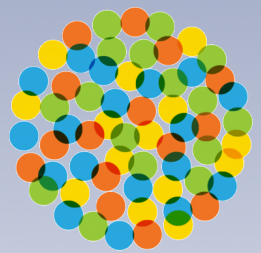
Comunicação entre janelas em domínios diferentes utilizando postMessage

CaioSBA, 2013

CaioSBA

- Bacharel em Ciência da Computação pela UFBA
- Mestrando em Ciência da Computação pela UFBA
- Desenvolvedor de Software






Uma boa referência

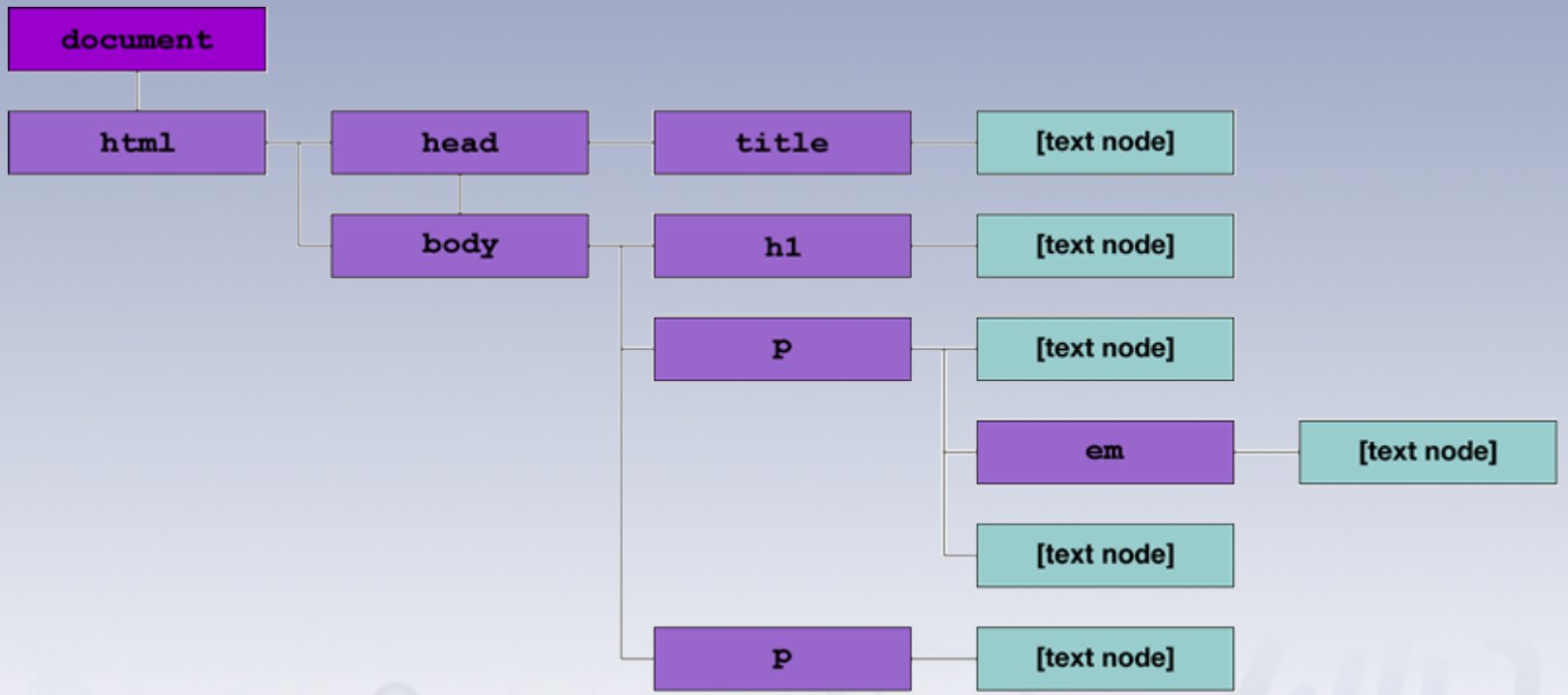
- JavaScript, the good parts
- … e as partes ruins?

Um pouco sobre JavaScript...

- Lançada inicialmente no Netscape com o nome LiveScript
- Tipagem fraca e dinâmica
- Assíncrona
- Prototipada
- Event-Based
- Baseada no ECMAScript
- Microsoft lança o JScript

DOM – Document Object Model

- O DOM é uma multi-plataforma que representa como as marcações em HTML, XHTML e XML são organizadas e lidas pelo navegador
- API
- Estrutura em árvore



O objeto *window*

- Representa uma janela do navegador
- A propriedade *document* aponta para o documento carregado na janela do navegador
- É o escopo padrão da maioria das aplicações JavaScript que executam no navegador
- window.document x document x document.defaultView
- Em navegadores com abas, cada aba possui seu próprio objeto *window*

Frames

- Vão contra o conceito de hipertexto
- Problemas com busca
- Incompatibilidade com navegadores (principalmente dispositivos móveis)
- Frameless
- Depreciado

```
<!DOCTYPE HTML PUBLIC
"-//W3C//DTD HTML 4.01
Frameset//EN"
"http://www.w3.org/TR/html4/frameset.
dtd">

<html>
<head><title>My First Frame
Page</title>
</head>

<frameset cols="30%, 70%">
<frame src="nav.html">
<frame src="content.html">
</frameset>

</html>
```

Iframes

- Uma página é inserida em outra como um objeto retangular
- Aparência pode ser melhorada se o atributo frameborder for removido
- Para acessar o conteúdo: iframe.contentWindow.document
- Para acessar os iframes:
  window.frames[0]
  window.frames['iframeName']
- Hierarquia
  window.frames[0].parent === window
  window.frames[0].frames[0].frames[0].top === window

```
<style> * { width: 100px; height:40px }
</style>
<ol>
  <li><iframe
src="JavaScript:'content'"></iframe></l
i>
  <li><iframe src="JavaScript:'content'"
style="border:0"></iframe></li>
  <li><iframe src="JavaScript:'content'"
frameborder="0"></iframe></li>
</ol>
```

O cabeçalho X-Frame-Options

- Cabeçalho HTTP definido pelo servidor web
- Controla se a página pode ser carregada dentro de (i)frames
- Valores: DENY, SAMEORIGIN, ALLOWFROM
- Apache:
  Header always append X-Frame-Options SAMEORIGIN
- Nginx:
  add_header X-Frame-Options SAMEORIGIN;

Ver exemplo 1

Same Origin Security Policy

- Limita o acesso de uma janela à outra
- Questão de segurança
- Uma janela pode trabalhar no contexto de outra apenas se possuem a mesma origem
- Mesma origem: mesmo protocolo, domínio e porta
  protocolo://domínio:porta

http://site.com
http://site.com/
http://site.com/my/page.html

http://www.site.com
http://site.org
https://site.com
http://site.com:8080

Ver exemplos 2 , 3 e 4

Comunicação

- Client-Server:
  - AJAX
  - JSONP

- Client-Client:
  - DOM
  - Post Message

Post Message: A solução para comunicação entre janelas de origens distintas

- Parte do HTML 5
- Suporte em todos os navegadores modernos
- Permite a comunicação segura entre janelas de diferentes origens

postMessage(data, targetDomain)

data: qualquer objeto JavaScript (apenas strings possuem suporte completo)

targetDomain: Limita os domínios do receptor (pode ser um wildcard '*')

Ver exemplo 5

Post Message: A solução para comunicação entre janelas de origens distintas

• Partes do evento “mensagem”:
data: dado enviado
origin: quem enviou o dado
source: referência à janela remetente

Ver exemplo 6

Post Message: A solução para comunicação entre janelas de origens distintas

- Segurança:

É um modelo two-sided: o remetente identifica o receptor (targetDomain) e o receptor identifica o remetente (event.origin)

- Se não deseja receber mensagens, basta não registrar o evento
- Ao receber mensagens, sempre checar a origem do remetente
- Qualquer janela pode enviar mensagens para qualquer outra
- Não há como saber quando uma janela enviará um código malicioso
- Evite XSS verificando o conteúdo das mensagens
- Defina o destinatário para evitar interceptação

Post Message: Quando utilizar?

- Extensões para navegadores
- Widgets
- Apps

Post Message: Fallback para browsers antigos

- O remetente altera a localização do destinatário utilizando âncora
- O destinatário verifica periodicamente se o endereço foi alterado

Ver exemplo 7

Post Message: Aplicações

- Sincronização entre janelas
- Troca de eventos entre janelas
- Widgets (Facebook, Twitter, Google +1)

Ver exemplo do Drupal Bookmarklet:

- Conteúdo inicia escondido, ao carregar, o pai é avisado e o exibe
- A janela avisa ao pai sempre que a altura é alterada
- Em casos de autenticação do Facebook, o redirecionamento é automático