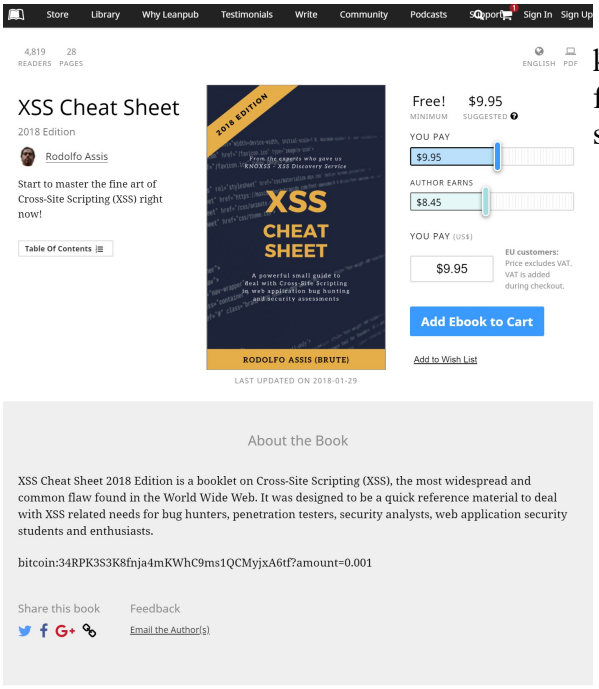
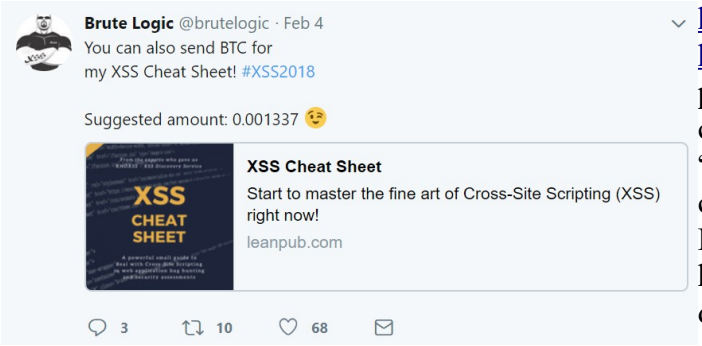


Brute created a XSS cheat sheet on Leanpub. I don't know about you but I'd assume to download something from there you need to pay. There are people had the same thought https://twitter.com/antisnatchor/status/958634877989081089. Brute could have just published the cheat sheet and asked for donation 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



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

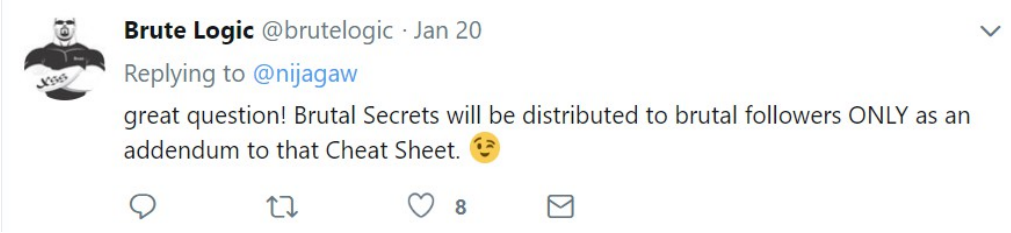
[e] Characters ignored between equals sign and parameter.

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

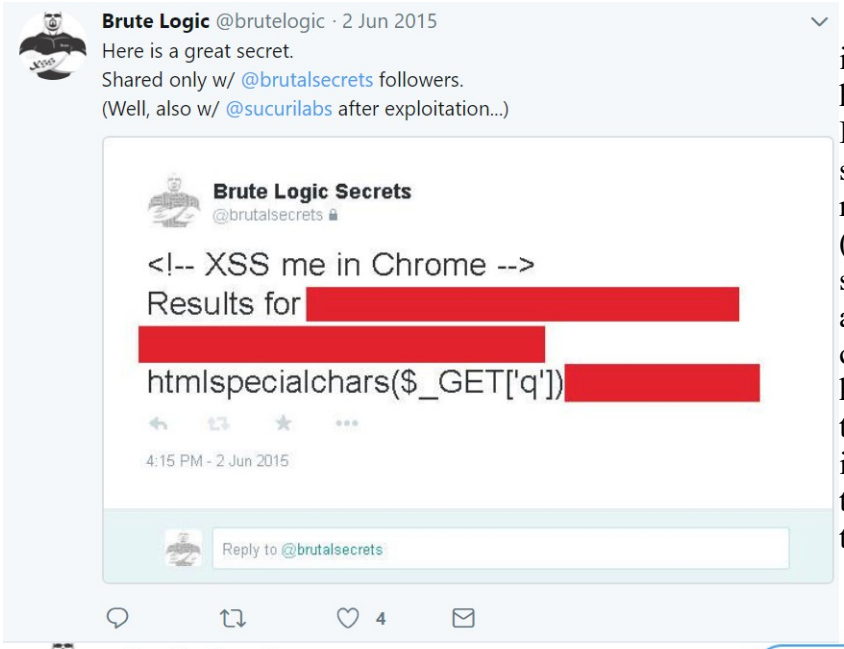
* Characters are given as decimal ASCII table index.
** There is a common rule that the unencoded null character does not exist for IE HTML parser.

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

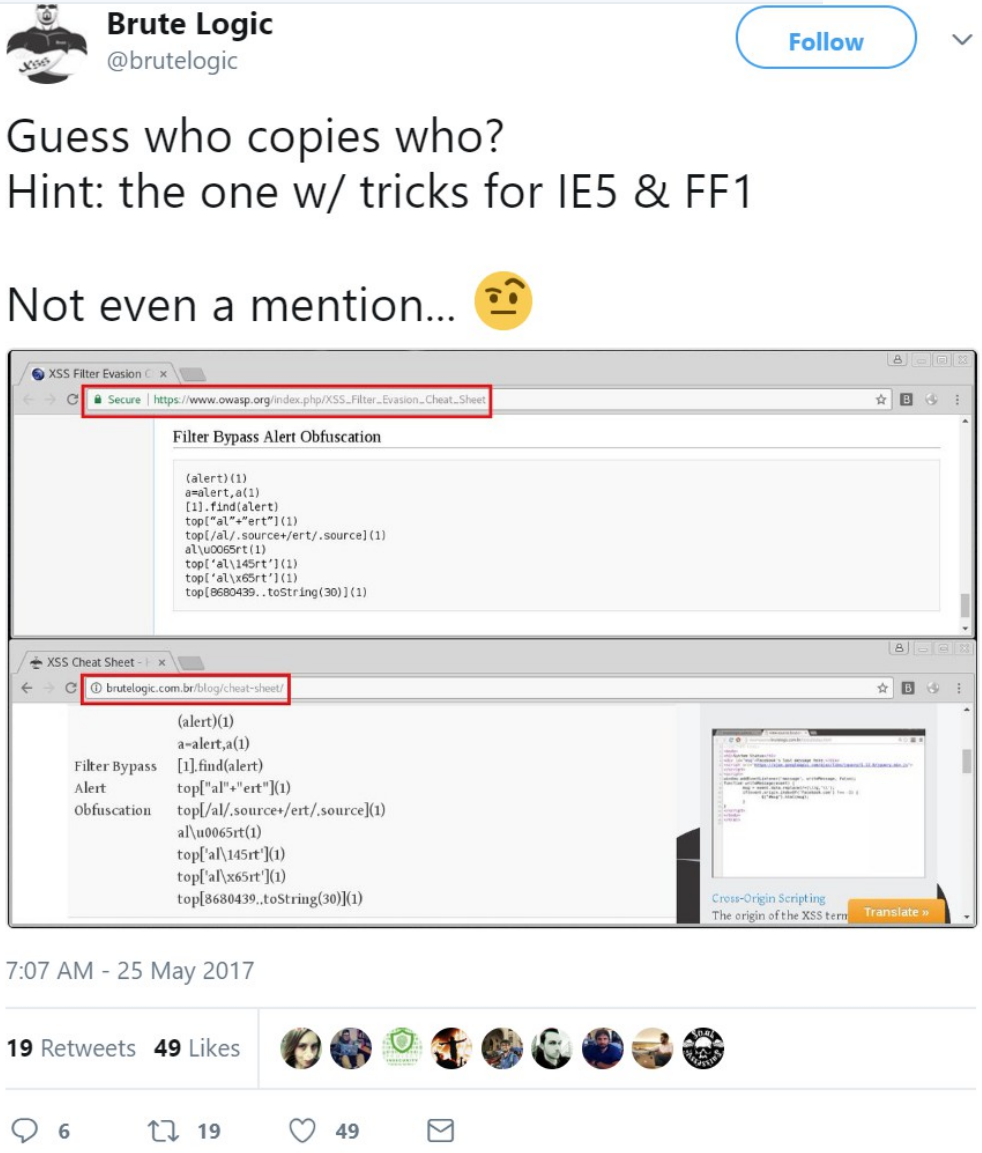
Oh, have I already mentioned Brute has something called Brute secret which you pay a subscription fee to his private Twitter account to access his exclusive XSS vectors? Looks like the cheat sheet is incomplete without you actually having to pay!



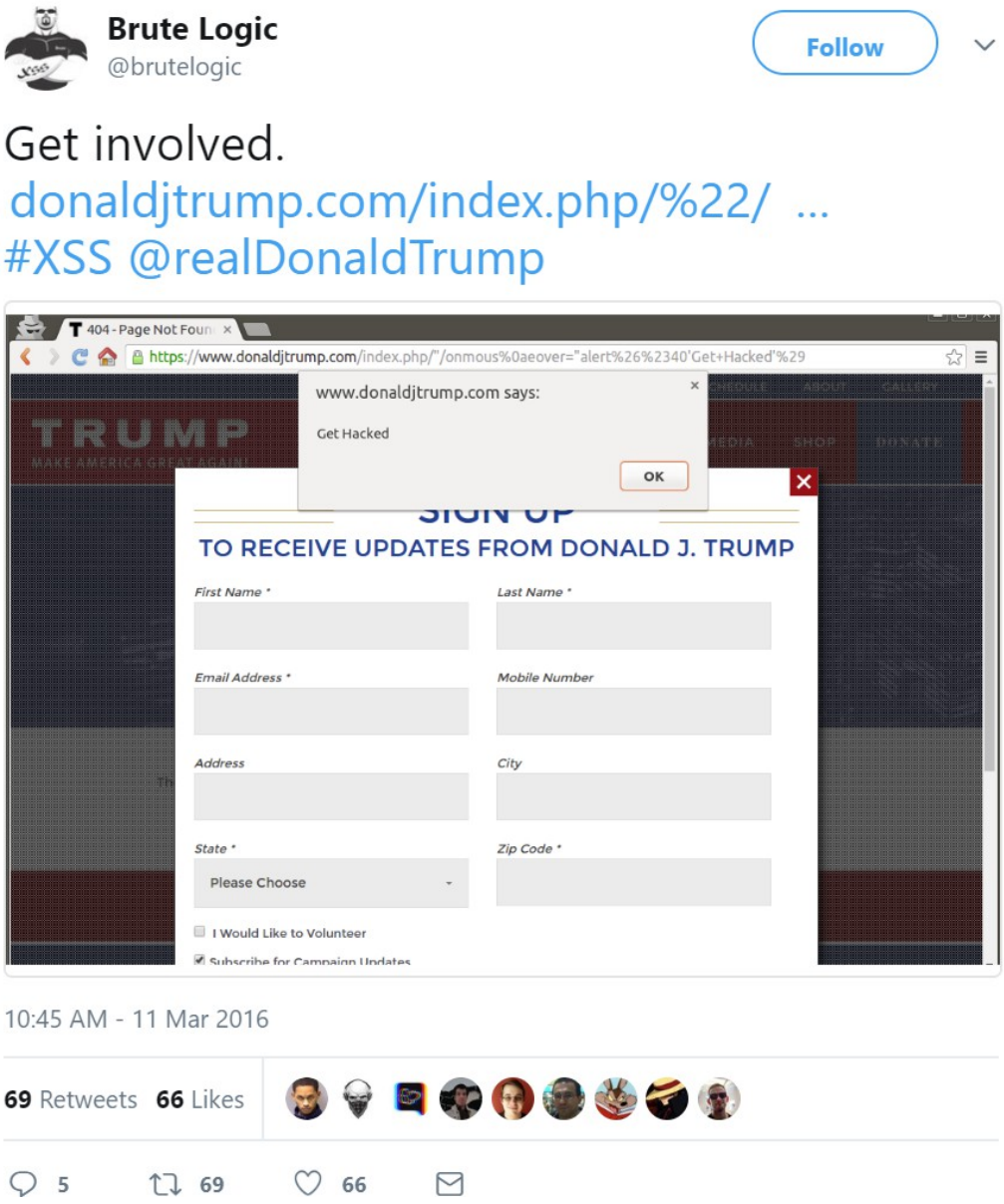
What's in Brute secret? As a non-subscriber I don't know, but some times Brute teases us with a little peek.



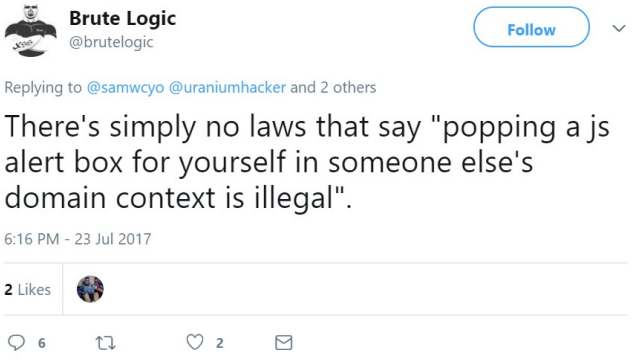
Did he mean you can XSS even your input is sanitized with htmlspecialchars in HTML context??! I gotta subscribe... Oh wait, I didn't see the red things there. In that case it must be in attribute context (htmlspecialchars is useless against scenario where you input appears on a/href, iframe/src and JavaScript 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.

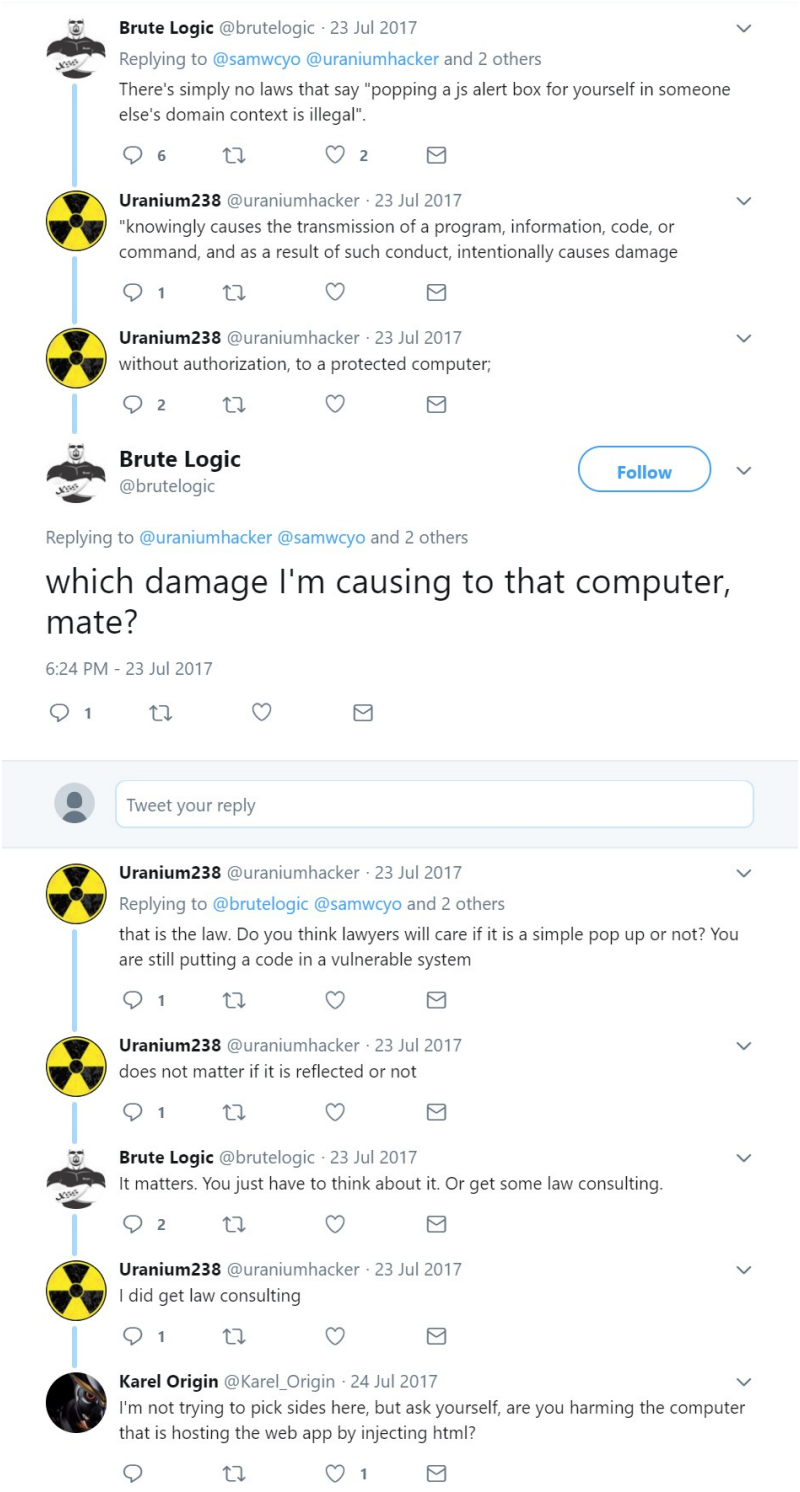


Brute really has the guts to say that. Is that "A taste of own medicine”? If this is not I don't know what is.



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





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

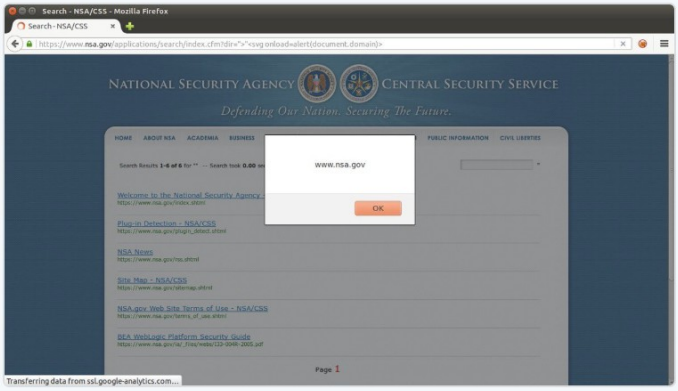
Brute Logic @brutelogic · 6 Mar 2016

NSA #XSS

(cleaned version)

nsa.gov/applications/s...

by @_lNobodyl_

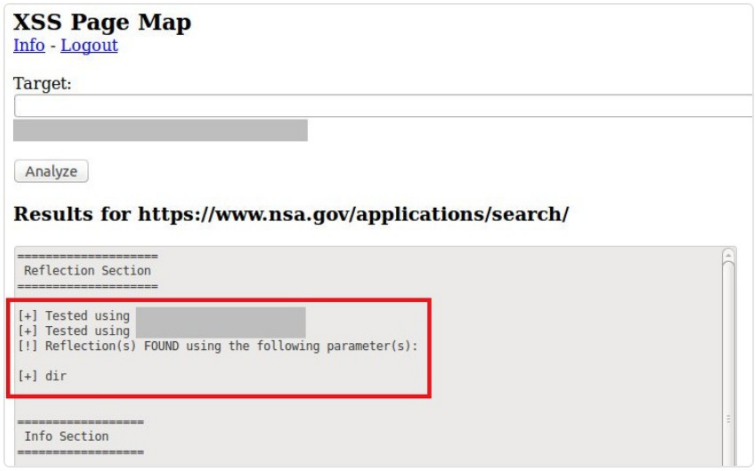


5 49 51

Brute Logic
@brutelogic

Follow

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

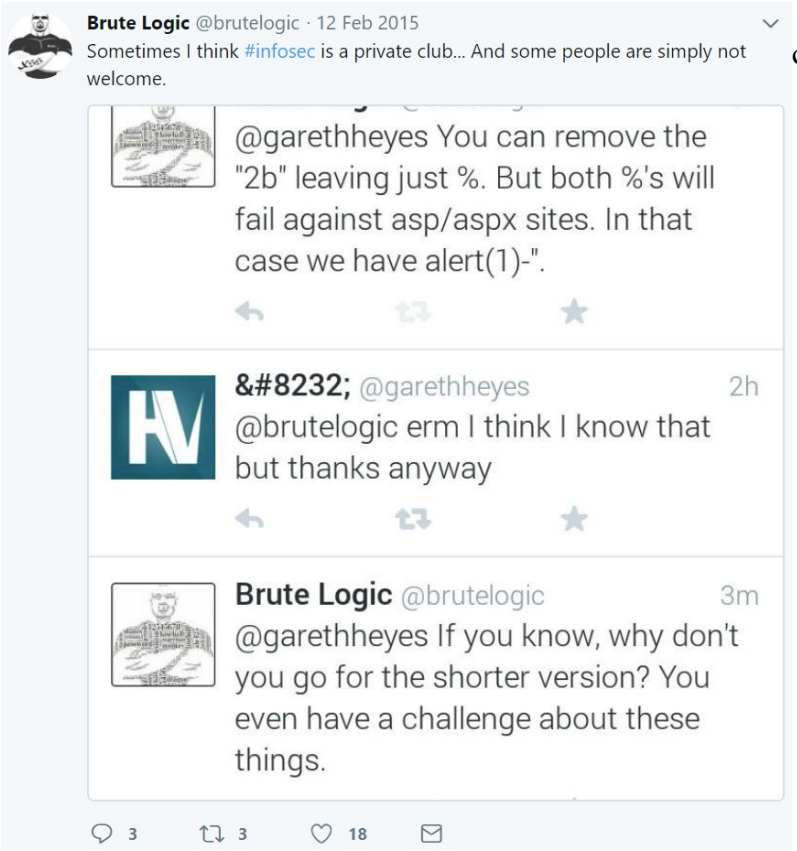


1:48 PM - 6 Mar 2016

9 Retweets **19** Likes

1 9 19

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



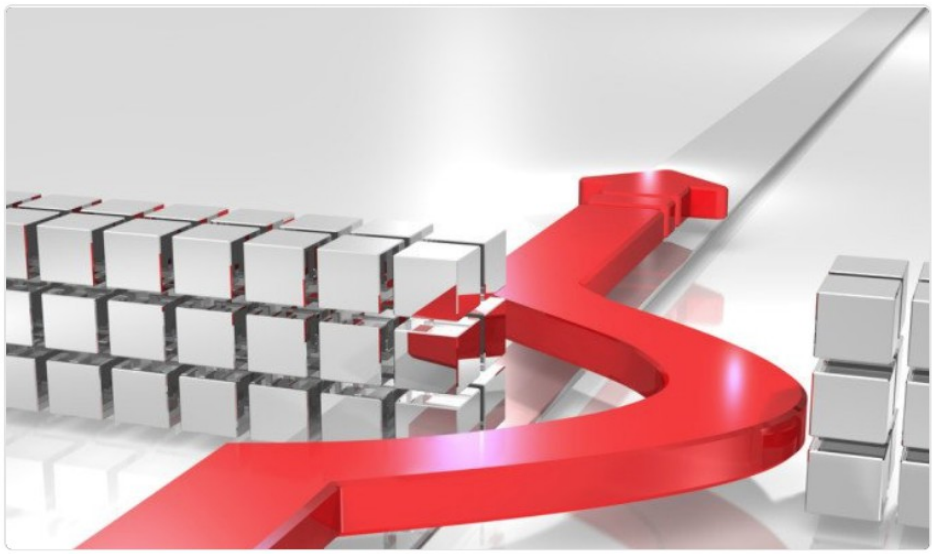
Did you find the irony? Hint: something containing the word “secret”.

Brute Logic
@brutelogic

Follow

HTML Entities for Filter Bypass

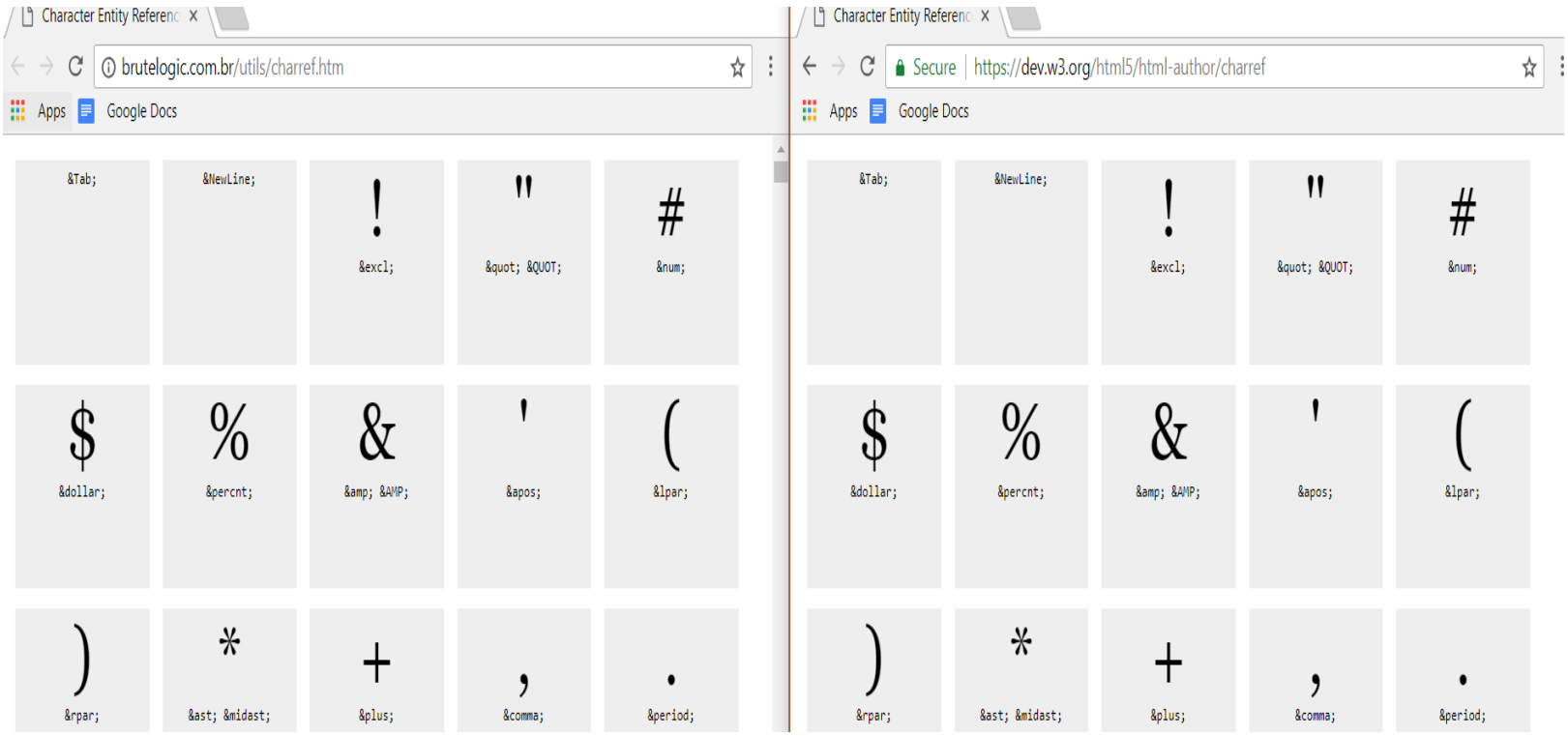
brutelogic.com.br/utils/charref....



7:49 AM - 28 Sep 2016

18 Retweets **39** Likes

3 18 39



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.

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.