✅ Top 25 Website Vulnerabilities (Bug Bounty Beginner List)

(ordered by frequency + importance)

There is an website called CWE which give common latest vulnerablities in websites

---

1. Cross-Site Scripting (XSS)

User-controlled input appears on the page without proper sanitization.
 Learn: input validation, output encoding, CSP.

2. Broken Access Control

Users can access data/actions they shouldn't (IDOR, forced browsing).
 Learn: authorization checks, object-level controls.

3. SQL Injection

Input is included in SQL queries unsafely.
 Learn: prepared statements, ORM, parameterization.

4. Cross-Site Request Forgery (CSRF)

Forces a victim to perform unwanted actions if they're logged in.
 Learn: CSRF tokens, SameSite cookies.

5. Server-Side Request Forgery (SSRF)

Website makes requests to internal systems based on user input.
 Learn: URL allow-listing, metadata protection.

6. Command Injection

Unsanitized input is passed to system shell commands.
 Learn: safe APIs, strict input validation.

7. File Upload Vulnerabilities

Unsafe upload allows web shells or malicious files.
 Learn: MIME checking, extension filtering, storage outside webroot.

8. Sensitive Data Exposure

Misconfigured endpoints leak private information.
 Learn: encryption, proper logging, secure storage practices.

9. Authentication Bypass

Weak login logic allows unauthorized access.
Learn: multi-factor design, brute-force protection.

10. Broken Session Management

Session IDs exposed or predictable; session fixation issues.
Learn: secure cookies, regeneration on login.

11. Insecure Direct Object Reference (IDOR)

Modifying IDs gives access to other users' data.
Learn: object-level authorization checks.

12. Path Traversal

Manipulating file paths to access unintended files.
Learn: normalize paths, allow-list filenames.

13. Open Redirects

Redirect parameter leads to phishing/abuse risks.
Learn: allow-list redirect destinations.

14. XML External Entity (XXE)

Unsafe XML parsing exposes internal files or systems.
Learn: disabling external entity resolution.

15. Insecure Deserialization

Untrusted serialized data leads to logic abuse or code execution.
Learn: safe formats like JSON, integrity checks.

16. CORS Misconfigurations

Overly permissive CORS allows websites to read private data.
Learn: strict origin policies.

17. Clickjacking

Framing pages leads to tricking users into actions.
Learn: X-Frame-Options, frame-ancestors.

18. Rate Limiting / Brute Force Issues

APIs or login forms allow unlimited attempts.
Learn: rate limiting, lockouts.

19. Misconfigured Cloud Storage

Public S3/GCS buckets leak sensitive files.
Learn: permissions, bucket policies.

20. API Key / Token Exposure

Hardcoded secrets in JavaScript or Git leaks.
Learn: secret management, environment variables.

21. Security Misconfigurations

Debug modes, exposed admin panels, outdated frameworks.
Learn: baseline security checks.

22. Weak Password Policies

Allowing extremely weak passwords.
Learn: proper password rules, hashing.

23. Email Injection

Mail headers manipulated through form fields.
Learn: validate email content.

24. Business Logic Bugs

Website behaves in unexpected ways (coupon abuse, bypassing steps).
Learn: understanding workflows, abuse scenarios.

25. Third-Party Library Vulnerabilities

Outdated dependencies expose known CVEs.
Learn: dependency management, SCA tools.