WEB APPLICATION ATTACK

**I. Khái niệm:**

+ Là hoạt động độc hại nhắm vào các ứng dụng web bằng cách khai thác các lỗ hổng trong thiết kế hoặc triển khai của chúng.

=> Dẫn đến truy cập trái phép, đánh cắp dữ liệu

+ Các loại tấn công web application phổ biến: SQL Injection, XSS, CSRF (cross-site request forgery) và file inclusion.

=> Kẻ tấn công sử dụng các công cụ tự động và giành quyền truy cập vào thông tin hoặc hệ thống nhạy cảm

**II. Hậu quả:**

+ Vi phạm dữ liệu

+ Trộm cắp danh tính

+ Tổn thất tài chính

+ Thiệt hại về danh tiếng

+ Hậu quả pháp lý

+ Gián đoạn kinh doanh

**III. Các loại tấn công web phổ biến (Top 10 OWASP):**

1. Broken Access Control (Kiểm soát truy cập bị hỏng):

+ Tổng quan:

* Kiểm soát truy cập thực thi cho người dùng không thể hành động ngoài quyền được cấp của họ
* Lỗ hổng dẫn đến: tiết lộ, sửa đổi/ phá hủy thông tin trái phép tất cả dữ liệu,…

+ Lỗ hổng bao gồm:

* Vi phạm nguyên tắc đặc quyền tối thiểu (quyền không được cấp đúng)
* Bypass bằng: + sửa đổi URL (giả mạo tham số hoặc buộc duyệt)

+ Bỏ qua trạng thái ứng dụng nội bộ

+ Bỏ qua trang HTML

+ Sử dụng công cụ tấn công sửa đổi yêu cầu API

* Cho phép xem, chỉnh sửa tài khoản của người khác bằng cách cung cấp mã định danh duy nhất của tài khoản đó (tham chiếu đối tượng trực tiếp không an toàn)
* Truy cập API thiếu biện pháp kiểm soát truy cập cho POST, PUT, DELETE
* Nâng cao đặc quyền (HĐ với tư cách người dùng mà không cần đăng nhập/ hoạt động với tư cách QTV khi đăng nhập với tư cách người dùng)
* Thao túng siêu dữ liệu
* Cấu hình sai CORS cho phép truy cập API từ nguồn gốc trái phép/không đáng tin cậy
* Buộc duyệt đến các trang được xác thực với tư cách là người dùng chưa được xác thực hoặc đến các trang đặc quyền với tư cách là người dùng

+ Ngăn chặn:

* Ngoại trừ tài nguyên public, từ chối theo mặc định
* Triển khai các cơ chế kiểm soát quyền truy cập một lần và tái sử dụng chúng trong toàn bộ ứng dụng
* Kiểm soát truy cập mô hình nên thực thi quyền sở hữu bản ghi thay vì chấp nhận rằng người dùng có thể tạo, đọc, cập nhật hoặc xóa bất kỳ bản ghi nào
* Vô hiệu hóa danh sách thư mục máy chủ web và đảm bảo siêu dữ liệu tệp (ví dụ: .git) và các tệp sao lưu không có trong web root
* Ghi lại các lỗi kiểm soát quyền truy cập, cảnh báo cho quản trị viên khi thích hợp
* …

1. Cryptographic Failures

+ Lỗ hổng bao gồm:

+ Ngăn chặn:

* Phân loại dữ liệu được xử lý, lưu trữ hoặc truyền đi bởi 1 ứng dụng
* Không lưu trữ dữ liệu nhạy cảm 1 cách không cần thiết. Loại bỏ nó càng sớm càng tốt hoặc sử dụng mã thông báo tuân thủ PCI DSS hoặc thậm chí cắt bớt
* Đảm bảo mã hóa tất cả dữ liệu nhạy cảm khi lưu trữ
* Tắt bộ nhớ đệm cho phản hồi có chứa dữ liệu nhạy cảm
* …….

1. Injection

+ Ứng dụng dễ bị tấn công khi:

* Dữ liệu người dùng cung cấp không được xác thực và lọc
* Các truy vấn động hoặc lệnh gọi không được tham số hóa mà không thoát theo ngữ cảnh được sử dụng trực tiếp trong trình thông dịch
* Dữ liệu thù địch được sử dụng trong các tham số tìm kiếm ánh xạ quan hệ đối tượng (ORM) để trích xuất các bản ghi nhạy cảm, bổ sung
* Dữ liệu thù địch được sử dụng trực tiếp hoặc nối. SQL hoặc lệnh chứa cấu trúc và dữ liệu độc hại trong các truy vấn động, lệnh hoặc thủ tục được lưu trữ

+ Ngăn chặn:

1. Insecure Design
2. Security Misconfiguration
3. Vulnerable and Outdated Components
4. Identification and Authentication Failures
5. Software and Data Integrity Failures
6. Security Logging and Monitoring Failures
7. Server-Side Request Forgery (SSRF)