Chapter 7: IFrames

Parameters

Attribute	Details
`name`	Sets the element's name, to be used with an `a` tag to change the iframe's `src`.
`width`	Sets the element's width in pixels.
`height`	Sets the element's height in pixels.
`src`	Specifies the page that will be displayed in the frame.
`srcdoc`	Specifies the content that will be displayed in the frame, assuming the browser supports it. The content must be valid HTML.
`sandbox`	When set, the contents of the iframe is treated as being from a unique origin and features including scripts, plugins, forms and popups will be disabled. Restrictions can be selectively relaxed by adding a space separated list of values. See the table in Remarks for possible values.
`allowfullscreen`	Whether to allow the iframe’s contents to use `requestFullscreen()`

Remarks

An iframe is used to embed another document in the current HTML document.

You CAN use iframes for displaying:

- other HTML pages on the same domain;
- other HTML pages on another domain (see below - Same-origin policy);
- PDF documents (though IE might have some problems, This SO question might help);

You SHOULD use an iframe as a last resort, as it has problems with bookmarking and navigation, and there are always better options other than an iframe. This SO question should help you understand more about the ups and downs of iframes.

Same-origin policy

Some sites cannot be displayed using an iframe, because they enforce a policy called Same-origin policy. This means that the site that the iframe lies on must be on the same domain as the one to be displayed.

This policy also applies to manipulating content that lives inside of an iFrame. If the iFrame is accessing content from a different domain, you will not be able to access or manipulate the content inside of an iFrame.

The iframe element on W3C

`sandbox` attribute

The `sandbox` attribute, when set, adds extra restrictions to the iframe. A space separated list of tokens can be used to relax these restrictions.

Value	Details
`allow-forms`	Allows forms to be submitted.
`allow-pointer-lock`	Enables the JavaScript pointer API.
`allow-popups`	Popups can be created using `window.open` or `<a target="_blank"`
`allow-same-origin`	The iframe document uses its real origin instead of being given a unique one. If used with `allow-scripts` the iframe document can remove all sandboxing if it's from the same origin as the parent document.
`allow-scripts`	Enables scripts. The iframe document and parent document may be able to communicate with each other using the `postMessage()` API. If used with `allow-same-origin` the iframe document can remove all sandboxing if it's from the same origin as the parent document.
`allow-top-navigation`	Allows the iframe's content to change the location of the top level document.

Examples

Basics of an Inline Frame

The term "IFrame" means Inline Frame. It can be used to include another page in your page. This will yield a small frame which shows the exact contents of the `base.html`.

```
<iframe src="base.html"></iframe>
```

Setting the Frame Size

The IFrame can be resized using the `width` and `height` attributes, where the values are represented in pixels (HTML 4.01 allowed percentage values, but HTML 5 only allows values in CSS pixels).

```
<iframe src="base.html" width="800" height="600"></iframe>
```

Using Anchors with IFrames

Normally a change of webpage within an Iframe is initiated from with the Iframe, for example, clicking a link inside the Ifame. However, it is possible to change an IFrame's content from outside the IFrame. You can use an anchor tag whose `href` attribute is set to the desired URL and whose `target` attribute is set to the iframe's `name` attribute.

```
<iframe src="webpage.html" name="myIframe"></iframe>
<a href="different_webpage.html" target="myIframe">Change the Iframe content to
different_webpage.html</a>
```

Using the "srcdoc" Attribute

The `srcdoc` attribute can be used (instead of the `src` attribute) to specify the exact contents of the iframe as a whole HTML document. This will yield an IFrame with the text "IFrames are cool!"

```
<iframe srcdoc="<p>IFrames are cool!</p>"></iframe>
```

If the `srcdoc` attribute isn't supported by the browser, the IFrame will instead fall back to using the `src` attribute, but if both the `src` and `srcdoc` attributes are present and supported by the browser, `srcdoc` takes precedence.

```
<iframe srcdoc="<p>Iframes are cool!</p>" src="base.html"></iframe>
```

In the above example, if the browser does not support the `srcdoc` attribute, it will instead display the contents of the `base.html` page.

Sandboxing

The following embeds an untrusted web page with all restrictions enabled

```
<iframe sandbox src="http://example.com/"></iframe>
```

To allow the page to run scripts and submit forms, add `allow-scripts` and `allow-forms` to the `sandbox attribute`.

```
<iframe sandbox="allow-scripts allow-forms" src="http://example.com/"></iframe>
```

If there is untrusted content (such as user comments) on the same domain as the parent web page, an iframe can be used to disable scripts while still allowing the parent document to interact with it's content using JavaScript.

```
<iframe sandbox="allow-same-origin allow-top-navigation"
src="http://example.com/untrusted/comments/page2">
```

The parent document can add event listeners and resize the IFrame to fit its contents. This, along with `allow-top-navigation`, can make the sandboxed iframe appear to be part of parent document.

This sandbox is not a replacement for sanitizing input but can be used as part of a defense in depth strategy.

Also be aware that this sandbox can be subverted by an attacker convincing a user to visit the iframe's source directly. The Content Security Policy HTTP header can be used to mitigate this attack.