

Forum:[Hack Forums](#)

Thread: [TWO XSS Vulnerabilities Found in HackForums - Reported](#)

Punisher - April 14, 2018, 1:43 pm

Hey guys,

I was messing around trying to find possible security incidents that could affect members and stumbled across two XSS reflection exploits.

The two vulnerable pages were the Buy Sticky and Sales Tags, both have been patched since reporting.

Glad to help keep everyone safe! ?

Proof:

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

vad0x - April 14, 2018, 1:46 pm

Lol nice find man!! Im surprised omni didnt give you a award or anything

iNuke - April 14, 2018, 1:52 pm

That is so cool, nice one mate. A cool bragging thread ?

Punisher - April 14, 2018, 2:01 pm

(Apr 14, 2018 01:46 PM)Blazius Wrote: [\[CITE\]](#) Lol nice find man!! Im surprised omni didnt give you a award or anything

Thanks!

That would be awesome!

(Apr 14, 2018 01:52 PM)iNuke Wrote: [\[CITE\]](#) That is so cool, nice one mate. A cool bragging thread ?

Appreciate it, thanks for the kind words man

Crystallize. - April 14, 2018, 2:05 pm

That is awesome dude Ive been watching your replies when you were helping Omni in some threads, good job!

Mr. Robot - April 14, 2018, 2:07 pm

I hope you get signature privileges back, assuming these were based on the recent mybb ones reported hence the timing between them?

Eccy - April 14, 2018, 2:08 pm

Thanks for keeping us safe (:

Elitas - April 14, 2018, 2:09 pm

Good job dude. I'd love to hear the actual PoC so I can maybe learn from this. I read your post on XMPP earlier and it inspired me to do a little bit of hunting myself.

I'm pretty sure I've tested out those pages before too though!

Punisher - April 14, 2018, 2:10 pm

(Apr 14, 2018 02:07 PM)Mr. Robot Wrote: [\[CITE\]](#) I hope you get signature privileges back, assuming these were based on the recent mybb ones reported hence the timing between them?

Thanks, I really appreciate it - indeed that was my request to him, but I don't know if I will get them back

I reported a bypass on signature/post restrictions, a recent bug in a mycode tag that the mybb team is patching, and now these two XSS reflections

Cypical - April 14, 2018, 2:11 pm

Thought Omni said he would give \$10k to someone who found a vulnerability that could potentially affect users.

Nachfolger - April 14, 2018, 2:17 pm

Why didn't you get the angel wings then?

You got scammed boi.

Elitas - April 14, 2018, 2:20 pm

Ha! Just found an XSS myself, reporting it now.

Thanks for inspiring me to search for something. Cheers!

Punisher - April 14, 2018, 2:21 pm

(Apr 14, 2018 02:08 PM)Eccy Wrote: [\[CITE\]](#) Thanks for keeping us safe (:
No problem! ;D

(Apr 14, 2018 02:09 PM)Elitas Wrote: [\[CITE\]](#) Good job dude. I'd love to hear the actual PoC so I can maybe learn from this. I read your post on XMPP earlier and it inspired me to do a little bit of hunting myself.

I'm pretty sure I've tested out those pages before too though!

It's in the OP, basically the page accidentally reflected the input from the URL without sanitizing it

That allowed me to close the input box using ">" and add anything you want to the page after that

(Apr 14, 2018 02:11 PM)Cypical Wrote: [\[CITE\]](#) Thought Omni said he would give \$10k to someone who found a vulnerability that could potentially affect users.

You have to access his profile from the database or drop a file like config.php to claim that reward

This was more of a reflected string problem. I definitely could have crafted a special link on the vulnerable page that grabbed his session, then sent him a pm saying "hey every time I click this link the page doesn't load properly" and once he loaded the page I could grab his session and login as him. But I enjoy being a member of HackForums and I'm not a malicious person. :D

Eccy - April 14, 2018, 2:23 pm

(Apr 14, 2018 02:20 PM)Elitas Wrote: [\[CITE\]](#) Ha! Just found an XSS myself, reporting it now.

Thanks for inspiring me to search for something. Cheers!
Damn, wish I knew what XSS meant so I could find one and get my first award.

Punisher - April 14, 2018, 2:29 pm

(Apr 14, 2018 02:20 PM)Elitas Wrote: [\[CITE\]](#) Ha! Just found an XSS myself, reporting it now.

Thanks for inspiring me to search for something. Cheers!

Nice work. These threads are great for keeping users aware that clicking links on the internet is not always safe!

Even sites that you think are 100% secure always have a few small bugs

Google, Facebook, etc all face these same issues

It's nice having an unofficial group of users going around the forum auditing security, it allows the good guys the time to report the exploits before they get abused.

Elitas - April 14, 2018, 3:46 pm

Hmm, think I found a persistent XSS too. I didn't test it but mentioned it to Omni and he said he fixed it. Glad it's all fixed up now, thanks for inspiring me to look into this stuff again BTW.. ?

Windows - April 14, 2018, 3:52 pm

(Apr 14, 2018 03:46 PM)Elitas Wrote: [\[CITE\]](#) Hmm, think I found a persistent XSS too. I didn't test it but mentioned it to Omni and he said he fixed it. Glad it's all fixed up now, thanks for inspiring me to look into this stuff again BTW.. ?

You shoulda gave me the XSS so I could report it to Omni and get the award ? ?

Elitas - April 14, 2018, 3:53 pm

(Apr 14, 2018 03:52 PM)???d??? Wrote: [\[CITE\]](#) You shoulda gave me the XSS so I could report it to Omni and get the award ? ?

? Giving the award to more people makes it worth less! To hell with that. Maybe now he'll remove the award from all these other noobs and I can be the kind of whitehatness.

Deep inside I got that urge to keep reporting and hope I become to first to get the award twice.

Crystallize. - April 14, 2018, 4:03 pm

Unity is proud to have members like you guys. :)

Elitas - April 14, 2018, 4:06 pm

Haha, thanks Crystallize. I have found 2 (sort of) reflected XSS issues today, not really very important at all.

1 persistent, which I would say is a medium risk. And now just looking at some bugs and other things, had a really good night. I'm not performing to my best because of what I'm drinking, but yeah maybe in the morning I'll wake up and read all these notes I'm making and figure out some more stuff lol.

Punisher - April 14, 2018, 5:59 pm

(Apr 14, 2018 02:17 PM)Nachfolger Wrote: [\[CITE\]](#) Why didn't you get the angel wings then?

You got scammed boi.

I should make a deal dispute, huh? Haha - actually Omni was nice enough to restore my signature privileges

(Apr 14, 2018 02:23 PM)Eccy Wrote: [\[CITE\]](#) Damn, wish I knew what XSS meant so I could find one

and get my first award.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications.

XSS enables attackers to inject client-side scripts into web pages viewed by other users.

(Apr 14, 2018 03:46 PM)Elitas Wrote: [\[CITE\]](#) Hmm, think I found a persistent XSS too. I didn't test it but mentioned it to Omni and he said he fixed it. Glad it's all fixed up now, thanks for inspiring me to look into this stuff again BTW.. ?

No problem, it's surprising there were so many hiding out in the open. It was like a late easter egg hunt LOL

(Apr 14, 2018 03:52 PM)???d??? Wrote: [\[CITE\]](#) You shoulda gave me the XSS so I could report it to Omni and get the award ? ?

Here I uploaded a c99 shell to the main directory, enjoy lol -

<https://admin:panel@hackforums.net/shell.php?login=admin>

(Apr 14, 2018 04:03 PM)Crystallize. Wrote: [\[CITE\]](#) Unity is proud to have members like you guys. :) Thanks Crystallize, proud to be a member!

(Apr 14, 2018 04:06 PM)Elitas Wrote: [\[CITE\]](#) Haha, thanks Crystallize. I have found 2 (sort of) reflected XSS issues today, not really very important at all.

1 persistent, which I would say is a medium risk. And now just looking at some bugs and other things, had a really good night. I'm not performing to my best because of what I'm drinking, but yeah maybe in the morning I'll wake up and read all these notes I'm making and figure out some more stuff lol.

Nice work Elitas ?

OrangeBBQ - April 14, 2018, 6:09 pm

Nice XSS man. Go get yourself a job with those skills! :P

f_ck - April 14, 2018, 6:38 pm

Awesome dude, they give you a bounty or something cx ?

Punisher - April 14, 2018, 7:35 pm

(Apr 14, 2018 06:09 PM)OrangeBBQ Wrote: [\[CITE\]](#) Nice XSS man. Go get yourself a job with those skills! :P

Thanks :D

That would be cool, currently have an awesome job though!

(Apr 14, 2018 06:38 PM)f_ck Wrote: [\[CITE\]](#) Awesome dude, they give you a bounty or something cx ?

Omni randomly rewards users on his own discretion.

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

Meow - April 15, 2018, 6:14 am

You could've at least gotten an award for that report. Anyway, nice one, I'm sure Omni is thankful for you reporting it.

Money- - April 15, 2018, 6:18 am

Nice find man , do you got some sort of black hat award where I seen some other users have it.

Punisher - April 15, 2018, 9:34 am

(Apr 15, 2018 06:14 AM)Meow? Wrote: [\[CITE\]](#) You could've at least gotten an award for that report. Anyway, nice one, I'm sure Omni is thankful for you reporting it. Maybe next time I report a bug. :D

(Apr 15, 2018 06:18 AM)Money- Wrote: [\[CITE\]](#) Nice find man, do you got some sort of black hat award where I seen some other users have it. That depends on if Omni thinks I deserve it.

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

Money- - April 16, 2018, 12:01 am

(Apr 15, 2018 09:34 AM)Punisher Wrote: [\[CITE\]](#) Maybe next time I report a bug :D

I've wanted that award for years man, YEARS!
Years huh? Haha , you actually spent your time searching for vulnerabilities hidden in this forum?

The award is kinda cool to be honest , I don't know how its obtained. Since there is like multiple of them with different descriptions that I seen some members have.

I wish I can have it too , ain't a security expert anyways.

Punisher - July 8, 2018, 7:23 pm

(Apr 16, 2018 12:01 AM)Money- Wrote: [\[CITE\]](#) Years huh? Haha , you actually spent your time searching for vulnerabilities hidden in this forum?

The award is kinda cool to be honest , I don't know how its obtained. Since there is like multiple of them with different descriptions that I seen some members have.

I wish I can have it too , ain't a security expert anyways.

I've just wanted the the BlackHat for years, not searched for vulns for years lmao.

I just decided one day that I wanted to challenge myself to find an exploit on one of the largest hacking forums out there.

Ended up unexpectedly finding many hiding in plain sight, I just had to think outside the box.

Actually ended up finding a few more:

<https://hackforums.net/showthread.php?tid=5859533>

Future Alts - July 31, 2018, 6:41 pm

Nice, good to have this site not vulnerable.