



**Hasso  
Plattner  
Institut**

IT Systems Engineering | Universität Potsdam

TinyMCE

Frederik Leidloff

2

- TinyMCE
  - Lizenz
  - Entwicklung
- Bug Beschreibung
- XSS und Same Origin Policy
- Problemlösung

3

- Tiny Moxiecode Content Editor
- Anpassbar durch Themes und Plugins
- Sprache konfigurierbar
- Leicht zu integrieren, AJAX kompatibel
- Entwickelt von Moxiecode
- Veröffentlicht am 11. März 2004 unter LGPL
- Version 3.2.7 ist aktuell (22.09.2009)

■ *"The TinyMCE project is one of the top 100 projects on Sourceforge, with an even increasing userbase. Various Open Source systems have also integrated TinyMCE into their own projects, making TinyMCE the most used WYSIWYG editor on the Internet."*

- Moxiecode.com

- Standard Content Editor in:  
wordpress, ImpressCMS, Pixie, Joomla, Plone, dotCMS,  
mojoPortal, SilverStripe, MODx, ...

- Lesser General Public License
- You can use, modify and distribute the software, but do so in the spirit of Open Source.
- You need to leave the copyright notices intact.
- You need to be able to share any modifications you make to the TinyMCE source
- Give credit where credit is due, spread the word, link to us if you can.

6

- Entwickelt von Moxiecode
- 2 Hauptentwickler
  - Johan "Spocke" Sörlin (Main developer and maintainer)
  - Joakim Lindkvist (Project administrator)
- Forum
- Wiki
- Keine Mailingliste
- Sourceforge Projekt
- Bug Tracker auf sourceforge
- GitHub seit 14.01.2010

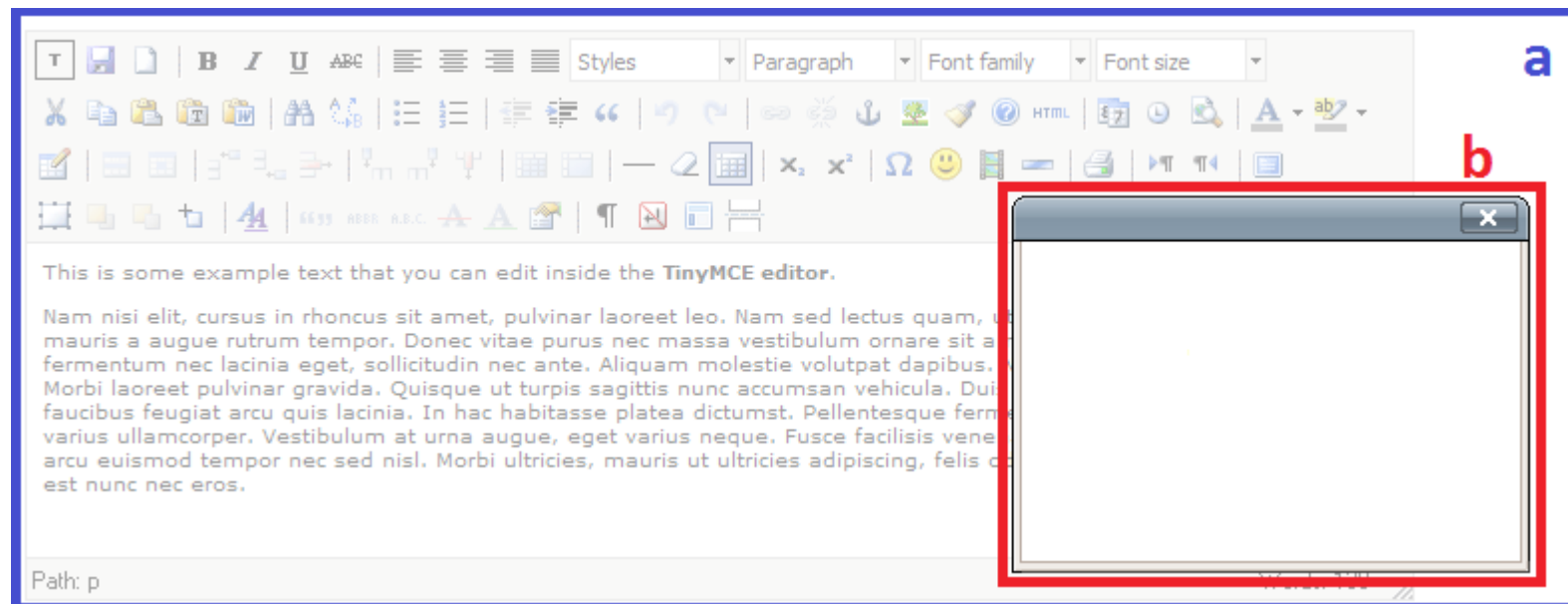
7

- **“HTML popup empty using firefox and examples”**
- (Nur) Firefox ist betroffen
- Verwandte Forendiskussionen
- Keine Reaktionen auf Bug
  
- Inline Popups sind echte Popups
- Problem besteht nur lokal, nicht auf Server
- Firefox Bug???

# Betroffener Code

8

```
3
4 var tinymce=null,tinyMCEPopup,tinyMCE;
5 tinyMCEPopup={
6   init:function() {
7     var b=this,a,c;
8     a=b.getWin();
9     tinymce=a.tinymce;
10    tinyMCE=a.tinyMCE;
11    b.editor=tinymce.EditorManager.activeEditor;
12    b.params=b.editor.windowManager.params;
13    b.features=b.editor.windowManager.features;
```



- XSS = Cross Site Scripting
  - JavaScript Same Origin Policy macht Browser sicherer
  - Same Origin Problem für lokale Dateien
  - Local Machine Zone Lockdown (Internet Explorer)
  - Strict Same Origin Policy seit Gecko 1.9 (Firefox)
- 
- **“A file can read another file only if the parent directory of the originating file is an ancestor directory of the target file”**

■ **“A file can read another file only if the parent directory of the originating file is an ancestor directory of the target file”**

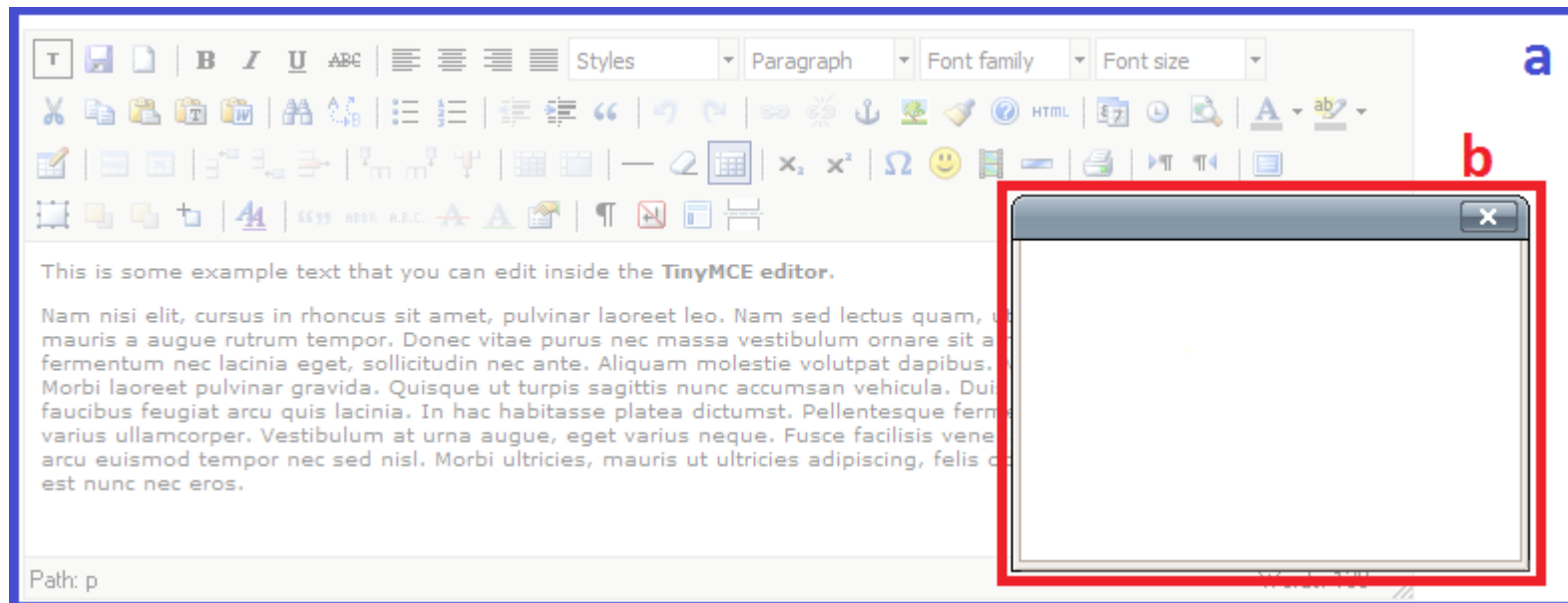
- Frameset = /home/user/foo.html
- Frame = /home/user/subdir/bar.html  
=> Same Origin!
- Frameset = /home/user/fred/bar.html
- Frame = /home/user/mike/foo.html  
=> different Origins!
- Frameset = /home/user/subdir/foo.html
- Frame = /home/user/bar.html  
=> different Origins!

11

- Strict Same Origin Policy abschalten
- `security.fileuri.strict_origin_policy` auf `false` setzen
  
- Hinweis in Programm einbauen?
- Popup, wenn Laden fehlschlägt?

12

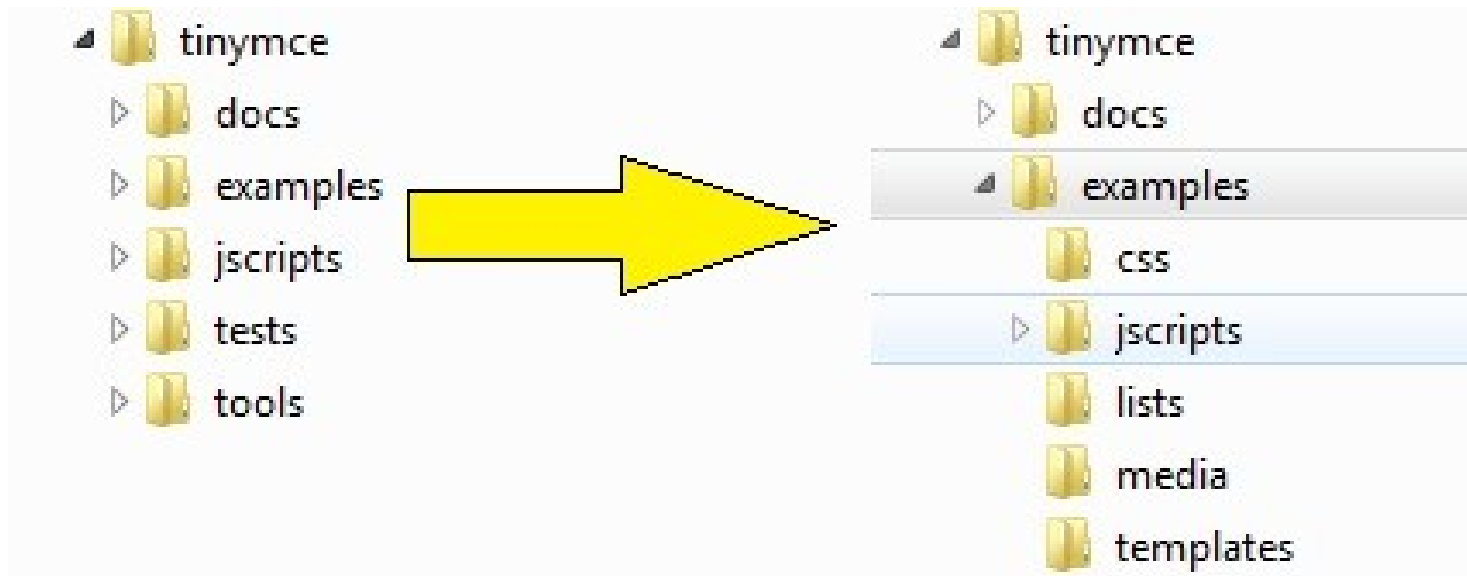
```
3
4   var tinymce=null,tinyMCEPopup,tinyMCE;
5   tinyMCEPopup={
6     init:function(){
7       var b=this,a,c;
8       a=b.getWin();
9
10      try
11      {
12        tinymce=a.tinymce;
13        tinyMCE=a.tinyMCE;
14      }
15      catch(err)
16      {
17        alert(err);
18      }
19
20
21      b.editor=tinymce.EditorManager.activeEditor;
22      b.params=b.editor.windowManager.params;
```



13

- Problem besteht nur, während Einrichtung
- Besser: Gut dokumentieren!
-

- Problem besteht nur, während Einrichtung
- Besser: Gut dokumentieren!
- Noch besser: Ordner neu strukturieren!



Ende

15

■ Fragen?

- <http://tinymce.moxiecode.com>
- <http://www.moxiecode.com>
- [https://developer.mozilla.org/En/Same\\_origin\\_policy\\_for\\_JavaScript](https://developer.mozilla.org/En/Same_origin_policy_for_JavaScript)
- [https://developer.mozilla.org/En/Same-origin\\_policy\\_for\\_file:\\_URIs](https://developer.mozilla.org/En/Same-origin_policy_for_file:_URIs)
- <http://tinymce.moxiecode.com/punbb/viewtopic.php?id=18470>
- <http://softwareas.com/cross-domain-communication-with-iframe>
- [http://sourceforge.net/tracker/?func=detail&aid=2801745&group\\_id=103281&atid=635682](http://sourceforge.net/tracker/?func=detail&aid=2801745&group_id=103281&atid=635682)
- <http://molily.de/js/sicherheit.html>
  
- Stand: 17.01.2010, 21:00