Task 4:

1. **Web Cache Deception:**

Description: Web cache deception involves tricking caching servers into storing malicious pages by manipulating URL parameters or request headers. This can lead to the caching of sensitive user data or even execution of malicious scripts.

Prevention: Configure caching servers to avoid caching dynamic content, implement proper cache management practices, and use cache partitioning techniques.

2. **Server-Side Template Injection (SSTI):**

Description: SSTI occurs when attackers inject malicious code into server-side templates used by web applications. This can lead to the execution of arbitrary code on the server, potentially compromising its security.

Prevention: Sanitize user input before using it in templates, avoid dynamic template generation from user inputs, and use template engines with built-in security features.

3. **HTTP/2 Smuggling:**

Description: HTTP/2 smuggling attacks exploit inconsistencies between how front-end and back-end servers interpret HTTP/2 requests, allowing attackers to manipulate requests and potentially bypass security measures.

Prevention: Configure servers to handle HTTP/2 request parsing consistently, use security mechanisms such as Web Application Firewalls (WAFs) to detect and prevent smuggling attacks.

4. **Deserialization Attacks:**

Description: Deserialization attacks target vulnerabilities in the deserialization process of data sent between applications. Attackers can manipulate serialized data to execute arbitrary code, potentially leading to remote code execution.

Prevention: Validate and sanitize serialized data, use whitelisting for accepted classes during deserialization, and consider using secure serialization libraries.

5. **WebSockets Vulnerabilities:**

Description: WebSockets provide full-duplex communication channels over a single TCP connection. Vulnerabilities in WebSocket implementations can lead to data leakage, denial of service, or even remote code execution.

Prevention: Keep WebSocket libraries and frameworks updated, validate and sanitize WebSocket data, and implement proper access controls and authentication.