

Forum:[Hack Forums](#)

Thread: [\[Suggestion\] Require valid code to disable 2fa](#)

Lrrr - September 26, 2016, 2:17 pm

While messing around with my account I found it was possible to disable 2fa by simply clicking the reset button while logged in (https://hackforums.net/gauth.php?action=clear&my_post_key=***)

This could theoretically be used to send a user to a link that disables their 2fa (if you knew their my_post_key).

Also, if I didn't clear the cookies on my browser, and my computer was stolen they could turn off my 2fa.

I think RESETS should be required to be done by an admin, or require the user to input a valid 2fa code to disable the feature.

minimalist - September 26, 2016, 2:27 pm

I suggested this here:

<https://hackforums.net/showthread.php?tid=5209610>

but Omniscient didn't want it, if memory serves correctly...don't want to read over the messages.

Also, the post key doesn't grant users access to anything unless said users are on said other user's account. Don't give it away though.

Neeeeeeeeeeel.- - September 26, 2016, 2:29 pm

I agree with this request, but it will also load Omni with disabling 2FA & repkilling more members because they'd lost their keys.

LordCoder - September 26, 2016, 2:43 pm

When my iPhone was stolen, the only way to switch 2FA was by doing this. Otherwise I'd have had a big problem.

Neeeeeeeeeeel.- - September 26, 2016, 5:02 pm

(Sep 26, 2016 02:43 PM)LordCoder Wrote: [\[CITE\]](#) When my iPhone was stolen, the only way to switch 2FA was by doing this. Otherwise I'd have had a big problem.If you use "Authy" you can always recover your auth tokens with the master password. I don't know if it's available for iOS but I think it is.

EIDoc - September 27, 2016, 6:57 pm

Build the wall Omni, close this down.

B?ker - September 28, 2016, 8:53 am

(Sep 26, 2016 05:02 PM)Neeeeeeeeeeel.- Wrote: [\[CITE\]](#) If you use "Authy" you can always recover your auth tokens with the master password. I don't know if it's available for iOS but I think it is.Yes it is on iOS I've been using it for years

Neeeeeeeeeeel.- - September 28, 2016, 10:02 am

(Sep 27, 2016 06:22 PM)xadamxk Wrote: [\[CITE\]](#) This^

I know Authy saves everything to your account.
But that kind of defeats the purpose of having that extra layer.
Otherwise it's just 2 passwords, and I'm sure some baboon used the same password for both accounts. You are right, it's indeed 2 password instead of real 2FA. But I prefer 2 passwords than a repkill if I lost my 2FA device.

Deathmask - September 28, 2016, 11:26 am

Wow, this seems like a pretty major bug, hope Omni fixes it.

Vitani - September 28, 2016, 11:27 am

I actually think it's a good thing you can reset it like this.
As the user above said, if you ever lose your phone and are stupid enough not to have any backup, then this is your best bet.

Lrrr - September 28, 2016, 11:31 am

(Sep 28, 2016 11:27 AM)Vitani Wrote: [\[CITE\]](#) I actually think it's a good thing you can reset it like this.

As the user above said, if you ever lose your phone and are stupid enough not to have any backup, then this is your best bet.
but that seems like you're trying to justify a bug based on a test-case that is flawed to begin with.

I mean I get it, it makes sense and is helpful in that scenario...but should you actually be in that scenario to begin with?

Vitani - September 28, 2016, 11:37 am

(Sep 28, 2016 11:31 AM)Lrrr Wrote: [\[CITE\]](#) but that seems like you're trying to justify a bug based on a test-case that is flawed to begin with.

I mean I get it, it makes sense and is helpful in that scenario...but should you actually be in that scenario to begin with?
You're right, honestly people should not even have to use this as last resort, as a simple backup would be sufficient.

This could potentially be exploited if someone got infected and the person behind it wants to steal their HF account. Maybe it has already been exploited.

Lrrr - September 28, 2016, 12:57 pm

(Sep 28, 2016 11:37 AM)Vitani Wrote: [\[CITE\]](#) This could potentially be exploited if someone got infected and the person behind it wants to steal their HF account. Maybe it has already been exploited.

One of the reasons I made this thread is that I believe this is how Regulus was compromised.

Vitani - September 28, 2016, 1:18 pm

(Sep 28, 2016 12:57 PM)Lrrr Wrote: [\[CITE\]](#) One of the reasons I made this thread is that I believe this is how Regulus was compromised.
Hmm could be.

It buggs the f*ck outta me that Regulus still hasn't tried to get his account back.
It's not like him.

05317832892 - September 28, 2016, 1:37 pm

(Sep 26, 2016 02:27 PM)Minimalist Wrote: [\[CITE\]](#) I suggested this here:
<https://hackforums.net/showthread.php?tid=5209610>

but Omniscient didn't want it, if memory serves correctly...don't want to read over the messages.

Also, the post key doesn't grant users access to anything unless said users are on said other user's account. Don't give it away though.

Not quite what I think he was getting at. The vulnerability here is if you know someone's post key you could send them a shortened link to it. Should they go through the effort of checking what's behind it, they may even fail to realize that it's an "unsafe" hf link.

Hypothetically if this was going to happen you would need to know their password, post key, and bait them into clicking the link. In reality this would never happen unless someone accidentally gave out their code.

Tbh the only way I can see this going wrong is if someone makes a YouTube video and they brush over a link that reveals their code. Even then some browsers may truncate the link when it's previewed.

This is all just speculation. I'm my opinion I don't think it's a massive flaw. The best idea in my opinion is just to make it a JavaScript button or something that can't be linked.

Making omni or someone else manually approve 2FA disables is very lengthy and time wasting. Systems like this should probably be automated.

Edit: Vitani has just made a very good point. Part of 2FA in my opinion is that if your computer is compromised they don't have access to you account. Most rats or botnets have a visit link function, running this through that would force them to open the link disabling their 2FA. At the same time if you ARE ratted then they may be able to manipulate your cookies/reverse proxy and open your HF account regardless.

Lrrr - September 28, 2016, 2:09 pm

(Sep 28, 2016 01:37 PM)?Cam? Wrote: [\[CITE\]](#) Hypothetically if this was going to happen you would need to know their password, post key, and bait them into clicking the link. In reality this would never happen unless someone accidentally gave out their code.

You would not need their password, you WOULD need to bait them, although if you baited them smart you wouldn't need to get their postkey.

Hypothetical P.O.C:

XSS Method: A link is clicked which grabs the user postid and redirects to the disabled link.

Non XSS: Create a userscript or trick the user into showing you the source of the page or in some way gain access to the post key. With the post key you don't need a password.

So all you would do is phish the users post key and bait them into clicking the link.

Most hacks are way more complicated than that, but this is at-least a hypothetical POC that makes me wonder if it is already being exploited.

(Sep 26, 2016 02:27 PM)Minimalist Wrote: [\[CITE\]](#) I suggested this here:
<https://hackforums.net/showthread.php?tid=5209610>

but Omniscient didn't want it, if memory serves correctly...don't want to read over the messages.

Also, the post key doesn't grant users access to anything unless said users are on said other user's account. Don't give it away though.

Same outcome, different reasons for suggestions :)

Omniscient - September 29, 2016, 1:31 pm

Quote:While messing around with my account I found it was possible to disable 2fa by simply clicking the reset button while logged in

Should not work because the \$mybb->user property isn't set by the post key. You're logged in so that's why it works.

Quote:When my iPhone was stolen, the only way to switch 2FA was by doing this. Otherwise I'd have had a big problem.

Exactly why I have it as it is. Lost phone or screwed up 2FA and you still have an option to disable 2FA if you have an active HF session. I already get so many, way too many, lost 2FA contacts. It's pretty ridiculous actually. Almost makes me regret adding the security measure it's that bad.

Quote:If you use "Authy" you can always recover your auth tokens with the master password.

Finding out that many members use Authy but don't enable backups.

Quote:but that seems like you're trying to justify a bug

There is no bug.

Quote:One of the reasons I made this thread is that I believe this is how Regulus was compromised.

Almost certain he was RAT infected.

Quote:The vulnerability here is if you know someone's post key you could send them a shortened link to it.

That's why you don't share your post key. Duh.

Quote:Hypothetically if this was going to happen you would need to know their password, post key, and bait them into clicking the link. In reality this would never happen

Pretty much. And why it's not a bug and why I won't fix it.

Quote:The best idea in my opinion is just to make it a JavaScript button or something that can't be linked.

Hmm....that is the best idea. Added a Javascript popup on clear/reset links. But that doesn't technically stop the so-called bug with CSRF. Technically rather tough since a lot of browsers now remove referers. But now we have a confirm JS popup at least.

To really stop this I'd have to change the link to a form post data which also isn't infallible. What's vital is that you DO NOT SHARE YOUR POST KEY. It is a security measure.

When your Gauth is disabled you'll get the notification when you go to your PMs or usercp. So it's not like you'll never notice it was disabled.

I know our 2FA solution is far from perfect.

Quote: So all you would do is phish the users post key

You're basically talking about having someone that's a complete idiot give you access to his post key. You can't dumb down the victim so much that you'll expect me to create a system so complex the dumb user can't figure it out. We're practically there already. We have idiots on this site who lose their 2FA access on a daily basis. I can't make members smarter.

In the end at worst your bug report is that someone can force you to clear your Gauth code. By itself is not a threat to accounts or site security.

Lrrr - September 29, 2016, 1:33 pm

Thank you Omni for the very detailed reply. -Closed