Web Security Cheat Sheet

🛡️ Threat / Concept	💡 What It Is	🔧 How to Prevent It / Best Practice
XSS	Injecting malicious JavaScript	Sanitize inputs, use CSP, encode output
CSRF	Forcing users to perform actions unknowingly	CSRF tokens, SameSite cookies
SQL Injection	Injecting SQL via input fields	Use prepared statements, ORM
Clickjacking	UI tricked into invisible frames	X-Frame-Options, frame busting via JS
Insecure Cookies	Cookies exposed to JS or sent over HTTP	Use HttpOnly, Secure, and SameSite flags
Broken Authentication	Weak login/session handling	Use OAuth, bcrypt, session expiration, 2FA
Open Redirects	Redirects to attacker sites	Validate redirect URLs strictly
Directory Traversal	Accessing files via ../ paths	Normalize paths, restrict file access
Sensitive Data Exposure	Leaking secrets like tokens, passwords	Use .env, encrypt data, never log sensitive info
Unvalidated Input	Accepting raw or dangerous input	Validate inputs strictly, use schema validators
Security Misconfig	Poor server or app configuration	Use secure headers, remove dev settings
Missing HTTPS	Insecure communication	Use SSL/TLS certificates (HTTPS everywhere)
Broken Access Control	Unauthorized access to resources	Enforce role-based access, never trust client-side
Insufficient Logging	Attacks go undetected	Use audit logs, monitor suspicious activity
Command Injection	Injecting system commands via input	Avoid shell commands, sanitize input, use APIs
IDOR	Users accessing data/resources they shouldn't	Validate user permissions on each request
Excessive Data Exposure	APIs returning too much data	Limit API responses, use DTOs or serializers
Outdated Libraries	Using vulnerable third-party packages	Regularly update dependencies, use Snyk/OWASP tools
Race Conditions	Two requests interfering with each other	Lock resources, use atomic operations
Subdomain Takeover	Dangling DNS points to deleted apps/sites	Audit DNS records, remove unused subdomains
CORS Misconfigurations	Exposing resources to unauthorized sites	Define strict origin policies, avoid * wildcards