

Forum: [Hack Forums](#)

Thread: [Help in Defacing XSS Vulnerable site needed](#)

skillrooted - January 18, 2013, 10:09 pm

I found a xss vulnerable site which is persistent i guess..:

<http://www.madgam.es/search?key=%3Cscript%3Ealert%28%22XSS%20Vulnerable%22%29%3C%2Fscript%3E&s=>

I want to deface it from here, i've not defaced earlier but I have read a no. of articles on it, but I'm unable to apply here.

Please help

?Fear - January 18, 2013, 10:25 pm

Let's get a few things straight.

1. That is not persistent, that is the opposite of persistent. Persistent is that every time you load that page (without doctoring the link) it loads.
2. XSS can't be used to deface, all you can do is play with client side.

Best bet? Report it and see if you get recognition.

CyberSyringe - January 18, 2013, 10:25 pm

(Jan 18, 2013 11:09 PM)skillrooted Wrote: [\[CITE\]](#) I found a xss vulnerable site which is persistent i guess..:

<http://www.madgam.es/search?key=%3Cscript%3Ealert%28%22XSS%20Vulnerable%22%29%3C%2Fscript%3E&s=>

I want to deface it from here, i've not defaced earlier but I have read a no. of articles on it, but I'm unable to apply here.

Please help

Nope, not persistent, but rather non-persistent.

It's only persistent if you don't have to inject the code every time into the vector.

The only way to deface is to hijack the admin's cookie session when he is logged in. To do that you must trick the website administrator into opening the XSS link and run a cookie stealer script.

skillrooted - January 18, 2013, 10:34 pm

(Jan 18, 2013 11:25 PM)?Fear Wrote: [\[CITE\]](#) Let's get a few things straight.

1. That is not persistent, that is the opposite of persistent. Persistent is that every time you load that page (without doctoring the link) it loads.
2. XSS can't be used to deface, all you can do is play with client side.

Best bet? Report it and see if you get recognition.

Thanks for correcting me..I've reported xss earlier in some sites, hardly they reply to mails :/

(Jan 18, 2013 11:25 PM)CyberSyringe Wrote: [\[CITE\]](#) Nope, not persistent, but rather non-persistent.

It's only persistent if you don't have to inject the code every time into the vector.

The only way to deface is to hijack the admin's cookie session when he is logged in. To do that you must trick the website administrator into opening the XSS link and run a cookie stealer script.

hmm..okay got it..i've read about cookie stealing.

Thanks a lot for help :)

sp3ctrum - January 18, 2013, 10:48 pm

Just to make a few corrections in this thread, yes the XSS is not persistent but you can deface with XSS if its persistent. Just by using

`<script>window.location="http://linktoyourdeface.com/deface.html";</script>` or you could use more javascript such as `document.write` or `document.getElementById`. Its pretty simple and can be done :3

skillrooted - January 18, 2013, 10:52 pm

(Jan 18, 2013 11:48 PM)LEGITimacy™ Wrote: [\[CITE\]](#) Just to make a few corrections in this thread, yes the XSS is not persistent but you can deface with XSS if its persistent. Just by using

`<script>window.location="http://linktoyourdeface.com/deface.html";</script>` or you could use more javascript such as `document.write` or `document.getElementById`. Its pretty simple and can be done :3

Can you please give me a persistent xss vulnerable site ?

I want to try defacing thing..

H4x0r r0cky - January 18, 2013, 11:07 pm

Skill rooted why not keep searching,you might come across a site that is vulnerable to persistent xss..But its rare.

CyberSyringe - January 18, 2013, 11:10 pm

(Jan 18, 2013 11:48 PM)LEGITimacy™ Wrote: [\[CITE\]](#) Just to make a few corrections in this thread, yes the XSS is not persistent but you can deface with XSS if its persistent. Just by using

`<script>window.location="http://linktoyourdeface.com/deface.html";</script>` or you could use more javascript such as `document.write` or `document.getElementById`. Its pretty simple and can be done :3

You forgot that in order to deface the main page, there must be a persistent that can be executed from the main page.

vehla - January 18, 2013, 11:14 pm

(Jan 19, 2013 12:10 AM)CyberSyringe Wrote: [\[CITE\]](#) You forgot that in order to deface the main page, there must be a persistent that can be executed from the main page.

He didn't meant to deface the main page though as I read. ?

sp3ctrum - January 18, 2013, 11:20 pm

Yes I'm aware of that. The possibility of finding a persistent XSS is very little and especially on the home page to begin with. I was implying defacing in general, although much more can be done with it besides defacing, xss shell, beef exploitation, taking advantages of redirect links to your shitcash or whatever, etc..

skillrooted - January 18, 2013, 11:21 pm

(Jan 19, 2013 12:07 AM)H4x0r r0cky Wrote: [\[CITE\]](#) Skill rooted why not keep searching,you might come across a site that is vulnerable to persistent xss..But its rare.

Yes, I'm searching to search for a persistent one:)

jp000006 - January 19, 2013, 12:27 am

try looking for websites that accepts comments, like forums or whatsoever..u can 'persistent xss' that

skillrooted - January 19, 2013, 3:06 am

(Jan 19, 2013 01:27 AM)jp006 Wrote: [\[CITE\]](#) try looking for websites that accepts comments, like forums or whatsoever..u can 'persistent xss' thatokay..thanks for the advice, i will look out for it :)

vehla - January 19, 2013, 3:26 am

Nowadays, I find most of sites vulnerable to Persistent xss. Just use your brain and you can find 1 for sure in every site.

LevelUp - January 19, 2013, 3:43 am

This is a non persistant XSS.

You can't do much with this site because it uses a Facebook Login rather than its own, and I can't seem to find the admin panel.

If circumstances were different:

Set up a PHP Cookie Stealer which stores the data in a .txt then hex/shorten this URI and send it to the admin.

Code

<http://www.madgam.es/search?key=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&s=>

skillrooted - January 19, 2013, 7:27 am

(Jan 19, 2013 04:43 AM)LevelUp Wrote: [\[CITE\]](#) This is a non persistant XSS.

You can't do much with this site because it uses a Facebook Login rather than its own, and I can't seem to find the admin panel.

If circumstances were different:

Set up a PHP Cookie Stealer which stores the data in a .txt then hex/shorten this URI and send it to the admin.

Code

<http://www.madgam.es/search?key=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E&s=>

yeah..cookie stealing is one good method indeed. :)

zombiehacker - January 19, 2013, 7:30 am

I'm sorry to say it but you cannot do much with that.

Whiteh4t - January 19, 2013, 8:27 am

Find a google dork list 4 persistent. it's easy.

skillrooted - January 19, 2013, 8:52 am

(Jan 19, 2013 08:30 AM)zombiehacker Wrote: [\[CITE\]](#) I'm sorry to say it but you cannot do much with that.hmmm..yeah sir..I've seen a number of tut's by you..great work!

and I know you are really good at XSS too :)

(Jan 19, 2013 09:27 AM)Whiteh4t Wrote: [\[CITE\]](#) Find a google dork list 4 persistent. it's easy.

I guess there is so specific dork for "persistent xss". The sites you search with dorks, you have to test them too for any type of XSS :)

Whiteh4t - January 19, 2013, 10:01 am

u genius skillrooted. absolutely. i takes about 10 min. search guestbook

21redallday12 - January 19, 2013, 1:40 pm

Does anyone know why this Non persistent XSS vuln, reflect my alert script?
(show two alerts instead of one?)