

Forum:[Hack Forums](#)

Thread: [Severe MyBB Bug](#)

Omniscient - December 28, 2014, 7:00 pm

Just a quick heads up that in the next 2-3 days a lot of rumors might spread about a 0day or MyBB exploit floating around.

It's nothing more than a very low security risk bug that requires credentials to be exposed as well as a malicious site visit (CSRF).

So don't be alarmed by news of this and start freaking out. You don't need to change your passwords or do anything different. Just exhibit the same common sense browsing habits you normally would to maintain your safety.

1. Don't download anything from potentially malicious sites.
2. Don't click links you're not familiar with. Important to hover over a link sometimes to ensure it's not forged anchor text.
3. Don't use the same password on HF anywhere else. This is seriously important.

Just don't worry about it though otherwise.

ZuGgY - December 28, 2014, 7:00 pm

Thanks for the heads up, omniscient

Seaking - December 28, 2014, 7:01 pm

Thanks for the update. I try to keep my HF info completely different from everything else.

.Matt - December 28, 2014, 7:01 pm

Thanks for the heads up omni! Hopefully people don't cry too much now.

Paranoid? - December 28, 2014, 7:02 pm

Thanks for the alert Omni, hopefully nothing happens.

iExploits - December 28, 2014, 7:05 pm

Thanks Omni. You are the best webmaster ever.

Aura - December 28, 2014, 7:08 pm

For those who want additional security, web extensions like ScriptSafe (on Google Chrome) and NoScript (Firefox) can help prevent these kind of "exploits". Maybe not at 100%, but when well used, they can stop a lot of script-based exploits.

Thank you for the heads up Omni.

ZuGgY - December 28, 2014, 7:09 pm

(Dec 28, 2014 08:08 PM)Aur? Wrote: [\[CITE\]](#) For those who want additional security, web extensions like ScriptSafe (on Google Chrome) and NoScript (Firefox) can help prevent these kind of "exploits". Maybe not at 100%, but when well used, they can stop a lot of script-based exploits.

Thank you for the heads up Omni.

Gonna get them on my PC tomorrow.
Thanks Yoan.

Mr. Lahey - December 28, 2014, 7:10 pm

Thank you for the heads up Omni. I wonder how many threads will be created when it gets out. ?

Sharjah - December 28, 2014, 7:11 pm

Thanks for letting us know OMni. Definitely made me feel more safe about my forum

R?DSPY - December 28, 2014, 7:20 pm

Most of my passwords are random jitters that I can't even remember.

Thanks for the update.
bruh

SwimmingPool - December 28, 2014, 7:39 pm

Thanks for notifying me about this.

NoScript - December 28, 2014, 7:40 pm

Thanks for the warning, Omniscient!

Noire Dragon - December 28, 2014, 7:42 pm

Is this all versions of mybb or older (1.6.x) ? What is the CSRF like just sending a post or what lol?

BLURRYF?CE - December 28, 2014, 7:59 pm

Thanks for letting us know, seems like a lot of people got IP banned during this downtime, me included. Sent you a PM about it, can confirm at least one of my friends got IP banned as well but he was at a friends house and is home now and he's not IP banned on that IP.

Shockley - December 28, 2014, 8:04 pm

(Dec 28, 2014 08:11 PM)Most Savage Wrote: [\[CITE\]](#) Thanks for letting us know OMni. Definitely made me feel more safe about my forum
I am really enjoying your forum, Most Savage. ?

Sharjah - December 28, 2014, 8:06 pm

(Dec 28, 2014 09:04 PM)Shockley Wrote: [\[CITE\]](#) I am really enjoying your forum, Most Savage. ?
Why dont u register u lurking fuck?? ?

PHANTOM - December 28, 2014, 8:08 pm

Thanks for the update Omni
I think this prevent a lot of threads about this

BlaqCat - December 28, 2014, 8:31 pm

3. Don't use the same password on HF anywhere else. This is seriously important.
I dont use the same password for any same site because that is common sense, but you made it stick out; so I ask, is there a security risk as in people try to get the passcodes of hf members allot?

Benjamin Franklin - December 28, 2014, 8:47 pm

(Dec 28, 2014 08:08 PM)Aur? Wrote: [\[CITE\]](#) For those who want additional security, web extensions like ScriptSafe (on Google Chrome) and NoScript (Firefox) can help prevent these kind of "exploits". Maybe not at 100%, but when well used, they can stop a lot of script-based exploits.

Thank you for the heads up Omni.

I always use NoScript. Best extension on FireFox.

Mimix - December 28, 2014, 9:17 pm

Let the asslicking begin!

"Thank you omni, may i kiss you ass now for the ass kisser award?"

Oak - December 28, 2014, 10:11 pm

I'm a bit confused about the nature of the exploit but I guess I won't worry. Thanks for the heads-up though, glad I will be aware if / when it hits the news.

adampelletgun - December 28, 2014, 10:18 pm

Thanks for the heads up.

Another few tips:

1. Never click coded hyperlinks from members. Always quote the PM/post to see the URL.
2. Never click hidden links. Links such as goo.gl. There are online tools out there that you can use to unmask these links.

Noire Dragon - December 28, 2014, 10:48 pm

(Dec 28, 2014 11:11 PM)Sir Wrote: [\[CITE\]](#) I'm a bit confused about the nature of the exploit but I guess I won't worry. Thanks for the heads-up though, glad I will be aware if / when it hits the news. XSRF I believe basically does on site functions such as posting a message or private messaging someone via a script on a remote site if you're logged in on the target site depending on the exploit it could be worst than posting a message.

'An0ny - December 28, 2014, 10:48 pm

(Dec 28, 2014 11:18 PM)adampelletgun Wrote: [\[CITE\]](#) Thanks for the heads up.

Another few tips:

1. Never click coded hyperlinks from members. Always quote the PM/post to see the URL.
2. Never click hidden links. Links such as goo.gl. There are online tools out there that you can use to unmask these links.

For goo.gl you can just add a + sign behind the link, example, <http://goo.gl/aEhE+>

I'll defiantly not open links, hopefully booters dosen't use this exploit.. that would be bad lol

(Dec 28, 2014 10:17 PM)Mimix Wrote: [\[CITE\]](#) Let the asslicking begin!

"Thank you omni, may i kiss you ass now for the ass kisser award?"

you may want to shut the fuck up and try better next time ?

Ahri????? - December 28, 2014, 10:53 pm

Quote:3. Don't use the same password on HF anywhere else. This is seriously important. Sad part is I totally forgot my password, my web browser stays logged in 24/7. Anyways tonight I will be 2 factor security on my remaining 3+ emails and accounts. Probably should try to remember what password is.

Simply™ - December 28, 2014, 10:56 pm

K I'll try. It's hard to hack my account since my username has modded characters + I have an original/hard password.

Ahri????? - December 28, 2014, 10:57 pm

(Dec 28, 2014 11:56 PM)SIMPLY Wrote: [\[CITE\]](#) K I'll try. It's hard to hack my account since my username has modded characters + I have an original/hard password.

You know they can always use your email instead of the username...

STR™ - December 28, 2014, 10:59 pm

Thank you for the heads up Omni Sir , will follow your command

Noire Dragon - December 28, 2014, 10:59 pm

(Dec 28, 2014 11:57 PM)Popstar Ahri Wrote: [\[CITE\]](#) You know they can always use your email instead of the username...They shouldnt be able to get/change the password via the xsrf bug anyway you should be safe.

Benjamin Franklin - December 28, 2014, 11:01 pm

(Dec 28, 2014 11:57 PM)Popstar Ahri Wrote: [\[CITE\]](#) You know they can always use your email instead of the username...

That has modded characters as well.

420 Blaze It - December 28, 2014, 11:03 pm

Thanks for the notice, looks like I was right on this issue. Hope this is fixed ASAP, wish you well Omni!

what is life - December 28, 2014, 11:04 pm

Thank you for the heads up!

Saw some Skype messages on this

'An0ny - December 28, 2014, 11:07 pm

(Dec 28, 2014 11:57 PM)Popstar Ahri Wrote: [\[CITE\]](#) You know they can always use your email instead of the username...

Ends up requiring them to have hes mail - which I doubt.

Programming - December 28, 2014, 11:08 pm

If anyone downloads shit they aren't 100% sure is legit; they deserve to have their accounts taken.

Simply™ - December 28, 2014, 11:17 pm

(Dec 28, 2014 11:57 PM)Popstar Ahri Wrote: [\[CITE\]](#) You know they can always use your email instead of the username...

Some people might no know that though

cyberducky - December 28, 2014, 11:18 pm

Thanks for the heads up Omni. I am confident HF will be fine like always.

h4xer - December 28, 2014, 11:20 pm

Thanks for the heads up, omniscient

Tony Stark - December 28, 2014, 11:24 pm

It's sad knowing how many people won't even be able to follow those 3 simple steps.

Cheers for the update.

Blazin - December 29, 2014, 1:09 am

Thanks for the update, finding bugs is always critical.

Omniscient - December 29, 2014, 1:59 am

Quote:HF members are always being targeted.

Yes, because HF accounts are valued.

Quote:I'll defiantly not open links, hopefully booters dosen't use this exploit.. that would be bad lol
There is no exploit. That's the point of this thread. In the near future I'm expecting rumors that one exists when in-fact it doesn't.

The bug is more like saying your car can explode if you throw a molotov cocktail at it. Simply don't throw the molotov cocktail at your car if you want to stay safe. Pretty basic really.

Noire Dragon - December 29, 2014, 2:22 am

(Dec 29, 2014 02:59 AM)Omniscient Wrote: [\[CITE\]](#) Yes, because HF accounts are valued.

There is no exploit. That's the point of this thread. In the near future I'm expecting rumors that one exists when in-fact it doesn't.

The bug is more like saying your car can explode if you throw a molotov cocktail at it. Simply don't throw the molotov cocktail at your car if you want to stay safe. Pretty basic really.Oh aren't you cute, I was looking for XSRF/XSS vulnerabilities on my test mybb installation..seems like a common sense "exploit" alert thread. ?

Sceptical - December 29, 2014, 2:43 am

Thanks for this great heads up news Omni this should help me keep my account for a long time.

T3h Hack3r - December 29, 2014, 3:52 am

Do you intend to offer an incentive to those that report valid high risk issues on Hackforums within the near future?

Krew - December 29, 2014, 4:17 am

I thought the MyBB CSRF vulns were all fixed upon the implentation of postkeys?

Dave Skylark - December 29, 2014, 4:18 am

Does it have anything to do with the index2.php on here we were redirected if clicked the logo?

T3h Hack3r - December 29, 2014, 4:38 am

(Dec 29, 2014 05:18 AM)Dave Skylark Wrote: [\[CITE\]](#) Does it have anything to do with the index2.php on here we were redirected if clicked the logo?

No that's seperate. Index2 is used when the site is under attack.

MrOrang - December 29, 2014, 5:52 am

Thanks for letting me know about this, I'll keep an extra eye out for malicious links.

SwimmingPool - December 29, 2014, 8:52 am

(Dec 29, 2014 05:17 AM)Krew Wrote: [\[CITE\]](#) I thought the MyBB CSRF vulns were all fixed upon the implentation of postkeys?

Read the thread again. There isn't any exploit. Omni is stating that false rumors of one might start.

Simply™ - December 29, 2014, 10:51 am

I love how so many people are saying "Thanks Omniscient" or "Thank you Omniscient" and that's all they put. Not sure if they are kissing ass or just using it for characters.

ot: Would this affect others forum sites using MyBB?

Ilikeponies69 - December 29, 2014, 1:15 pm

Omni, thanks for ruining my new years eve gift. Fine, just be like that :(

Lol jk, but seriously Omni, you had to be mean and post about it, ay?

Since people will ask me how omni found out about it, and/or ask proof its me who is going to release it, might as well:

You can see a full disclosure here with project ideas if you want to make it a nice product since it can be used as a helpful API if you want: <https://hackforums.net/showthread.php?tid=4609063>

(Dec 29, 2014 11:51 AM)SIMPLY Wrote: [\[CITE\]](#) I love how so many people are saying "Thanks Omniscient" or "Thank you Omniscient" and that's all they put. Not sure if they are kissing ass or just using it for characters.

ot: Would this affect others forum sites using MyBB?

Yeah, it's just a CSRF bypass pretty much if you can swipe the "keys to the castle"

Omniscient - December 29, 2014, 2:01 pm

Quote:Since people will ask me how omni found out about it

Let's clarify a few a things. Your bug report is nonsense. Already had a lengthy discussion with you about it. I even gave you the tester account post key but you were unable to do anything about it.

In hacking and pen testing there is such a thing as "proof of concept". All you have is concept. Not an original one either. Something that was addresses and fixed by MyBB years ago.

Quote:Yeah, it's just a CSRF bypass pretty much if you can swipe the "keys to the castle"

It's ridiculous statements like that which piss me off. You make it seem like having the post key opens up the doors. It doesn't. I gave you a tester account postkey and you could not perform one function with it.

You think you helped when in-fact you wasted hours of my time and then you say you're going to release this in 2 days which to the untrained eye will appear a legitimate bug which it's not. You'll spread rumors and create more problems than is warranted.

I'm not going to let you freak out tens of thousands of members because you're excited that you think you found something.

For example you made this post on another thread:

Quote:It used to be the code for a MyBB CSRF bug

There is no bug. You're making up a rumor. You have nothing. You can do nothing. Your concept is trash.

Lastly...you're gone.

He B TeMy - December 29, 2014, 3:43 pm

Can i ask what version of MyBB does hackforums.net use?

Not relevant to the thread but, i have a thing for updates.

Omniscient - December 29, 2014, 4:57 pm

(Dec 29, 2014 04:43 PM)He B TeMy Wrote: [\[CITE\]](#) Can i ask what version of MyBB does hackforums.net use?

Not relevant to the thread but, i have a thing for updates. The HF version at this point isn't really truly a MyBB version release because it's patched a lot with core file edits and my own security changes.

\$lick - December 31, 2014, 9:06 pm

(Dec 28, 2014 08:00 PM)Omniscient Wrote: [\[CITE\]](#) 3. Don't use the same password on HF anywhere else. This is seriously important.

I have no idea what my HF password is, the site generated it for me.

zombieman - December 31, 2014, 9:27 pm

Can someone elaborate on this bug more? I get that it's a CSRF, but what are the specifics? I would like to see if this is present in 1.8 as well.

Also, one of the forums I frequent had its ACP compromised and shelled 2 days ago. Would that be possible/feasible through an exploitation of this CSRF bug?

Omniscient - January 2, 2015, 12:38 pm

User said he was doing full disclosure on New Years Day. That's up to him to publish his findings. It's well-written but at the end of the day it's pointless.

well then - January 2, 2015, 12:48 pm

(Jan 2, 2015 01:38 PM)Omniscient Wrote: [\[CITE\]](#) User said he was doing full disclosure on New Years Day. That's up to him to publish his findings. It's well-written but at the end of the day it's pointless.

'Full disclosure,' and could barely back up his claims and findings.

zombieman - January 3, 2015, 12:40 pm

(Jan 2, 2015 01:38 PM)Omniscient Wrote: [\[CITE\]](#) User said he was doing full disclosure on New Years Day. That's up to him to publish his findings. It's well-written but at the end of the day it's pointless.

I've also gotten word that there's a second 0-day going (SQLi?) around on a couple underground forums, and two pretty large forums had their ACP's breached and one got shelled as a result. Are you aware of anything like this, or is it just speculation?

T3h Hack3r - January 3, 2015, 1:45 pm

I saw the OP's thread prior to it being removed. It was well written I must admit. It's unfortunate he had to be an asshole about it and have his account closed.

T3h Hack3r - January 3, 2015, 1:56 pm

(Jan 3, 2015 02:52 PM)xadamxk Wrote: [\[CITE\]](#) We all know Omni has a tendency to over react at times.

Wasn't an overreaction. Just the user was a moron about it. Just couldn't admit they were on the wrong for once. ?

Omniscient - January 3, 2015, 3:42 pm

Quote:I've also gotten word that there's a second 0-day going (SQLi?) around on a couple underground forums, and two pretty large forums had their ACP's breached and one got shelled as a result.

We'd be a high-profile target of any attack. I have to assume if we're vulnerable to something we'd get hit with it by now. I have layers and layers of additional security for HF. I can't say about what other forums do for their own protection. Often times penetrations aren't only at the application layer. They can also be at the service level.

Quote:We all know Omni has a tendency to over react at times.

No idea what you're taking about. I'm RF'ing you now.

Indecisive enough - January 3, 2015, 7:01 pm

(Jan 3, 2015 04:48 PM)xadamxk Wrote: [\[CITE\]](#) I was referring to exactly what I quoted of the originally OP being a dick about this subject.

(Originally OP being the person that first addressed the bug)

EDIT: Atleast i'm honest xDHey atleast your still not repfucked.

HIGH PAID FELLA - January 8, 2015, 10:53 am

(Dec 28, 2014 11:48 PM)An0ny Wrote: [\[CITE\]](#) For goo.gl you can just add a + sign behind the link, example, <http://goo.gl/aEhE>+

I'll defiantly not open links, hopefully booters dosen't use this exploit.. that would be bad lol

you may want to shut the fuck up and try better next time ?

Dude, this is a MyBB exploit that will steal your post key and can do functions like repping, posting, and all what you can do with your account if you click the link.

(Jan 3, 2015 02:45 PM)T3h Hack3r Wrote: [\[CITE\]](#) I saw the OP's thread prior to it being removed. It was well written I must admit. It's unfortunate he had to be an asshole about it and have his account closed.

It's a really good friend of mine.

If you want to contact him lmk.