

Forum:[Hack Forums](#)

Thread: [XSS CNN vector, need explanation please](#)

unnamednoob - September 8, 2012, 6:35 pm

edition.cnn.com/search/index.html?sortBy=date&primaryType=mixed&source=money&query="><iframe+onload%3Dalert%28%2FXSS%2F%29>

i don't understand how this work, im not the best at XSS, if someone mind explaining that for me? :)

KernelMode - September 8, 2012, 6:39 pm

I'm pretty sure this is how it would work... :L

"> was used to escape the value="search here".
<iframe creates an iframe.
onload= onload is when the page loads.
alert(/XSS/) displays the message box and closes the tag.

Desmolicious - September 8, 2012, 6:47 pm

That XSS was patched awhile ago. XD Same with money.cnn.com

unnamednoob - September 8, 2012, 7:06 pm

(Sep 8, 2012 06:39 PM)Affine Wrote: [\[CITE\]](#) I'm pretty sure this is how it would work... :L

"> was used to escape the value="search here".
<iframe creates an iframe.
onload= onload is when the page loads.
alert(/XSS/) displays the message box and closes the tag.
yea, i though so too, but what confussed me is when i only typed "><script>alert(0)</script> it didn't work

(Sep 8, 2012 06:47 PM)Desmolicious Wrote: [\[CITE\]](#) That XSS was patched awhile ago. XD Same with money.cnn.com
still works for me O_o, are u sure?

Jae? - September 8, 2012, 7:16 pm

(Sep 8, 2012 06:47 PM)Desmolicious Wrote: [\[CITE\]](#) That XSS was patched awhile ago. XD Same with money.cnn.com
It's obviously not patched if it's still functioning. ?

Desmolicious - September 8, 2012, 7:22 pm

(Sep 8, 2012 07:16 PM)Jewel Wrote: [\[CITE\]](#) It's obviously not patched if it's still functioning. ?D: It doesn't Function for any of my webBrowsers.. @Failure?

Jae? - September 8, 2012, 7:25 pm

(Sep 8, 2012 07:22 PM)Desmolicious Wrote: [\[CITE\]](#) D: It doesn't Function for any of my webBrowsers.. @Failure?
Strange. Check the URL hasn't messed up, it's working fine for me.

Desmolicious - September 8, 2012, 7:27 pm

(Sep 8, 2012 07:25 PM)Jewel Wrote: [\[CITE\]](#) Strange. Check the URL hasn't messed up, it's working fine for me. Alright, Maybe there's an error in the Script i'm using.

ownster - September 8, 2012, 7:35 pm

This is cooler :L

<http://edition.cnn.com/search/index.html?sortBy=date&primaryType=mixed&source=money&query=%22%3E%3Ch1%3ETROLL,%20lol%20what%20a%20fail%20page%20XD%3C/h1%3E%3Cmarquee%3E>

:D, Anyways they should fix this lmao.

JrMn - September 9, 2012, 1:22 am

(Sep 8, 2012 07:22 PM)Desmolicious Wrote: [\[CITE\]](#) D: It doesn't Function for any of my webBrowsers.. @Failure?

Chrome has a XSS filter against reflected (or non-persistent) XSS.