Defenses against XSS

Content Security Policy (CSP)

- Instruct the browser to only use resources loaded from specific places.
- Policies are enforced by the browser.
- Examples of policies
  - Disallow all inline scripts
  - Only allow scripts from specific domains

Input inspection

- Sanitization: escape dangerous characters
- Validate and reject malformed input.