**Tool pentesting objection**

**Khái Niệm:**

Objection là một công cụ kiểm thử tấn công (pentesting tool) được sử dụng trong lĩnh vực kiểm thử bảo mật, đặc biệt là cho ứng dụng di động chạy trên nền tảng Android và iOS. Nó được xây dựng trên nền tảng Frida và cung cấp khả năng tương tác động với quá trình chạy của ứng dụng.

**Cấu trúc:**

1.Giao Diện Dòng Lệnh (CLI):

* Giao diện dòng lệnh của Objection là nơi người dùng nhập các lệnh để thực hiện các tác vụ kiểm thử và tấn công.
* Cung cấp các tùy chọn và lệnh để tương tác với ứng dụng di động và thực hiện các chức năng kiểm thử bảo mật.

2.Frida Backend:

* Frida đóng vai trò quan trọng trong cấu trúc của Objection. Nó là một framework cho phép tương tác động với quá trình chạy của ứng dụng.
* Objection sử dụng Frida để chèn mã tùy chỉnh vào quá trình chạy của ứng dụng và theo dõi sự thay đổi, can thiệp, hoặc thu thập thông tin.

3.Plugins:

* Objection hỗ trợ các plugin để mở rộng khả năng của công cụ. Các plugin có thể thực hiện các chức năng cụ thể như phân tích bảo mật, can thiệp vào giao tiếp mạng, hoặc thực hiện các tác vụ tự động hóa.
* Các plugin giúp mở rộng chức năng và linh hoạt cho người sử dụng.

4.Scripts:

* Objection cho phép người dùng thực hiện các tác vụ thông qua các script. Các script này có thể được viết bằng JavaScript, giúp người dùng tùy chỉnh và mở rộng khả năng của Objection.

5.Tùy Chọn Cấu Hình:

* Các tùy chọn cấu hình cho phép người dùng điều chỉnh cách Objection tương tác với ứng dụng và thiết lập các thông số khác nhau như địa chỉ IP, cổng kết nối, v.v.

**Cách hoạt động:**

1. Kết Nối và Chèn Frida Mã:

* Objection sử dụng Frida để kết nối với quá trình chạy của ứng dụng di động. Frida có khả năng chèn mã JavaScript vào quá trình chạy.
* Khi bạn khởi động Objection, nó sẽ tạo kết nối với Frida server trên thiết bị di động và chèn mã Frida vào quá trình chạy của ứng dụng.

1. Tương Tác với Quá Trình Chạy:

* Mã JavaScript được chèn thông qua Frida sẽ tương tác động với quá trình chạy của ứng dụng. Điều này cho phép theo dõi, can thiệp và thậm chí thay đổi hành vi của ứng dụng trong thời gian chạy.

1. Giao Diện Dòng Lệnh (CLI):

* Người dùng tương tác với Objection thông qua giao diện dòng lệnh (CLI). Tại đây, họ có thể nhập các lệnh để thực hiện các chức năng kiểm thử và tấn công.

1. Sử Dụng Plugins và Scripts:

* Objection hỗ trợ việc sử dụng các plugin và scripts. Các plugin cung cấp chức năng mở rộng, trong khi scripts cho phép thực hiện các tác vụ tùy chỉnh.
* Các lệnh và chức năng của Objection có thể được mở rộng bằng cách sử dụng các plugin có sẵn hoặc viết các script tùy chỉnh.

1. Thực Hiện Các Chức Năng Kiểm Thử:

* Objection cung cấp các lệnh để kiểm thử bảo mật ứng dụng, bao gồm theo dõi và can thiệp vào giao tiếp mạng, kiểm tra lỗ hổng bảo mật, và thậm chí tự động hóa một số hành động tấn công.

1. Tương Tác với Các Thành Phần Cụ Thể Của Ứng Dụng:

* Người dùng có thể tương tác với các thành phần cụ thể của ứng dụng, như các hàm, biến, hoặc luồng thực thi, để kiểm tra và kiểm thử tính bảo mật.

**Tác dụng:**

1. Kiểm Thử Bảo Mật Toàn Diện:

* Objection cung cấp một môi trường kiểm thử bảo mật mạnh mẽ cho ứng dụng di động. Nó giúp chuyên gia bảo mật xác định và đánh giá lỗ hổng bảo mật từng chi tiết trong quá trình chạy của ứng dụng.

1. Theo Dõi và Can Thiệp vào Giao Tiếp Mạng:

* Objection cho phép người dùng theo dõi và can thiệp vào giao tiếp mạng của ứng dụng di động. Điều này giúp kiểm tra tính bảo mật của các phương thức kết nối và truyền thông.

1. Bypassing SSL Pinning:

* Một trong những tác dụng quan trọng của Objection là hỗ trợ việc bypassing SSL pinning. SSL pinning là một biện pháp bảo mật để đảm bảo an toàn trong giao tiếp mạng, và Objection giúp bỏ qua nó để kiểm thử tính bảo mật hiệu quả hơn.

1. Kiểm Thử Động và Tương Tác Thời Gian Chạy:

* Objection cho phép chuyên gia bảo mật thực hiện kiểm thử động trực tiếp trong thời gian chạy của ứng dụng. Điều này giúp đào sâu vào quá trình thực thi và định rõ các lỗ hổng có thể xuất hiện.

1. Tự Động Hóa Các Tác Vụ Kiểm Thử:

* Các plugin và scripts của Objection cho phép tự động hóa một số tác vụ kiểm thử. Điều này giúp tăng cường hiệu suất và đồng thời giảm khối lượng công việc lặp lại cho người thử nghiệm.

1. Phân Tích Ứng Dụng Đa Nền Tảng:

* Objection không chỉ hỗ trợ kiểm thử trên nền tảng Android mà còn trên iOS. Điều này giúp chuyên gia bảo mật có khả năng kiểm thử và đánh giá tính bảo mật trên nhiều hệ điều hành di động.

1. Theo Dõi và Can Thiệp vào Các Thành Phần Cụ Thể:

* Objection cho phép người dùng tương tác với các thành phần cụ thể của ứng dụng như hàm, biến, và luồng thực thi, giúp kiểm tra và kiểm thử tính bảo mật của từng phần của ứng dụng.

1. Mở Rộng và Linh Hoạt:

* Các plugin và scripts mở rộng khả năng của Objection, giúp người sử dụng có thể thích ứng với các tình huống và yêu cầu kiểm thử cụ thể.

**Cách cài đặt.**

Để cài đặt công cụ kiểm thử tấn công Objection, bạn cần thực hiện một số bước cài đặt cơ bản.

**Yêu Cầu Tiên Quyết:**

1. Python:

* Objection được xây dựng bằng Python, vì vậy bạn cần cài đặt Python trên hệ thống của mình. Bạn có thể tải Python từ trang chính thức: <https://www.python.org/>.

1. Frida:

* Objection sử dụng Frida như một backend, nên bạn cần cài đặt Frida trước khi sử dụng Objection. Cài đặt Frida bằng cách sử dụng npm (Node Package Manager) với lệnh sau:

npm install -g frida

**Cài Đặt Objection:**

1. Sử dụng pip:

* Mở terminal hoặc command prompt và nhập lệnh sau để cài đặt Objection:

pip install objection

1. Kiểm Tra Việc Cài Đặt:

* Để kiểm tra xem Objection đã được cài đặt thành công hay không, bạn có thể nhập lệnh sau:

objection –version

Nếu bạn nhìn thấy phiên bản của Objection, điều này có nghĩa là cài đặt đã thành công.

**Khởi Chạy Objection:**

1. Mở Giao Diện Dòng Lệnh:

* Mở terminal hoặc command prompt và nhập lệnh sau để bắt đầu sử dụng Objection:

objection

1. Kết Nối Đến Ứng Dụng Di Động:

* Sau khi Objection đã chạy, bạn cần kết nối nó với ứng dụng di động bạn muốn kiểm thử. Sử dụng lệnh sau để kết nối:

android connect

1. Kiểm Tra Kết Nối:

* Để kiểm tra xem kết nối đã được thiết lập chưa, nhập lệnh sau:

android status

1. Bắt Đầu Sử Dụng:

* Bây giờ bạn đã kết nối thành công và có thể bắt đầu sử dụng Objection để kiểm thử và tương tác với ứng dụng.