

Forum:[Hack Forums](#)

Thread: [Account Security Roadmap](#)

Omniscient - May 4, 2016, 2:01 pm

Here are the important steps I will be taking over the next week to enhance account security on HF.

1. Offer a \$1k BTC bounty for the working exploit. (DONE)
2. Create logging of all PW changes with both date and IP (pw's never stored in plain text). (DONE)
3. Force a full password reset on the entire community.
4. Add to Trust Scan the last PW change date. (DONE)
5. Force password changes if PW is older than X months/days.
6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.

Vitani - May 4, 2016, 2:03 pm

These are some great improvements on the current security.

I especially like setp 6 since that will reduce scams with stolen/compromised accounts close to if not actually zero.

Step 5 will be a pain in the ass but it's a good idea since alot of people use the same password for multiple sites.

sHAY - May 4, 2016, 2:03 pm

Thank you for keeping the forum safe!

I really like the exploit hunt.

Fish - May 4, 2016, 2:03 pm

wow thanks omni! looks like a good todo list :D

Rikk?a - May 4, 2016, 2:04 pm

Thanks a bunch for trying making the community a safe place.

Cryptic™ - May 4, 2016, 2:04 pm

Good changes. Step 6 is awesome.

DeadCode - May 4, 2016, 2:05 pm

Not bad. Thanks for keeping us safe from dem hackers and SE'ers.

F16™ - May 4, 2016, 2:06 pm

6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.
Awesome Change ?

?Fazzer - May 4, 2016, 2:06 pm

Damn it. This should have been done a long time ago. But whatever rule 6 gonna be awesome.

Looking forward for this.

Sevn Alias - May 4, 2016, 2:07 pm

(May 4, 2016 02:06 PM)?Fazzzer Wrote: [\[CITE\]](#) Damn it. This should have been done a long time ago. But whatever rule 6 gonna be awesome.

Looking forward for this.

Yes, indeed. +1.

Gt403cyl - May 4, 2016, 2:07 pm

This should really lockdown members accounts against theft!

While I am happy to see you taking more steps to secure the site and accounts of the members, I still hate to see so many people didn't take the precautions that were already there in front of them such as 2FA ect.....

minimalist - May 4, 2016, 2:08 pm

#5: What was your mentality behind it? Just curious to hear if changing an uncompromised password with 2FA enabled would bring security improvements or if it'd just inconvenience the user.

Rikk?a - May 4, 2016, 2:11 pm

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.Are you going to make "Last Gauth/2FA Validation" Play a role in this? Such as you cannot post in the marketplace unless you Validate your 2FA. When it has not been Validated in awhile.

Granny Bacon - May 4, 2016, 2:14 pm

(May 4, 2016 02:06 PM)?Fazzzer Wrote: [\[CITE\]](#) Damn it. This should have been done a long time ago. But whatever rule 6 gonna be awesome.

Looking forward for this.

It shouldn't be done long time ago, it is called "improvement". Updates are there to be released. You can't expect every site to have all the features in the beginning.

Great roadmap btw.

7even - May 4, 2016, 2:15 pm

Everything seems good other than #5. Seems like some good improvements, thanks Omni ?

Rikk?a - May 4, 2016, 2:16 pm

(May 4, 2016 02:15 PM)RAINY Wrote: [\[CITE\]](#) Everything seems good other than #5. Seems like some good improvements, thanks Omni ?

5. Force password changes if PW is older than X months/days.

I have no idea why this is not a good idea, is it because you don't like changing your password constantly?

Ritract - May 4, 2016, 2:21 pm

Congratulations to whoever found the exploit.

FiftyTwo - May 4, 2016, 2:21 pm

I think the third, fifth and sixth step would be very effective in slowly lessening the amount of stolen

accounts.

Awesome changes Omni.

'Cynical - May 4, 2016, 2:22 pm

Gauth required to PM?

You're really kicking this up.

Needless to say, I am honestly impressed by how seriously you're taking this matter. Not surprised, though.

Glad to see you keeping the community in the light for upcoming changes.

YayHar - May 4, 2016, 2:27 pm

I don't see anybody in protest, which I for one, think is a good thing.

Epic??? - May 4, 2016, 2:31 pm

Excellent plans for dealing with this issue.

Just a bit concerned for the people who don't have a phone capable of using Gauth and want to post in the marketplace.

dopepizza - May 4, 2016, 2:46 pm

I've just validated my 2FA and changed my password. No way of me getting compromised.

Jimmie - May 4, 2016, 2:47 pm

I like everything except the last thing forcing people to use gauth isn't fair at all myself I don't use a cell phone because I never had a need for one.

ra1d - May 4, 2016, 2:47 pm

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 1. Offer a \$1k BTC bounty for the working exploit. (DONE)

I'm sure some of the great blackhats on HF will have a go at it.

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 5. Force password changes if PW is older than X months/days. Really like this, it should be a standard feature on all community / forum sites with a large userbase.

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.

This is great, really like this approach.

Overall looks good. :)

dopepizza - May 4, 2016, 2:49 pm

(May 4, 2016 02:47 PM)jimmie Wrote: [\[CITE\]](#) I like everything except the last thing, forcing people to use gauth isn't fair at all myself, I don't use a cell phone because I never had a need for one.

Hey Jimmie, just take a look at [this](#).

It's a chrome extension for 2FA, you could also do this on Firefox or any browser.

Also,

You can use [AUTHY](#) on your computer.

Problem solved.

Omniscient - May 4, 2016, 2:49 pm

Quote:#5: What was your mentality behind it? Just curious to hear if changing an uncompromised password with 2FA enabled would bring security improvements or if it'd just inconvenience the user. Because I think it's a good security practice to rotate passwords. I already close accounts that are inactive. It's likely going to be a 6 month change. So I don't think twice a year PW change is going to be too bad. Slight inconvenience but a good trade-off that old dumps will eventually be worthless. I'm hoping even if the DB is dumped with a required 12 character PW that it will be near impossible to crack the hashed passwords within 6 months.

Right now I'm shocked that the 10 character PW's are being unhashed at such a rate. Either these are simpler passwords like "Password12" or they have a buttload of computing power in a botnet doing billions of attempts per second.

If I'm logging PW dates then it's not difficult to setup a new PW expiration time.

Quote:Are you going to make "Last Gauth/2FA Validation" Play a role in this? Such as you cannot post in the marketplace unless you Validate your 2FA. When it has not been Validated in awhile. Maybe. It's possible. What I've outlined is stuff I intend to do and that needs to be done. It's unlikely these steps are the only ones I will take.

Quote:Damn it. This should have been done a long time ago. Maybe true but as the only guy coding HF I mainly have to deal with immediate stuff that's the highest priority. As many can attest, I have done a fair amount of work this year related to Trust Scan. I do lots of work everyday. I have to prioritize.

Quote:Gauth required to PM?

Yes, because let's say you're a scammer. You need one of two things.

1. Access to post in Marketplace.
2. Ability to send PMs.

So, that's why those particular actions will require Gauth. For those who aren't that big into Marketplace activity or don't need to send PMs then they won't need Gauth.

Quote:Just a bit concerned for the people who don't have a phone capable of using Gauth and want to post in the marketplace.

Yes, that's true. Hopefully we can get more people to use Authy and 2FA because in today's world it's extremely important to do so. Members consistently want me to do more about scammers but sometimes that's going to hurt Marketplace activity. Members have to be willing to trade-off their sales for security.

Cap - May 4, 2016, 2:49 pm

(May 4, 2016 02:47 PM)jimmie Wrote: [\[CITE\]](#) I like everything except the last thing forcing people to use gauth isn't fair at all myself I don't use a cell phone because I never had a need for one. Authy isn't just for phones, it can be used on your desktop as well.

ra1d - May 4, 2016, 2:49 pm

(May 4, 2016 02:47 PM)jimmie Wrote: [\[CITE\]](#) I like everything except the last thing forcing people to use gauth isn't fair at all myself I don't use a cell phone because I never had a need for one. You can use Authy on your PC.

t0ks1ck™ - May 4, 2016, 2:50 pm

Thats good steps to improve HF !! was not using gauth before and now I am !! & I like to thing to change passwords every X amount of times ! been doing this for all my accounts already every 2-3 months so why not a forced step !!

Fudster - May 4, 2016, 2:51 pm

Thanks Omni.

Been waiting for this one for a while now.

Quote:6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.
Looking forward to the site wide password wipe. ..Sadly I know its going to cause alot of chaos.

People confused, using contact forums, Lost access to emails etc.. Going to be a on going thing for a while. But in the end it will all work out for the greater good.

Sucker for pain - May 4, 2016, 2:51 pm

Thank you for keeping the forum safe!

I really like the exploit hunt.

Omniscient - May 4, 2016, 2:59 pm

Quote:Sadly I know its going to cause alot of chaos.

Wasn't terrible before. Maybe a full month of recovery requests and contacts. I can deal with it.

Fudster - May 4, 2016, 3:00 pm

(May 4, 2016 02:59 PM)Omniscient Wrote: [\[CITE\]](#) Wasn't terrible before. Maybe a full month of recovery requests and contacts. I can deal with it.

Oh. Well. That is good to hear. I just assumed it would be a stressful, time consuming process.

Glad that you can deal with it :P Thanks for everything you do.

Hope it works out.

Sevn Alias - May 4, 2016, 3:00 pm

(May 4, 2016 02:59 PM)Omniscient Wrote: [\[CITE\]](#) Wasn't terrible before. Maybe a full month of recovery requests and contacts. I can deal with it.

Why you don't hire a hacker? I know someone who hacked HF before and he can probably find some exploits in this site.

minimalist - May 4, 2016, 3:04 pm

(May 4, 2016 03:00 PM)Sevn Alias Wrote: [\[CITE\]](#) Why you don't hire a hacker? I know someone who hacked HF before and he can probably find some exploits in this site.

That's what he's doing now. He's offering \$1000 per exploit reported.

Sevn Alias - May 4, 2016, 3:06 pm

(May 4, 2016 03:04 PM)Minimalist Wrote: [\[CITE\]](#) That's what he's doing now. He's offering \$1000 per exploit reported.

The funny thing is that the hacker who hacked HF before found a exploit in HF 1-2 months ago. He shared it before in skype chat.

Yin Yang - May 4, 2016, 3:07 pm

Nice implementations to make HF safe Omni. I also activated Gauth and changed my pw.

Rikk?a - May 4, 2016, 3:07 pm

(May 4, 2016 03:06 PM)Sevn Alias Wrote: [\[CITE\]](#) The funny thing is that the hacker who hacked HF before found a exploit in HF 1-2 months ago. He shared it before in skype chat.

If you have any information regarding this please forward it to Omniscient, he will pay you 1K if you manage to exploit it right now if give him his own password, from the DB.

Armada - May 4, 2016, 3:08 pm

I can only see improvements with what is being proposed here.

and I am sure with a vuln bounty people will likely be much more willing to report directly to you rather than try risk getting ripped off from someone else. lol

The 2FA part kind of surprises me it was not a default enforcement on upgraded accounts from a while back, I was always under the impression being upgraded and secure was the premiere benefit of upgrading, but to each their own I suppose.

The only other thing I could possibly say as input here really, which to a degree has already been covered is about the type of passwords used here.

Although it should be common sense not to use the same password on multiple sites, most people do. It only makes sense to suggest not using the same password here as on other sites. I would personally add that a totally randomized PW is likely the best solution in a scenario like this. Randomized PWs are a whole lot harder to crack/hash.

minimalist - May 4, 2016, 3:09 pm

(May 4, 2016 03:06 PM)Sevn Alias Wrote: [\[CITE\]](#) The funny thing is that the hacker who hacked HF before found a exploit in HF 1-2 months ago. He shared it before in skype chat.

So what was it? You've not reported an exploit that you have been aware of for months now?

Cyber - May 4, 2016, 3:10 pm

Nice to see you taking care of everything. I was going to suggest that members should have to have 2FA enabled to post or anything. Looks like you are already doing it =]

dopepizza - May 4, 2016, 3:11 pm

(May 4, 2016 03:06 PM)Sevn Alias Wrote: [\[CITE\]](#) The funny thing is that the hacker who hacked HF before found a exploit in HF 1-2 months ago. He shared it before in skype chat.

That's not funny.

12Chainz - May 4, 2016, 3:12 pm

(May 4, 2016 03:09 PM)Minimalist Wrote: [\[CITE\]](#) So what was it? You've not reported an exploit that you have been aware of for months now?

He told everyone in squad chat, everyone assumed he was just talking a big game, or thought it was the old DB. The problem is there are so many people who claim to have done something separating them from real threats is not easy ,which is why I'm assuming Omni wants them to come to him first.

minimalist - May 4, 2016, 3:14 pm

(May 4, 2016 03:12 PM)12Chainz Wrote: [\[CITE\]](#) He told everyone in squad chat, everyone assumed he was just talking a big game, or thought it was the old DB.

I'm confused. There wasn't a single Squad member who thought that it'd be a good idea to at least give him the benefit of the doubt and report it to Omniscient?

haydrazs - May 4, 2016, 3:15 pm

i've seen the dumps but everybody claims responsibility, i wouldn't trust anybody

Rikk?a - May 4, 2016, 3:15 pm

(May 4, 2016 03:14 PM)Minimalist Wrote: [\[CITE\]](#) I'm confused. There wasn't a single Squad member who thought that it'd be a good idea to at least give him the benefit of the doubt and report it to Omniscient?

Because they assumed he was talking big apparently and didn't believe him, but now it could be possibly he knows what happened and he didn't inform Omniscient.

The case possibly being either he didn't want to tell him. (Which is a dumb thing to do)

Or he was afraid considering all the people who say the DB was leaked and almost all of them BSed it.

minimalist - May 4, 2016, 3:17 pm

(May 4, 2016 03:15 PM)Rikk????????????????a Wrote: [\[CITE\]](#) Or he was afraid considering all the people who say the DB was leaked and almost all of them BSed it.

Yeah, I understand what you're saying here but it pains me to see that an entire group lacked the common sense to report it to Omniscient.

mrnapolean1 - May 4, 2016, 3:17 pm

I feel step 5 would be a pain but it in for the sake of account security.

reBELLYus - May 4, 2016, 3:17 pm

Solid steps. As always, thanks. The bounty will bring a lot of people out of the woodwork who will subsequently look for bugs. Excellent plan.

Junx - May 4, 2016, 3:18 pm

(May 4, 2016 03:14 PM)Minimalist Wrote: [\[CITE\]](#) I'm confused. There wasn't a single Squad member who thought that it'd be a good idea to at least give him the benefit of the doubt and report it to Omniscient?

How many kids say shit like this though?

When you think about it Omnis inbox would be filled with people reporting kids that talk shit saying they can hack HF.

Unless someone showed me absolute proof I personally would not inform Omni because that would just be a waste of his time as I'm sure he gets enough PMs as it is.

12Chainz - May 4, 2016, 3:19 pm

(May 4, 2016 03:14 PM)Minimalist Wrote: [\[CITE\]](#) I'm confused. There wasn't a single Squad member who thought that it'd be a good idea to at least give him the benefit of the doubt and report it to Omniscient?

No because omni would ask for proof and he provided none?

Rikk?a - May 4, 2016, 3:20 pm

(May 4, 2016 03:14 PM)Minimalist Wrote: [\[CITE\]](#) I'm confused. There wasn't a single Squad member who thought that it'd be a good idea to at least give him the benefit of the doubt and report it to Omniscient?

It's a matter of "proof or gtfo" if there is no proof, he won't believe it.

haydrazs - May 4, 2016, 3:21 pm

(May 4, 2016 03:20 PM)Sevn Alias Wrote: [\[CITE\]](#) So you are actually saying that HF is not possible to hack? Mate, there was a guy before who was just able to browse HF threads without having a account on Hackforums. I don't know much about it but i was watching him with 3-8 people via

join.me.

you're embarrassing the echo userbar, please stop posting

Junx - May 4, 2016, 3:22 pm

(May 4, 2016 03:21 PM)haydrazs Wrote: [\[CITE\]](#) you're embarrassing the echo userbar, please stop posting

Spoofing user agent to act as a web crawler is top tier hacking bro...

T3h Hack3r - May 4, 2016, 3:24 pm

As someone that has found and reported vulnerabilities in hackforums within the past, I reward the idea of a Bounty Program. Good work.

Omniscient - May 4, 2016, 3:26 pm

Quote:I just assumed it would be a stressful, time consuming process.

You just described the last 9 years of my life.

Quote:I am sure with a vuln bounty people will likely be much more willing to report directly to you rather than try risk getting ripped off from someone else

My guess is that someone will dump first, wait and try to earn money from it, and when that dries up or the community catches on they'll request the bounty. Still, I think and I hope that the bounty is a good idea. Time will tell. At the very least members know I take the security of HF seriously.

Quote:The 2FA part kind of surprises me it was not a default enforcement on upgraded accounts from a while back

Very surprisingly we have a lot of members unfamiliar with 2FA.

Quote: I would personally add that a totally randomized PW is likely the best solution in a scenario like this. Randomized PWs are a whole lot harder to crack/hash.

Funny you mention that. It's on my notes sheet as part of a side project to add a random password generator to the site.

Quote:There wasn't a single Squad member who thought that it'd be a good idea to at least give him the benefit of the doubt and report it to Omniscient?

It's possible they did. I get reports of dumps and leaks way too often and when I follow up on the lead they either don't produce any evidence or I end up finding out it's the old dump and their buddy was just falsely bragging. Skids love to say..."I hacked HF, here is proof" then show a screenshot of the old dump. Apparently this impresses some people. But I do follow up on reports given to me. It's just that 99% of them are bullshit. Even this current situation. I only believe there is an exploit and that we have been dumped. I have no actual proof. I'm just drawing that conclusion based on some extremely fishy logins to nearly 50 Ub3r accounts.

Quote:I'm going to assume those type of jokes get thrown around all the time. You reckon it's right for someone to bother Omniscient everytime that occurs?

If you think it's credible and you have a screenshot I don't consider myself bothered with a simple PM saying "I have this screenshot from a chat making the claim the site is compromised. Maybe you can verify it. I'm just passing this on just in case."

What I don't need is alarming threads telling people to change their PW's and that HF is hacked. I'll be happy to inform members myself if it turns out to be true.

Epic??? - May 4, 2016, 3:27 pm

(May 4, 2016 02:49 PM)Omniscient Wrote: [\[CITE\]](#) Yes, that's true. Hopefully we can get more

people to use Authy and 2FA because in today's world it's extremely important to do so. Members consistently want me to do more about scammers but sometimes that's going to hurt Marketplace activity. Members have to be willing to trade-off their sales for security.

I guess it won't be as bad as I made out originally since, as someone mentioned, it is possible to have Authy as a desktop application. With that cleared up, I'm looking forward to all the changes being implemented :)

BahNahNah - May 4, 2016, 3:32 pm

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 5. Force password changes if PW is older than X months/days.

Welp, I guess it's time to setup LastPass.

Cyber - May 4, 2016, 3:35 pm

(May 4, 2016 03:32 PM)BahNahNah Wrote: [\[CITE\]](#) Welp, I guess it's time to setup LastPass.

Nah I wouldn't use that if anything that's one of the biggest targets and they've already been hacked.

Ahri????? - May 4, 2016, 4:30 pm

Shouldn't you add a 2fa cool down? For example must have 2fa on for at least a week.

Marshmallow Man - May 4, 2016, 4:51 pm

6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.

What's to stop a hacker from taking an account with no gauth then enabling it? I think there should be more strict policy.

Skirtt - May 4, 2016, 4:52 pm

(May 4, 2016 02:06 PM)?Fazzer Wrote: [\[CITE\]](#) Damn it. This should have been done a long time ago. But whatever rule 6 gonna be awesome.

Looking forward for this.

Omni is very busy and we should respect that huge implementations like this take time.

FamousHater - May 4, 2016, 4:53 pm

umm for #5 what would be the amount of days? as hope it's not every 30 days as would get annoying changing it that often

Armada - May 4, 2016, 4:57 pm

(May 4, 2016 03:26 PM)Omniscient Wrote: [\[CITE\]](#) Funny you mention that. It's on my notes sheet as part of a side project to add a random password generator to the site.

Cough Forgot Password *Cough*

Quite honestly, that's what I use. ?

Could theoretically just disable user entered passwords and use the forgot PW function, maybe improve its generation a bit, and automatically set User PW, I have seen other sites do this for security measures. - Admittedly I know it would be a real pain for many.

Rikk?a - May 4, 2016, 4:59 pm

(May 4, 2016 04:57 PM)Armada Wrote: [\[CITE\]](#) *Cough* Forgot Password *Cough*

Quite honestly, that's what I use. ?

Could theoretically just disable user entered passwords and use the forgot PW function, maybe

improve its generation a bit, and automatically set User PW, I have seen other sites do this for security measures. - Admittedly I know it would be a real pain for many.

It's a real pain for me, but I am doing it to ensure the security of my account, so it's a risk I am willing to take.

#Skyline - May 4, 2016, 5:00 pm

Happy with these changes, great to see Omni, even number 6.

Ahri????? - May 4, 2016, 5:48 pm

(May 4, 2016 03:35 PM)Wicket Wrote: [\[CITE\]](#) Nah I wouldn't use that if anything that's one of the biggest targets and they've already been hacked.

You're fine if you're using lastpass. In fact I recommend people to use it. My personal lastpass is country locked and 2FA secured. The master password is written on paper in a hidden location for backup purpose.

Retribute - May 4, 2016, 5:59 pm

I really like that you decided to set up a bounty program. ?

Backopy - May 4, 2016, 9:06 pm

I like the new changes! the more secure, the better IMO.

The Implementation of 2FA whilst secure, is cumbersome in such a large community, it's sad to see the sheer amount of users who can't manage to get it right and those that do get it right forget that they should backup their 2FA keys, lol.

I propose an interesting suggestion (sorry for posting it wrongly in this thread but I've seen others too) that might work for people who don't have the capacity to use 2FA, or it might be an interesting security addition to HF and pretty easy to Implement whilst raising the security considerably.

HF currently only uses a password (and optional 2FA for upgraded members) it would be nice to have an additional layer under that password because security in depth is always a pretty solid idea. Something like having to use a combination of a 6 digit pin (numbers 0-9) AND a regular password would be great. I've seen such Implemented in enterprise infrastructure for security and it has worked perfectly. It would mean an attacker would need to crack not one, but two sets of "passwords" even if they somehow miraculously obtained database access.

Nonetheless I hope the attackers come out of hiding, it's only a matter of time now that the announcement has been made and a bounty offered.

Insane Developer - May 4, 2016, 10:19 pm

Rule 5 and 6 would be awesome. 2FA ftw!

Coton Pker - May 4, 2016, 10:22 pm

nigguhdayyum shit gettin serious now O.o

I guess I understand the concern.. but god damn man.

Cyrus - May 5, 2016, 1:04 am

Great changes, especially number 6! ?

Dave Skylark - May 5, 2016, 1:24 am

MPGH has the change password if X months old thing and it's a pain in the ass, but it's safe.

Pittinger - May 5, 2016, 3:02 am

I just saw what's going on. Haven't read all of it yet as I'm busy, so I'll just ask.

Is the time of the breach known? Because my 2fa was enabled fairly recently, so I'm wondering if I'm in danger.

Obviously changing pw and email now.

Omniscient - May 5, 2016, 7:20 pm

These are now done.

2. Create logging of all PW changes with both date and IP (pw's never stored in plain text).

4. Add to Trust Scan the last PW change date.

Rikk?a - May 5, 2016, 7:22 pm

(May 5, 2016 07:20 PM)Omniscient Wrote: [\[CITE\]](#) These are now done.

2. Create logging of all PW changes with both date and IP (pw's never stored in plain text).

4. Add to Trust Scan the last PW change date.

Have you found the exploit and was it fixed?

Omniscient - May 5, 2016, 8:04 pm

(May 5, 2016 07:22 PM)Rikk????????????????a Wrote: [\[CITE\]](#) Have you found the exploit and was it fixed?

Not even 100% sure we were compromised. I have yet to see any official valid proof.

Prince™ - May 5, 2016, 8:23 pm

No not this. ?

"Force password changes if PW is older than X months/days."

Whenever my bank does this to me, I feel so weird.

Cyber - May 5, 2016, 8:25 pm

(May 5, 2016 08:04 PM)Omniscient Wrote: [\[CITE\]](#) Not even 100% sure we were compromised. I have yet to see any official valid proof.

Well it's better to be safe than sorry. I'm sure you wouldn't think it out of the blue if your gut didn't tell you something was wrong.

Rikk?a - May 5, 2016, 8:52 pm

(May 5, 2016 08:04 PM)Omniscient Wrote: [CITE](#) Not even 100% sure we were compromised. I have yet to see any official valid proof.

Are you planning to do a site wide password reset once everything is patched or no official proof is yet to be found, or is the time you are going to do a mass password reset kept private?

Judicious? - May 5, 2016, 9:00 pm

Damn. You've been busy Omni. Thanks for keeping it secure around here. The big first step was when you started letting leet's use Gauth awhile back.

Fr3shN3rd - May 5, 2016, 9:03 pm

Time to collect my 1k bounty sirrrrrrrrrrrrrrrrr

GamersHeaven - May 5, 2016, 9:10 pm

This is a very nice to-do list.

CyberGuard - May 6, 2016, 4:35 pm

Guess 6 can almost be crossed off

Ace Of Jesus - May 6, 2016, 4:42 pm

I'm still wondering how they find exploit.... But well so glad I had authy on.

AAA+ - May 6, 2016, 4:45 pm

Can you hurry up with that password reset please. Ive been dying to change my password but to change it twice.... ::cry::

You Just Got Sarged - May 6, 2016, 5:25 pm

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.

Is there a way to get this on opera web browsers?

ra1d - May 6, 2016, 5:34 pm

(May 6, 2016 05:25 PM)Computer Professor Wrote: [\[CITE\]](#) Is there a way to get this on opera web browsers?Not exactly sure what you mean, but I assume you're asking if there is a Opera 2FA extension.

You may want to just download Authy on your PC.

<https://www.authy.com/app/desktop/>

You Just Got Sarged - May 6, 2016, 5:45 pm

(May 6, 2016 05:34 PM)Delicious Wrote: [\[CITE\]](#) Not exactly sure what you mean, but I assume you're asking if there is a Opera 2FA extension.

You may want to just download Authy on your PC.

<https://www.authy.com/app/desktop/>

You need a cell phone for this? ? I may have to go out and buy a cell phone and disconnected my landline.

I like my landline so I can connect to Bulletin board systems... :/

ra1d - May 6, 2016, 5:47 pm

(May 6, 2016 05:45 PM)Computer Professor Wrote: [\[CITE\]](#) You need a cell phone for this? ? I may have to go out and buy a cell phone and disconnected my landline.

No, you can download it to your computer.

You might have to link your phone number to your Authy account though for backup purposes.

Can't remember the process fully, but take a look on Authys website and it should answer most of your questions.

You Just Got Sarged - May 6, 2016, 5:59 pm

(May 6, 2016 05:47 PM)Delicious Wrote: [\[CITE\]](#) No, you can download it to your computer.

You might have to link your phone number to your Authy account though for backup purposes.

Can't remember the process fully, but take a look on Authys website and it should answer most of your questions.

I found this. Is there a way to mess with this program without enabling it on HF to see if I have to put in my number or not? I don't wish to be locked out of HF and have to go through the support with HF trying to get back in.

Quote:NO MORE SMS OR PHONE CALLS

Don't have a smartphone or tablet? No problem.

Authy for PCs gives you access to tokens without the hassle of SMS or phone calls.

ra1d - May 6, 2016, 6:07 pm

(May 6, 2016 05:59 PM)Computer Professor Wrote: [\[CITE\]](#) I found this. Is there a way to mess with this program without enabling it on HF to see if I have to put in my number or not? I don't wish to be locked out of HF and have to go through the support with HF trying to get back in.

You can try enabling it on a less valuable account. (For example a throw-away email account.)

If you enable 2FA on HackForums you will have to confirm that you have added the 2FA generated code, by supplying one of the randomly generated codes inside Authy.

It's really fool proof, so you shouldn't worry.

Also if anything screws up with Authy, you can disabled 2FA if you're already logged in, and then enable it again once you've fixed the issue.

You Just Got Sarged - May 6, 2016, 6:31 pm

(May 6, 2016 06:07 PM)Delicious Wrote: [\[CITE\]](#) You can try enabling it on a less valuable account. (For example a throw-away email account.)

If you enable 2FA on HackForums you will have to confirm that you have added the 2FA generated code, by supplying one of the randomly generated codes inside Authy.

It's really fool proof, so you shouldn't worry.

Also if anything screws up with Authy, you can disabled 2FA if you're already logged in, and then enable it again once you've fixed the issue.

I click the version of operating system I am running (Windows) and it sends me here. I don't use google chrome and from the looks of it this is a add on to chrome. It also pops up this message:

Quote:You will need Google Chrome to install most apps, extensions and themes.

Download Google Chrome

<https://chrome.google.com/webstore/detail/authy/gaedmjdfmmahhbjefcbgaolhhanlaolb?hl=en>

Crypter_ - May 6, 2016, 6:53 pm

Does HackForums use MyBB's unmodified 1.x login system? If so, moving it off of MD5 for password hashing should be on that list (probably before resetting everyone's passwords).

CyberGuard - May 6, 2016, 8:22 pm

(May 6, 2016 06:53 PM)Crypter_ Wrote: [\[CITE\]](#) Does HackForums use MyBB's unmodified 1.x login system? If so, moving it off of MD5 for password hashing should be on that list (probably before resetting everyone's passwords).

I recall hf using 8-round bCrypt in one of the more recent leaks.

ra1d - May 7, 2016, 5:29 am

(May 6, 2016 06:31 PM)Computer Professor Wrote: [\[CITE\]](#) I click the version of operating system I am running (Windows) and it sends me here. I don't use google chrome and from the looks of it this is a add on to chrome. It also pops up this message:

<https://chrome.google.com/webstore/detail/authy/gaedmjdfmmahhbjefcbgaolhhanlaolb?hl=en>

Yes it is listed as a chrome plugin, but you will actually get authy on your PC when you download it.

You Just Got Sarged - May 7, 2016, 6:00 am

(May 7, 2016 05:29 AM)Delicious Wrote: [\[CITE\]](#) Yes it is listed as a chrome plugin, but you will actually get authy on your PC when you download it.

I don't have chrome on machine. It will run poorly on my laptop and my desktop it will keep eating up my ram to the point where I have to restart my computer if I going to play a game that requires more than 3gb or when I render a video. I also have no use for chrome so I don't see why I have to download a browser just for the program.

To me it's kind of like saying go out and buy a 2014 Ford E350 Passenger van to haul a family of 4. Its silly. There has to be another way besides me downloading a 3rd web browser.

DokoNico - May 7, 2016, 6:03 am

I think someone could make alot more than 1k BTC for the exploit

ra1d - May 7, 2016, 6:26 am

(May 7, 2016 06:00 AM)Computer Professor Wrote: [\[CITE\]](#) I don't have chrome on machine. It will run poorly on my laptop and my desktop it will keep eating up my ram to the point where I have to restart my computer if I going to play a game that requires more than 3gb or when I render a video. I also have no use for chrome so I don't see why I have to download a browser just for the program.

To me it's kind of like saying go out and buy a 2014 Ford E350 Passenger van to haul a family of 4. Its silly. There has to be another way besides me downloading a 3rd web browser.

It's because they've coded it to run with the Chrome Apps framework.

NurSpec - May 7, 2016, 7:14 am

In my opinion the forced password reset is the best option here. Clears everything.

You Just Got Sarged - May 7, 2016, 2:07 pm

(May 7, 2016 06:26 AM)Delicious Wrote: [\[CITE\]](#) It's because they've coded it to run with the Chrome Apps framework.

Which requires Chrome so I am screwed. Well thanks. Time to wait for omni to change it. I'll probably take my PM's to threads, or tell people not to pm me and contact me via thread.

Roger Waters - May 7, 2016, 2:13 pm

(May 7, 2016 02:07 PM)Computer Professor Wrote: [\[CITE\]](#) Which requires Chrome so I am screwed. Well thanks. Time to wait for omni to change it. I'll probably take my PM's to threads, or tell people not to pm me and contact me via thread.

I'm surprised you don't have a cell phone or any device that can run chrome smooth enough to just have Authy running on it.

Get with the times, man.

You Just Got Sarged - May 7, 2016, 2:25 pm

(May 7, 2016 02:13 PM)Roger Waters Wrote: [\[CITE\]](#) I'm surprised you don't have a cell phone or any device that can run chrome smooth enough to just have Authy running on it.

Get with the times, man.

I don't need a cell phone. I don't wish to be one of those people that look down at my phone all day long. Also I like to connect to bulletin board systems that my friends have.

Chrome is just a browser I don't like or use. I simply don't like it, and it has a massive memory leak

on my systems. If omni would have a 2nd option besides Authy I am all for it. I prefer Opera and I don't wish to have to download an unneeded web browser on my computer. I can back up statements why I prefer Opera > Chrome if needed with article links.

I have a feeling though Omni will only do Authy though.

ra1d - May 7, 2016, 2:27 pm

(May 7, 2016 02:25 PM)Computer Professor Wrote: [\[CITE\]](#) I don't need a cell phone. I don't wish to be one of those people that look down at my phone all day long. Also I like to connect to bulletin board systems that my friends have.

Chrome is just a browser I don't like or use. I simply don't like it, and it has a massive memory leak on my systems. If omni would have a 2nd option besides Authy I am all for it. I prefer Opera and I don't wish to have to download an unneeded web browser on my computer. I can back up statements why I prefer Opera > Chrome if needed with article links.

I have a feeling though Omni will only do Authy though. I don't think you understand. You only need to install chrome ONCE, you do not have to use Chrome to actually use Authy. You'll be able to use Authy from your desktop like so; <https://i.imgur.com/eSaXc7W.png>

Pluxo - May 7, 2016, 2:34 pm

Pay that \$1,000 to Kevin Mitnick to find exploits.

Mr. Lahey - May 7, 2016, 2:38 pm

Thanks for update. I really don't mind not being able to PM or post in marketplace, #6 seems like too much effort.

BTC BTC BTC - May 7, 2016, 2:40 pm

Step 6 is a very thoughtful and good idea. Well done omni. Glad to see you're sorting all this shit out :)

Roger Waters - May 7, 2016, 2:46 pm

(May 7, 2016 02:25 PM)Computer Professor Wrote: [\[CITE\]](#) I don't need a cell phone. I don't wish to be one of those people that look down at my phone all day long. Also I like to connect to bulletin board systems that my friends have.

Chrome is just a browser I don't like or use. I simply don't like it, and it has a massive memory leak on my systems. If omni would have a 2nd option besides Authy I am all for it. I prefer Opera and I don't wish to have to download an unneeded web browser on my computer. I can back up statements why I prefer Opera > Chrome if needed with article links.

I have a feeling though Omni will only do Authy though.

Well, unless something has changed in the past month you can use any Google Authenticator application (which Authy is a variation of) to set-up Gauth. With a quick Google Search I came up with this, which is a Windows Application which serves the purpose you might be looking for.

<https://winauth.com/download/>

DuguWudi - May 8, 2016, 12:19 pm

(May 7, 2016 02:46 PM)Roger Waters Wrote: [\[CITE\]](#) Well, unless something has changed in the past month you can use any Google Authenticator application (which Authy is a variation of) to set-up Gauth. With a quick Google Search I came up with this, which is a Windows Application which serves the purpose you might be looking for.

<https://winauth.com/download/>

Any tutorial, on how to setup using this tool would be nice.

Omniscient - May 8, 2016, 2:31 pm

<https://hackforums.net/showthread.php?tid=5263387>

Doctor Blue - May 9, 2016, 6:57 pm

I think the problem with password expiration is that users are more tempted to use an easy to remember password and will just change it a tiny bit to pass the check.

Maybe you can avoid it a bit by checking the similarity of the new and the old password, PHP has a function for it.

<http://php.net/manual/en/function.similar-text.php>

Would also be a nice with a "common complex passwords" list of some sort showing common patterns of upper/lower letters, symbols and numbers, just to avoid stuff like "qwertyQWERTY123456!"#%&/", but I'm not sure if something like that exists.

Hydra - May 9, 2016, 8:55 pm

Password expirations every 6 months sounds like fun. I'm going to have to memorize a new 16+ char password every 6 months I suppose. I feel like it may come with problems such as users getting locked out or becoming more vulnerable to hackers if they reuse a previous password or an easy one (like Doctor Blue stated above me) but we'll see how it goes. Either way, it should be good thing and benefit the overall community. We'll adapt, I doubt it'll be too hard to do so for most people.

glitchgxd - May 9, 2016, 9:19 pm

(May 9, 2016 08:55 PM)iHydra Wrote: [\[CITE\]](#) Password expirations every 6 months sounds like fun. I'm going to have to memorize a new 16+ char password every 6 months I suppose. I feel like it may come with problems such as users getting locked out or becoming more vulnerable to hackers if they reuse a previous password or an easy one (like Doctor Blue stated above me) but we'll see how it goes. Either way, it should be good thing and benefit the overall community. We'll adapt, I doubt it'll be too hard to do so for most people.

For people that can't memorize passwords they should use tools like keypass that way they can have a master password to unlock their website passwords. I don't recommend doing that if you're capable of memorizing some different variations.

DuguWudi - May 9, 2016, 9:32 pm

(May 9, 2016 06:57 PM)Doctor Blue Wrote: [\[CITE\]](#) I think the problem with password expiration is that users are more tempted to use an easy to remember password and will just change it a tiny bit to pass the check.

Maybe you can avoid it a bit by checking the similarity of the new and the old password, PHP has a function for it.

<http://php.net/manual/en/function.similar-text.php>

Would also be a nice with a "common complex passwords" list of some sort showing common patterns of upper/lower letters, symbols and numbers, just to avoid stuff like "qwertyQWERTY123456!"#%&/", but I'm not sure if something like that exists.

Well, I just resetted my password on a site which I seldom visit. The problem started when the site force me to use a new password, since then each time I visit the site, I can't remember what password I use and I always reset it each time I visit it.?

Hydra - May 9, 2016, 9:51 pm

(May 9, 2016 09:19 PM)Glitch. Wrote: [\[CITE\]](#) For people that can't memorize passwords they should use tools like keypass that way they can have a master password to unlock their website passwords. I don't recommend doing that if you're capable of memorizing some different variations. Another great tip is Crypto.

<http://crypto.bz.ms/encryptors>

Use the very last section of the encryptors, MegaPhrase. You type in any keyword you can memorize and use the #Hash generated from it. Any time you type that case-sensitive text, it'll generate the same exact #hash. It's a great way to have a strong and long password and avoid using tools like keypass. Just an alternative :)

b?xxy - May 9, 2016, 10:05 pm

I completely support #6.
Amazing idea.

DuguWudi - May 9, 2016, 10:06 pm

(May 9, 2016 09:51 PM)iHydra Wrote: [\[CITE\]](#) Another great tip is Crypto.

<http://crypto.bz.ms/encryptors>

Use the very last section of the encryptors, MegaPhrase. You type in any keyword you can memorize and use the #Hash generated from it. Any time you type that case-sensitive text, it'll generate the same exact #hash. It's a great way to have a strong and long password and avoid using tools like keypass. Just an alternative :)

Nice idea but what if that website been hijack/hack?

Hydra - May 9, 2016, 10:30 pm

(May 9, 2016 10:06 PM)DuguWudi Wrote: [\[CITE\]](#) Nice idea but what if that website been hijack/hack?

You can always save the HTML file and keep a backup of it. Nothing you enter is saved on the server side that I know of. Pretty sure it's jS client side. Plus, even if it's hacked, they can't really identify you based on what you type in. No accounts needed to use it. I've been using it for almost 3 years now, it's helped me a lot. I was never a fan of tools like keypass. This is much better for me since it works on anything with a web browser(consoles, PC, mobile, etc.)

DuguWudi - May 10, 2016, 2:46 am

(May 9, 2016 10:30 PM)iHydra Wrote: [\[CITE\]](#) You can always save the HTML file and keep a backup of it. Nothing you enter is saved on the server side that I know of. Pretty sure it's jS client side. Plus, even if it's hacked, they can't really identify you based on what you type in. No accounts needed to use it. I've been using it for almost 3 years now, it's helped me a lot. I was never a fan of tools like keypass. This is much better for me since it works on anything with a web browser(consoles, PC, mobile, etc.)

What if one day, the site shutdown, what would happen to your secret password then??

Prince™ - December 21, 2016, 9:26 pm

"5. Force password changes if PW is older than X months/days."

No, not this please. ;-;

Bennynguyen100 - December 21, 2016, 10:07 pm

I really dont want these to happen:

3. Force a full password reset on the entire community.
5. Force password changes if PW is older than X months/days.

However I think this is a really good idea:

6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.

Armada - December 21, 2016, 10:33 pm

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 5. Force password changes if PW is older than X months/days.

I god honestly do not even know my current password.

Random generation of new/lost passwords (IMO) eliminated the requirement.

wander is a multi dwc - December 21, 2016, 10:51 pm

(May 4, 2016 02:01 PM)Omniscient Wrote: [\[CITE\]](#) 6. Require Gauth on all upgraded accounts for ability to PM or post in Marketplace.

This would be lovely.

Patzan - December 22, 2016, 5:13 am

Step 6 will be awesome.

For sold accs and more.

Dredd - December 22, 2016, 7:01 am

(Dec 21, 2016 11:33 PM)Armada Wrote: [\[CITE\]](#) I god honestly do not even know my current password.

Random generation of new/lost passwords (IMO) eliminated the requirement.

Got to the login page, inspect element on the password box. Then change the type from password to text.

?????s? - December 22, 2016, 7:05 am

On the password change, will we be able to use the same password if it's not recurring? Like, use 2 passwords only and keep switching out every time?

B?ker - December 22, 2016, 7:07 am

#6 is so required can't tell you how many sketchy accounts I see in the SE area

Armada - December 22, 2016, 8:13 am

(Dec 22, 2016 08:01 AM)Dredd Wrote: [\[CITE\]](#) Got to the login page, inspect element on the password box. Then change the type from password to text.

Dredd - December 22, 2016, 8:14 am

(Dec 22, 2016 09:13 AM)Armada Wrote: [\[CITE\]](#)

Better than losing your account fam ?

Armada - December 22, 2016, 8:16 am

(Dec 22, 2016 09:14 AM)Dredd Wrote: [\[CITE\]](#) Better than losing your account fam ?

Or, you know keep your 2FA secure and request a new Password when needed. lol

#Unhackable
trololol...

Bennynguyen100 - December 22, 2016, 1:47 pm

(Dec 22, 2016 08:07 AM)?MrDark Wrote: [\[CITE\]](#) #6 is so required can't tell you how many sketchy accounts I see in the SE area

Yeah this would be great