**API Testing**

APIs (Application Programming Interfaces) cho phép các phần mềm hệ thống và ứng dụng giao tiếp và chia sẻ dữ liệu với nhau. Kiểm thử API rất quan trọng vì các lỗ hổng trong API có thể làm suy yếu tính toàn vẹn, bảo mật và tính sẵn có của trang web.

Tất cả trang web động thường có API, vì vậy các lỗ hổng kinh điển như SQL Injection có thể được xếp vào lớp kiểm thử API. Trong chủ đề này, chúng ta sẽ học cách kiểm thử APIs, tập trung vào RESTful và JSON APIs. Chúng ta sẽ học cách kiểm thử các lỗ hổng làm ngộ độc tham số ở phía máy chủ có thể ảnh hưởng đến các APIs nội bộ.

**Thu thập API**

Để bắt đầu kiểm thử API, đầu tiên bạn cần tìm càng nhiều thông tin về API càng tốt, để mở rộng phạm vi tấn công.

Để bắt đầu, bạn nên xác định các điểm cuối API.

GET /api/books HTTP/1.1

Host: example.com

Điểm cuối API là /api/books, lấy các cuốn sách từ thư viện. Một điểm cuối API khác là /api/books/mystery sẽ lấy những cuốn sách huyền bí.

Khi bạn đã tìm được các điểm cuối API, bạn cần tìm cách tương tác với chúng. Điều này cho phép bạn thực hiện các yêu cầu HTTP hợp lệ để kiểm thử API. Ví dụ, bạn nên tìm hiểu thông tin về những điều sau:

* Đầu vào dữ liệu mà api xử lí, bao gồm các tham số bắt buộc và tùy chọn.
* Các loại yêu cầu mà api chấp nhận, bao gồm các phương thức HTTP và định dạng dữ liệu.
* Rate limits và các cơ chế xác thực

**Các tài liệu về api**

Thường có các tài liệu về api để lập trình viên biết cách sử dụng và tích hợp chúng.

Tài liệu api có hai hình thức: người có thể đọc và đọc bằng máy. Tài liệu đọc được để lập trình viên hiểu cách dùng API. Nó bao gồm lời giải thích chi tiết, các ví dụ, và tình huống thực tế. Còn tài liệu đọc bằng máy được viết bằng định dạng cấu trúc như JSON hoặc XML.

Ta nên bắt đầu thu thập api từ các tài liệu có sẵn trên mạng.

Khám phá tài liệu API

* /api
* /swagger/index.html
* /openapi.json

Nếu bạn tìm được điểm cuối có tài nguyên, điều tra thêm đường dẫn gốc. Ví dụ, nếu bạn xác định được điểm cuối /api/swagger/v1/users/123, bạn nên điều tra thêm đường dẫn sau:

* /api/swagger/v1
* /api/swagger
* /api