

Forum:[Hack Forums](#)

Thread: [\[XSS\]XSS in Yahoo.com\[XSS\]](#)

Lozab - September 6, 2013, 12:05 pm

Spoiler ([Click to View](#))

Alexa rank: 4

I don't like to share stuff, so that's why I blacked out most of the page, I'd love to see if anyone finds it though.

Thoughts?

Dr41DeY - September 6, 2013, 12:23 pm

Thanks, for posting! :D

Looks, good :p

Gonna, check this out :^)

PickledHax - September 6, 2013, 12:34 pm

Wow, that's a nice find... Are you going to report it? :P

P????ce - September 6, 2013, 12:38 pm

I am sure that many people now would have reported to yahoo in order to get credits :p you should have reported it to yahoo first.

Lozab - September 6, 2013, 12:53 pm

lol I doubt it, plus if they found it on there own, I don't mind, but using my picture is useless since they don't have the codes needed for the XSS.

Cathal - September 6, 2013, 12:55 pm

(Sep 6, 2013 12:53 PM)Lozab Wrote: [\[CITE\]](#) lol I doubt it, plus if they found it on there own, I don't mind, but using my picture is useless since they don't have the codes needed for the XSS.

Finding the vector is the easy part.

Lozab - September 6, 2013, 1:01 pm

(Sep 6, 2013 12:55 PM)MrCathal09 Wrote: [\[CITE\]](#) Finding the vector is the easy part.

well yeah if its the normal <script> alert stuff, but yeah idc, I have already reported it so yeah.

?????Thr????? - September 6, 2013, 1:05 pm

I don't think anyone saw this one coming.

SHADOW REALM - September 6, 2013, 8:30 pm

(Sep 6, 2013 01:05 PM)Thr??? Wrote: [\[CITE\]](#)

I don't think anyone saw this one coming.

Omg Gimme Plz, i want It Sooo Bad

/troll

P???ce - September 7, 2013, 1:54 am

(Sep 6, 2013 01:05 PM)Thr??? Wrote: [\[CITE\]](#)

I don't think anyone saw this one coming.
there was a video on youtube of 2012 regarding this dear :)

byRadial - September 7, 2013, 2:06 am

This thread is getting more interesting by the minute.

Atrocious? - September 7, 2013, 3:35 am

Can you give me the link (without vector)

Thanks :)

Lozab - September 7, 2013, 5:14 am

(Sep 7, 2013 02:06 AM)byRadial Wrote: [\[CITE\]](#) This thread is getting more interesting by the minute.
I'm gonna post more cool XSS findings later, Bing is one of them. ;)

momoattacker - September 7, 2013, 5:53 am

Cool man.. ????

smiegles - September 7, 2013, 7:32 am

bing, no problem

<https://i.imgur.com/qlfb8XU.png>

?Alexander - September 7, 2013, 11:31 am

(Sep 6, 2013 01:05 PM)Thr??? Wrote: [\[CITE\]](#)

I don't think anyone saw this one coming.
Didn't saw this coming, did you?

Gee4rce - September 7, 2013, 6:00 pm

@Lozab (OP):

Very nice find of yours, Congrats!

Sadly yahoo will pay no money for finds, instead you get a yahoo T-Shirt for free, so i would keep it
Oday if i were you.

Would not suggest it to send around or show it to anybody else,- especially not HF Members ;)

@All others:

Nice finds (congratz also to Smiegles on the bing one!) and funny to read, but i'm not shure though
if the hackforums ones are real, but still funny to read, lol ^^

@byRadial:

Yes this thread indeed is turning out very interesting :3

Greets, Gee.

P.S.:

Google, Main search API... DOM-Based XSS - Persistent and kept 0day for about 1,5 years.

[img]http://img577.imageshack.us/img577/2153/qr9b.png[/img]

Greetings, Gee.

webdev77 - September 7, 2013, 6:03 pm

(Sep 7, 2013 06:00 PM)Gee4rce Wrote: [\[CITE\]](#) @Lozab (OP):

Very nice find of yours, Congrats!

Sadly yahoo will pay no money for finds, instead you get a yahoo T-Shirt for free, so i would keep it 0day if i were you.

Would not suggest it to send around or show it to anybody else,- especially not HF Members ;)

@All others:

Nice finds (congratz also to Smiegles on the bing one!) and funny to read, but i'm not shure though if the hackforums ones are real, but still funny to read ?

Greetings, Gee.

P.S.:

Google, Main search API... DOM-Based XSS - Persistent and 0day.

[img]http://img577.imageshack.us/img577/2153/qr9b.png[/img]

Greetings, Gee.

Let us know when you receive your award from google if that's real.

133720 - September 7, 2013, 7:32 pm

Nice found .

Very Good in XSS.

I need to learn more about the XSS from you.

Lozab - September 7, 2013, 11:49 pm

(Sep 7, 2013 07:32 AM)smiegles Wrote: [\[CITE\]](#) bing, no problem

<https://i.imgur.com/qlfb8XU.png>

Spoiler [\(Click to View\)](#)

XSS^

@Gee4rce

I will keep this as a 0day, since Yahoo haven't responded to me if they reward peeps.

and Really nice find bro. :O

EXPLICIT CONTENT - September 8, 2013, 1:25 am

Since, we all are bragging about our 1337 0-Dayz, here we go

Spoiler [\(Click to View\)](#)

Yup, its persistent XSS, got multiple of them, all are non reported :P

Lozab - September 8, 2013, 1:40 am

(Sep 8, 2013 01:25 AM)Codah Wrote: [\[CITE\]](#) Since, we all are bragging about our 1337 0-Dayz, here we go

Spoiler ([Click to View](#))

Yup, its persistant XSS, got multiple of them, all are non reported :P
Isn't this XSS on 1337day?

actersss

EXPLICIT CONTENT - September 8, 2013, 1:42 am

(Sep 8, 2013 01:40 AM)Lozab Wrote: [\[CITE\]](#) Isn't this XSS on 1337day?

actersss

It is, and also in the Deepweb, but there are multiple ones, and soon there will be one for sale here, as I am in need for some cash

Lozab - September 8, 2013, 1:45 am

(Sep 8, 2013 01:42 AM)Codah Wrote: [\[CITE\]](#) It is, and also in the Deepweb, but there are multiple ones, and soon there will be one for sale here, as I am in need for some cash
Oh, So its one of those stored XSS's in paypal right?

EXPLICIT CONTENT - September 8, 2013, 1:48 am

(Sep 8, 2013 01:45 AM)Lozab Wrote: [\[CITE\]](#) Oh, So its one of those stored XSS's in paypal right?
It is stored and it affects two sites, means you kinda can "infect" another one by interacting with other users, with sending money or via other ways.
Once they login, the vector will execute and they are fucked (nah, depends on the Vector)

HolyGates - September 8, 2013, 1:56 am

daym nice find man! yahoo got rocked.

eight - September 8, 2013, 1:59 am

Nice find. Have you decided on reporting it yet?

Lozab - September 8, 2013, 2:01 am

(Sep 8, 2013 01:59 AM)drugs? Wrote: [\[CITE\]](#) Nice find. Have you decided on reporting it yet?
Well I'm currently waiting for there Response.

but some people say Yahoo doesn't reward people who find Exploits, not sure about that.

TheKingOfArabs - September 8, 2013, 2:16 am

(Sep 8, 2013 02:01 AM)Lozab Wrote: [\[CITE\]](#) Well I'm currently waiting for there Response.

but some people say Yahoo doesn't reward people who find Exploits, not sure about that.
I'm pretty sure they send you a yahoo shirt.

Google and Facebook reward \$500.

EXPLICIT CONTENT - September 8, 2013, 2:25 am

(Sep 8, 2013 02:16 AM)Clash of clans Wrote: [\[CITE\]](#) I'm pretty sure they send you a yahoo shirt.

Google and Facebook reward \$500. Google's minimum is 100\$, and Facebook's minimum reward is 500, you get more than 500\$ for an XSS ;)

TheKingOfArabs - September 8, 2013, 2:29 am

(Sep 8, 2013 02:25 AM)Codah Wrote: [\[CITE\]](#) Google's minimum is 100\$, and Facebook's minimum reward is 500, you get more than 500\$ for an XSS ;)

I know.

You just repeated what I said.

EXPLICIT CONTENT - September 8, 2013, 2:31 am

(Sep 8, 2013 02:29 AM)Clash of clans Wrote: [\[CITE\]](#) I know.

You just repeated what I said.

I did not, you said they both reward 500 Dollars, which in fact is not true.

No offense, just saying ;)

smiegles - September 8, 2013, 2:58 am

Yahoo gives a 25\$ code for there company store.

Gee4rce - September 9, 2013, 12:09 am

(Sep 7, 2013 06:03 PM)webdev77 Wrote: [\[CITE\]](#) Let us know when you receive your award from google if that's real.

I understand your worries, things have been faked here in the past...

But i have proofed at several hard XSS challenges in the past, and if you have been active in this section for longer,

you should know that i am able to afford a find like the google.com one ?

Also, i need to get something straight here:

The google XSS i posted about is not active anymore- i kept it 0day for about 1,5 year, until it was gone some day due to code redesign i am shure.

This was my only chance till now to get into google's Hall of Fame - but i just didn't bother, lol ^^ I have quitted reporting at this point and feel happy with it :)

I have wrote 0day, since i have copied the Description out of a txt file where i keep info of my XSS. I have corrected my post.

But anyways, i may drop a video here from it soon i think...

(Sep 7, 2013 11:49 PM)Lozab Wrote: [\[CITE\]](#) ...Really nice find bro. :O

Thanks, and the bing one seems also great! :)

@Codah: Nice one on paypal mate!!

And thanks to the others for the gratz! ?