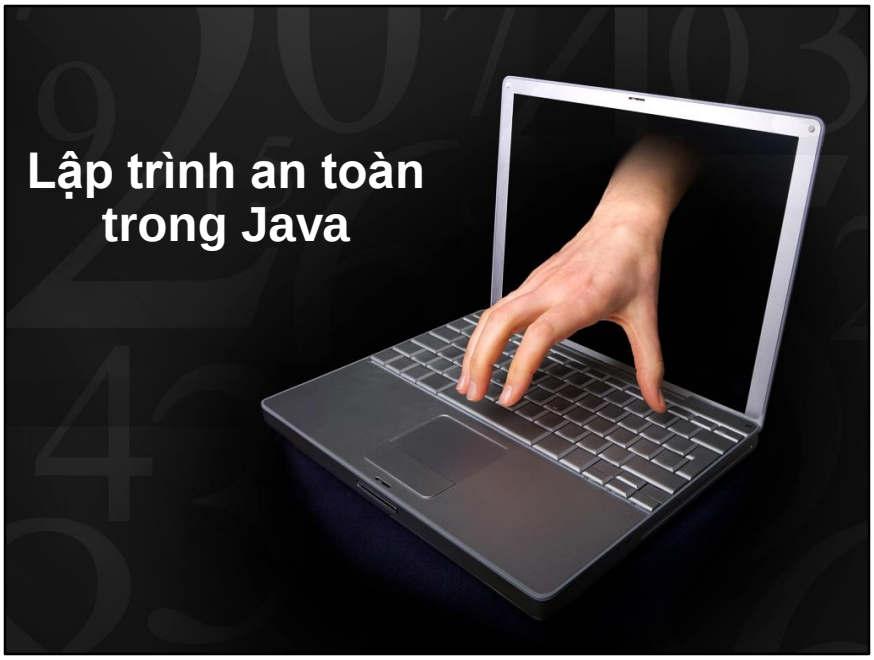
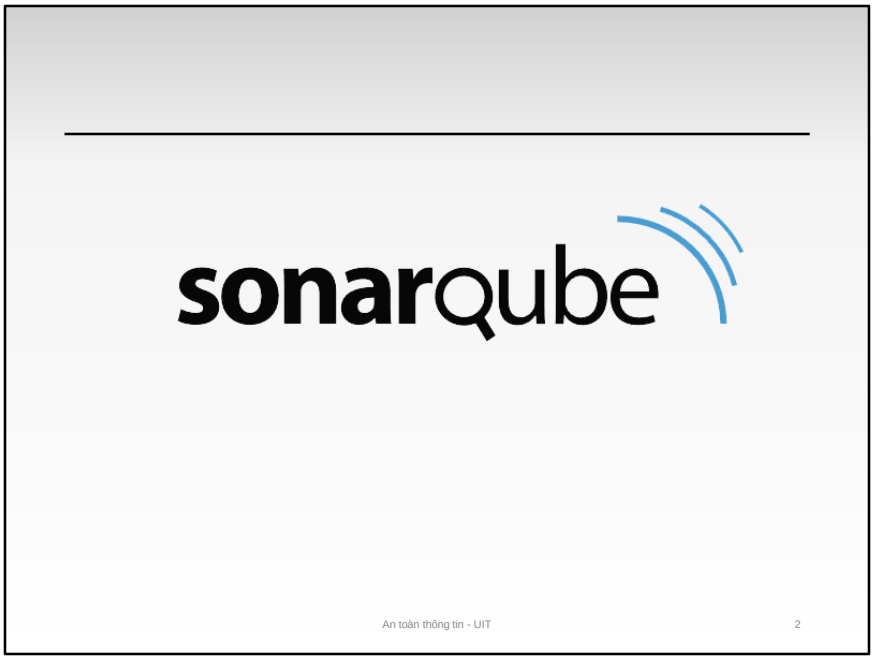




Chất lượng mã nguồn là vấn đề được đặt ra khi phát triển phần mềm.
Chất lượng kém là nguyên nhân dẫn đến nhiều vấn đề:

- Tốc độ của team thấp
- Ứng dụng dừng hoạt động
- Phá hỏng sản phẩm
- Danh tiếng công ty giảm

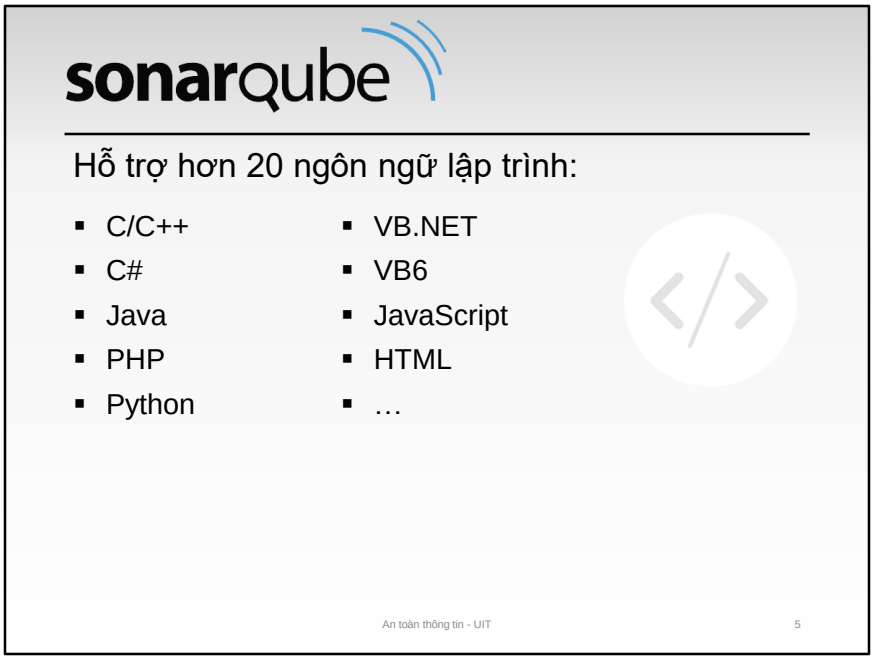
SonarQube cung cấp giải pháp cải tiến khả năng bảo trì, độ tin cậy và bảo mật.

Nội dung

- Giới thiệu
- Tính năng

cuu duong than cong . com

- Code Smell: (mã thối) mã xấu, dùng để chỉ phần code cảm thấy "*không ổn*" do thói quen viết code "miễn sao chạy được" của newbie.
- Bug: lỗi làm cho hệ thống hoạt động không như mong đợi, kết quả không chính xác.
- Vulnerability: là điểm yếu của chương trình giúp kẻ tấn công khai thác thông tin hệ thống.



+ Sử dụng ở hơn 80.000 tổ chức cơ quan: eBay, Thales, BMW.
+ Cài đặt:
    - Online: free → open source; fee → private project
    - Offline:

Continuous Inspection

Kiểm tra liên tục

Một phần trong quy trình phát triển phần mềm

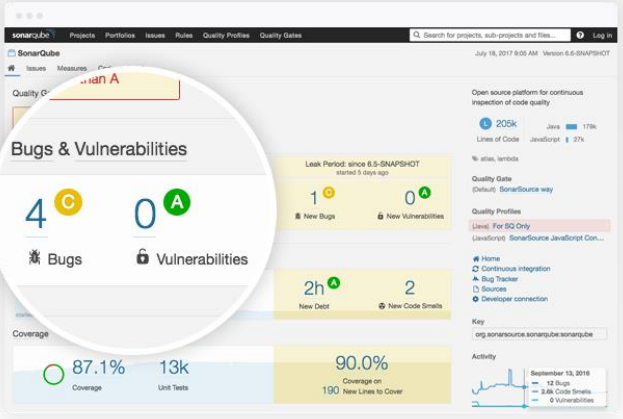
- Thể hiện chất lượng của ứng dụng
- Đưa ra các vấn đề của mã nguồn

→ Sửa chữa để cải thiện chất lượng

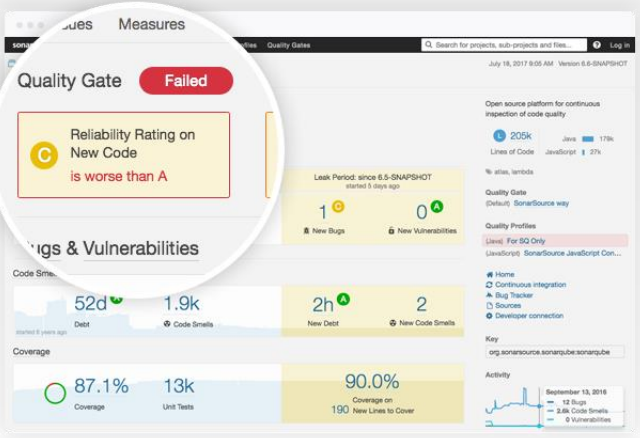
Kiểm tra liên tục: một phần trong quy trình phát triển phần mềm.
Trong CI (tích hợp liên tục) yêu cầu các thành viên tích hợp liên tục công việc. Mỗi tích hợp sẽ được build tự động để phát hiện lỗi nhanh nhất có thể.

Cung cấp cái nhìn tổng quan về chất lượng mã nguồn.

Continuous Inspection



Quality Gate



cuu duong than cong . com

Phát hiện: Code Smells

"Smelly" code:

- Khó để bảo trì
- Quá rối → người bảo trì có thể vô tình đưa ra bug

Ví dụ:

- Trùng mã nguồn
- Mã không được kiểm tra bởi unit test (quá cũ)
- Mã quá phức tạp

Vấn đề khả năng bảo trì thường được gọi là món nợ kĩ thuật.
Phần mềm được mong được thay đổi theo thời gian, mã nguồn được viết hôm nay có thể được cập nhật vào ngày mai.
Khả năng, chi phí thời gian dựa trực tiếp vào khả năng bảo trì → hiệu năng của team phát triển.

Khả năng bảo trì:
+ Tính mô đun
+ Khả năng hiểu được
+ Khả năng thay đổi
+ Khả năng kiểm tra
+ Khả năng tái sử dụng
Là kết quả của hàng vạn vấn đề nhỏ.

Phát hiện: Bugs

Ảnh hưởng đến độ tin cậy.

- Null-pointers Dereferences
- Logic Errors
- Lỗ hỏng tài nguyên

Bug tiềm ẩn hay mã nguồn có hành vi không mong đợi khi chạy.
Thường là lỗi lập trình, thiếu tuân thủ quy tắc.
Bug sẽ được phát hiện bằng cách phân tích sâu và thực thi mã nguồn để hiểu trạng thái tại của biến tại thời điểm bất kì.

Dereference operator dùng để lấy nội dung của địa chỉ mà biến đó trỏ vào.
Ví du: để lấy giá trị được lưu trữ trong biến a có hai cách: gọi trực tiếp biến a hoặc gọi gián tiếp qua con trỏ ip.

Lỗ hỏng tài nguyên: thiếu bộ nhớ.

Phát hiện: Vulnerabilities

Giúp theo dõi và tìm ra mã không an toàn

Lỗ hỏng bảo mật:

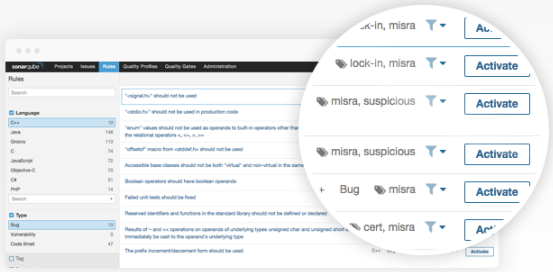
- SQL Injection
- Hard-coded passwords
- Cross-site scripting (XSS)

Lỗ hỏng trong chương trình dẫn đến việc sử dụng khác với cách được thiết kế.

Hard-coded passwords: mật khẩu được ghi cứng vào mã nguồn.

Tự thiết lập luật

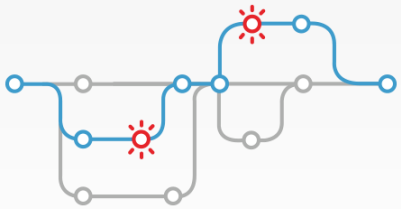
- SonarQube sử dụng Quality Profile mặc định
- Cho phép điều chỉnh luật:
  - Nhiều tiêu chí
  - Đơn
  - Kết hợp



Cho phép điều chỉnh để đáp ứng yêu cầu tại trang thiết lập luật.

Khai thác đường dẫn thực thi

Khai thác tất cả đường dẫn thực thi có thể để phát hiện ra những bug phức tạp nhất



Một function đơn giản chứa chỉ 10 nhánh khác nhau có thể dẫn đến 100 đường dẫn thực thi tại lúc chạy. Việc kiểm tra thủ công là không thể.

Lợi ích

Tối đa chất lượng, quản lý rủi ro.

- Lập trình viên:

  Đưa ra phản hồi tại mỗi bước trong quy trình phát triển để đưa ra giải pháp kịp thời

- DevOps:
  - Đảm bảo phần mềm được xây dựng đúng cách
  - Cung cấp cổng kiểm tra chất lượng cho mỗi bước xây dựng / kiểm thử / triển khai
- Điều hành:

  Cung cấp cái nhìn tổng quan về rủi ro đang phải đối mặt, giúp ước lượng chi phí và nâng cao hiệu quả của team

DevOps (kết hợp của cụm từ tiếng Anh "software DEVelopment" và "information technology OPerationS").

SonarCloud

Sử dụng online:

- Kết nối tài khoản GitHub
- Chuẩn bị project (trả phí để private)
- Thực hiện phân tích

cuu duong than cong . com

Tóm tắt

SonarQube

- Phù hợp cho mọi khách hàng
- Cung cấp cái nhìn tổng quan về chất lượng code
- Giúp giảm thiểu rủi ro và cung cấp phần mềm tốt hơn

Tối đa chất lượng, giảm thiểu rủi ro

Sản phẩm nguồn mở và thương mại.
Phù hợp cho lập trình viên, hướng dẫn, quản lý và giám đốc kỹ thuật, người chịu trách nhiệm vài đến vài ngàn dự án.