Bài tập 1:(2đ) Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu

* Tiêu đề: Lỗ hổng là SSRF cho phép kẻ tấn công gửi 1 yêu cầu chỉnh sửa thủ công đến 1 đích không mong muốn, ngay cả khi được bảo vệ bởi tường lửa, VPN, ACL
* Mô tả: Xảy ra với bất kỳ ứng dụng web nào tải 1 tài nguyên từ xa và không xác thực URL của người dùng
* Tóm tắt: Ta sẽ thực hiện giao thức file:// để có thể đọc file từ người dùng
* Các bước thực hiện

+ Bước 1: Ta truy cập vào trang web thì thấy có 1 thanh textbox để có thể nhập URL để có thể kiểm tra gì đó. Ta nhập thử 1 trang web bất kỳ

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

+ Bước 2: Sau khi bấm nút “Test it” thì ở dưới kết quả cho ta thấy đó là mã HTML của trang web(Lưu ý ta cần phải nhập đầy đủ URL của 1 trang web bao gồm cả http://)

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Trang web

Mô tả được tạo tự động

+ Bước 3: Từ đây ta có thể biết là trang web có thể bị lỗ hổng SSRF vì nó không có cơ chế để xác thực đầu vào nên ta có thể lợi dụng nó để có thể khai thác

+ Bước 4: Vì nó chỉ hỗ được URL nên không thể tiến hành khai thác INJECTION

+ Bước 5: file:// là một giao thức được sử dụng trong địa chỉ URL để truy cập tệp tin trên máy tính từ trình duyệt web.

+ Bước 6: Ta tiến hành khai thác bằng cách đọc 1 file từ /etc/passwd để có thể lấy mật khẩu của người dùng. Trong đó file:// là giao thức còn /etc/passwd là đường dẫn để có thể lấy tài khoản của người dùng. Do đây là localhost nên ta sử dụng giao thức file để có thể khai thác

Ảnh có chứa văn bản, phần mềm, Biểu tượng máy tính, Phần mềm đa phương tiện

Mô tả được tạo tự động

+ Ngoài ra ta có thể sử dụng <http://website/tai>-nguyen để có thể truy cập vào tài nguyên của trang web nếu như nó có tài nguyên đó

+ Bước 7: Khai thác thành công

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

* Mức độ ảnh hưởng: Mức độ ảnh hường tùy thuộc vào cách khai thác. Một số tác động có thể kể đến như là DoS, lấy dữ liệu nhạy cảm từ các hệ thống, tấn công mạng nội bộ của tổ chức,..
* Khuyến khích cách khắc phục: Để khắc phục thì ta nên có các thao tác để xử lý, lọc các dữ liệu đầu vào, giới hạn quyền truy cập, cập nhật thường xuyên các phiên bản phần mềm

Bài tập 2:(2đ) Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu

* Tiêu đề: Lỗ hổng broken access control
* Mô tả: Quyền truy cập luôn có sẵn cho bất kỳ ai mà không được cấp cho người dùng hay vai trò cụ thể. Cho phép xem hoặc chỉnh sửa tài khoản của người khác bằng cách sử dụng định danh duy nhất
* Tóm tắt
* Các bước thực hiện

+ Bước 1: Truy cập vào trang web thì ta thấy nó là 1 trang web đăng nhập với yêu cầu nhập username và password. Nếu nhập sai thì nó xuất ra 1 thông báo

Ảnh có chứa phần mềm, Phần mềm đa phương tiện, Biểu tượng máy tính, Trang web

Mô tả được tạo tự động

+ Bước 2: Ta truy cập với tài khoản user bình thường là johndoe và password là password1

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

* Mức độ ảnh hưởng của lỗ hổng

Bài tập 3:(2đ) Tìm kiếm thông tin các thư viện trên website \*.rmit.edu.vn có tồn tại lỗ hổng đã biết hoặc báo cáo lỗ hổng tồn tại trên \*.rmit.edu.vn

* Tiêu đề: Lỗ hổng Directory Listing là lỗ hổng liệt kê thư mục.Tài sản bị ảnh hưởng là tập tin và thư mục nhạy cảm, quyền riêng tư của người dùng và cấu trúc hệ thống.
* Mô tả: Lỗ hổng Directory Listing (hay còn gọi là Directory Traversal) là một lỗ hổng bảo mật phát sinh khi một ứng dụng web không kiểm soát hoặc không hạn chế đúng cách quyền truy cập vào các thư mục trên máy chủ web
* Tóm tắt: Sử dụng google hacking để tìm thông tin nhạy cảm
* Các bước thực hiện

+ Bước 1: Ta sử dụng google hacking để có thể tìm kiếm các thông tin nhạy cảm của tên miền \*.rmit.edu.vn

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

+ Ta nhập site:\*.rmit.edu.vn intext:"powered by WordPress" sẽ tìm kiếm được các trang web được cài đặt bởi wordpress

+ Bước 2: Từ đây ta có ý tưởng sẽ tìm thử các trang mục của trang \*.rmit.edu.vn thử xem

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

+ Ta thấy có 1 trang web hiện ra với tên là Index of

+ Bước 3: Truy cập vào thì ta thấy các thư mục của trang web hiện lên từ đây ta có thể truy cập và xem các dữ liệu nếu không được quản lý kỹ

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Mức độ ảnh hưởng: Mức độ tùy thuộc vào các thông tin bị leak ra từ đó kẻ tấn công có thể lợi dụng các thông tin này để khai thác trái phép và gây ảnh hướng nghiêm trọng
* Khuyến cáo khắc phục: Cấu hình máy chủ web, kiểm tra và loại bỏ các quyền truy cập không hợp lệ. Đảm bảo các thông tin nhạy cảm bị loại bỏ trong máy chủ, xác thực và kiểm tra đầu vào

Bài tập 4:(4đ) Báo cáo 2 lỗ hổng tìm thấy. Sử dụng format theo mẫu

* Tiêu đề: Application Flow Tampering Vulnerability là một lỗ hổng bảo mật trong ứng dụng Android. Tài sản bị ảnh hưởng đó là dữ liệu người dùng, quyền truy cập
* và ủy quyền, tính toàn vẹn của ứng dụng và khả năng hoạt động đúng đắn của ứng
* dụng
* Mô tả lỗ hổng: Cho phép kẻ tấn công thay đổi luồng ứng dụng và chuyển hướng người dùng sang các trang web hoặc các ứng dụng khác mà người dùng không mong muốn.
* Tóm tắt: Thực hiện kỹ thuật activity hijacking để thay đổi luồng hoạt động
* Các bước thực hiện

+ Bước 1: Cài đặt và truy cập vào ứng dụng thì nó yêu cầu ta đăng nhập

Ảnh có chứa ảnh chụp màn hình, văn bản

Mô tả được tạo tự động

+ Bước 2 ta thử reverse file apk để xem các tệp tin smali và androidmanifest.xml như thế nào

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

+ Bước 3: Xem thử file Androidmanifest.xml ta thấy có 1 số activity được gán export là true. Đây là những hành động ẩn và chỉ được gọi bởi các ứng dụng khác

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

+ Bước 4: Chúng ta thử sử dụng Activity Hijacking là một kỹ thuật thay đổi luồng hoạt động và kích hoạt hành động mà chúng ta muốn, và bây giờ chúng ta sẽ kích hoạt hành động đó.



+ Bước 5: Ta đã gọi được activity mà không cần đăng nhập hay làm bất cứ gì

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động

* Mức độ ảnh hưởng: Nó có thể dẫn đến các hành động độc hại khác, như chuyển hướng người dùng đến các trang web giả mạo hoặc cài đặt phần mềm độc hại trên điện thoại của họ. Nó ảnh hưởng đến tính toàn vẹn và quyền riêng tư của người dùng
* Khuyến cáo khắc phục: Xác thực và ủy quyền, kiểm tra dữ liệu đầu vào, mã hóa
* dữ liệu, xác minh luồng hoạt động, kiểm tra và phân tích bảo mật, cập nhật và bảo
* trì, giáo dục và đào tạo và theo dõi và giám sát.

5. Kịch bản 05: Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

- Tiêu đề: Insecure logging. Tài sản ảnh hưởng là các dữ liệu, thông tin các nhân, mật khẩu tài khoản và các thông tin quan trọng

- Mô tả lỗ hổng: Là lỗ hổng mà attacker có thể lấy được tài khoản hoặc mật khẩu được lưu trữ mà không có cách thức mã hóa hay bảo vệ gì

- Tóm tắt: Ta sử dụng adb logcat để xem log được ghi lại của ứng dụng

- Các bước thực hiện:

+ Bước 1: Sử dụng bytecode viewer để xem và phân tích tập tin apk

Ảnh có chứa văn bản, đồ điện tử, ảnh chụp màn hình, phần mềm

Mô tả được tạo tự động

+ Bước 2: Trong com ta thấy có file LoginActivity.class ta mở ra xem thử

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

+ Bước 3: Ta có thể thấy rằng là username và password của ta được ghi log lại mà không thấy có bất kỳ mã hóa hay cách bảo vệ gì

+ Bước 4: Ta sử dụng adb logcat và lọc ra password thì ta thấy mật khẩu ta nhập đã được ghi log

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

- Mức độ ảnh hưởng: Nó ảnh hưởng tùy thuộc vào dữ liệu mà attacker có thể khai thác từ tài khoản của người dùng và đó là ứng dụng gì. Phổ biến có thể là các app ngân hàng hay những tài khoản dùng để lưu trữ nhưng thông tin các nhân , thông tin quan trong

- Khuyến cáo khắc phục: Không nên ghi lại log liên quan đến username hoặc password. Nếu có lưu thì không nên lưu dưới dạng plaintext mà lưu dưới dạng đã được mã hóa. Thêm các phương thức xác thực khác, xác thực 2 lớp để tránh attacker lợi dụng và đăng nhập dễ dàng