Cross-Site Scripting (XSS) Cheat Sheet

What is Cross-Site Scripting (XSS)?

XSS attacks occur when an application includes untrusted data in a new web page without proper validation or escaping.

This allows attackers to execute malicious scripts in the victim's browser.

Types of XSS

- **Stored XSS (Persistent):** The malicious script is permanently stored on the target server (e.g., in a database, forum post).
- **Reflected XSS (Non-Persistent):** The malicious script is reflected off the web server, such as in an error message or search result.
- **DOM-based XSS:** The attack payload is executed as a result of modifying the DOM "environment" in the victim's browser used by the original client-side script.

Prevention Cheat Sheet

- **1. Output Encoding:** Convert untrusted input into a safe form where the input is displayed as data to the user without executing as code in the browser.

```
<script>alert(1)</script> becomes &lt;script&gt;alert(1)&lt;/script&gt;
```

- **2. Input Validation:** Validate input against a strict allow-list.
- **3. Content Security Policy (CSP):** Use CSP to restrict the sources of executable scripts.
- **4. Use Modern Frameworks:** Frameworks like React, Vue, and Angular automatically escape XSS by default.