CHECKMARX

CxCodebashing

Обучение безопасной разработке

Best Innovation in Mobile Development DEVIES Awards 2018

Концепция «shift left» широко распространена в мире разработки программного обеспечения: чем раньше будут обнаружены дефекты, тем легче и дешевле будет их исправление. Однако, реальность такова, что около 60% разработчиков* не уверены в безопасности своих собственных приложений. Этот факт существует потому, что разработчики нацелены на скорость и отсутствие багов в своем коде, а не на безопасность и устранение возможных уязвимостей.
Чтобы закрыть этот пробел, необходимо предоставить своим разработчикам обучение безопасной разработке. Проблема заключается в том, что обычные методы обучения, такие как видеоуроки, периодическое обучение группами и обязательные онлайн-курсы, часто не позволяют достичь нужного уровня компетенций, поскольку они являются теоретическими и не относятся к каким-то конкретным вещам, которыми разработчик занимается в данный момент.

Тут как раз и поможет CxCodebashing. CxCodebashing — это новое поколение образовательных и интерактивных образовательных решений для обучения безопасной разработке. Обучение проводится на месте, когда это необходимо и без «отрыва от производства». Сделав разработчиков «первой линией защиты» можно действительно сказать, что концепция «shift left» применена и в конечном счете мы получаем безопасные приложения при минимальных затратах.

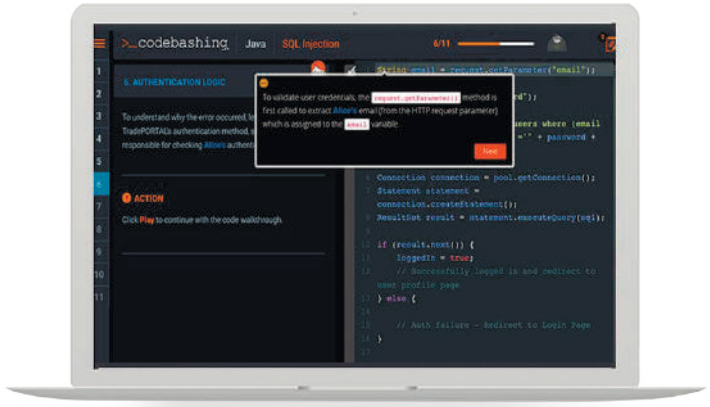
Уникальные возможности CxCodebashing

- **Практический, контекстный и интересный**
  Разработчикам предлагают побыть хакером и проэксплуатировать уязвимость самим, чтобы понять насколько она опасна.

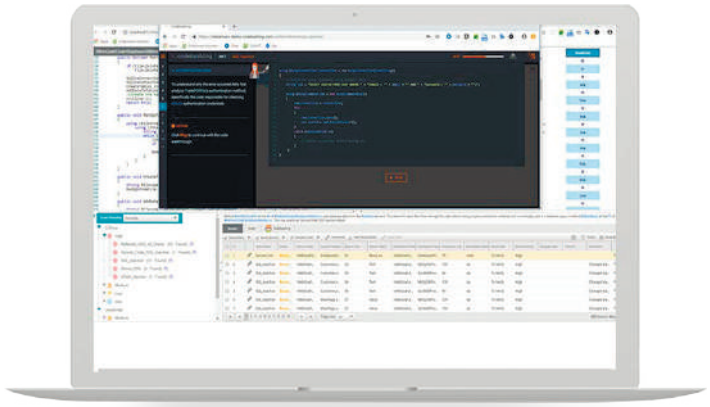
- **Создан экспертами в своей области**
  Checkmarx является лидером в области обнаружения уязвимостей и обучения безопасной разработке.

- **Часть платформы Checkmarx**
  Описание уязвимостей, обнаруженных в CxSAST, включает в себя ссылку на соответствующий урок CxCodebashing.

- **Даже для больших компаний**
  Подробные отчеты для аналитики, поддержка SAML/SSO



Интерактивное пояснение по коду



Интеграция CxCodebashing и CxSAST

*По данным опроса, проведенного NodeSource and Sqreen. .

«Shifting left» — это реально!

CxCodebashing воплотит «shifting left» в реальность не на словах, а в деле. Платформа обучения безопасной разработке позволит разработчикам комфортно и без отговорок взять безопасность в свои руки.

Обучение непосредственно в процессе разработки

В отличие от традиционного обучения в классе или видео, CxCodebashing — это практическое интерактивное решение, которое вписывается в повседневную рутину разработчиков. Вместо того, чтобы тратить целый день на изучение уязвимостей безопасности вне контекста, разработчики по необходимости получают доступ к урокам, которые соответствуют конкретным проблемам, с которыми они сталкиваются в своем коде

Найти и сразу исправить

Уникальная интеграция Checkmarx между CxCodebashing и CxSAST означает, что обнаруженные в CxSAST уязвимости ведут к практическому уроку в CxCodebashing. На этом уроке объяснят почему возникла проблема, как ее исправить и, что более важно, как предотвратить повторение этой же ошибки.

Повысить компетенции разработчиков

CxCodebashing позволяет быстро, основательно и масштабно повысить базовые знания разработчиков в безопасности. Философия, лежащая в основе CxCodebashing, заключается в долгосрочном расширении возможностей разработчиков, обучая их тому, как думать в парадигме безопасной разработки, а не как решать конкретные проблемы. Руководители имеют полный контроль и видимость — они могут легко назначать конкретные курсы языков программирования для своих команд и постоянно отслеживать их успехи.

Соответствие стандартам

CxCodebashing соответствует стандартам, к примеру PCI-DSS, который требует проведения тренингов по безопасной разработке.

Поддерживаемые языки и фреймворки

Поддерживаемые уязвимости

- 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

О Checkmarx

Checkmarx представляет платформу приложений для средних и крупных организаций. Более 1,400 компаний по всему миру доверяют анализ приложений Checkmarx. Checkmarx работает с 5 из 10 ведущих разработчиков программного обеспечения, крупнейшими банками и государственными учреждениями, а так же компаниями из списка Fortune 500, включая SAP, Samsung и Salesforce.com. For more information about Checkmarx, visit www.checkmarx.com