40 percent of the Fortune 100 and large government agencies. Learn more at Checkmarx.com