

Database Testing

Đội 12:

Phạm Đình Thiện

Cao Văn Cường

Trần Văn Thắng

Phùng Văn Dương

Hồ Nam Anh

Trần Hải Dương

Mục lục



01
Thực trạng

02
Nguyên nhân

03
Bài toán

04
Giải pháp đề xuất

05
Kế hoạch phát triển

06
Kế hoạch áp dụng

Thực trạng

Đặt tên bảng, thủ tục, hàm, ... sai convention.

- Một dự án chiếm tỷ lệ 10 - 20% sai convention.
- Gây ra khó khăn trong việc quản lý DB và phát hành.

VD: Demo trên tool.

Kiểm tra SQL Injection thủ công, theo kinh nghiệm.

- Gây ra lỗi lốt, tạo điều kiện cho hacker tấn công.

VD: Trong dự án C&B, hoạt động review SQL được thực hiện bởi SA hoặc DEV có kinh nghiệm. Tuy nhiên, chủ quan trong quá trình review đã dẫn tới lỗi lốt SQL Injection.



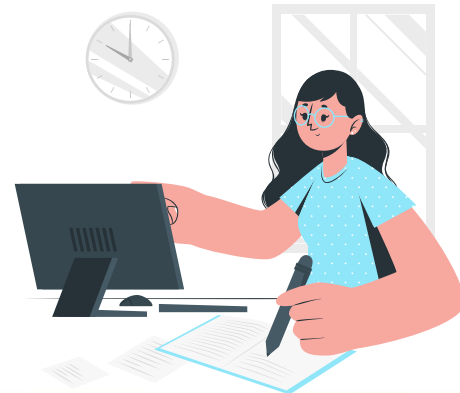
Nguyên nhân

Convention

- DEV mới chưa nắm rõ convention.
- DEV cũ chưa nắm được cách đặt tên theo convention.

SQL Injection

- DEV không có kinh nghiệm, chủ quan.
- Chưa có công cụ kiểm tra SQL Injection cho DEV.



Bài toán

1. Làm thế nào để giám sát việc tuân thủ Convention DB của DEV ?
 2. Làm thế nào để nhanh chóng phát hiện SQL Injection ngay trong giai đoạn phát triển ?
- Khảo sát 7 khối trong Khối Sản Xuất bao gồm:
 - Khối DA nền tảng quản trị kinh doanh.
 - Khối DA Hành chính sự nghiệp.
 - Viện Đào tạo và Nghiên cứu Công nghệ.
 - Khối DA nền tảng Quản trị Nhân sự - Điều hành.
 - Khối DA nền tảng tài chính DN.
 - Khối DA nền tảng giáo dục.
 - Khối DA Customize.
 - Điểm chung: Chưa có công cụ hỗ trợ kiểm tra convention DB và SQL Injection.

Giải pháp đề xuất

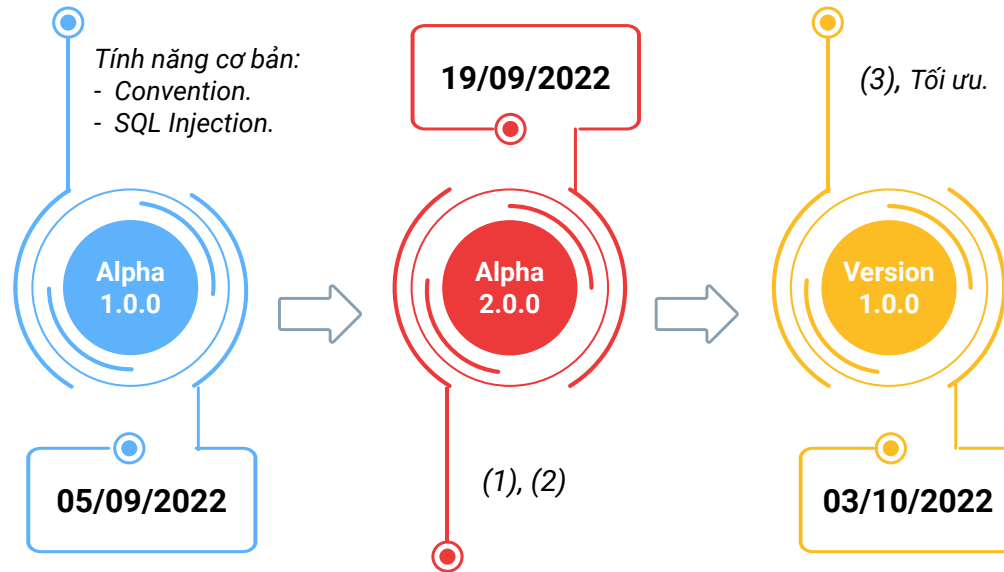
Xây dựng tool hỗ trợ thi công DB:

- Check Convention.
 - Check SQL Injection.
1. Giải pháp dựa trên kinh nghiệm.
 2. Ưu điểm: Hỗ trợ, tối ưu thời gian, tăng hiệu quả, năng suất cho việc thi công DB.
 3. Nhược điểm:
 - DEV cần thời gian làm quen tool, thay đổi thói quen code.
 - Chỉ áp dụng cho án sử dụng SQL (MySQL).
 4. Cách đo đếm hiệu quả: Dựa trên thời gian thi công, thời gian sửa lỗi KH.

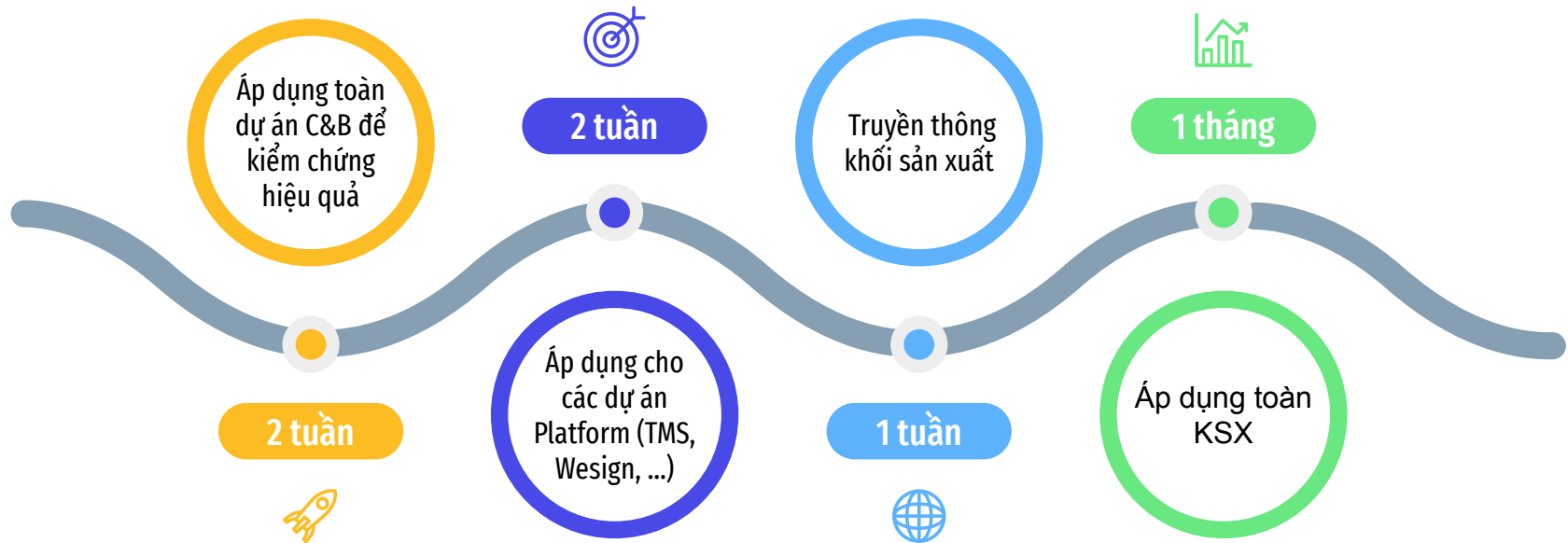


Kế hoạch phát triển

1. Tiếp tục phát triển tính năng kiểm tra Convention, SQL Injection chính xác hơn.
2. Tự động tạo file model (BE và FE) theo bảng trong DB.
3. MySQL Profiler.



Kế hoạch áp dụng



Thanks!

