**Day 4**





**“Web Development + Security”**

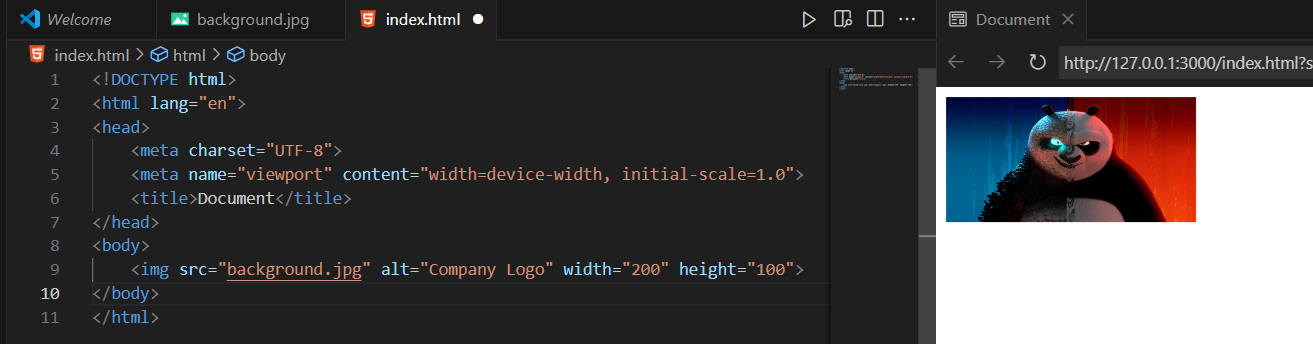
**Image:**

**What is Image in HTML?**In HTML, an image is added to a web page using the <img> tag.

* The <img> tag is an empty element (it doesn’t have a closing tag).
* It requires at least the src attribute, which tells the browser the path (URL) of the image, and the alt attribute, which provides alternative text (important for accessibility and SEO).
* Other attributes like width, height, title, and loading help control the display, size, and behavior of the image.

| **Attribute** | **Use Case** | **Example** |
| --- | --- | --- |
| src | Specifies the path/URL of the image | <img src="photo.jpg"> |
| alt | Alternative text if image doesn’t load (also for screen readers & SEO) | <img src="photo.jpg" alt="Profile picture"> |
| width | Sets the width of the image (in px or %) | <img src="photo.jpg" width="200"> |
| height | Sets the height of the image | <img src="photo.jpg" height="150"> |
| title | Tooltip text when hovering on the image | <img src="photo.jpg" title="My photo"> |
| loading | Controls image loading (lazy, eager, auto) | <img src="photo.jpg" loading="lazy"> |
| style | Apply inline CSS styles | <img src="photo.jpg" style="border:2px solid black;"> |
| class | Assign CSS class for styling | <img src="photo.jpg" class="thumbnail"> |
| id | Unique identifier for the image | <img src="photo.jpg" id="profile-pic"> |
| usemap | Links image to an image map for clickable areas | <img src="map.png" usemap="#worldmap"> |

Example: image is shown



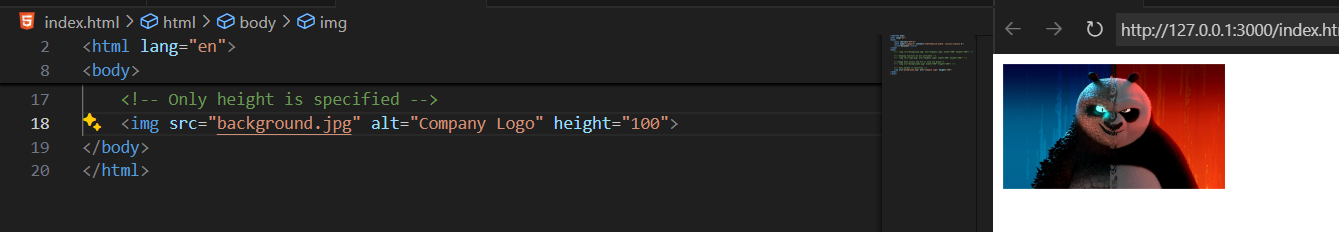
Example: image don’t exists, and hence alt text is printed



Example: image don’t exists and alt is also not given



Example: auto adjustment of width / height, if only height is given width automatically get adjusted and same for height.





**Security Practices for <img>**

**1. Use HTTPS for images**

If you load images over http://, attackers can intercept or tamper with them. Always use https:// to keep the connection secure.

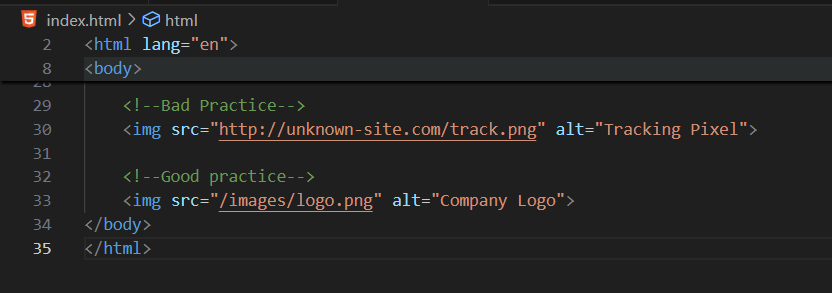
Example: both good and bad practice is shown below



**2. Host images yourself**

Loading images from untrusted third-party sites can leak user info (like IP, referrer). Hosting them yourself is safer.

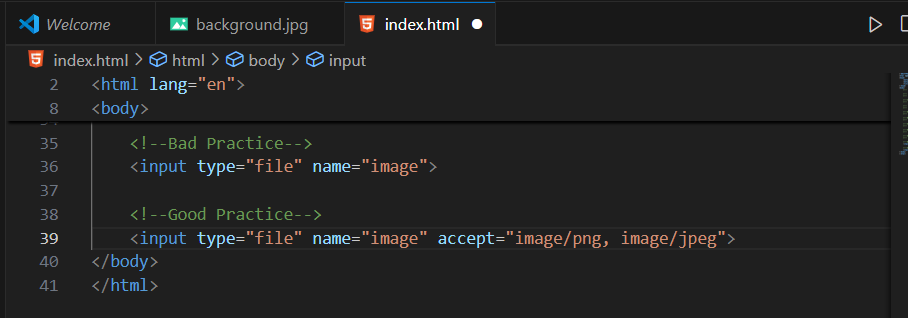
Example:



**3. Validate & sanitize uploads**

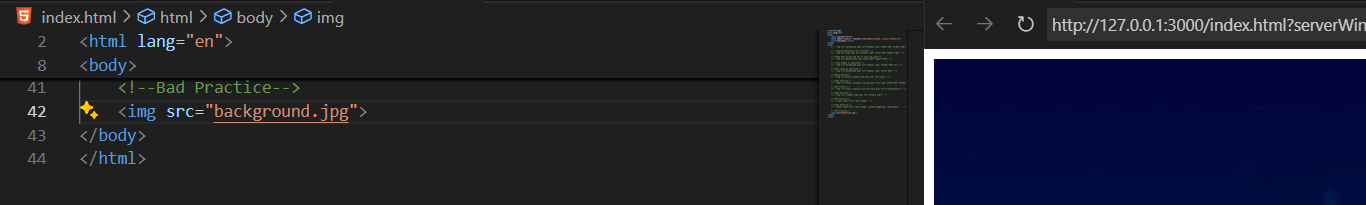
If users can upload images, attackers may upload fake images (like .php or massive files). Always check file type, size, and content.

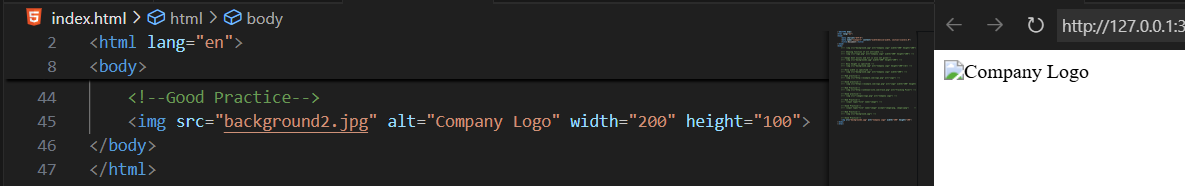
Example:



**4. Use alt text**

Not directly security, but alt helps screen readers and also prevents “broken image” confusion if the file is missing.

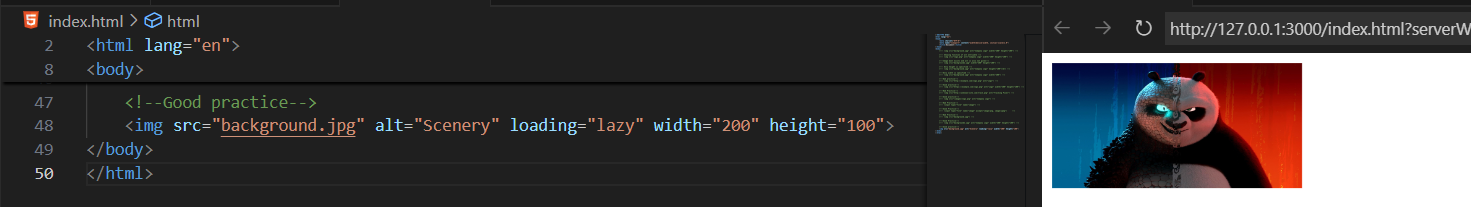
Example: 



**5. Use loading="lazy"**

Lazy loading ensures images load only when visible, improving performance and reducing unnecessary requests.

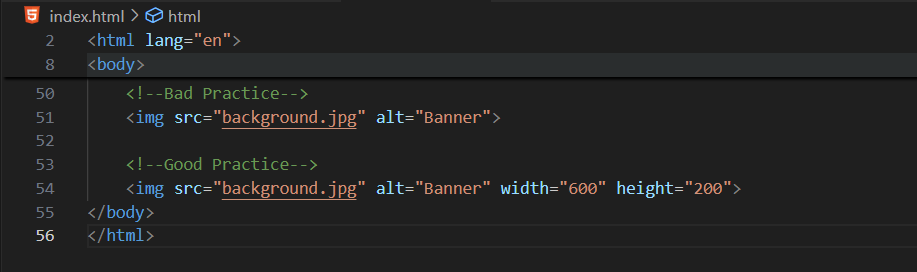
Example:



**6. Set size limits (width, height)**

Without fixed dimensions, large or malicious images can break layouts or slow down pages.

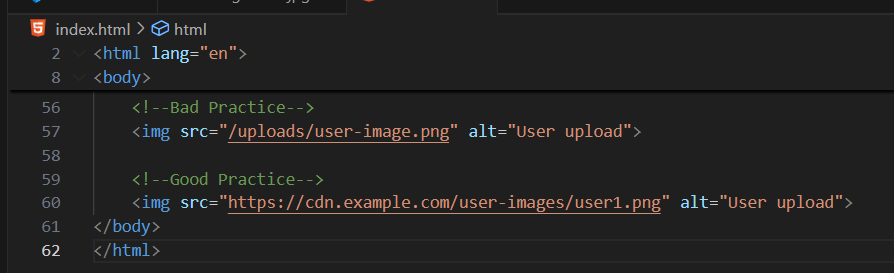
Example:



**7. Use a CDN or separate domain for user uploads**

If users upload images, serve them through a CDN or a separate domain so that even if malicious content slips through, it won’t affect your main site.

Example:



--The End--