Forum:Hack Forums

Thread: [XSS]4chan.org[XSS]

Lozab - *September 25, 2013, 3:08 am*

Method: Post XSS
Spoiler (Click to View)

Not many people have found vulns in 4chan so this is a great little achievement for me. lol

and also for those who will say this is probably fake, the page isn't fully loaded.

if you know 4chan, it'll ask you to type out a captcha after the message that was shown in the screen shot.

Anyways Thoughts?

Night Baron - *September 25, 2013, 6:34 am*

If it is persistent one, then it is very useful >:)
(evil laugh)

Well, congrats! :D

Lil Benadryl - *September 25, 2013, 6:44 am*

How the hell did you get so good at XSS? I need to learn it, but I have been procrastinating :/. Anyways nice find ?!

frictionless - *September 25, 2013, 7:35 am*

he blacked out half of the link to hide the fact that it is nothing more than a self xss

Lozab - *September 25, 2013, 8:20 am*

(Sep 25, 2013 07:35 AM)frictionless Wrote: *[CITE]* he blacked out half of the link to hide the fact that it is nothing more than a self xss
Are you mentally retarded Mr.Sherlock? I said its a post XSS.
and I obviously blacked out the link because I'd rather keep it as a 0day than give it out to some idiot and probably will take the credits for himself.

Hell even when I click on "OK"
This shit shows up

frictionless - *September 25, 2013, 8:58 am*

(Sep 25, 2013 08:20 AM)Lozab Wrote: *[CITE]* Are you mentally retarded Mr.Sherlock? I said its a post XSS.
and I obviously blacked out the link because I'd rather keep it as a 0day than give it out to some idiot and probably will take the credits for himself.

Hell even when I click on "OK"
This shit shows up

xss != 0day.

do you feel accomplished with yourself for earning your first skidmark

Lozab - *September 25, 2013, 9:21 am*
(Sep 25, 2013 08:58 AM)frictionless Wrote: [CITE] xss != 0day.

do you feel accomplished with yourself for earning your first skidmark
Actually, lots of people call it a 0day, you're just little noob aren't you? :)

Seriously if you're gonna flame, just get off this thread.

Rayquaza™ - *September 25, 2013, 9:24 am*
(Sep 25, 2013 08:58 AM)frictionless Wrote: [CITE] xss != 0day.

do you feel accomplished with yourself for earning your first skidmark
A 0DAY is when it hasn't been discovered you moron.

OhNoMoney - *September 25, 2013, 9:27 am*
(Sep 25, 2013 09:24 AM)Dev?l Wrote: [CITE] A 0DAY is when it hasn't been discovered you moron.
If it's not discovered how can you apply it?

Zero day simply means the Receiver of the attack had zero days to patch the vuln..
It's a rare exploit in other hands, and it's unknown by the system that it's being used.

Lozab - *September 25, 2013, 9:29 am*
(Sep 25, 2013 09:27 AM)OhNoMoney Wrote: [CITE] If it's not discovered how can you apply it?

Zero day simply means the Receiver of the attack had zero days to patch the vuln..
It's a rare exploit in other hands, and it's unknown by the system that it's being used.
Eh? 0day means that has not been released or known about by the general public.

MaXoNe - *September 25, 2013, 9:32 am*
I thought IE users dies with dinosaurs.

Lozab - *September 25, 2013, 9:35 am*
(Sep 25, 2013 09:32 AM)MaXoNe Wrote: [CITE] I thought IE users dies with dinosaurs.
it's actually hell of a lot easier to find XSS with IE...For me at least.

MaXoNe - *September 25, 2013, 10:05 am*
Use Owasp Mantra , it's like Mozilla on steroids :)

Mario - *September 25, 2013, 6:40 pm*
Anyone calling this is 0day is retarded. Plain and simple

Good find OP

Corwin - *September 25, 2013, 6:42 pm*
Nice find, OP.

Some of the people in here need to learn their interwebsss.

Ryan?? - *September 25, 2013, 6:51 pm*
The above conversations were amusing.

Way to go, OP. Nice find!

harveyhf - *September 25, 2013, 9:23 pm*
(Sep 25, 2013 09:35 AM)Lozab Wrote: [CITE] it's actually hell of a lot easier to find XSS with IE...For me at least.
what? How does the browser effect how easily it is to find XSS exploits....

Lozab - *September 25, 2013, 11:31 pm*
(Sep 25, 2013 09:23 PM)harveyhf Wrote: [CITE] what? How does the browser effect how easily it is to find XSS exploits....
Well you're probably still haven't learned much about XSS filters, most people will tell you to use Firefox because it doesn't filter out XSS, that's not entirely true because Firefox filters some queries that are important, however IE if you disable XSS filters, there is more chances of you finding XSS, I can't really explain it because I'm on a phone atm, but my XSS on 4chan seems to be working on both browsers.

So I use IE so I don't miss any valuable XSS vulns.

cheatson - *September 25, 2013, 11:48 pm*
(Sep 25, 2013 09:23 PM)harveyhf Wrote: [CITE] what? How does the browser effect how easily it is to find XSS exploits....
More than a few differences, although XSS vulns in IE aren't a catch-all, each of the browsers potentially can render DOM XSS differently so it is kinda contextual. The main difference in normal XSS scope are that Internet explorer allows in-style expression statements which can run javascript, <IE6 could bypass filters when character encoding was not specified in the HTTP header, and back-tick operators could be used in certain situations in place of quotation marks.

3vilHacker - *September 26, 2013, 12:40 pm*
Um forget what I just said im tired....

?Alexander - *September 27, 2013, 10:01 am*
(Sep 25, 2013 09:27 AM)OhNoMoney Wrote: [CITE] If it's not discovered how can you apply it?

Zero day simply means the Receiver of the attack had zero days to patch the vuln..
It's a rare exploit in other hands, and it's unknown by the system that it's being used.
LOLing at you. You're probably just quoting the wikipedia page of 0day, am I right?

Please just leave if you don't know shit and have to look it up on wikipedia.

B0$$ - *September 27, 2013, 10:42 am*
Nice find OP !! and i totally have to agree had a good laugh !~! ;D

Spoiler (Click to View)Quote: OhNoMoney Wrote: If it's not discovered how can you apply it?

Zero day simply means the Receiver of the attack had zero days to patch the vuln..
It's a rare exploit in other hands, and it's unknown by the system that it's being used.
busted !! ? ? ?