Revisiting XSS Sanitization

Ashar Javed | Ruhr University Bochum, Germany
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

[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 3a
  - * 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/translator s-general-discussion/topics/new)
Froala WYSIWYG Editor

A beautiful jQuery WYSIWYG text editor

http://editor.froala.com/
Cross-Site Scripting (XSS)
XSS — An Epidemic

#XSS is everywhere & it is not going anywhere.
It was there .. It is there & It will be there.
#nothingmoretosay #thatsit

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
Identification of Common Injection Points in WYSIWYG Editors
Injection Points in WYSIWYG Editors

- Insert/Edit Image
- Insert/Edit URL
- Set Attributes
- Insert/Upload File
- Insert/Upload Video
Attacking Insert/Edit Link Feature
WYSIWYG's Insert Link

Insert link

- URL
- Target: Same window

- Url
- Text to display: em
- Title
- Target: None
  - None
  - New window
URL Context Attack Methodology
XSSed FreeTextBox (ASP.NET) Based WYSIWYG Editor
Who is using FreeTextBox?

Selected Clients

http://www.freetextbox.com/
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
Microsoft
intel
HP
Liberal.ca
Liberal Party of Canada
XSSed Mercury (Rails)

The page at jejack0n.github.io says:

1

OK

gem 'mercury-rails'
rails generate mercury:install

Mercury Editor

click
Who is using Mercury?

http://jejacks0n.github.io/mercury/
XSSed Jive
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
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
Let's XSS ... step #1

[twitter] (https://twitter.com) has been internally converted into
<a href="https://twitter.com">twitter</a>
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%201%29)
has been internally converted into
<a href="javascript:alert%28%201%29">twitter</a>
After Fix ... @ndm Replied

Neil Matatall
@ndm

@soaj1664ashar @HttpSecHeaders damn 3rd party libraries

https://twitter.com/ndm/status/456129160411234304
Which 3rd Party Library (WYSIWYG)?

MarkDown
XSSed MarkDown

http://daringfireball.net/projects/markdown/dingus
Enough Breaking ...
Lets Present
Unbreakable
Sanitizer/Filter
What? ... Unbreakable? :-D

http://demo.chm-software.com
/7fc785c6bd26b49d7a7698a7518a73ed/
"The solutions all are simple... after you have arrived at them."

(Robert M. Pirsig, American novelist)
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.

https://twitter.com/ssstephenson/status/507931945594937344
Thank You!
@soaj1664ashar