

Store Library Why Leanpub Testimonials Write Community Podcasts **Support** Sign In Sign Up

4,819 READERS 28 PAGES

XSS Cheat Sheet

2018 Edition

Rodolfo Assis

Start to master the fine art of Cross-Site Scripting (XSS) right now!

Table of Contents



Free! \$9.95
MINIMUM SUGGESTED

YOU PAY
\$9.95

AUTHOR EARNs
\$8.45

YOU PAY (USD)
\$9.95

EU customers: Price excludes VAT. VAT is added during checkout.

Add Ebook to Cart

Add to Wish List

RODOLFO ASSIS (BRUTE)

LAST UPDATED ON 2018-01-29

Brute created a XSS cheat sheet on Leanpub. I don't know about you but I'd assume to download something from there you need to pay. There are people had the same thought

About the Book

XSS Cheat Sheet 2018 Edition is a booklet on Cross-Site Scripting (XSS), the most widespread and common flaw found in the World Wide Web. It was designed to be a quick reference material to deal with XSS related needs for bug hunters, penetration testers, security analysts, web application security students and enthusiasts.

bitcoin:34RPK3S3K8fja4mKWhC9ms1QCMyjxA6tf?amount=0.001

Share this book Feedback

Twitter Facebook Google+ Email the Author(s)

<https://twitter.com/antisnatchor/status/958634877989081089>. Brute could have just published the cheat sheet and asked for donation instead of having people to pay first only to find out that is actually free. There are many great examples that use GitHub for “read first, pay later” like

Brute Logic @brutellogic · Feb 4

You can also send BTC for my XSS Cheat Sheet! #XSS2018

Suggested amount: 0.001337 🙄



XSS Cheat Sheet

Start to master the fine art of Cross-Site Scripting (XSS) right now!

leanpub.com

3 10 68

✓ <https://github.com/bitcoinbook/bitcoinbook> and <https://github.com/crypto101/book>. Brute even put his Bitcoin address down below so why couldn't he do the same? Before you tell me “oh it's for people who want to pay him in cash”, Leanpub supports only credit cards and PayPal which you might as well send money to his PayPal account via the good old “PayPal donation button”.

His work so far has absolutely **zero reference**, and so is this cheat sheet. If you stay in the XSS field long enough you will immediately spot some of the vectors are rips-off. I know it's unfair to say it because XSS vectors are not trademarked or the source is hard to find, but for a paper with 27 pages without a single reference or footnote? Are you telling me Brute found everything on his own? I'll just show you one example below and of course there are many others. The first picture shown is from Brute's cheat sheet and the other one is from <https://html5sec.org>. Notice the difference? “B...But Brute's has the JS context while html5sec's doesn't!” heh.

HTML Alternative Separators

Use when default spaces are not allowed. Slash and quotes (single or double) might be URL encoded (%2F, %27 and %22 respectively) also, while plus sign (+) can be used only in URLs.

Tag Scheme:

`<name [1] attrib [2] = [3] value [4] handler [5] = [6] js [7]>`

[1], [2], [5] => %09, %0A, %0C, %0D, %20, / and +

[3] & [4] => %09, %0A, %0C, %0D, %20, + and ' or " in both

[6] & [7] => %09, %0A, %0B, %0C, %0D, %20, /, + and ' or " in both

HTML separators and ignored characters

test #100

[a] Characters accepted as tag name/attribute separators.

Firefox, Internet Explorer, Safari, Google Chrome, Opera : 9,10,12,13,32,47
Internet Explorer (5-9 SM): 11

[b] Characters ignored before attributes (and not accepted as parameter/attribute separators).

Firefox, Internet Explorer, Safari, Google Chrome, Opera : 47
Internet Explorer (5-9 SM): 0**

[c] Characters ignored between attribute name and equals sign.

Firefox, Internet Explorer, Safari, Google Chrome, Opera : 9,10,12,13,32
Internet Explorer (5-9 SM): 0,11

[d] Characters accepted as parameter/attribute separators.

Firefox, Internet Explorer, Safari, Google Chrome, Opera : 9,10,12,13,32
Internet Explorer (5-9 SM): 11

[e] Characters ignored between equals sign and parameter.

Firefox, Internet Explorer, Safari, Google Chrome, Opera : 9,10,12,13,32
Internet Explorer (5-9 SM): 0,11

* Characters are given as decimal ASCII table index.

** There is a common rule that the unencoded null character does not exist for IE HTML parser.

```
<img[a][b]src=x[d]onerror[c]=[e]"alert(1)">
```

Oh, have I already mentioned Brute has something called Brute secret which you pay a subscription fee to his private Twitter account to access his exclusive XSS vectors? Looks like the cheat sheet is incomplete without you actually having to pay!



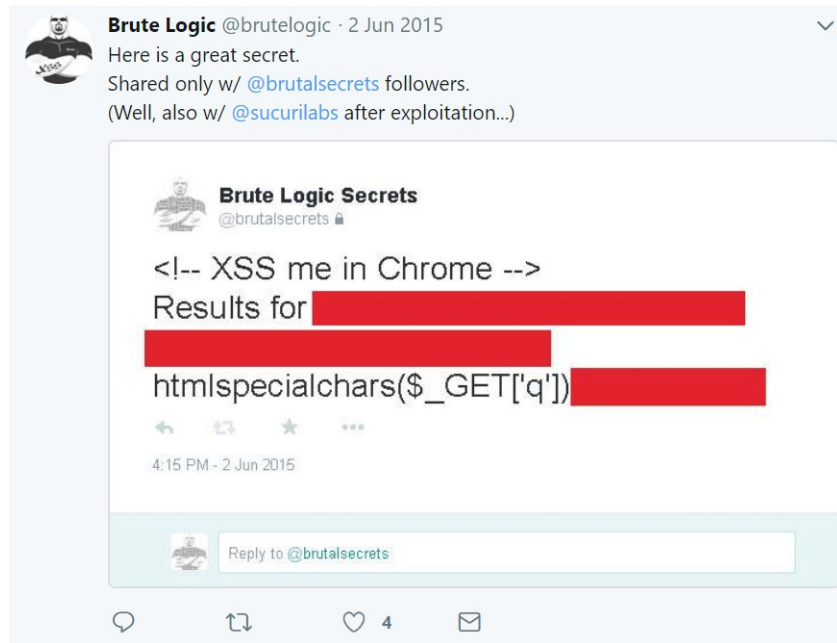
Brute Logic @brutellogic · Jan 20

Replying to @nijagaw

great question! Brutal Secrets will be distributed to brutal followers ONLY as an addendum to that Cheat Sheet. 🤔



What's in Brute secret? As a non-subscriber I don't know, but some times Brute teases us with a little peek.



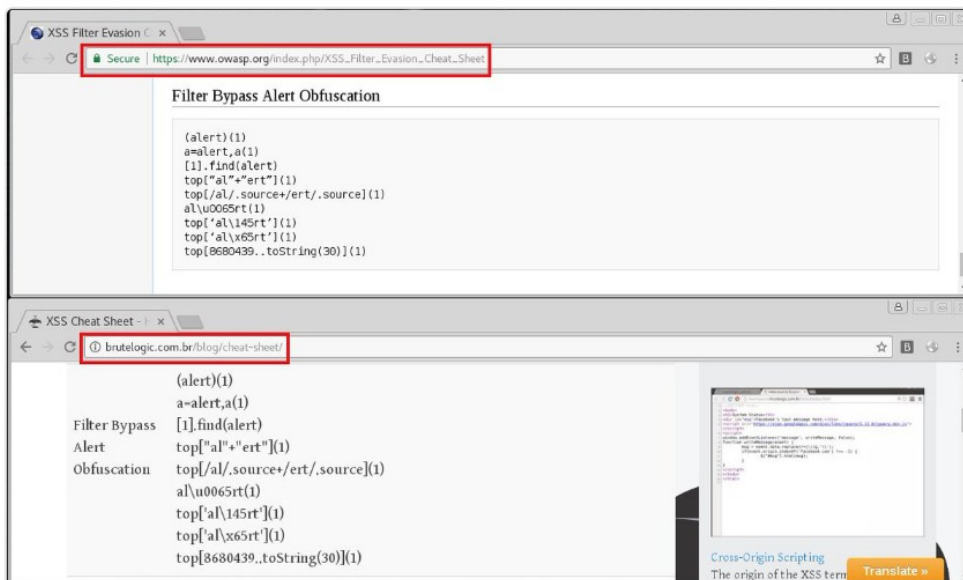
Did he mean you can XSS even your input is sanitized with htmlspecialchars in HTML context??! I gotta subscribe... Oh wait, I didn't see the red things there. In that case it must be in attribute context (htmlspecialchars is useless against scenario where you input appears on a/href, iframe/src and JavaScript context). Nice try Brute! I wouldn't have known that if I didn't subscribe to Brute secret! Seriously though, this is a complete misleading tweet tricking people to subscribe to his thing.

Brute Logic
@brutelogic

Follow

Guess who copies who?
Hint: the one w/ tricks for IE5 & FF1

Not even a mention... 🙄



7:07 AM - 25 May 2017

19 Retweets 49 Likes



6

19

49



Brute really has the guts to say that. Is that "A taste of own medicine"? If this is not I don't know what is.

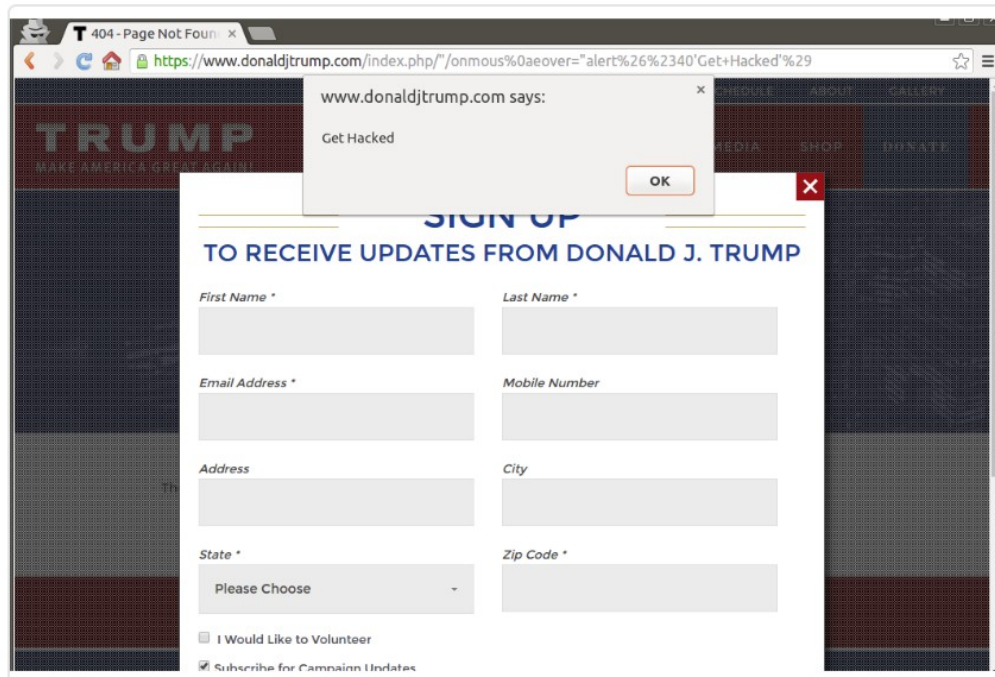


Brute Logic
@brutellogic

Follow

Get involved.

[donaldjtrump.com/index.php/%22/](https://www.donaldjtrump.com/index.php/%22/) ...
#XSS @realDonaldTrump



10:45 AM - 11 Mar 2016

69 Retweets 66 Likes



5 69 66

Uh oh the President was hacked! Can someone tell me what ethical means?



Brute Logic
@brutellogic

Follow

Replying to @samwcyo @uraniumhacker and 2 others

There's simply no laws that say "popping a js alert box for yourself in someone else's domain context is illegal".

6:16 PM - 23 Jul 2017

2 Likes



6 2



Brute Logic @brutellogic · 23 Jul 2017

Replying to @samwcyo @uraniumhacker and 2 others

There's simply no laws that say "popping a js alert box for yourself in someone else's domain context is illegal".

6 2



Uranium238 @uraniumhacker · 23 Jul 2017

"knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage

1



Uranium238 @uraniumhacker · 23 Jul 2017

without authorization, to a protected computer;

2



Brute Logic

@brutellogic

Follow

Replying to @uraniumhacker @samwcyo and 2 others

which damage I'm causing to that computer, mate?

6:24 PM - 23 Jul 2017

1



Tweet your reply



Uranium238 @uraniumhacker · 23 Jul 2017

Replying to @brutellogic @samwcyo and 2 others

that is the law. Do you think lawyers will care if it is a simple pop up or not? You are still putting a code in a vulnerable system

1



Uranium238 @uraniumhacker · 23 Jul 2017

does not matter if it is reflected or not

1



Brute Logic @brutellogic · 23 Jul 2017

It matters. You just have to think about it. Or get some law consulting.

2



Uranium238 @uraniumhacker · 23 Jul 2017

I did get law consulting

1

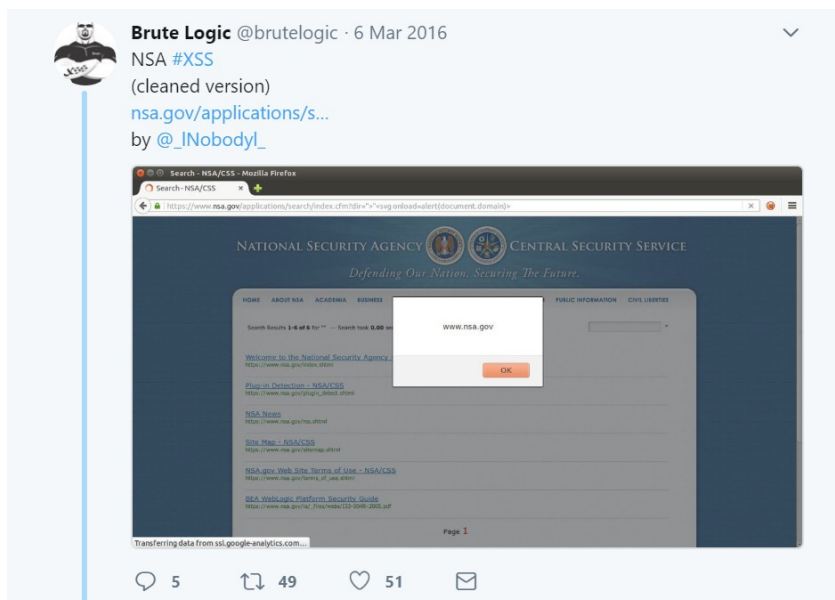


Karel Origin @Karel_Origin · 24 Jul 2017

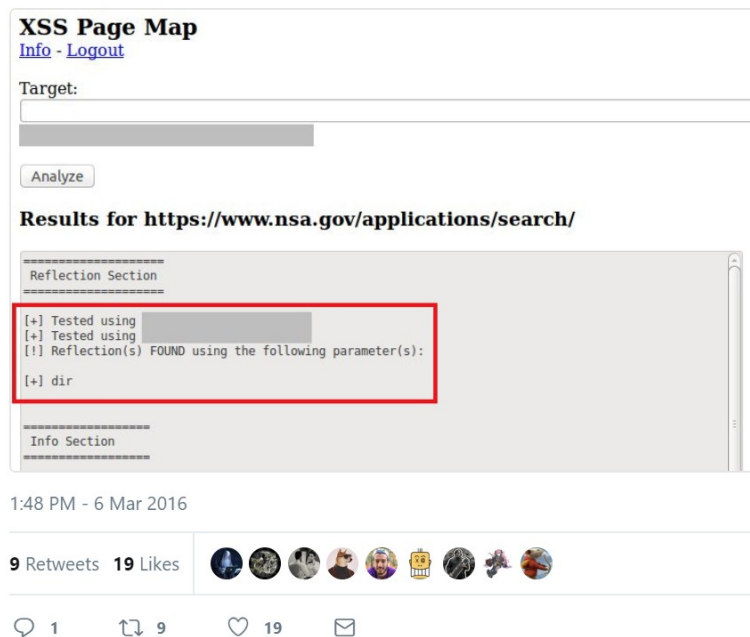
I'm not trying to pick sides here, but ask yourself, are you harming the computer that is hosting the web app by injecting html?

1

I see, thanks Brute! I guess everyone saw the the tweet can only attack themselves!



This latest NSA #XSS could have been found by my new tool pmap, exclusive to @brutalsecrets followers.



Looks like NSA could benefit from purchasing access to Brute secret, before anyone who saw the tweet to exploit it on their own computers!



Brute Logic @brutellogic · 12 Feb 2015

Sometimes I think #infosec is a private club... And some people are simply not welcome.



@garethheyes You can remove the "2b" leaving just %. But both %'s will fail against asp/aspx sites. In that case we have alert(1)-".



  @garethheyes 2h
@brutellogic erm I think I know that but thanks anyway



Brute Logic @brutellogic 3m
@garethheyes If you know, why don't you go for the shorter version? You even have a challenge about these things.



3



3



18



Did you find the irony? Hint: something containing the word "secret".

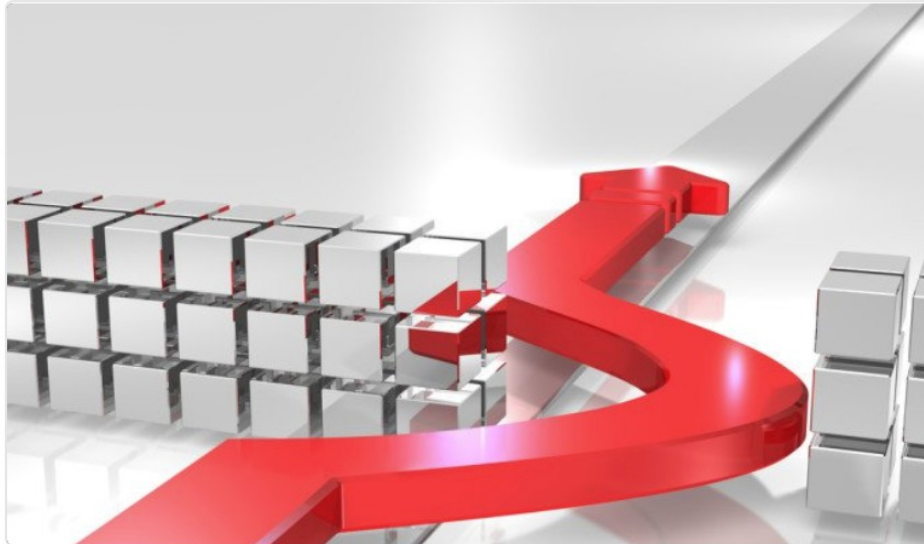


Brute Logic
@brutellogic

Follow

HTML Entities for Filter Bypass

brutellogic.com.br/utills/charref...



7:49 AM - 28 Sep 2016

18 Retweets 39 Likes



3 18 39

Character Entity Reference X

brutellogic.com.br/utills/charref.htm

		
	!	"	#
		!	" "	#
\$	%	&	'	(
$	&percent;	& &	'	(
)	*	+	,	.
)	* *	+	,	.

Character Entity Reference X

Secure | https://dev.w3.org/html5/html-author/charref

		
	!	"	#
		!	" "	#
\$	%	&	'	(
$	&percent;	& &	'	(
)	*	+	,	.
)	* *	+	,	.

I surely do enjoy playing “spot the difference”. Anyway, W3C has <https://dev.w3.org/html5/html-author/charref> which shows what character maps to which HTML entity representations, and Brute simply ripped off it again, line by line (I've checked the source code, 99% matched), with zero reference. What's the point cloning your own? Even if you wanted to mirror the site you should have at least mentioned this is NOT your work, Brute.



Brute Logic

@brutellogic

Follow



Character Entity Reference Chart
[dev.w3.org/html5/html-aut...](https://dev.w3.org/html5/html-author/charref) A must know
for filter evasion. #XSS #SQLi

4:11 AM - 16 Dec 2015

10 Retweets 18 Likes



↺ 10

♡ 18



Oh there's the reference! I definitely didn't Google it to find out. Now I'm confused why Brute posted the original one but then made his own, and again zero reference?

Don't get me wrong. Brute surely did a lot to the community. I've heard many great things of him helping others, and his blog is great for beginners. But think about those who got their credit stolen. If you are patient enough to scroll through his Twitter timeline, you will find more and his questionable personality.