

Forum:[Hack Forums](#)

Thread: [Found multiple XSS exploits in MyBB / HackForums](#)

Punisher - July 8, 2018, 7:10 pm

<https://blog.mybb.com/2018/07/04/mybb-1-8-16-released-security-maintenance-release/>

- High risk: Image & URL MyCode Persistent XSS — reported by Punisher_HF
- Low risk: Non-video content embedding via Video MyCode — reported by Punisher_HF

I asked the MyBB team to link my HF profile but they didn't :(it was worth a try lmao!

I found a persistent XSS injection exploit on HackForums a few months ago, it allowed me to inject Javascript into both posts as well as signatures. Very high risk exploit, worked simply by crafting a special image tag with a URL tag inside of it causing the closing tag for the URL to break. This allowed me to load certain functions every time someone viewed one of my posts or my profile. Could have been very bad for users had someone malicious found these exploits. Omni was very quick to patch these exploits, he had them fixed within hours of reporting.

MyBB took over 2 months to release a fix after I reported it to them. Thousands of forums were vulnerable for MONTHS!

Another exploit involved malformed video tags. I was able to force users to download files from *.youtube.com, I was able to embed a chat box into posts, I was also able to embed an entire playlist and force videos to autoplay on page load even under a spoiler.

These exploits were found the same time as this thread where I found 2 other XSS exploits in HackForums (4-14-18):

<https://hackforums.net/showthread.php?tid=5825006>

I couldn't post about them at the time without risking a disclosure and the exploit falling into malicious hands.

I'm happy to have helped keep HackForums a safer place, and MyBB by extension.

What would YOU have done if you had found this exploit?

Should I have kept quiet and profited off the exploit, or did I do the right thing?

?
?

Also:

Big shout out to the Unity crew for being so bad ass!

Some of the best web application pentesters on HackForums.

Crystallize. - July 9, 2018, 2:49 am

To be honest myBB team sometimes are cocky. They should have linked your profile.

Good job man and thanks for the shoutout!

Aussie - July 9, 2018, 2:53 am

Well done! You do deserve recognition especially when you haven't used it for any malicious purposes or sold the method like most others would've/could've done.

iNuke - July 9, 2018, 2:58 am

This is so cool! Thank you for keeping HF safe. It really makes me want to learn more about pentesting.

Two-Ton 21 - July 9, 2018, 3:16 am

Time to bust out BeEF. Kidding of course, that's pretty scary though.

Chol - July 9, 2018, 5:51 am

This is cool . Hope omni reads this.

JBurk - July 9, 2018, 11:15 am

Omni fixing it straight away was a very good decision by him. Props!

Bossk - July 9, 2018, 11:26 am

props to you for not exploiting this, op could have stolen any user's account using this.

Hyperhacktive - July 9, 2018, 12:32 pm

Good job mate, you've done the best thing ! ?

Ganja - July 9, 2018, 1:02 pm

Great job on doing the right thing and reporting it! Nice find, keep up the good work!

Kosmos - July 9, 2018, 1:16 pm

You're a good person for doing the right thing. I don't know what I'd do if something happened to HF.

mawrek - July 11, 2018, 4:38 am

smart kids use vbulletin forum systems

juulstar - July 12, 2018, 9:32 pm

Where are your "Wings"?

You deserve that award dude.

Sir-Teabag - July 13, 2018, 4:21 pm

That's really awesome man, good on you. Did you find them on accident or were you trying to see what you could do?

Personally I would've fucked around a little before I reported it. Like going to different MyBB forums and putting autoplay orgasm sounds on the index lol

Punisher - July 13, 2018, 8:48 pm

(Jul 9, 2018 02:49 AM)Crystallize. Wrote: [\[CITE\]](#) To be honest myBB team sometimes are cocky.They should have linked your profile.

Good job man and thanks for the shoutout!

It's all good, at least they acknowledged how serious the issue was and were very nice and respectful when chatting.

(Jul 9, 2018 02:53 AM)Aussie Wrote: [\[CITE\]](#) Well done! You do deserve recognition especially when

you haven't used it for any malicious purposes or sold the method like most others would've/could've done.

Thank you, I definitely considered it, but then I thought about all the hard work has gone into MyBB and all the work people put into their forums. It's not worth ruining it for everyone else just for a bit of money.

(Jul 9, 2018 02:58 AM)iNuke Wrote: [\[CITE\]](#) This is so cool! Thank you for keeping HF safe. It really makes me want to learn more about pentesting.

No problem, I have spent a long time on these forums, HF is like home to me :)

(Jul 9, 2018 03:16 AM)Two-Ton 21 Wrote: [\[CITE\]](#) Time to bust out BeEF. Kidding of course, that's pretty scary though.

Haha, not quite that easy ?

(Jul 9, 2018 05:51 AM)Chol Wrote: [\[CITE\]](#) This is cool . Hope omni reads this.

I actually reported it to him first, he suggested I pass the bug report on to the MyBB team.

(Jul 9, 2018 11:15 AM)JBurk Wrote: [\[CITE\]](#) Omni fixing it straight away was a very good decision by him. Props!

He fixed it within hours of reporting it, but then I bypassed his filter a few times.

It's now completely patched.

(Jul 9, 2018 11:26 AM)Bossk Wrote: [\[CITE\]](#) props to you for not exploiting this, op could have stolen any user's account using this.

Absolutely, I could have wrote a worm that spread through the whole forum within hours via posts/signatures and had control over everyone online viewing any of the affected posts. Could've forced people to vacation ban themselves, could've made everyone who viewed my posts automatically give me rep, honestly the possibilities were endless. I love HackForums too much to risk getting myself banned for doing any of those things, so I decided it'd be a good idea to report it.

(Jul 9, 2018 12:32 PM)Hyperhacktive Wrote: [\[CITE\]](#) Good job mate, you've done the best thing ! ?

Thanks :)

(Jul 9, 2018 01:02 PM)El Pusstolero Wrote: [\[CITE\]](#) Great job on doing the right thing and reporting it! Nice find, keep up the good work!

Glad to hear it. I'll keep looking for ways to help any way I can.

(Jul 9, 2018 01:16 PM)K?osmos Wrote: [\[CITE\]](#) You're a good person for doing the right thing. I don't know what I'd do if something happened to HF.

That's the way I see it, this is my hangout spot, I want to keep this place safe and fun. :D

(Jul 11, 2018 04:38 AM)mawrek Wrote: [\[CITE\]](#) smart kids use vbulletin forum systems

It's too late to ever switch to any other forum system to run HackForums on, it's too customized at this point.

(Jul 12, 2018 09:32 PM)???? Wrote: [\[CITE\]](#) Where are your "Wings"?

You deserve that award dude.

I'm glad to have been given an award, Omni actually awarded me The Protector award for reporting 5+ exploits in a month.

(Jul 13, 2018 04:21 PM)Sir-Teabag Wrote: [\[CITE\]](#) That's really awesome man, good on you. Did you find them on accident or were you trying to see what you could do?

Personally I would've fucked around a little before I reported it. Like going to different MyBB forums and putting autoplay orgasm sounds on the index lol

I actually sat down one morning on a weekend, and decided; "Today I am going to find an exploit on HackForums"

I spent a good chunk of time brainstorming of methods of user input that could be targeted for exploitation.

I thought the best way to get javascript to execute on the page would be via a URL or IMG tag.

I experimented with different ways to break them and ended up finding an XSS vulnerability.

I didn't really experiment with the exploits too much simply because just by using them it would alert other hackers that a vulnerability exists, and it would be discovered and spread before the MyBB team could patch it.

I still won't share a PoC simply because I bet there are still thousands of forums that haven't installed the latest security patch.

Careful out there guys, even sites you think are 100% unhackable can have security holes that could compromise you.

Bossk - July 14, 2018, 2:45 am

OP still tryna find some exploits ?

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

Animeschoolgirl - July 14, 2018, 5:52 pm

Props to you for doing the right thing!

Punisher - July 21, 2018, 10:14 am

(Jul 14, 2018 02:45 AM)Bossk Wrote: [\[CITE\]](#) OP still tryna find some exploits ?

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

Actually found another persistent XSS in MyBB a few days ago. Reported to MyBB and Omni yesterday. ?

Originalkillit - July 22, 2018, 1:28 am

(Jul 14, 2018 02:45 AM)Bossk Wrote: [\[CITE\]](#) OP still tryna find some exploits ?

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

Hey how did you manage to see the byte history of other member

?

TYLER - July 22, 2018, 1:39 am

(Jul 22, 2018 01:28 AM)Originalkillit Wrote: [\[CITE\]](#) Hey how did you manage to see the byte history of other member

?

Click the users bytes amount to pull up the popup window as if you're donating then at the bottom right corner, it says History.

Originalkillit - July 22, 2018, 1:40 am

(Jul 22, 2018 01:39 AM)TYLER Wrote: [\[CITE\]](#) Click the users bytes amount to pull up the popup window as if you're donating then at the bottom right corner, it says History.

It shows my history buddy not other members history

?

Bossk - July 22, 2018, 3:24 am

(Jul 22, 2018 01:28 AM)Originalkillit Wrote: [\[CITE\]](#) Hey how did you manage to see the byte history of other member

?

you need a mybb exploit

Originalkillit - July 22, 2018, 3:25 am

(Jul 22, 2018 03:24 AM)Bossk Wrote: [\[CITE\]](#) you need a mybb exploit

OK thank you but I did not understand anything ? Because I have never been in web exploits

So I will begin to learn it soon ?

Evanescent - July 23, 2018, 2:01 am

Are you allowed to do pentest on HF ?

Once I wanted to start then I feared that Omni may not like it and the consequences would be bad.

Bossk - July 23, 2018, 3:15 am

(Jul 23, 2018 02:01 AM)Evanescent Wrote: [\[CITE\]](#) Are you allowed to do pentest on HF ?

Once I wanted to start then I feared that Omni may not like it and the consequences would be bad. disallowing it would do nothing but harm because then the blackhats would be able to find and exploit vulnerabilities, while the whitehats won't report the exploits they find in fear of being banned or whatever.

Elitas - July 23, 2018, 3:19 am

(Jul 23, 2018 02:01 AM)Evanescent Wrote: [\[CITE\]](#) Are you allowed to do pentest on HF ?

Once I wanted to start then I feared that Omni may not like it and the consequences would be bad.

It's allowed. I regularly find vulnerabilities in plugins on here and report it to Omni.

Evanescent - July 23, 2018, 3:30 am

(Jul 23, 2018 03:15 AM)Bossk Wrote: [\[CITE\]](#) disallowing it would do nothing but harm because then the blackhats would be able to find and exploit vulnerabilities, while the whitehats won't report the exploits they find in fear of being banned or whatever.

(Jul 23, 2018 03:19 AM)Elitas Wrote: [\[CITE\]](#) It's allowed. I regularly find vulnerabilities in plugins on here and report it to Omni.

Alright. Sounds good, I'll give a shot when I'll be free.

Punisher - July 23, 2018, 11:12 am

(Jul 23, 2018 02:01 AM)Evanescent Wrote: [\[CITE\]](#) Are you allowed to do pentest on HF ?

Once I wanted to start then I feared that Omni may not like it and the consequences would be bad.

Only manual testing is allowed, scripts and scanning can get you banned or even closed

Krueger - July 23, 2018, 1:10 pm

Gj man not much to say about it besides keep us safe pls xd

Omniscient - July 23, 2018, 1:23 pm

Pisses me off pretty bad that we reported these very high risk vulns to MyBB and they said patch would be out in 2-3 weeks and they took 3 months. They could have alerted the community and released a simple fix.

This was a report coming from Hack Forums. They should have assumed immediately that this was going to be leaked and used maliciously. We could have pwned hundreds of MyBB forums possibly even thousands in the time they took to release the update.

Even worse, they have not successfully patched the vulnerability.

I gotta say, their MyCode parser has been fucked for many months. It's frustrating that these reports to them aren't immediately dealt with. I've complained to them about their secrecy of development. A high-risk vuln should be made public within 72 hours with a patch.

This was bullshit and I've lost confidence in the team.

Personally I think OP should release the vulns public if only to embarrass the team for their lack of security. They deserve nothing less than the middle-finger for this bullshit.

Evanescent - July 23, 2018, 4:38 pm

(Jul 23, 2018 11:12 AM)Punisher Wrote: [\[CITE\]](#) Only manual testing is allowed, scripts and scanning can get you banned or even closed

Using a proxy like owasp ZAP or burp suite should be fine i guess?

euan - July 24, 2018, 11:00 am

Hi,

I just want to chime in here, I created an account after seeing some screenshots from this thread.

Punisher was great and reported 2 issues that they discovered via Private Message to myself via the MyBB Community Forums, with Omniscient also contacting me just prior to the report to warn me that a report was incoming (we have talked briefly previous to this, so I imagine this was a courtesy on his part - it was appreciated anyway!).

As soon as the issues were reported we created internal threads for each containing the PoC that was provided to us. From there we then obviously had to verify for ourselves that the PoC worked on forums other than the official community forums, so some of the development team tried it out on their local installs and confirmed the issue. Unfortunately, we then dropped the ball from there. I was handling both of the reported issues, but unfortunately real life work got the better of me for a while. I know it's not a good excuse, but it's the only reason I can give. Burnout is a real bitch. In addition, our project leader (Stefan) had disappeared and some of us on the team were taking on extra tasks to try and cover (answering support emails sent to contact@mybb - which for a while went only to me; handling username change requests; etc.).

Obviously there is no real excuse for taking upwards of 2.5 months to handle serious security issues, all I can do in this case is apologise.

I do want to try and reassure everyone that we realise we have cocked up and that we are taking things on board. We are currently discussing how we can improve our handling of both releases as a whole and our handling of security issues. Some ideas I've personally floated to the rest of the team so far include (note that these are all my own opinions, and the team will be discussing them in an ongoing RFC):

A dependable release schedule. We've previously aimed for releases every 2 months, but I'm not sure if we've ever actually hit this target. I would personally prefer to see smaller releases happening more often. Smaller releases also have the advantage of being less likely to completely break like our god awful 1.8.16 release. Having a dependable release schedule with clear signalling when the merge window closes (proposed to be 1 week before release) and pre-release packages should make our releases much more reliable and might even prompt more contribution from the community in the form of testing before a full release.

Sharing of security patches with vulnerability reporters. We currently receive reports, then go radio silent as we work on patches in the private forums. Instead, we should share all proposed patches in the original security report thread in order to get feedback from the original reporter and have less

chance of releasing a partial patch. We used to do this in the past, but the practice was stopped for reasons none of the current team can remember.

Public disclosure of security reports after release. In the case of threads in Private Inquiries we would move these threads to a public forum that is closed to new threads and discussion. This makes the original report and any PoC code public, along with any discussion from the team and any and all patches. Reports received via PM would be directed towards Private Inquiries threads for this reason (and so that if 1 team member is unavailable a report isn't missed).

[i]Possibly[i]: support for reporting issues via hackerOne. We don't currently have the means to have proper monetary bounties for issues on hackerOne or anything, but their platform is really nice and is already pretty widely used by many security researchers. Reports here would be treated the same as reports in PI - they would be disclosed on release, and patches would be shared. I haven't personally used HackerOne much myself, but they seem to be the platform of choice at the moment...

Posting of all disclosed vulnerability reports to the @mybbsecurity Twitter account. We already control this account, but it is currently only used for release announcements really. Posting all disclosed vulnerabilities gives a single place to follow to stay up to date.

Again, I would like to apologise to Punisher and the rest of the community who have either tried to work with us in the past or been put off from working with us in any way. We are trying to be better, and any feedback at all on how we currently operate and how we can improve is always greatly appreciated and taken to heart.

PS: I did include your request to link your HF profile in the original report, I think the only reason it wasn't included is due to profiles not being viewable to guests here - people not logged in instead get a blank white page with only links to "Login" or "Register". I can't say for 100% that's why it wasn't included, but that's what I'd imagine was the reason. We're not so uptight about the whole "denied support" rubbish as we used to be these days, and forums like this aren't quite the taboo subjects they once were on the community forums.

Gee4rce - July 26, 2018, 2:21 pm

(Jul 24, 2018 11:00 AM)euan Wrote: [\[CITE\]](#) Hi, ...
Hi euan,

you have the courage to show up here and openly discuss what went wrong, this is a good move into the right direction already and me for my part, i respect your honesty very much!

We all have a real life besides our digital life, and both of these lives have their own kind of challenges, indeed.

When looking at the digital life, a coder already has lots of work to do, coding a whole forum and maintaining

functionality and support is surely a task on it's own, and same applies for the security section-IT-Security

today forms a complete own section in the field of Information technology.

Especially then it is even more important to work together with those researchers, that offer their (mostly hard) work

for free when reporting a vulnerability which they have prior invested hours or days of research into.

There are several

WhiteHats today that do this, and i think the recent events have showed how important communication is at this point.

You euan have now already done the first step to improve dealing with vulnerabilities in the future, by stepping up here and get in contact with the security community.

Next thing would be to improve MyBB's incident handling process, here are some suggestions:

- establish an email that is meant for vulnerability reports only (i.e.: security@mybb.com)
- establish up to date incident response plans (this prevents that a vuln gets forgotten or takes weeks to fix)
- provide responsible disclosure policy on mybb website
- Let go of your "we roll out fix every 2 months",
an issue like the Mycode XSS would have required immediate patch (max. 1 week), even if the patch only fixes that single issue!
- Use a seperate mailinglist to inform users of security vulnerabilities that require immediate updating of mybb forums, independantly from regular product updates,
- maybe move to hackerOne, yes
(short note here; yes there are researchers at hackerOne that hunt for free, but involving bounties would at a minimum triple the chances of quality reports)
(example here: i'm on hackerOne too, but i only participate in hunts that offer money. MyBB without bounties would be ignored by me and several others.)
(Note there are also blackmarkets for exploits, GreyHats may look whats more profitable and choose the side that offers better money. Good bounties prevent that mostly).
- and as said already but mentioning here again: a fair and reliable communication with the security community and reporters of vulnerabilities are an essential key for solving issues.

That's it already,
i think after euans post, things are sorted now and we can expect a better security handling in the future from MyBB.

@Euan;
incase you recognise me from a specific twitter post to myBB, i have taken this post down and removed the pocs from pastebin, after seing your post here.

Punisher Wrote:What would YOU have done if you had found this exploit?
Should I have kept quiet and profited off the exploit, or did I do the right thing?
Incase you read this; great find,
definitely requires skill and you did the right thing reporting it to keep myBB users safe!

Cheers, Gee.

euan - July 26, 2018, 2:47 pm

(Jul 26, 2018 02:21 PM)Gee4rce Wrote: [\[CITE\]](#) Hi euan,

you have the courage to show up here and openly discuss what went wrong,
this is a good move into the right direction already and me for my part, i respect your honesty very much!

We all have a real life besides our digital life, and both of these lifes have their own kind of

challenges, indeed.

When looking at the digital life, a coder already has lots of work to do, coding a whole forum and maintaining functionality and support is surely a task on it's own, and same applies for the security section-IT-Security today forms a complete own section in the field of Information technology.

Especially then it is even more important to work together with those researchers, that offer their (mostly hard) work for free when reporting a vulnerability which they have prior invested hours or days of research into. There are several WhiteHats today that do this, and i think the recent events have showed how important communication is at this point.

You euan have now already done the first step to improve dealing with vulnerabilities in the future, by stepping up here and get in contact with the security community.

Next thing would be to improve MyBB's incident handling process, here are some suggestions:

- establish an email that is meant for vulnerability reports only (i.e.: security@mybb.com)
- establish up to date incident response plans (this prevents that a vuln gets forgotten or takes weeks to fix)
- provide responsible disclosure policy on mybb website
- maybe move to hackerOne, yes
(short note here; yes there are researchers at hackerOne that hunt for free, but involving bounties would at a minimum triple the chances of quality reports)
(example here: i'm on hackerOne too, but i only participate in hunts that offer money. MyBB without bounties would be ignored by me and several others.)
(Note there are also blackmarkets for exploits, GreyHats may look whats more profitable and choose the side that offers better money. Good bounties prevent that mostly).
- Let go of your "we roll out fix every 2 months", an issue like the Mycode XSS would have required immediate patch (max. 1 week), even if patch only fixes that single issue!
- Use a seperate mailinglist to inform users of security vulnerabilities that require immediate updating of mybb forums, independantly from regular product updates,
- and as said already but mentioning here again: a fair and reliable communication with the security community and reporters of vulnerabilities
are an essential key for solving issues.

That's it already,
i think after euans post, things are sorted now and we can expect a better security handling in the future from MyBB.

@Euan;
incase you recognise me from a specific twitter post to myBB, i have taken this post down and removed the pocs from pastebin, after seing your post here.

@OP;
if you read this, great find, definately requires skill and you did the right thing reporting it to keep myBB users safe!
Hit me up on twitter if you want to see a working xss worm example for the mycode xss ;)

Cheers, Gee.

Hey, thanks for the response. I did see your Tweet in fact, but likely wouldn't have put 2 + together ;) Taking it down wasn't necessary - we don't want to shy away from the fact that we've made mistakes or to try and erase history.

I'm going to try and answer some of your points:

We actually do have an email address for reporting vulnerabilities, but as far as I can tell it isn't currently publicised at all - we'll get on that. For reference, the address is "security@mybboard.net" (or @mybb.com - the .com is an alias). Emails sent to this address can also be PGP signed and/or encrypted - the team that use PGP list their information on the "About the Team" page.

We're currently working on that, and will also be adding a "SECURITY" document to the repository to detail some security considerations for the software. We also have the existing "Security Research" page that provides some guidance of standard reporting procedures.

See above, I hope the "Security Research" page covers this - if not, please let us know what we can add to improve it! We also have the "Security Workflow" page too that explains how we operate when dealing with a report.

Both of these pages are managed through GitHub pages too, so if anybody has any feedback we'd welcome it

Yeah, HackerOne is still up in the air. At the moment we would struggle to pay meaningful bounties, being an open source project and having a single donation source that is currently sitting at \$40 - maybe enough to cover a month or two of hosting. Most of the project's infrastructure and maintenance is paid for out of pocket at the moment.

We're definitely aiming to be more fluid with releases, the fixed release model would apply only when there are either no security patches involved, or when the reported security vulnerabilities are classified as very low risk (eg: stored XSS in the ACP that requires ACP privileges to both enact and to be hit by - we know the ACP is full of holes and that it's generally a pain to do any work with - we're planning a full ACP rewrite for 1.10).

[*Mailing list wie, our mailing list is currently handled by WordPress who host our blog. We're currently in the process of leaving WordPress due to a lack of theming options with their hosted platform and moving to GitHub pages instead. As part of this, we'll be running our own mailing list through MailGun so we'll have the chance to expand this offering then. We do also have the @mybbsecurity Twitter account where security updates are posted too in the meantime.

Thanks a lot for the feedback, it's much appreciated!

PS: Links are missing from the above as I don't have permission to post links yet - seems I need another 48 posts ;) I've created a pastern with ID uVvAbQSt containing the URLs if anybody wants to see them...

Gee4rce - July 26, 2018, 4:10 pm

Looking at your reply,

you already seem to have the necessary setup.

It seems that the process just wasn't that fluid in execution then, well this comes by time, 2 - 3 vuln reports and the team will get used to the process flow.

About 4.,

i did not know of that and feel sorry for not thinking of such possibility before.
I would then suggest the following: sign up at multiple bug hunting platforms,
instead of only hackerOne. This uppers the volume of WhiteHats that may work for free.

Some platforms:

- BugCrowd <https://www.bugcrowd.com/>
- OpenBugBounty <https://www.openbugbounty.org/>
- hackenproof.com <https://www.hackenproof.com/>
- hackerOne (as already mentioned)
- BountyFactory <https://bountyfactory.io>
- synack.io <http://synak.io>
- .. and more.

Coming here for a talk was a good thing-
after your open post, things are more clearer now for for the researcher community
and if you stick to the plans you've posted above then MyBB users can most likely expect better
security for the upcoming future.

All the best!

Cheers, Gee.

n0XZe - July 26, 2018, 9:59 pm

I'm jealous over your skills man! i no fuck all about any of this and have no patience on reading up!
so ill carry on pretending ;D

You did the right thing bro and you will get more and more fans!