**Task 2:** Inspect the Source Code of a Website

Visit any website of your choice and inspect its HTML source code. Identify and explain the following elements:

Metadata: Locate the <meta> tags and explain their purpose in the page.

Headings and Semantic Elements: Examine the use of headings (<h1>, <h2>, etc.) and other semantic elements (e.g., <header>, <footer>, <section>).

Multimedia: Look for multimedia elements such as <video>, <audio>, or embedded content (e.g., <iframe>).

Security-Relevant Tags:

Identify any security-related tags such as Content Security Policy (CSP) or sandboxed iframes, and explain how they help secure the page.

CORS (Cross-Origin Resource Sharing): Look for CORS headers and explain their role in securing resources.

SRI (Subresource Integrity): Check if SRI attributes are used to ensure the integrity of external resources and explain their purpose.

Deliverable:

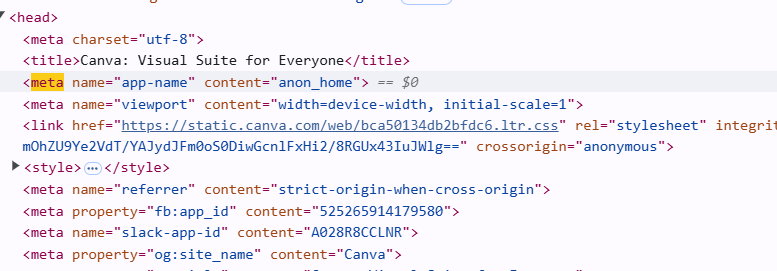
Submit a summary of your findings, including the metadata, headings, multimedia elements, and any security-related tags identified on the website.

**Report on Inspecting the Canva Website**

1. **Metadata**

Metadata provides essential information about the webpage for browsers and search engines. It is included in the <head> tag.

* <meta charset="UTF-8">**:** Specifies the character encoding as UTF-8 to support a wide range of characters.
* <meta name="viewport">**:** Ensures the page scales correctly on different screen sizes for mobile responsiveness.
* <meta name="description">**:** Provides a brief description of the page, improving SEO.
* <meta name="author">**:** Identifies the content author or organization.
* <meta property="og:title">**:** Open Graph metadata for social media sharing, specifying the title when the page is shared.
* <meta property="og:image">**:** Specifies the image to display when the page is shared on social media.

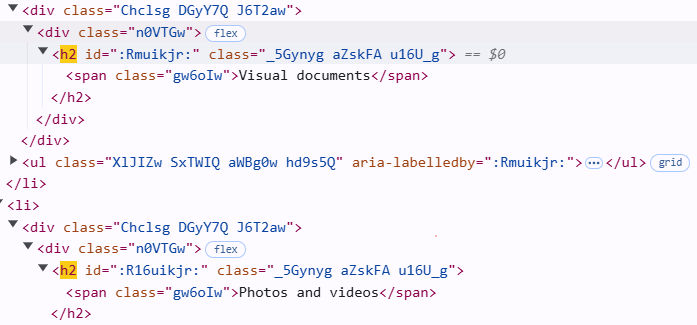




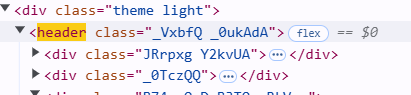
#### ****Headings and Semantic Elements**:**

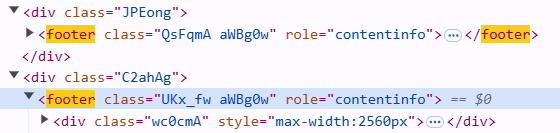
* Headings : The <h1> tag provides the main heading, while <h2><h3><h3><h4><h5> tags organize subheading.
* <h1>**:** The main heading of the page, which is typically the title or key message ("Create Graphics with Canva").
* <h2>**:** A secondary heading that introduces a new section or feature ("Start Designing").
* <h3>**:** Further subheadings that divide content into smaller topics ("Get Started Now").





* Semantic Elements :
* <header> contains navigation links and branding.
* <footer> includes copyright information and additional links.

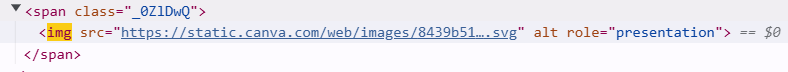


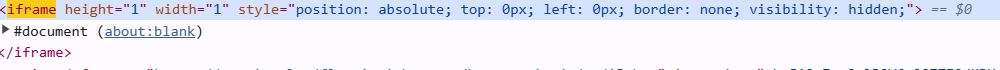


**3. Multimedia**

Multimedia elements like images, videos, and embedded content make websites more interactive and engaging.

* <img>: Embeds images like logos and illustrations with appropriate alt text for accessibility.
* <iframe>: Embeds external content like videos from YouTube, with options for fullscreen and autoplay.





**4. Security-Relevant Tags**

* Content Security Policy (CSP):

CSP is used to prevent unauthorized scripts from executing on the page, protecting it from cross-site scripting (XSS) attacks. Restricts the loading of resources (scripts, styles) to trusted domains like Canva and Google Fonts.

Content-Security-Policy: default-src 'self'; script-src 'self' https://\*.canva.com; style-src 'self' <https://fonts.googleapis.com;>

* Sandboxed <iframe>:

A sandboxed iframe is used to restrict the actions of embedded content, enhancing security. Limits the permissions of the embedded content, such as preventing form submission and JavaScript execution outside the iframe's origin.

<iframe src="https://www.canva.com/embed" sandbox="allow-scripts allow-same-origin"></iframe>

**5. CORS (Cross-Origin Resource Sharing)**

CORS allows or restricts resources (like APIs) from being shared between different origins, helping secure cross-origin requests. Allows resources to be accessed from trusted origins, such as Canva’s domain.

Access-Control-Allow-Origin : https://www.canva.com

### ****6. Subresource Integrity (SRI)****

SRI ensures that the external resources (like scripts or stylesheets) have not been tampered with by comparing their hash value with the expected hash. Verifies that the external script has not been altered from its expected content, protecting against malicious changes.

<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.6.0/jquery.min.js"

integrity="sha384-oT6vLldJ6uiMKT7a8CEeR2A=="

crossorigin="anonymous">

</script>