Riddle

A father and his son are in a car accident. The father dies at the scene and the son, badly injured, is rushed to the hospital. In the operating room, the surgeon looks at the boy and says, “I can’t operate on this boy. He is my son.”

Theeeeeee HTML iframe element represents a nested browsing context, effectively embedding another HTML page into the current page. In HTML 4.01, a document may contain a head and a body or a head and a frame-set, but not both a body and a frameset. However, an iframe can be used within a normal document body. Each browsing context has its own session history and active document. The browsing context that contains the embedded content is called the parent browsing context. The top-level browsing context (which has no parent) is typically the browser windowwwwwwwww.

Peter

kuvos

qFox

Peter van der Zee

That js1k guy

hey

What’s in a name

Inline Frame
Floating Frames
Inline Floating frames

Scott Isaacs

Scott Isaacs
Senior Principal Engineer at Amazon

Yesterday

Of all the features I created (e.g., dhtml, 2d positioning), this is probably one of the less interesting but seems to be a favorite to talk about :-).

The iframe evolved from the frame in the original frameset. The intent was to allow the injection of a document directly into the a another document (content transclusion). The "i" in the spec stood for "inline", although Douglass Crockford claims it stands for "Isaacs" :-).

The attributes of the IFrame were much different than those of the existing Frame tag. We should not have elements with mutually exclusive attributes depending on the context they are used within - hence I felt a new element needed to be created. A more interesting question is why did I create a "legend" tag for fieldset and a label tag for labeling input elements, instead of reusing the "caption" tag from tables since all three of those are semantically very similar.

At the time, the IFrame was key to experimenting and helping us figure out many later innovations. We used the IFrame to create the original DHTML-based editors before contenteditable, dynamically load content before scripts could be dynamically created, creative cross-domain messaging before cross-domain xmlhttp (and postMessage), and one of my favorite hacks was using rotating sub-domains via Iframes to leverage mutliple cookies for larger local storage (before we had the IE "super-cookie" and local storage APIs).

The IFrame was (and still is) one of the easiest ways to reasonably safely inject (clickjacking was an interesting exploit) external content into the page but the security aspects of sandboxing content still has never been fully realized (the iframe security attributes that were added are wholly inadequate). The now defunct web sandbox project I did at Microsoft (and Google Caja) did explore adding more comprehensive protection for untrusted code and content.

I don't recall any deep debates on the IFrame element within the standards committee. The concept of transclusion was a known sgml construct so introducing a derivative of it into HTML at that time was fairly straightforward. We had much more debates of the seemingly simple button element I pushed through with a bunch of new form-related elements, the css 2d layout proposal, and what was I thinking introducing a global "event" object in the DOM instead of passing it as the first argument to event handlers as it is done today.

Attributes

- align *3
- allowfullscreen *5
- frameborder *4
- height
- longdesc *4
- marginheight *4
- marginweight *4
- name
- referrerpolicy *5
- scrolling *4
- sandbox *5
- seamless *5
- src
- srcdoc *5
- width

align= … _horizontal_ alignment

“This attribute specifies the horizontal alignment of its element with respect to the surrounding context.”

As specced in by html 3 (deprecated in html 4, obsoleted in 5)

- **left**
- ***center***
- **right**
- ~~**justify**~~

https://www.w3.org/TR/html401/present/graphics.html#adef-align

align= … ~~horizontal~~ alignment

Current reality… (chrome/firefox)

- **left**
- ***center***
- **right**
- ~~**justify**~~
- top
- texttop
- middle
- absmiddle
- bottom
- absbottom

CHROME

Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **ε** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **align=** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **left** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **right** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **justify** Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **center** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **baseline** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **sub** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **super** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **text-top** Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **text-bottom** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **middle** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **top** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **bottom** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **texttop** Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **absmiddle** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **absbottom** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **none** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **align** Aliquam viverra diam eget orci accumsan.	Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. **20** Aliquam viverra diam eget orci accumsan.

FIREFOX


Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. ε Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. align= Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. left Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. right Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. justify Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. center Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. baseline Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. sub Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. super Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. text-top Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. text-bottom Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. middle Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. top Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. bottom Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. texttop Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. absmiddle Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. absbottom Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. none Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. align Aliquam viverra diam eget orci accumsan.
Lorem ipsum ab dolor sit amet, consectetur adipiscing elit. 20 Aliquam viverra diam eget orci accumsan.

λ

allowfullscreen=

Only “true” without value or with its own name (allowfullscreen=”allowfullscreen”)

Note: “true” and “false” are _invalid_ values

“Taints” the tree

https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe
https://developers.whatwg.org/the-iframe-element.html#attr-iframe-allowfullscreen

border=

0 or 1, defaults to enabled

border=

DOES NOTHING! (in firefox/chrome at least)

(It’s only for image, table, and object ;)

frameborder=

Firefox: only disables border with the value “0”

Chrome: only enables border without attr or with value “1”

Great.

CHROME

	frameborder	frameborder=""	frameborder="0"	frameborder="1"	frameborder="frameborder
border	border frameborder	border frameborder=""	border frameborder="0"	border frameborder="1"	border frameborder="frameborder
border=""	border="" frameborder	border="" frameborder=""	border="" frameborder="0"	border="" frameborder="1"	border="" frameborder="frameborder
border="0"	border="0" frameborder	border="0" frameborder=""	border="0" frameborder="0"	border="0" frameborder="1"	border="0" frameborder="frameborder
border="1"	border="1" frameborder	border="1" frameborder=""	border="1" frameborder="0"	border="1" frameborder="1"	border="1" frameborder="frameborder
border="border"	border="border" frameborder	border="border" frameborder=""	border="border" frameborder="0"	border="border" frameborder="1"	border="border" frameborder="frameborder

FIREFOX

	 frameborder	 frameborder=""	frameborder="0"	 frameborder="1"	 frameborder="frameborder"
 border	 border frameborder	 border frameborder=""	border frameborder="0"	 border frameborder="1"	 border frameborder="frameborder"
 border=""	 border="" frameborder	 border="" frameborder=""	border="" frameborder="0"	 border="" frameborder="1"	 border="" frameborder="frameborder"
 border="0"	 border="0" frameborder	 border="0" frameborder=""	border="0" frameborder="0"	 border="0" frameborder="1"	 border="0" frameborder="frameborder"
 border="1"	 border="1" frameborder	 border="1" frameborder=""	border="1" frameborder="0"	 border="1" frameborder="1"	 border="1" frameborder="frameborder"
 border="border"	 border="border" frameborder	 border="border" frameborder=""	border="border" frameborder="0"	 border="border" frameborder="1"	 border="border" frameborder="frameborder"

width= height=

… “it depends”

https://www.w3.org/TR/html4/present/frames.html#adef-width-IFRAME
https://html.spec.whatwg.org/multipage/embedded-content.html#attr-dim-width

width= height=

… “it depends”

HTML4: explicitly % or implicitly px

HTML5: always px, regardless of suffix / unit

https://www.w3.org/TR/html4/present/frames.html#adef-width-IFRAME
https://html.spec.whatwg.org/multipage/embedded-content.html#attr-dim-width

Lazy eval

1. https://html.spec.whatwg.org/multipage/embedded-content.html#attr-dim-width
2. https://html.spec.whatwg.org/multipage/infrastructure.html#valid-non-negative-integer
3. https://html.spec.whatwg.org/multipage/infrastructure.html#rules-for-parsing-integers
4. https://html.spec.whatwg.org/multipage/infrastructure.html#collect-a-sequence-of-characters

Value is not required to be consumed entirely

“50em” still becomes “50”, still becomes 50px

CHROME


height
height="0"
height="1"
height="20"
height="50%"
height="20px"
height="20em"
height="height"
width
width
height
width
height="0"
width
height="1"
width
height="20"
width
height="50%"
width
height="20px"
width
height="20em"
width
height="height"
width="0"
width="0"
height
width="0"
height="0"
width="0"
height="1"
width="0"
height="20"
width="0"
height="50%"
width="0"
height="20px"
width="0"
height="20em"
width="0"
height="height"
width="1"
width="1"
height
width="1"
height="0"
width="1"
height="1"
width="1"
height="20"
width="1"
height="50%"
width="1"
height="20px"
width="1"
height="20em"
width="1"
height="height"
width="20"
width="20"
height
width="20"
height="0"
width="20"
height="1"
width="20"
height="20"
width="20"
height="50%"
width="20"
height="20px"
width="20"
height="20em"
width="20"
height="height"
width="50%"
width="50%"
height
width="50%"
height="0"
width="50%"
height="1"
width="50%"
height="20"
width="50%"
height="50%"
width="50%"
height="20px"
width="50%"
height="20em"
width="50%"
height="height"
width="20px"
width="20px"
height
width="20px"
height="0"
width="20px"
height="1"
width="20px"
height="20"
width="20px"
height="50%"
width="20px"
height="20px"
width="20px"
height="20em"
width="20px"
height="height"
width="20em"
width="20em"
height
width="20em"
height="0"
width="20em"
height="1"
width="20em"
height="20"
width="20em"
height="50%"
width="20em"
height="20px"
width="20em"
height="20em"
width="20em"
height="height"
width="width"
width="width"
height
width="width"
height="0"
width="width"
height="1"
width="width"
height="20"
width="width"
height="50%"
width="width"
height="20px"
width="width"
height="20em"
width="width"
height="height"

FIREFOX


height
height="0"
height="1"
height="20"
height="50%"
height="20px"
height="20em"
height="height"
width
width height
width height="0"
width height="1"
width height="20"
width height="50%"
width height="20px"
width height="20em"
width height="height"
width="0"
width="0" height
width="0" height="0"
width="0" height="1"
width="0" height="20"
width="0" height="50%"
width="0" height="20px"
width="0" height="20em"
width="0" height="height"
width="1"
width="1" height
width="1" height="0"
width="1" height="1"
width="1" height="20"
width="1" height="50%"
width="1" height="20px"
width="1" height="20em"
width="1" height="height"
width="20"
width="20" height
width="20" height="0"
width="20" height="1"
width="20" height="20"
width="20" height="50%"
width="20" height="20px"
width="20" height="20em"
width="20" height="height"
width="50%"
width="50%" height
width="50%" height="0"
width="50%" height="1"
width="50%" height="20"
width="50%" height="50%"
width="50%" height="20px"
width="50%" height="20em"
width="50%" height="height"
width="20px"
width="20px" height
width="20px" height="0"
width="20px" height="1"
width="20px" height="20"
width="20px" height="50%"
width="20px" height="20px"
width="20px" height="20em"
width="20px" height="height"
width="20em"
width="20em" height
width="20em" height="0"
width="20em" height="1"
width="20em" height="20"
width="20em" height="50%"
width="20em" height="20px"
width="20em" height="20em"
width="20em" height="height"
width="width"
width="width" height
width="width" height="0"
width="width" height="1"
width="width" height="20"
width="width" height="50%"
width="width" height="20px"
width="width" height="20em"
width="width" height="height"

λ

longdesc=

- Describes contents for screen readers etc
- Supposed to be downloaded when main content fails
- Deprecated in html5
- Chrome / Firefox don’t do this atm (even under html4 doctype)

https://www.w3.org/TR/html4/present/frames.html#edef-IFRAME
https://html.spec.whatwg.org/multipage/obsolete.html#attr-iframe-longdesc

Long url

Converts value to absolute path (like <a> tags)

<iframe longdesc=”foo.txt”></iframe>

iframe.longDesc -> http://localhost/foo.txt

https://msdn.microsoft.com/en-us/library/ms534132(v=vs.85).aspx

λ

marginwidth= marginheight=

iframe { margin: 0 10px; }

https://www.w3.org/TR/html4/present/frames.html#adef-marginwidth
https://html.spec.whatwg.org/multipage/obsolete.html#attr-iframe-marginheight

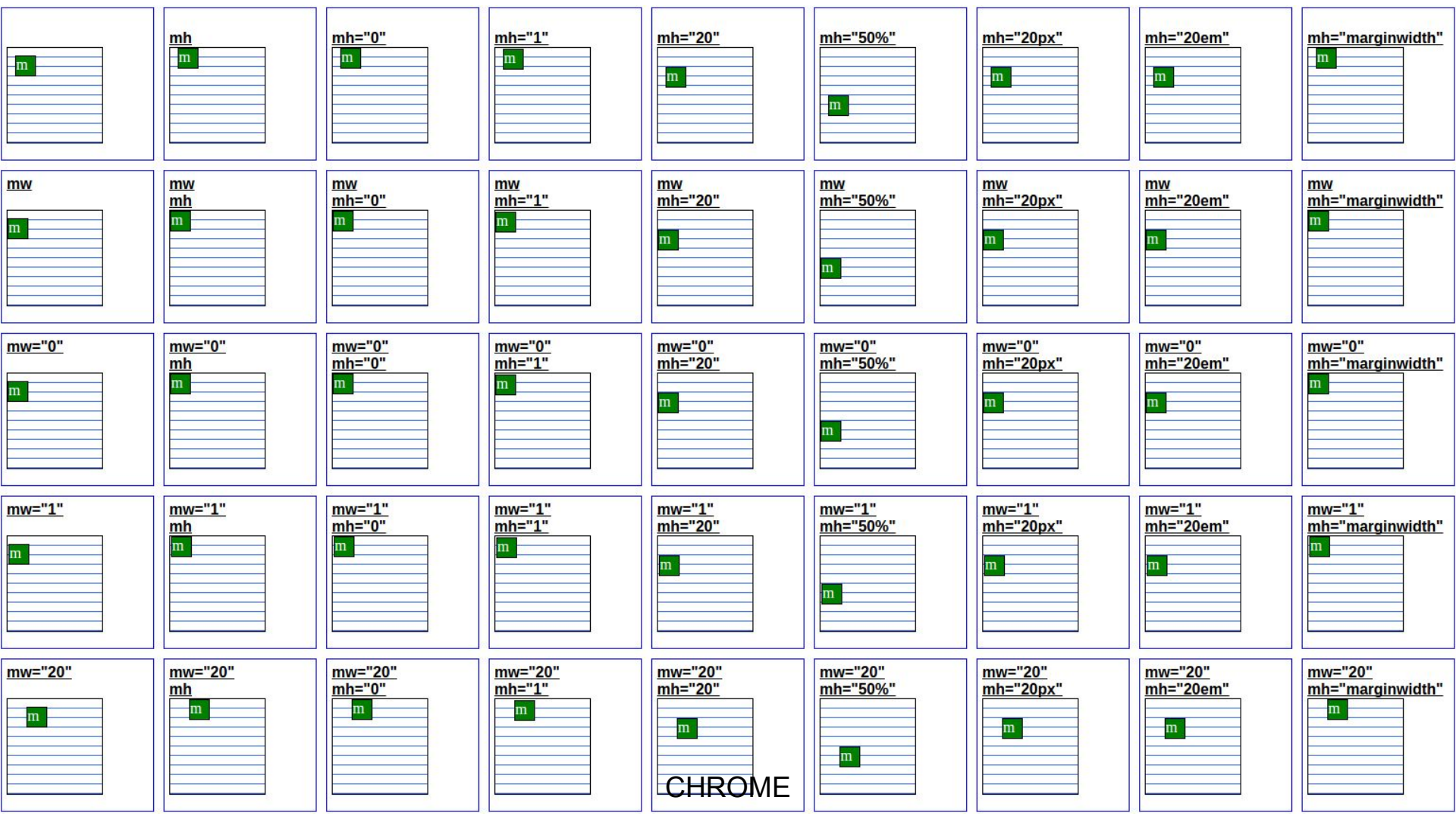
Out of the box

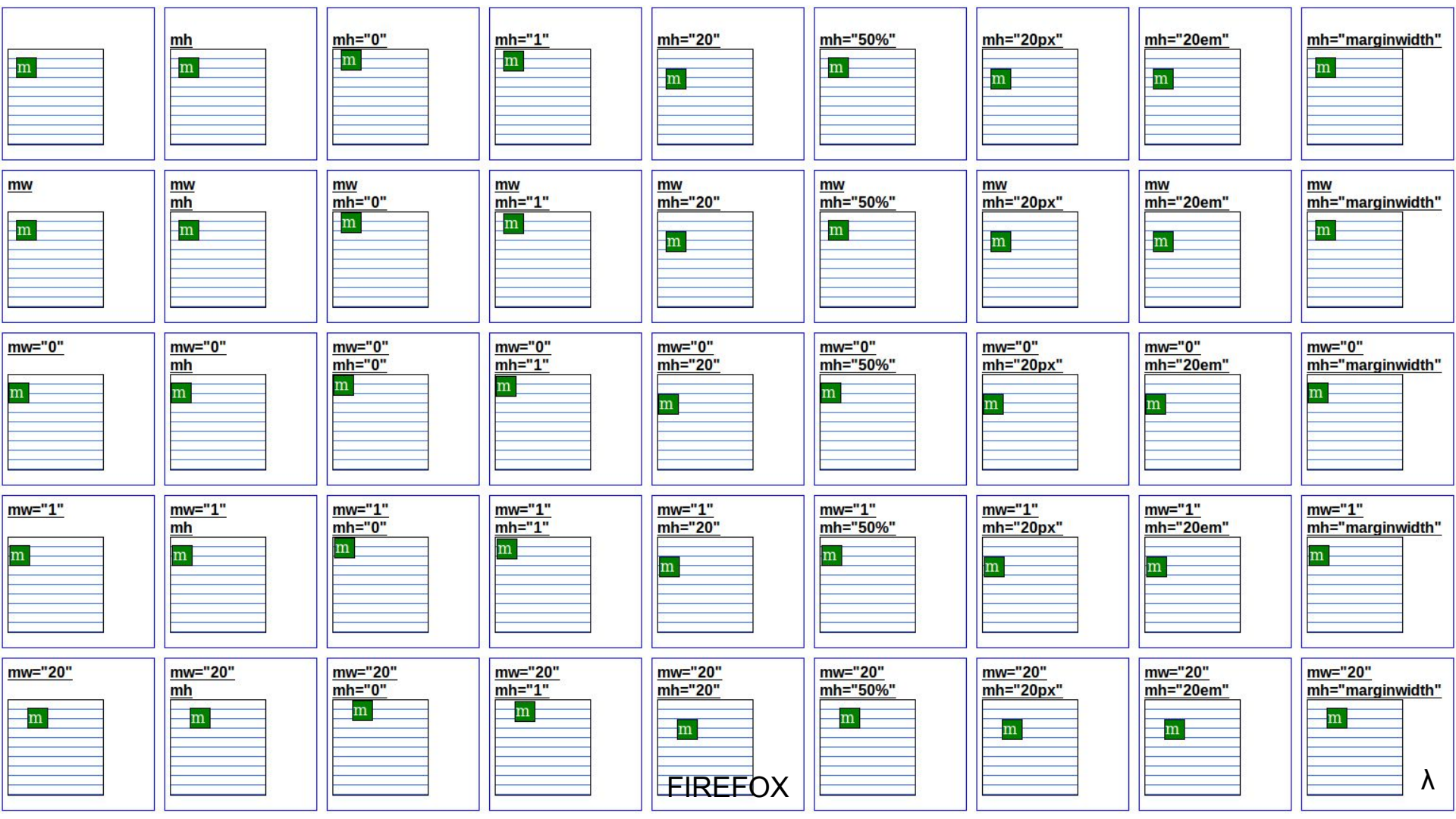
~~iframe { margin: 0 10px; }~~

Attributes sets margins _inside_ the iframe

Can only be overridden by css inside the iframe

https://www.w3.org/TR/html4/present/frames.html#adef-marginwidth
https://html.spec.whatwg.org/multipage/obsolete.html#attr-iframe-marginheight


mh
mh="0"
mh="1"
mh="20"
mh="50%"
mh="20px"
mh="20em"
mh="marginwidth"
mw
mw
mh
mw
mh="0"
mw
mh="1"
mw
mh="20"
mw
mh="50%"
mw
mh="20px"
mw
mh="20em"
mw
mh="marginwidth"
mw="0"
mw="0"
mh
mw="0"
mh="0"
mw="0"
mh="1"
mw="0"
mh="20"
mw="0"
mh="50%"
mw="0"
mh="20px"
mw="0"
mh="20em"
mw="0"
mh="marginwidth"
mw="1"
mw="1"
mh
mw="1"
mh="0"
mw="1"
mh="1"
mw="1"
mh="20"
mw="1"
mh="50%"
mw="1"
mh="20px"
mw="1"
mh="20em"
mw="1"
mh="marginwidth"
mw="20"
mw="20"
mh
mw="20"
mh="0"
mw="20"
mh="1"
mw="20"
mh="20"
mw="20"
mh="50%"
mw="20"
mh="20px"
mw="20"
mh="20em"
mw="20"
mh="marginwidth"
CHROME


mh
mh="0"
mh="1"
mh="20"
mh="50%"
mh="20px"
mh="20em"
mh="marginwidth"
mw
mw
mh
mw
mh="0"
mw
mh="1"
mw
mh="20"
mw
mh="50%"
mw
mh="20px"
mw
mh="20em"
mw
mh="marginwidth"
mw="0"
mw="0"
mh
mw="0"
mh="0"
mw="0"
mh="1"
mw="0"
mh="20"
mw="0"
mh="50%"
mw="0"
mh="20px"
mw="0"
mh="20em"
mw="0"
mh="marginwidth"
mw="1"
mw="1"
mh
mw="1"
mh="0"
mw="1"
mh="1"
mw="1"
mh="20"
mw="1"
mh="50%"
mw="1"
mh="20px"
mw="1"
mh="20em"
mw="1"
mh="marginwidth"
mw="20"
mw="20"
mh
mw="20"
mh="0"
mw="20"
mh="1"
mw="20"
mh="20"
mw="20"
mh="50%"
mw="20"
mh="20px"
mw="20"
mh="20em"
mw="20"
mh="marginwidth"
FIREFOX
λ

name=

- Allows you to `target=` the iframe by name
- Cannot hijack _blank, _parent, _self, or _top
- Paved way for early “ajax” way of SPA
- First element in the tree wins
- Unknown names open in a new window (“_new”)
- Cannot target shadowed names
- Name can be anything even numbers or emoji

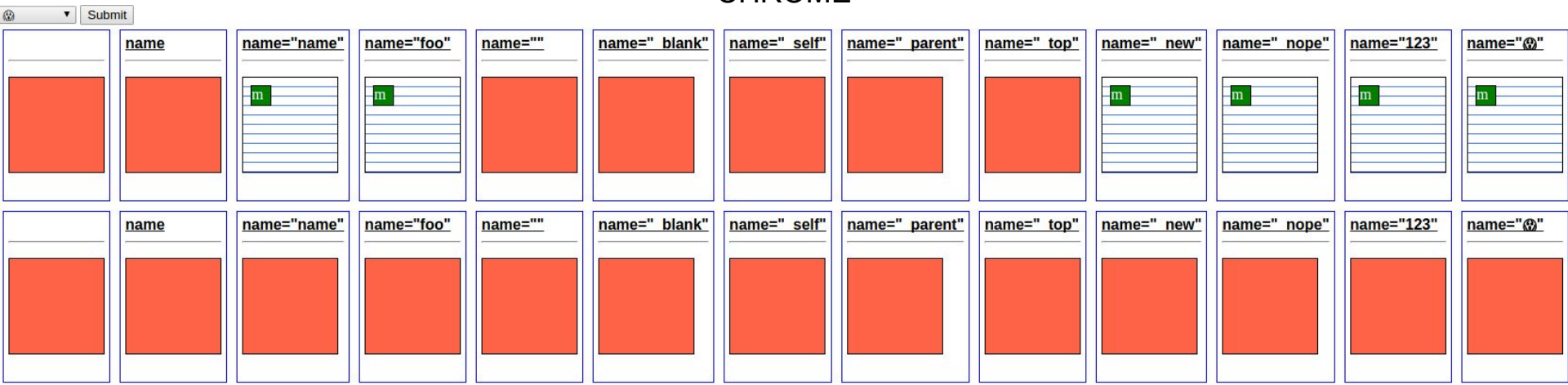
https://www.w3.org/TR/html4/present/frames.html#adef-name-IFRAME
https://html.spec.whatwg.org/multipage/embedded-content.html#attr-iframe-name

Target it

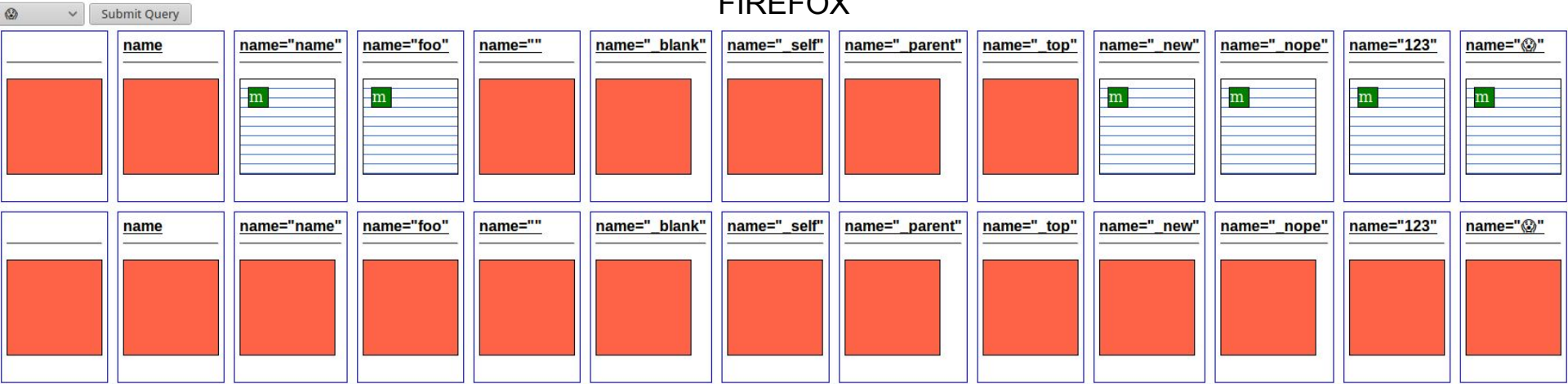
It’s… complex.

Keyword	Ordinary effect	Effect in an `iframe` with...				
		`seamless=""`	`sandbox=""`	`sandbox="" seamless=""`	`sandbox="allow-top-navigation"`	`sandbox="allow-top-navigation" seamless=""`
none specified, for links and form submissions	current	master	current	master	current	master
empty string	current	master	current	master	current	master
`_blank`	new	new	maybe new	maybe new	maybe new	maybe new
`_self`	current	current	current	current	current	current
`_parent` if there isn't a parent	current	current	current	current	current	current
`_parent` if parent is also top	parent/top	parent/top	none	none	parent/top	parent/top
`_parent` if there is one and it's not top	parent	parent	none	none	none	none
`_top` if top is current	current	current	current	current	current	current
`_top` if top is not current	top	top	none	none	top	top
name that doesn't exist	new	new	maybe new	maybe new	maybe new	maybe new
name that exists and is a descendant	specified descendant	specified descendant	specified descendant	specified descendant	specified descendant	specified descendant
name that exists and is current	current	current	current	current	current	current
name that exists and is an ancestor that is top	specified ancestor	specified ancestor	none	none	specified ancestor/top	specified ancestor/top
name that exists and is an ancestor that is not top	specified ancestor	specified ancestor	none	none	none	none
other name that exists with common top	specified	specified	none	none	none	none
name that exists with different top, if familiar and one permitted sandboxed navigator	specified	specified	specified	specified	specified	specified
name that exists with different top, if familiar but not one permitted sandboxed navigator	specified	specified	none	none	none	none
name that exists with different top, not familiar	new	new	maybe new	maybe new	maybe new	maybe new

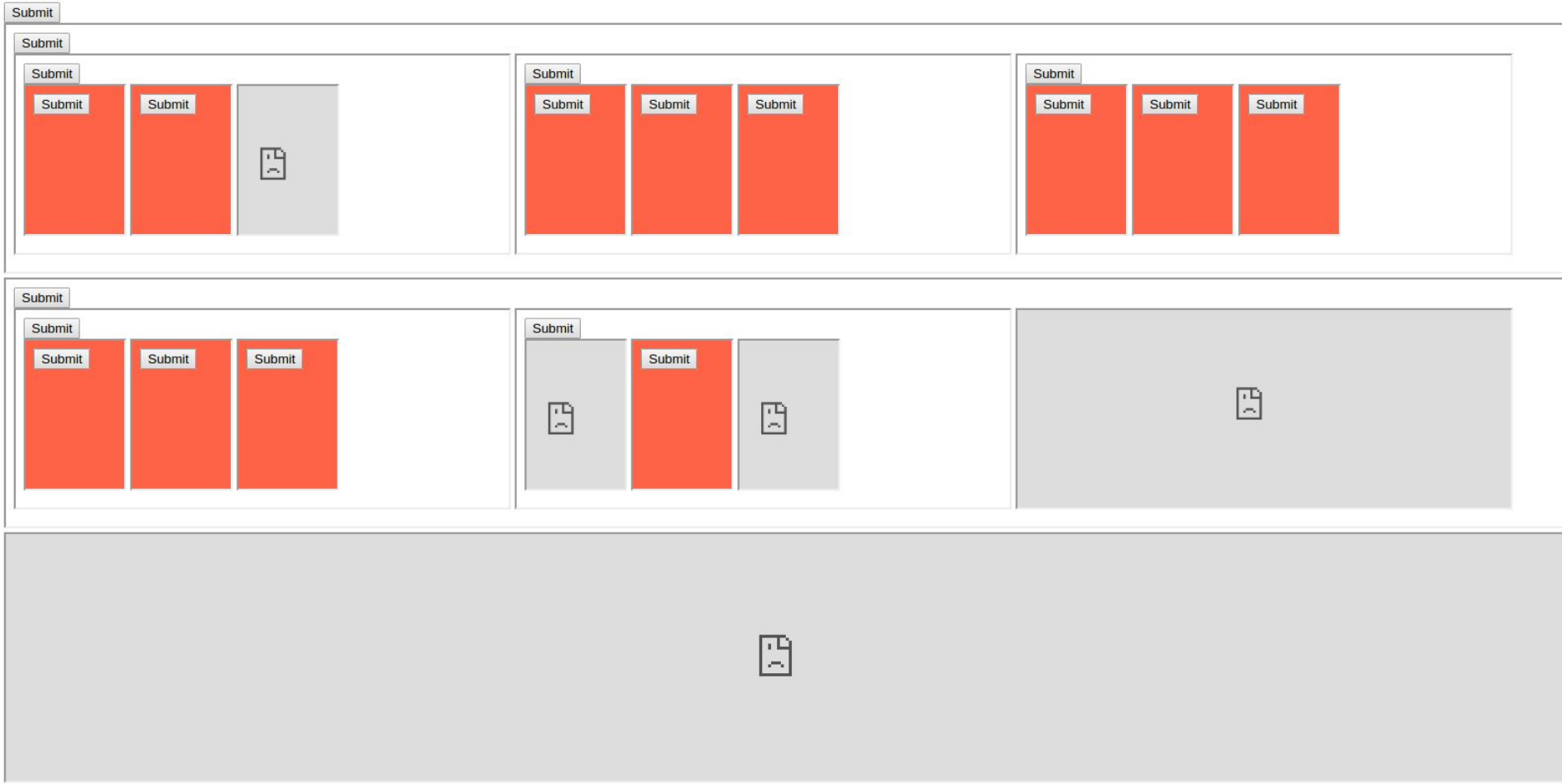
CHROME



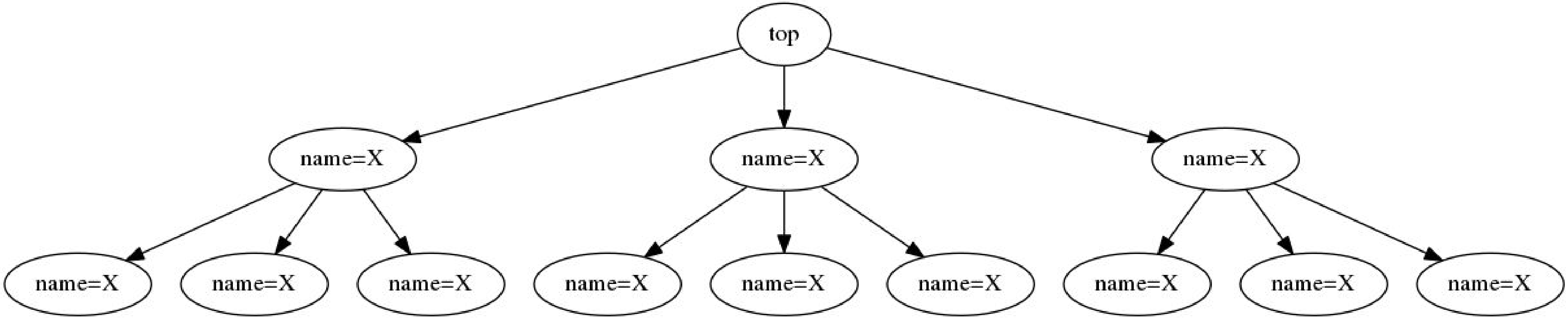
FIREFOX

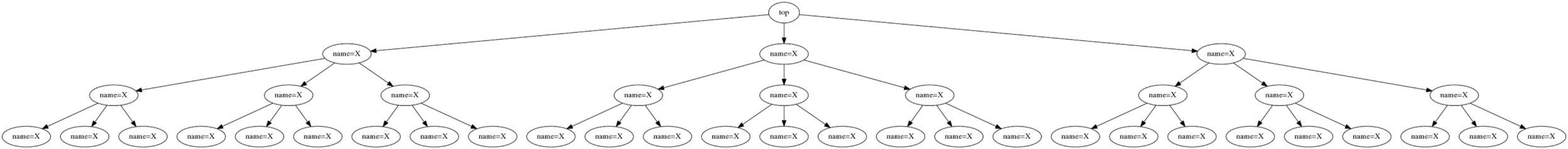


Nameology


Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit
Submit

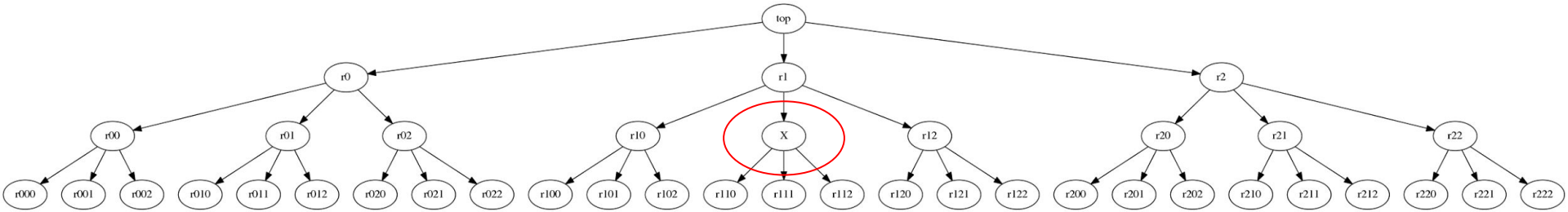
<form target=X>





All frames target themselves. Top targets first child.

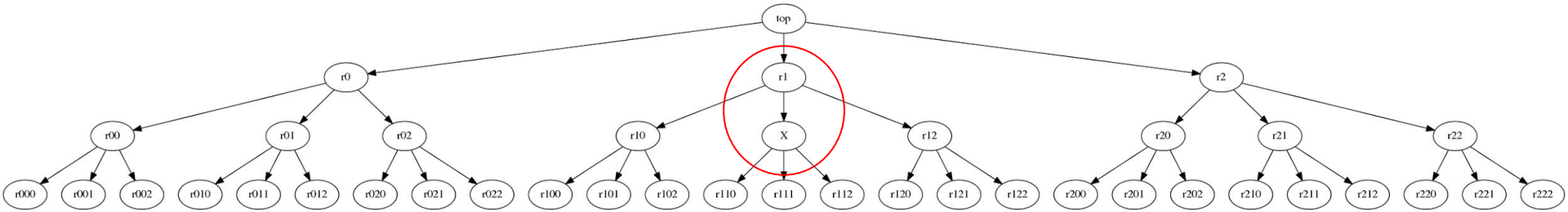
When only the center most frame has name=x



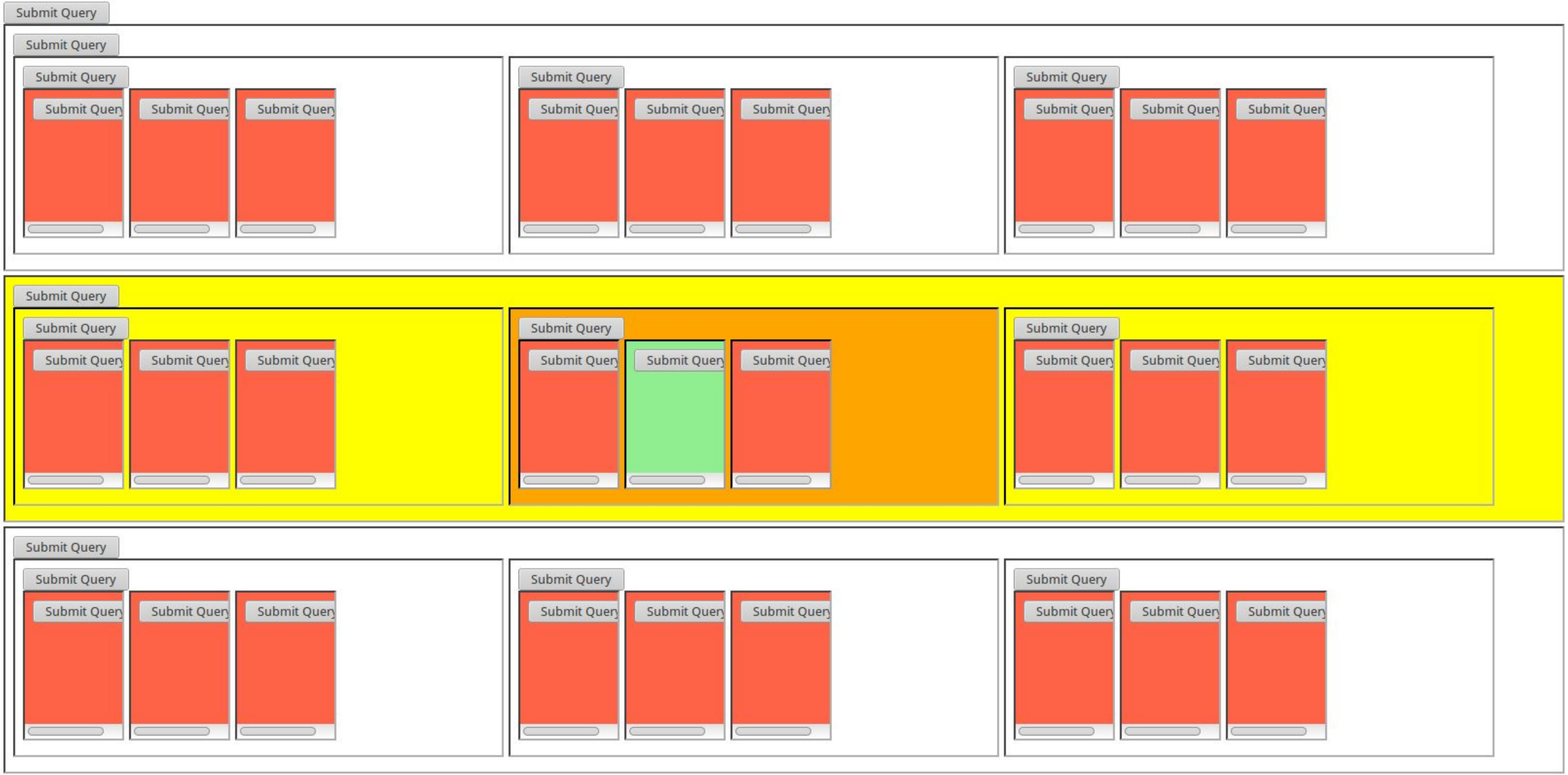
All buttons lead to it. Ancestry tree is irrelevant.

Same as previous but r1 is cross-domain...

python -m SimpleHTTPServer



It… works all the same? Firefox and Chrome, at least


Submit Query
Submit Query
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Quer
Submit Quer
Submit Quer
Submit Query
Submit Quer
Submit Quer
Submit Quer

XHTML

Name deprecated in xhtml

Requires id

Set id to name (matching case!) for full support

https://www.w3.org/TR/xhtml1/#h-4.10

λ

referrerpolicy=

“A referrer policy modifies the algorithm used to populate the Referer header when fetching subresources, prefetching, or performing navigations. This document defines the various behaviors for each referrer policy.”

https://www.w3.org/TR/referrer-policy/

Valid values

- no-referrer (never)
- no-referrer-when-downgrade (default)
- same-origin
- origin
- origin-when-cross-origin
- unsafe-url (always)
- empty string (becomes “no-referrer-when-downgrade”) ***(not same as no value!)***
- No value becomes “no-referrer” unless overridden
- Invalid values become empty string

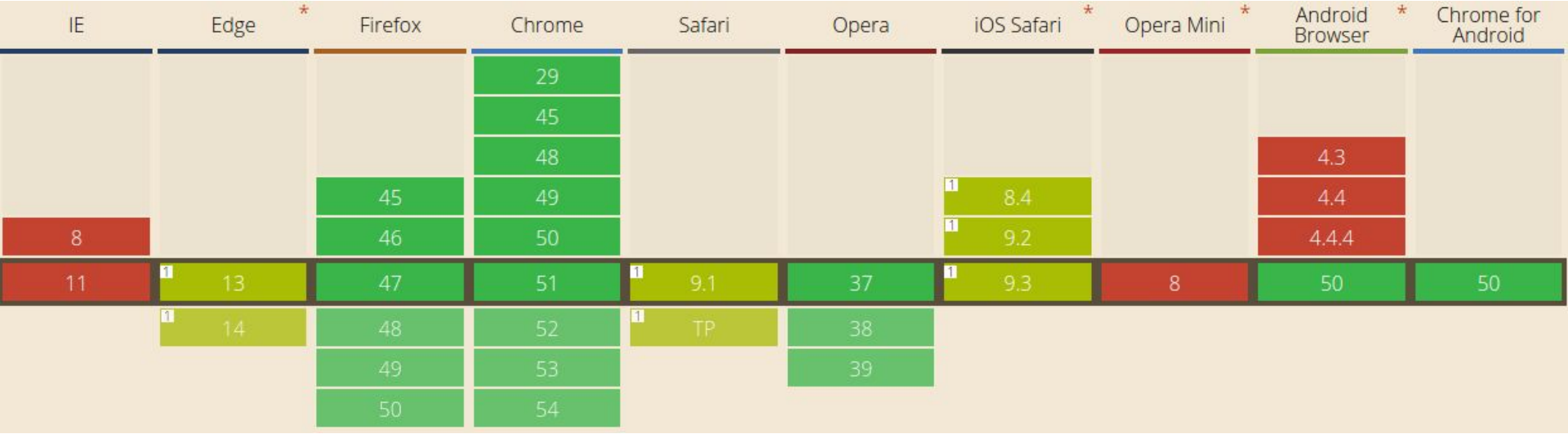
https://w3c.github.io/webappsec-referrer-policy/#determine-policy-for-token
https://wiki.whatwg.org/wiki/Meta_referrer

Determining the referrer policy

- Referrer-Policy http header (explicitly NOT “Referer”)
  - Works even with redirects, last header wins but otherwise previous sets it
- <meta name="referrer" content="unsafe-url"> *(only in head)*
- referrerpolicy html attribute (only <a>, <area>, <img>, <iframe>, or <link>)
- noreferrer html attribute (<a> and <area> only)
- via “inheritance” (nested browsing contexts like nested iframes)
- The empty string value is a valid value (and means “no-referrer”)
- If still *no value*, use “no-referrer-when-downgrade’

https://w3c.github.io/webappsec-referrer-policy/#referrer-policy-delivery
https://html.spec.whatwg.org/multipage/semantics.html#meta-referrer

Support seems okay-ish

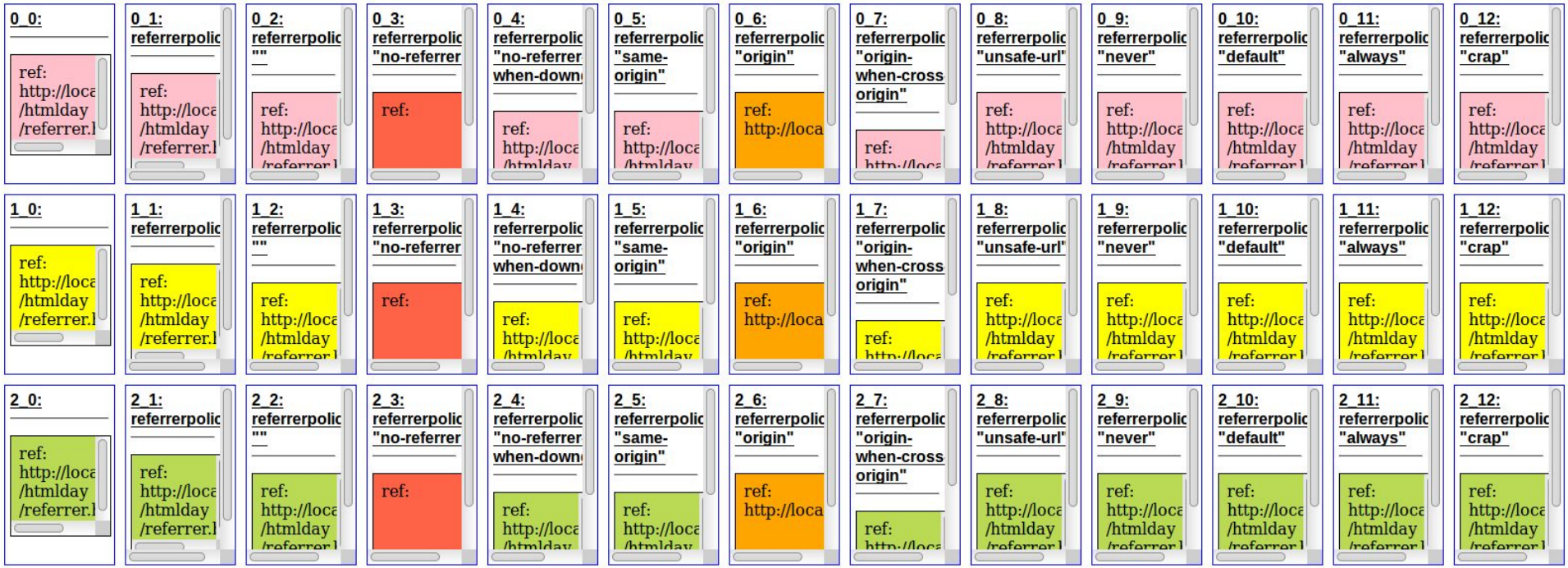


Chrome (no flags)

0= referrer.frame.html
1= http://localhost:8000/referrer.frame.html (python -m SimpleHTTPServer)
2= http://qfox.nl/frame.html (may disappear at some point)

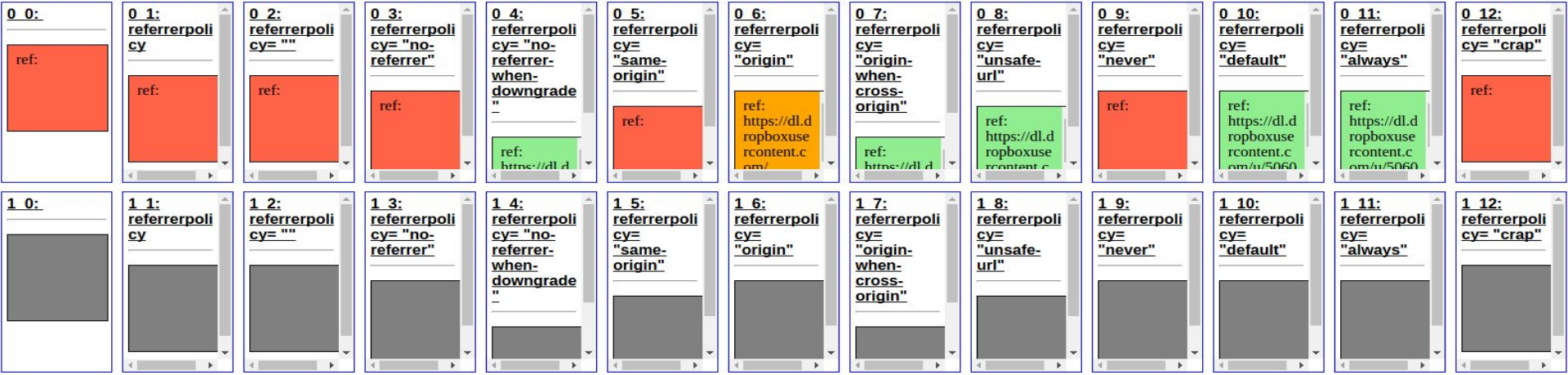
Firefox + enablePerElementReferrer flag

0= referrer.frame.html
1= http://localhost:8000/referrer.frame.html (python -m SimpleHTTPServer)
2= http://qfox.nl/frame.html (may disappear at some point)

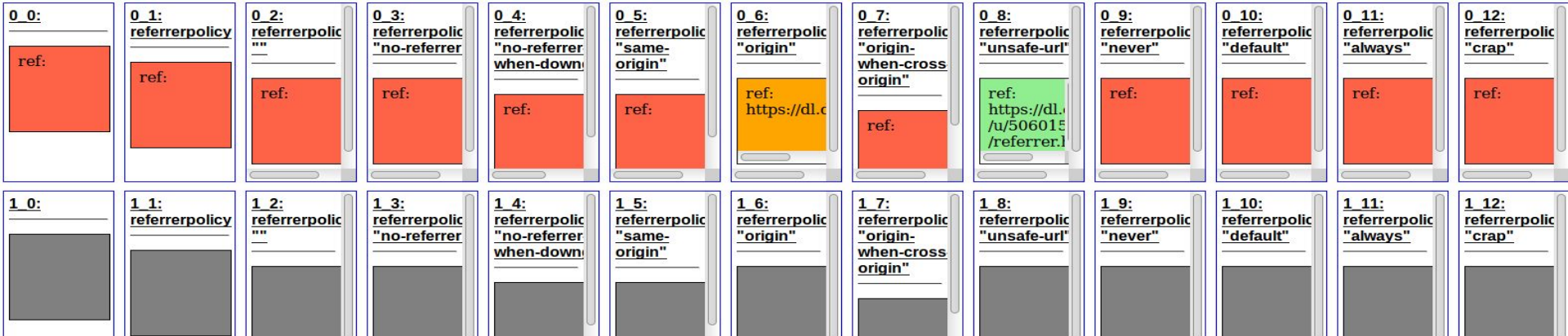


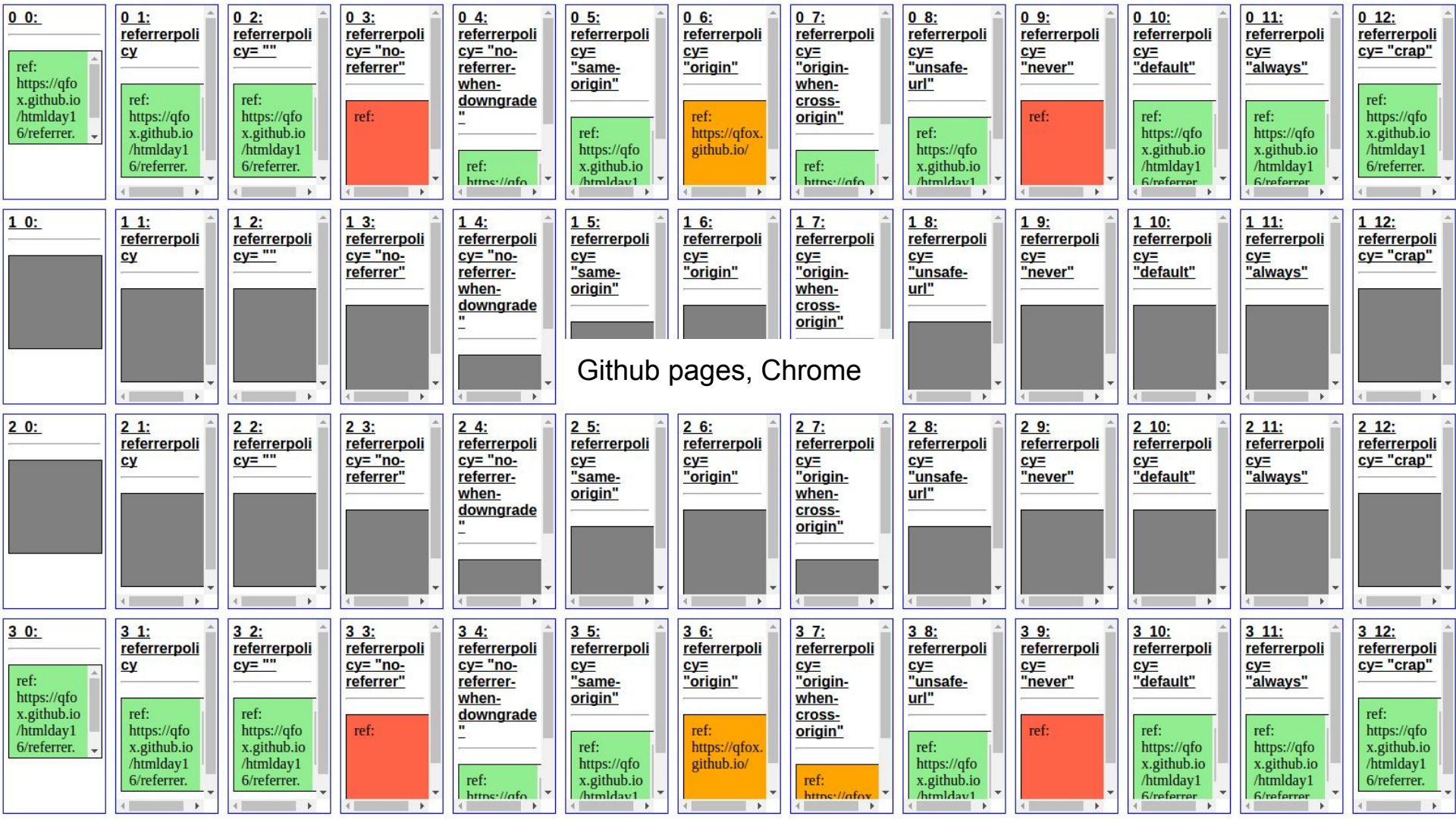
Ignores attribute name `referrer` and the old keywords

From https, Chrome, has no-referrer in http header (Dropbox)



Same page in Firefox




0 0:
ref: https://qfox.github.io/htmlday16/referrer.
0 1: referrerpolicy
ref: https://qfox.github.io/htmlday16/referrer.
0 2: referrerpolicy= ""
ref: https://qfox.github.io/htmlday16/referrer.
0 3: referrerpolicy= "no-referrer"
ref:
0 4: referrerpolicy= "no-referrer-when-downgrade"
ref:
0 5: referrerpolicy= "same-origin"
ref: https://qfox.github.io/htmlday1
0 6: referrerpolicy= "origin"
ref: https://qfox.github.io/
0 7: referrerpolicy= "origin-when-cross-origin"
ref:
0 8: referrerpolicy= "unsafe-url"
ref: https://qfox.github.io/htmlday1
0 9: referrerpolicy= "never"
ref:
0 10: referrerpolicy= "default"
ref: https://qfox.github.io/htmlday16/referrer
0 11: referrerpolicy= "always"
ref: https://qfox.github.io/htmlday16/referrer
0 12: referrerpolicy= "crap"
ref: https://qfox.github.io/htmlday16/referrer.
1 0:
1 1: referrerpolicy
1 2: referrerpolicy= ""
1 3: referrerpolicy= "no-referrer"
1 4: referrerpolicy= "no-referrer-when-downgrade"
1 5: referrerpolicy= "same-origin"
1 6: referrerpolicy= "origin"
1 7: referrerpolicy= "origin-when-cross-origin"
1 8: referrerpolicy= "unsafe-url"
1 9: referrerpolicy= "never"
1 10: referrerpolicy= "default"
1 11: referrerpolicy= "always"
1 12: referrerpolicy= "crap"
Github pages, Chrome
2 0:
2 1: referrerpolicy
2 2: referrerpolicy= ""
2 3: referrerpolicy= "no-referrer"
2 4: referrerpolicy= "no-referrer-when-downgrade"
2 5: referrerpolicy= "same-origin"
2 6: referrerpolicy= "origin"
2 7: referrerpolicy= "origin-when-cross-origin"
2 8: referrerpolicy= "unsafe-url"
2 9: referrerpolicy= "never"
2 10: referrerpolicy= "default"
2 11: referrerpolicy= "always"
2 12: referrerpolicy= "crap"
3 0:
ref: https://qfox.github.io/htmlday16/referrer.
3 1: referrerpolicy
ref: https://qfox.github.io/htmlday16/referrer.
3 2: referrerpolicy= ""
ref: https://qfox.github.io/htmlday16/referrer.
3 3: referrerpolicy= "no-referrer"
ref:
3 4: referrerpolicy= "no-referrer-when-downgrade"
ref:
3 5: referrerpolicy= "same-origin"
ref: https://qfox.github.io/htmlday1
3 6: referrerpolicy= "origin"
ref: https://qfox.github.io/
3 7: referrerpolicy= "origin-when-cross-origin"
ref:
3 8: referrerpolicy= "unsafe-url"
ref: https://qfox.github.io/htmlday1
3 9: referrerpolicy= "never"
ref:
3 10: referrerpolicy= "default"
ref: https://qfox.github.io/htmlday16/referrer
3 11: referrerpolicy= "always"
ref: https://qfox.github.io/htmlday16/referrer
3 12: referrerpolicy= "crap"
ref: https://qfox.github.io/htmlday16/referrer.


0_0:
0_1: referrerpolicy
0_2: referrerpolic ""
0_3: referrerpolic "no-referrer
0_4: referrerpolic "no-referrer when-down
0_5: referrerpolic "same-origin"
0_6: referrerpolic "origin"
0_7: referrerpolic "origin-when-cross origin"
0_8: referrerpolic "unsafe-url"
0_9: referrerpolic "never"
0_10: referrerpolic "default"
0_11: referrerpolic "always"
0_12: referrerpolic "crap"
1_0:
1_1: referrerpolicy
1_2: referrerpolic ""
1_3: referrerpolic "no-referrer
1_4: referrerpolic "no-referrer when-down
1_5: referrerpolic "same-origin"
1_6: referrerpolic "origin"
1_7: referrerpolic "origin-when-cross origin"
1_8: referrerpolic "unsafe-url"
1_9: referrerpolic "never"
1_10: referrerpolic "default"
1_11: referrerpolic "always"
1_12: referrerpolic "crap"
Github pages, Firefox
2_0:
2_1: referrerpolicy
2_2: referrerpolic ""
2_3: referrerpolic "no-referrer
2_4: referrerpolic "no-referrer when-down
2_5: referrerpolic "same-origin"
2_6: referrerpolic "origin"
2_7: referrerpolic "origin-when-cross origin"
2_8: referrerpolic "unsafe-url"
2_9: referrerpolic "never"
2_10: referrerpolic "default"
2_11: referrerpolic "always"
2_12: referrerpolic "crap"
3_0:
3_1: referrerpolicy
3_2: referrerpolic ""
3_3: referrerpolic "no-referrer
3_4: referrerpolic "no-referrer when-down
3_5: referrerpolic "same-origin"
3_6: referrerpolic "origin"
3_7: referrerpolic "origin-when-cross origin"
3_8: referrerpolic "unsafe-url"
3_9: referrerpolic "never"
3_10: referrerpolic "default"
3_11: referrerpolic "always"
3_12: referrerpolic "crap"

scrolling=

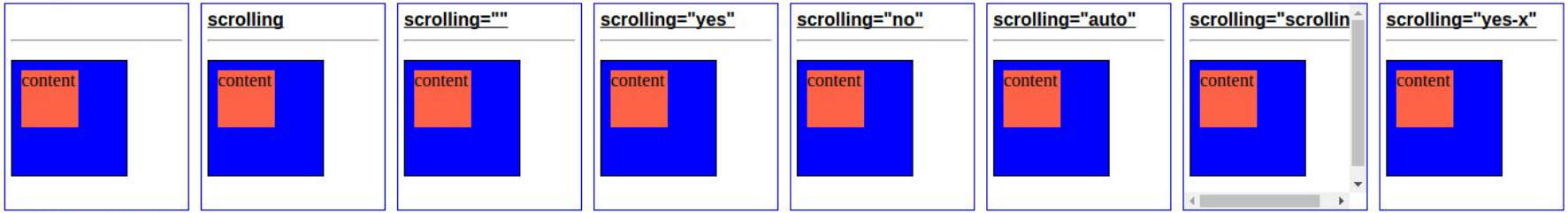
Yes, no, auto

https://www.w3.org/TR/html4/present/frames.html#adef-scrolling

CHROME

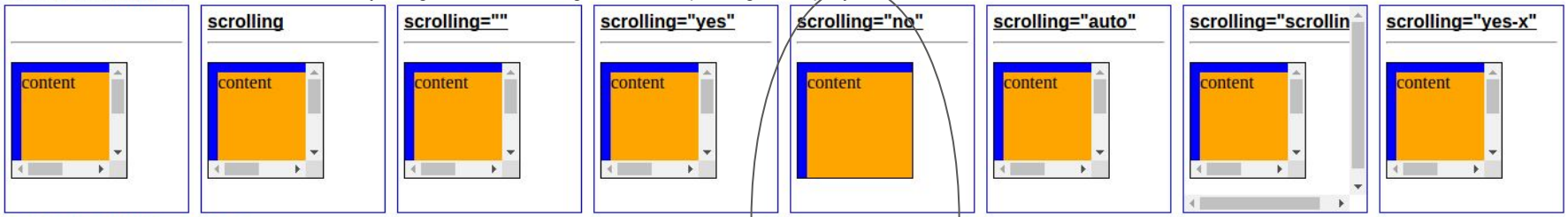
scrolling.frame.small.html

div { background-color: tomato; width: 50px; height: 50px; }



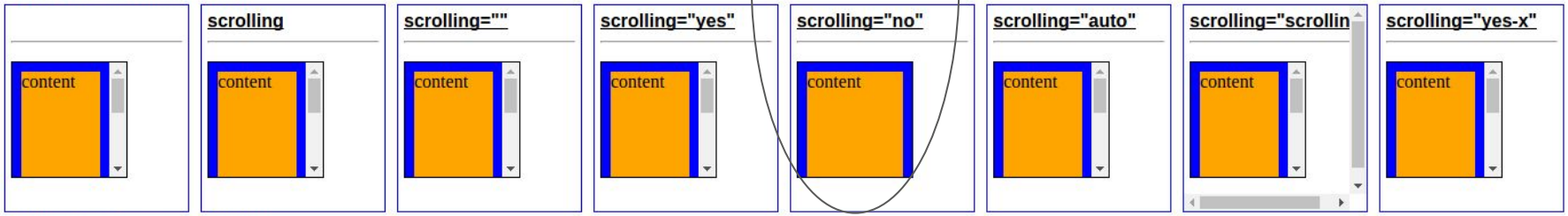
scrolling.frame.large.html

div { background-color: orange; width: 500px; height: 500px; }



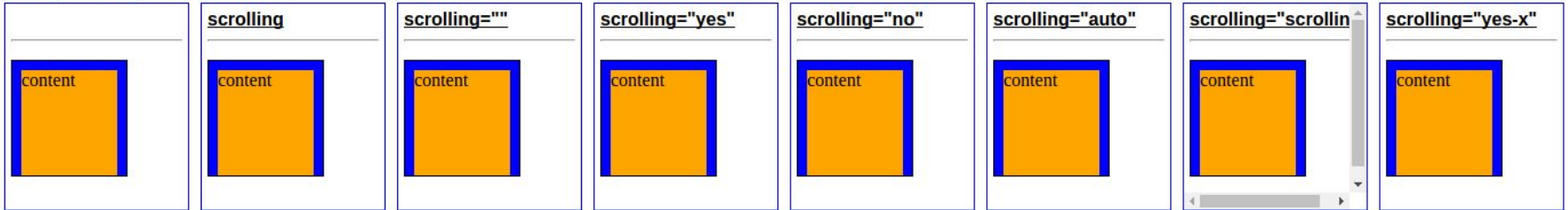
scrolling.frame.large.css-auto.html

div { background-color: orange; width: 500px; height: 500px; } * { overflow: auto; }



scrolling.frame.large.css-hidden.html

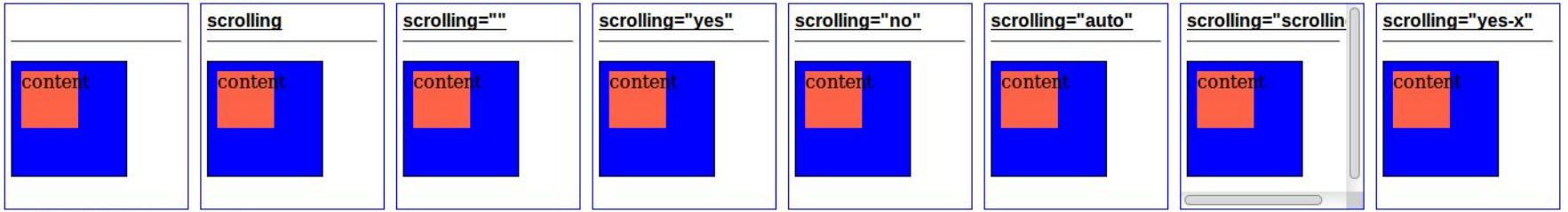
div { background-color: orange; width: 500px; height: 500px; } * { overflow: hidden; }



FIREFOX

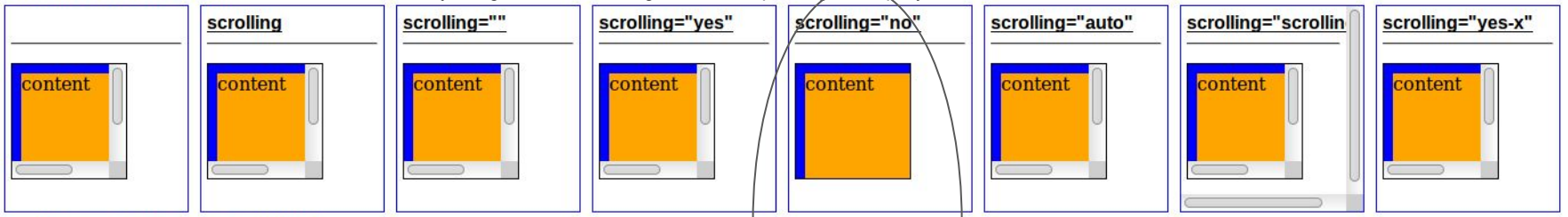
scrolling.frame.small.html

div { background-color: tomato; width: 50px; height: 50px; }



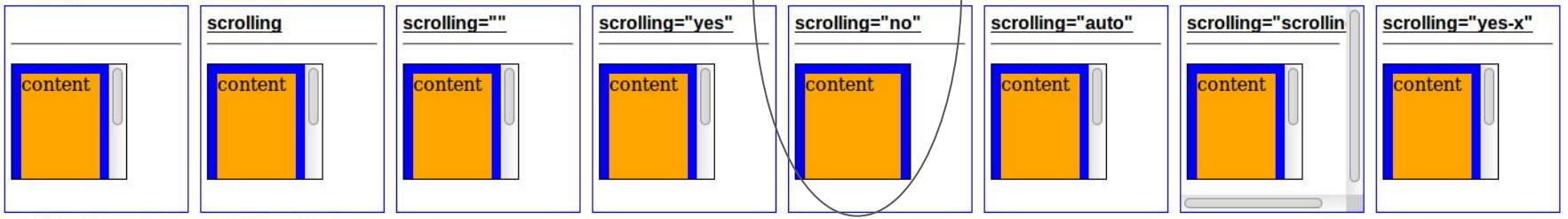
scrolling.frame.large.html

div { background-color: orange; width: 500px; height: 500px; }



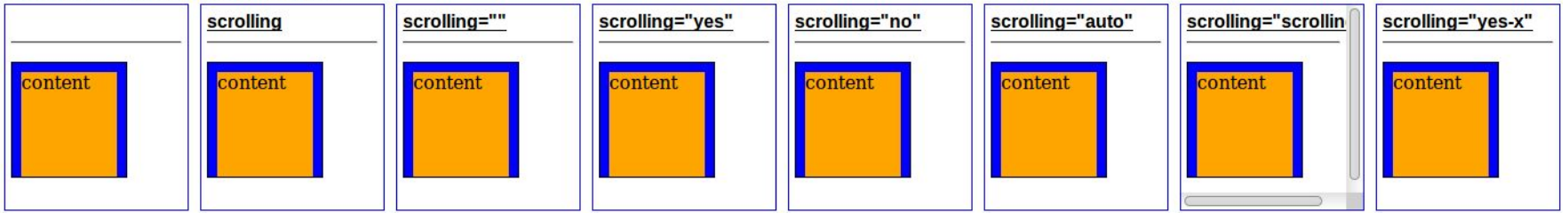
scrolling.frame.large.css-auto.html

div { background-color: orange; width: 500px; height: 500px; } * { overflow: auto; }



scrolling.frame.large.css-hidden.html

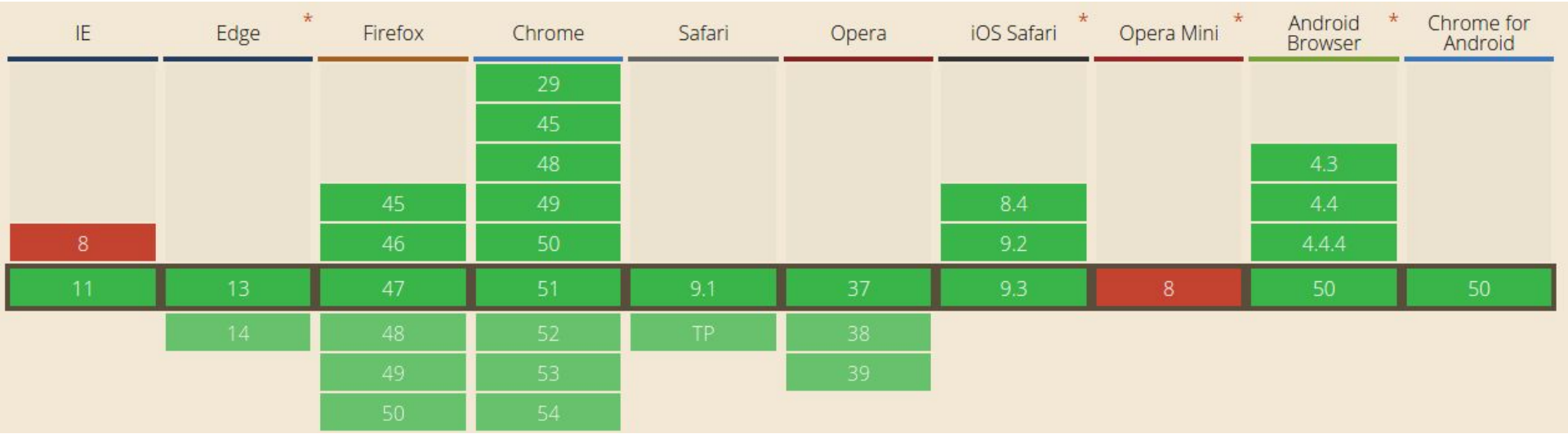
div { background-color: orange; width: 500px; height: 500px; } * { overflow: hidden; }



sandbox=

- allow-forms
- allow-modals
- allow-orientation-lock
- allow-pointer-lock
- allow-popups
- allow-popups-to-escape-sandbox
- allow-same-origin
- allow-scripts
- allow-top-navigation

https://html.spec.whatwg.org/multipage/embedded-content.html#attr-iframe-sandbox



http://caniuse.com/#search=sandbox

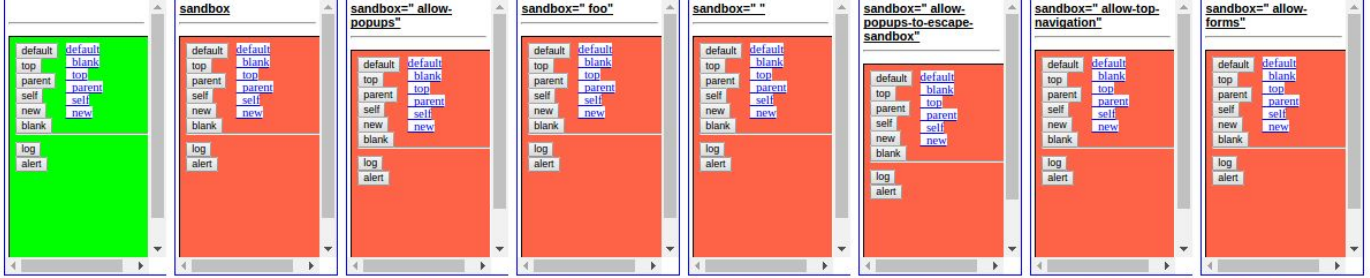
Browser compatibility

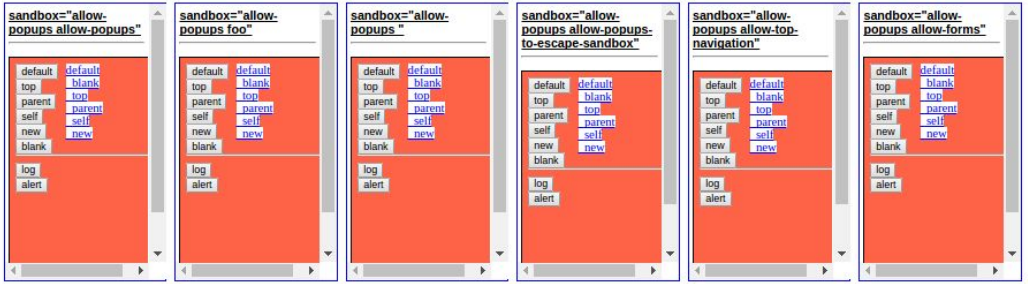
Desktop | Mobile

Feature	Chrome	Edge	Firefox (Gecko)	Internet Explorer	Opera	Safari (WebKit)
Basic support	1.0	(Yes)	(Yes)[3]	(Yes)	(Yes)	(Yes)
`sandbox`	4.0	(Yes)	17.0 (17.0)	10	15	5
`seamless`	No support	No support	No support	No support	No support	No support
`srcdoc`	20.0	No support	25.0 (25.0)	No support	15	6
`allowfullscreen`	17.0 webkit 27.0	(Yes)	9.0 (9.0) moz 18.0 (18.0)	11 ms	(Yes)	(Yes) webkit 7
`sandbox="allow-popups"`	?	(Yes)	27.0 (27.0)	?	?	?
`sandbox="allow-popups-to-escape-sandbox"`	46.0	No support	49.0 (49.0)	?	32	?
`sandbox="allow-modals"`	?	?	49.0 (49.0)	?	?	?
`referrerpolicy`	46.0 [1]	No support	42.0 (42.0) [2]	?	?	?

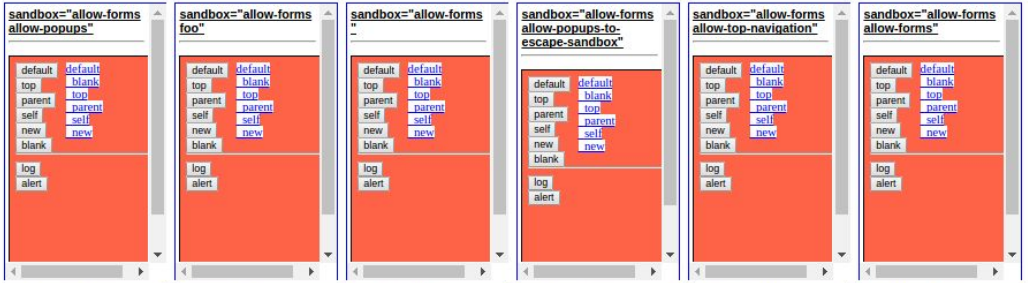
https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe#Browser_compatibility

Targeting

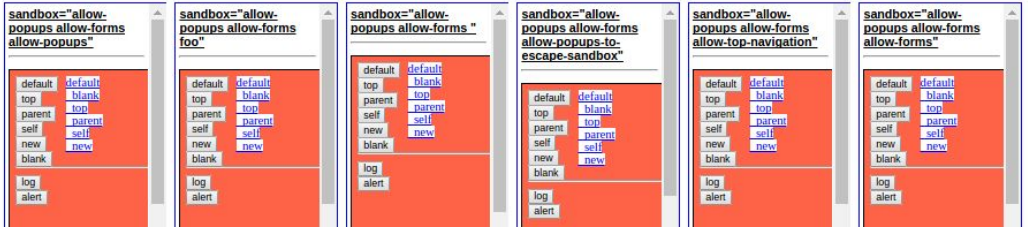




allow-popups



allow-forms



both

_parent in a sandbox

- Unable to target _parent frame
- Allow-top-navigation will not unblock _parent unless _top == _parent

Additionally

- Popup names are not remembered (_new and _parent behave like _blank)

(at least in chrome / firefox)

sandbox=allow-fullscreen

No.

Iframes have this disabled by default. Absence of sandbox would (“should”) mean iframes can be fullscreened by default.

https://fullscreen.spec.whatwg.org/#fullscreen-enabled-flag

Sandbox only applied on navigation

Dynamic changes only reflected after navigating

Bad synergies

Allow-scripts + allow-same-origin with a same origin url allows frame to remove its own sandbox and reload to escape the sandbox

seamless=

- Like inlining a template…
- Support retracted or never existed
- Scrapped from html5 spec

https://developers.whatwg.org/the-iframe-element.html#attr-iframe-seamless
https://github.com/whatwg/html/issues/331

λ

src=

- Regular urls
- JavaScript urls
- Empty
- Special urls
- Data-uri

https://www.w3.org/TR/html4/present/frames.html#adef-src-FRAME
https://html.spec.whatwg.org/multipage/embedded-content.html#attr-iframe-src

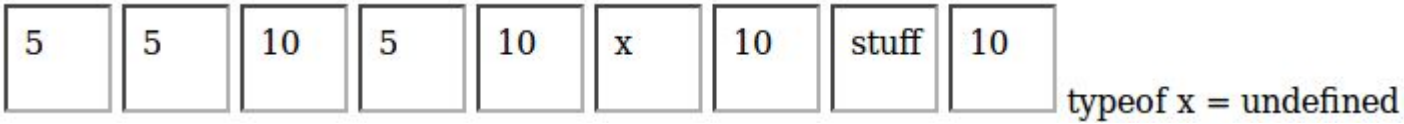
src=”javascript:’foo’”

- Evals your code and display the result if it is a string, 204 otherwise
- Return value is used as html document
- Can be used to generate complete html pages, inc doctype!
- Requires html encoding of the outer quote, js encoding of inner quote
- URL length limits
- js1k.com used this for demo frames in a frameset for a long time
- Not restricted to a string...

- <iframe src="javascript:**'5'**"></iframe>
- <iframe src="javascript:**5**"></iframe>
- <iframe src="javascript:**5+5**"></iframe>
- <iframe src="javascript:**5,'5'**"></iframe>
- <iframe src="javascript:**x=5+5,String(x)**"></iframe>
- <iframe src="javascript:**if(true)'x';else 'y';**"></iframe>
- <iframe src="javascript:**if(true)'x';else 'y';5+5;**"></iframe>
- <iframe src="javascript:**for(var i=0;i<10;++i)'stuff';**"></iframe>
- <iframe src="javascript:**x=5+5,'<script>alert(x)</script>'**"></iframe>
  <script>document.write('typeof x = ' + typeof x)</script>

Chrome:

Firefox:



javascript: url spec

Parse url:

https://html.spec.whatwg.org/multipage/browsers.html#javascript-protocol
https://w3c.github.io/html/browsers.html#javascript-urls

Run “classic” script:

https://w3c.github.io/html/webappapis.html#run-a-classic-script

- Content type is text/html
- If not string, considered “undefined” with http status 204
- Globals owner is not obvious from the spec

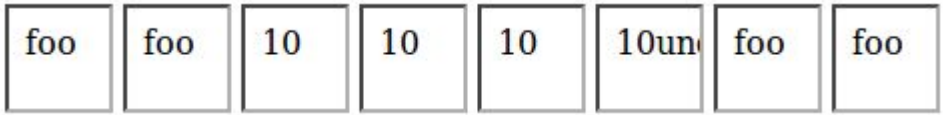
Must dig deeper

<iframe src="javascript:document.write('<body> foo '),document.querySelector('div').innerHTML"></iframe>
<iframe src="javascript:document.write("<body> foo "),document.querySelector("div").innerHTML"></iframe>

<iframe src="javascript:**x=10;x+'';**"></iframe>
<iframe src="javascript:**x=10;'<script>document.write(x);</script>'**"></iframe>
<iframe src="javascript:**this.x=10;'<script>document.write(x);</script>'**"></iframe>
<iframe src="javascript:**document.x=10;document.x + '<script>document.write(document.x);</script>'**"></iframe>
<iframe src="javascript:**document.write('foo')**"></iframe>
<iframe src="javascript:**document.write('foo'),document.close(),'bar'**"></iframe>

Chrome:

Firefox:



The other way around

```
<script>function foo(){}</script>
<iframe src=”javascript:foo();”></iframe>
<iframe src=”javascript:parent.foo();”></iframe>
```

source

Data-uri

<iframe src="data:text/html,foo"></iframe>

Works as you'd expect. Well, except in IE.

Outer frame runs/continues first… (race condition? Seems consistent)

Considered cross domain; we can't access the frame from JS in parent.
It looks that way but that's only the race condition.

```
<iframe id=A src="data:text/html;charset=utf-8,<!DOCTYPE html><html><head></head><body><h1>FAIL</h1></body></html>"></iframe>
<script>
  console.log(A.contentDocument.body.innerHTML); // ""
  A.contentDocument.body = 'PASS 1'; // works because data uri has not yet resolved. Will be overwritten.
  setTimeout(function(){ A.contentDocument.body = 'PASS 2'; }, 10); // throws security error
</script>
```

Special urls

- about:blank
- about:invalid
- about:
- about:html
- about:”html”

Behave the same. Accessible from parent frame. Chrome will create a body, Firefox does not until onload. All iframes are empty.
The quoted html version reports “about:” for url… the others as is.

- chrome://about

Special to Chrome, won’t load it. Firefox acts as about:blank

Empty pages

- No src <iframe></iframe>
- No value <iframe src></iframe>
- Empty string as value <iframe src=””></iframe>

Acts similar to about:blank.

When src is omitted, iframe.src is empty.

When src is present but empty, iframe.src is parent url...

λ

srcdoc=

It’s like a javascript:”string” url but just the string sans quotes

Prevents a fetch in certain cases

Fallback should be the src

Designed to be used in conjunction with sandbox *(and seamless)*

Requires script tags to be closed in order for them to execute

Not in Edge (yet)

https://html.spec.whatwg.org/multipage/embedded-content.html#attr-iframe-srcdoc

Double edged syntax

- Doctype is optional
- Title is optional
- Only body is required, rest is implied

- Content has to be doubly encoded

Anti-climactic

The location.href of a srcdocced iframed is … “about:srcdoc”

λ

Cross frame navigation in JS

- window -> iframe: **window.frameElement**
- document -> window: **document.defaultView**
- iframe -> window; **iframe.contentWindow**
- iframe -> document: **iframe.contentDocument**
- window -> parent: **parent**
- iframe -> top: **top**
- window -> document: **window.document**
- element -> document: **el.ownerDocument**

(the last one is the doc that created it, not the doc who has the frame in its DOM!)

λ

Stones unturned

- document.domain
- onload
- onerror
- contenteditable
- document.write
- xml
- Global attributes
- postMessage
- Other cross domain stuff
- More javascript urls
- X-Frame-Options
- Iframes in svg

Thank you

http://qfox.nl
http://c80.nl
@kuvos
http://github.com/qfox/htmlday16

Riddle

From a presentation at JSConf.eu ‘15
Lieke Boon: “Unconscious Bias: we’re all guilty”
https://www.youtube.com/watch?v=5mcyUUf20Ng