Cơ bản về Web Security

- **Browser security**: Same Origin Policy (SOP) – cách ly site trong cùng trình duyệt.
- **Server-side security**: Máy chủ phải chấp nhận bất kỳ request HTTP nào → cần kiểm soát input.
- **Client-side security**: Bảo vệ người dùng khỏi social engineering, tracker, rò rỉ dữ liệu.

DNS & HTTP

- **DNS hijacking**: Chuyển hướng tên miền tới IP kẻ tấn công → phishing, ads, crypto mining.
- Cách thực hiện: chiếm recursive resolver, nameserver, tài khoản DNS provider, malware thay đổi DNS local, router bị chiếm quyền.

Same Origin Policy (SOP)

- **Nguyên tắc**: Hai trang khác origin không được can thiệp nhau. Origin = (protocol, hostname, port).
- **Ví dụ**:
  - Cùng origin: https://example.com/a → https://example.com/b
  - Khác origin: khác hostname, protocol, hoặc port.
- Ngăn chặn JavaScript cross-origin đọc dữ liệu trái phép.

Cookie & Session

- **Cookie**: Lưu trên client, gửi kèm request.
- **Session**: Server lưu trạng thái duyệt web của user (login, giỏ hàng…).
- **Tấn công**:
  - Session hijacking (nghe lén cookie qua HTTP, XSS đánh cắp cookie).
  - CSRF lợi dụng cookie được gửi tự động.
- **Bảo vệ cookie**: Secure, HttpOnly, SameSite, domain/path, expiration.

Cross-Site Request Forgery (CSRF)

- Ép user đã đăng nhập thực hiện hành động trái phép (chuyển tiền, đổi email…).
- Phòng chống:
  - Re-authenticate khi thao tác quan trọng.
  - Token ẩn trong form.

- SameSite cookie.

OWASP Top 10 & Cách phòng tránh

1. **Injection**: chèn lệnh SQL/command → Validate input, dùng Prepared Statement.
2. **Broken Access Control**: bỏ sót kiểm tra quyền → Kiểm tra ở server & client, deny by default.
3. **Cryptographic Failures**: dùng thuật toán yếu → dùng AES, SHA-256, TLS mới.
4. **Insecure Design**: thiết kế không tính bảo mật → Security by design.
5. **Security Misconfiguration**: lỗi cấu hình → tắt tính năng thừa, đổi default password.
6. **Vulnerable Components**: dùng thư viện lỗi thời → cập nhật, virtual patching.
7. **Auth Failures**: sai trong xác thực → MFA, timeout, kiểm tra mật khẩu mạnh.
8. **Software & Data Integrity Failures**: cập nhật bị chèn mã độc → chữ ký số, SBOM.
9. **Logging Failures**: không log hoặc không giám sát → bật log, cảnh báo bất thường.
10. **SSRF**: server fetch URL user gửi mà không kiểm tra → validate URL, giới hạn port.

Một số lỗ hổng phổ biến minh hoa

- **Command Injection**: Chèn lệnh hệ điều hành.
- **SQL Injection**: Chèn lệnh SQL để đọc/sửa/xóa DB.
- **XSS**: Chèn script chạy trên trình duyệt nạn nhân.
- **CSRF**: Lợi dụng session cookie gửi request trái phép.
- **SSRF**: Server bị lợi dụng để truy cập dịch vụ nội bộ.

Thực hành an toàn

- **Phía client**: Escape output, CSP, sandbox iframe, cập nhật framework.
- **Phía server**: Validate input, dùng HTTPS, bật bảo vệ CSRF/XSS, cấu hình secure cookie.
- **Quản trị hệ thống**: Cập nhật phần mềm, giới hạn quyền, bật tường lửa ứng dụng web (WAF), backup định kỳ.