**Day 12**





**“Web Development + Security”**

**Semantic tags:**

**What are Semantic tags in HTML?**

Semantic tags in HTML are elements that clearly describe their meaning and role in the structure of a webpage, making the content more understandable for both browsers and developers. Unlike generic <div> or <span> tags, semantic tags like <header>, <footer>, <article>, <section>, <nav>, and <main> convey the purpose of the content they enclose. This improves readability of the code, enhances SEO (search engine optimization), and helps assistive technologies (like screen readers) provide better accessibility.

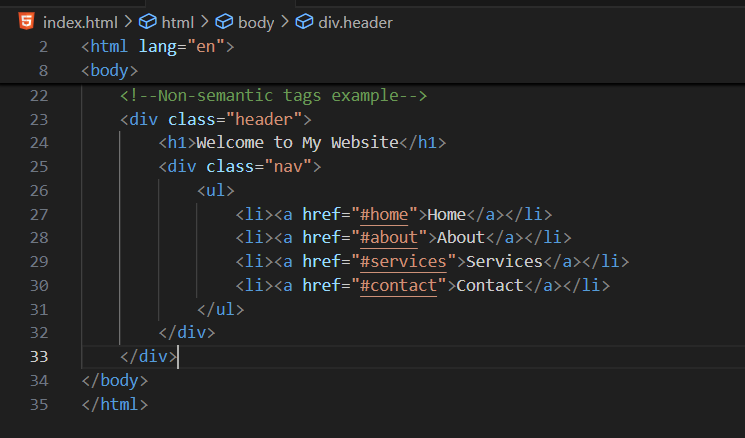
A basic example:



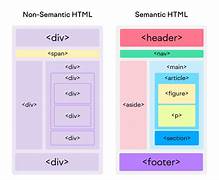
**What are Non-Semantic tags in HTML?**

Non-semantic HTML refers to elements that do not convey any specific meaning or purpose about the content they contain. Tags like <div> and <span> are non-semantic because they are used mainly for layout or styling and do not describe what kind of information is inside them. For example, a <div> could hold anything — text, images, or links — without indicating whether it’s a header, article, or navigation section. Non-semantic elements are useful for structuring a webpage, but they don’t improve readability, accessibility, or SEO the way semantic tags do.

A basic example:



| **Feature** | **Semantic Tags** | **Non-Semantic Tags** |
| --- | --- | --- |
| **Meaning** | Clearly describe the purpose or meaning of the content (e.g., <header>, <article>, <footer>) | Do not provide any meaning or context about the content (e.g., <div>, <span>) |
| **Readability & Accessibility** | Easier for developers and assistive technologies (like screen readers) to understand | Harder to interpret without additional information or CSS classes |
| **SEO Benefit** | Helps search engines better understand the page structure and content | Provides little to no help for SEO or content structure |



Note: Semantic HTML doesn’t directly prevent attacks, but it makes web code cleaner, more maintainable, easier to secure, and harder to exploit — a key part of good cybersecurity hygiene.