

Forum:[Hack Forums](#)

Thread: [Firewall Security](#)

Omniscient - May 6, 2016, 1:41 am

I am still investigating the details of the account breaches. As part of the investigation and an attempt to increase security I have enabled all available options in our WAF (web application firewall). That could create blocks when attempt to create posts or PMs.

I will monitor this closely but please be aware this change is necessary while I review the situation and perform the needed forensics to find the exploit.

Thank you.

xLelouch - May 6, 2016, 1:50 am

Glad to see you working hard to improve security. Thanks for updating us.

Omniscient - May 6, 2016, 1:51 am

It's 2am. Yes, I am working hard. I did take a short break for dinner and I relaxed a few minutes in the backyard. But it's been a rather long day of work.

Irish™ - May 6, 2016, 1:58 am

(May 6, 2016 01:51 AM)Omniscient Wrote: [\[CITE\]](#) It's 2am. Yes, I am working hard. I did take a short break for dinner and I relaxed a few minutes in the backyard. But it's been a rather long day of work.

I've noticed a severe speed decrease today; taking as long as 20 seconds to load a page. You may already be aware of this, but I didn't see any posts and thought that I'd point it out. Apologizes if I'm repeating what others have said.

I'm assuming that the speed decrease is in direct correlation to the added security features and services will be restored to normal within good time?

Anyway, appreciate the hard work man, best of luck.

Omniscient - May 6, 2016, 2:03 am

(May 6, 2016 01:58 AM)MrIrishLeprechaun™ Wrote: [\[CITE\]](#) I've noticed a severe speed decrease today; taking as long as 20 seconds to load a page. You may already be aware of this, but I didn't see any posts and thought that I'd point it out. Apologizes if I'm repeating what others have said.

I'm assuming that the speed decrease is in direct correlation to the added security features and services will be restored to normal within good time?

Anyway, appreciate the hard work man, best of luck.

No, that's a network issue being worked on. Slowing the site down for some people at random times for the past 12 or so hours. I've experienced it myself.

BahNahNah - May 6, 2016, 2:04 am

Are the new filewall rules making the site slow for anyone else? its taking 20-ish seconds to load every page. Other websites are fine so i dont think its my internet.

Edit:

(May 6, 2016 02:03 AM)Omniscient Wrote: [\[CITE\]](#) No, that's a network issue being worked on. Slowing the site down for some people at random times for the past 12 or so hours. I've experienced it myself.
d/w, sorry for repeating MrIrishLeprechaun.

xLelouch - May 6, 2016, 2:05 am

(May 6, 2016 01:58 AM)MrIrishLeprechaun™ Wrote: [\[CITE\]](#) I've noticed a severe speed decrease today; taking as long as 20 seconds to load a page. You may already be aware of this, but I didn't see any posts and thought that I'd point it out. Apologizes if I'm repeating what others have said.

I'm assuming that the speed decrease is in direct correlation to the added security features and services will be restored to normal within good time?

Anyway, appreciate the hard work man, best of luck.

To be honest, forum seems normal to me. I am using my phone to access at this time and i don't see any difference. Maybe its because of country, platform and other things. However, we will have to endure that even if there are some problems. Security takes the first priority.

Rubixa - May 6, 2016, 2:07 am

(May 6, 2016 02:04 AM)BahNahNah Wrote: [\[CITE\]](#) Are the new firewall rules making the site slow for anyone else? its taking 20-ish seconds to load every page. Other websites are fine so i dont think its my internet.

Edit:

d/w, sorry for repeating MrIrishLeprechaun.
New firewall rules have nothing to do with the site being slow, Omni has said it is a network issue and is working on a fix.

Edit: Nevermind you edited.

Stashyy - May 6, 2016, 2:11 am

(May 6, 2016 02:03 AM)Omniscient Wrote: [\[CITE\]](#) No, that's a network issue being worked on. Slowing the site down for some people at random times for the past 12 or so hours. I've experienced it myself.
Yeah, it happened to a few friends of mine.
I myself didn't see a speed decrease.
Glad to see that you're bumping up security. :)

Irish™ - May 6, 2016, 2:19 am

(May 6, 2016 02:03 AM)Omniscient Wrote: [\[CITE\]](#) No, that's a network issue being worked on. Slowing the site down for some people at random times for the past 12 or so hours. I've experienced it myself.
No worries. Appreciate the prompt reply.

Rubixa - May 6, 2016, 2:25 am

For anyone who doesn't know what an WAF is, it's basically a plugin for the server that places rules to HTTP so it ensures the site is covered from common attacks and allows attacks to be identified and blocked.

Edit: Which is good for the site, Obviously :) Good luck with it Omni, Thanks for the updates and the hard work you're putting in.

? Soufian ? - May 6, 2016, 4:20 am

HF has became extremely slow for me.
It literally takes 10 ~ 20 seconds to load a page.

No HF for me today. ?

Roytoy - May 6, 2016, 4:21 am

Understood. Security should be top priority.

ahemokay - May 6, 2016, 4:22 am

(May 6, 2016 04:20 AM)? Soufian ? Wrote: [\[CITE\]](#) HF has became extremely slow for me.
It literally takes 10 ~ 20 seconds to load a page.

No HF for me today. ?

Same, sometimes its fast sometimes it takes about 10 seconds to load :/

257207954 - May 6, 2016, 7:11 am

The site currently takes around 2 minutes for me to load. :/

Rubixa - May 6, 2016, 7:14 am

(May 6, 2016 07:11 AM)MeNoSkidPIs Wrote: [\[CITE\]](#) The site currently takes around 2 minutes for me to load. :/

Network issue which hopefully will be resolved. Just be patient on page loads. -Omni

TRAUMA - May 6, 2016, 9:05 am

On my side, the site loads the second I click it.
Curious on why some are slow and some are not.

?cary - May 6, 2016, 9:21 am

A big applause for the man behind HF life. Everyone appreciate the effort you are putting on site omni. ?

Firewall page(DDOS page) is coming frequently today (every 5-6 minute) , is it because you have enabled extra security ? or is it just me :/

TRAUMA - May 6, 2016, 9:24 am

(May 6, 2016 09:21 AM)RedWine™ Wrote: [\[CITE\]](#) A big applause for the man behind HF life.
Everyone appreciate the effort you are putting on site omni. ?

Firewall page(DDOS page) is coming frequently today (every 5-6 minute) , is it because you have enabled extra security ? or is it just me :/

I agree, I catch myself sending him PM's every once and a while just showing appreciation.

Not even ass kissing, like it seriously takes some dedication, a smart man, and hard work to do and handle the stuff Omni does.

BooGod - May 6, 2016, 9:25 am

Thanks for doing this, don't pursh yourself to much, I know its important but you already got to many health issues, don't create another one. I hope you can find it fast, if I see or any other member find the exploit (if possible) I hope they report it as fast as they can

?Kill? - May 6, 2016, 9:26 am

Thanks for the update Omni hope it goes well man ?

FiftyTwo - May 6, 2016, 9:48 am

Glad to see how well you're taking this possible breach, Omni!

Thanks for all the hard work and determination you're putting in to make HF a lot safer.

Best of luck! ?

grady - May 6, 2016, 9:51 am

You should open a sandboxed version of the site for those wanting to attempt to find and help fix the exploit.

?cary - May 6, 2016, 9:59 am

(May 6, 2016 09:51 AM)?Infamy Wrote: [\[CITE\]](#) You should open a sandboxed version of the site for those wanting to attempt to find and help fix the exploit.

I think Omni already talked about this . He said HF is using mybb 1.6.x so first we need to exploit this and then try it on HF. Also, creating HF sandbox might take extra effort from Omni ,which he is already giving to keep HF secure. So , currently there is no point for HF sandbox version .

?

Black Shadow - May 6, 2016, 3:57 pm

I am amazed at the amount of time and effort that goes into looking after this site you deserve a gold medal.

AAA+ - May 6, 2016, 4:08 pm

You know if you ask the right person you might find it for the right price... the exploit..

Thanks for the heads up

RumbleFrog - May 6, 2016, 4:52 pm

Hopefully, this will be done soon, can't send PM :3

Silicon Valley - May 6, 2016, 8:43 pm

(May 6, 2016 01:51 AM)Omniscient Wrote: [\[CITE\]](#) It's 2am. Yes, I am working hard. I did take a short break for dinner and I relaxed a few minutes in the backyard. But it's been a rather long day of work.

2AM? Damn. Get some sleep man!

ZuGgY - May 6, 2016, 8:49 pm

Love the way you handle things. Thanks for the update.

Prince™ - May 6, 2016, 10:33 pm

(May 6, 2016 02:03 AM)Omniscient Wrote: [\[CITE\]](#) No, that's a network issue being worked on. Slowing the site down for some people at random times for the past 12 or so hours. I've experienced it myself.

It's still going on though. I'm still facing it.

And I don't know what you're talking about the account breaches. Let us know exactly what's going on as soon as possible.

Thanks for the warning though.

johnthontaylor - May 6, 2016, 10:34 pm

are any accounts protected by gauth in any danger?

Or is this some exploit that allows the person to gain access regardless

Sadistic - May 6, 2016, 10:39 pm

Its a rather good compromise, rather have security than speed.

grady - May 6, 2016, 10:44 pm

(May 6, 2016 10:34 PM)johnnathontaylor Wrote: [\[CITE\]](#) are any accounts protected by gauth in any danger?

Or is this some exploit that allows the person to gain access regardless

The database was dumped as far as I know - anyone feel free to correct me if they have better info.

That means the IP addresses, usernames, emails, and passwords (albeit hashed & salted) are available at the hacker's whim.

No, GAuth account are not vulnerable, as there's not method for him to bypass that level of auth, password-only accounts are the only ones that they're able to get in.

Omniscient Wrote: [\[CITE\]](#) In my logs I found that nearly 40 accounts had attempts to login and it became obvious these were not sold accounts. Indeed these appear stolen. I conclude that because out of the 40 accounts only the ones without 2FA were actually logged into and stolen. And more than a few members of these stolen accounts closed have contacting me to claim they were not sold and their computers are not infected.

Grim - May 6, 2016, 10:48 pm

Glad you take security so seriously man. Hope you get it sorted out quickly.

Mr Kewl - May 7, 2016, 12:12 am

Eh it started fucking up again. :c

Can't perform any actions without waiting a minute or two, or seeing 503 page.. It was fine before 8 hours but again hard to browse.

Danny Khalifa - May 7, 2016, 12:17 am

Appreciate your hard effort Omni.
Waiting for updates.

Seasonal - May 7, 2016, 12:24 am

(May 7, 2016 12:12 AM)Mr Kewl Wrote: [\[CITE\]](#) Eh it started fucking up again. :c

Can't perform any actions without waiting a minute or two, or seeing 503 page.. It was fine before 8 hours but again hard to browse.

Same, but its been that way for me nonstop for about 48 hr now lol

Omniscient - May 7, 2016, 12:42 am

Quote:are any accounts protected by gauth in any danger?
They seem protected with Gauth.

Quote:The database was dumped as far as I know

I still have no confirmation of that and the more time passes the more I think it's not actually dumped. Lots and lots of talk yet not one honest shred of proof.

I'm starting to believe it's something simple being exploited.

#Merky - May 7, 2016, 12:51 am

(May 7, 2016 12:42 AM)Omniscient Wrote: [\[CITE\]](#) They seem protected with Gauth.

I still have no confirmation of that and the more time passes the more I think it's not actually dumped. Lots and lots of talk yet not one honest shred of proof.

I'm starting to believe it's something simple being exploited.

Since you say only a small number of accounts have been stolen is it possible that another forum has been dumped with a small number of HF users using the same passes and them being brute forced on here? To find the working ones?

Omniscient - May 7, 2016, 12:53 am

(May 7, 2016 12:51 AM)#Merky Wrote: [\[CITE\]](#) Since you say only a small number of accounts have been stolen is it possible that another forum has been dumped with a small number of HF users using the same passes and them being brute forced on here? To find the working ones?

The problem is that it's all Ub3r accounts with a few l33t accounts. And way too many for all of these to be sold accounts.

I don't know yet, still wrapping my head around this thing. Making me lose sleep. I'm dreaming of reading server logs now.

#Merky - May 7, 2016, 12:58 am

(May 7, 2016 12:53 AM)Omniscient Wrote: [\[CITE\]](#) The problem is that it's all Ub3r accounts with a few l33t accounts. And way too many for all of these to be sold accounts.

I don't know yet, still wrapping my head around this thing. Making me lose sleep. I'm dreaming of reading server logs now.

Maybe the bruteforcing config could have a capture which tells them if they are ub3r/l33t or maybe I am talking utter nonsense you should get some sleep though you'll find the problem!

Paradoxum - May 7, 2016, 5:32 am

(May 6, 2016 01:58 AM)MrIrishLeprechaun™ Wrote: [\[CITE\]](#) I've noticed a severe speed decrease today; taking as long as 20 seconds to load a page. You may already be aware of this, but I didn't see any posts and thought that I'd point it out. Apologizes if I'm repeating what others have said.

I have been experiencing this since yesterday and regrettably there is no improvement as of this writing. Is the site loading normally for you now?

ra1d - May 7, 2016, 5:39 am

(May 7, 2016 05:32 AM)Paradoxum Wrote: [\[CITE\]](#) I have been experiencing this since yesterday and regrettably there is no improvement as of this writing. Is the site loading normally for you now?

There's currently a server network issue.

<https://hackforums.net/showthread.php?tid=5260890&pid=50823887#pid50823887>

(May 6, 2016 02:03 AM)Omniscient Wrote: [\[CITE\]](#) No, that's a network issue being worked on. Slowing the site down for some people at random times for the past 12 or so hours. I've experienced it myself.

Paradoxum - May 7, 2016, 5:49 am

(May 7, 2016 05:39 AM)Delicious Wrote: [\[CITE\]](#) There's currently a server network issue.

<https://hackforums.net/showthread.php?tid=5260890&pid=50823887#pid50823887>

Oh, I am aware. Omniscient has made a [newer statement](#) regarding the matter. I am inquiring just to make sure the issue still stands as of late for someone else other than myself. ?

ra1d - May 7, 2016, 5:55 am

(May 7, 2016 05:49 AM)Paradoxum Wrote: [\[CITE\]](#) Oh, I am aware. Omniscient has made a [newer statement](#) regarding the matter. I am inquiring just to make sure the issue still stands as of late for someone else other than myself. ?

Pretty sure it's still the same issue.

I feel bad for Omni, having to wrap his head around both these two things at the same time.

However, the security is more important than to be able to load the site normally, at least for now.

Rubixa - May 7, 2016, 6:06 am

(May 7, 2016 05:55 AM)Delicious Wrote: [\[CITE\]](#) However, the security is more important than to be able to load the site normally, at least for now.

Correct, security over speed! Massive props to Omni dealing with this

\$ZEUS - May 7, 2016, 6:26 am

Glad your looking into it, but hopefully PM's are working soon!

Mr Kewl - May 7, 2016, 10:33 pm

(May 7, 2016 05:49 AM)Paradoxum Wrote: [\[CITE\]](#) Oh, I am aware. Omniscient has made a [newer statement](#) regarding the matter. I am inquiring just to make sure the issue still stands as of late for someone else other than myself. ?

Not just you, I've been facing this since past 2/3 days now I guess..

Anyway Omni, any update on this? When will this get taken down? Very hard to perform any action including opening a thread or opening a PM.

Closing/Junking/Replying takes way more time.

Riyu - May 7, 2016, 10:34 pm

Thanks for everything you do Omni.

Leroy Jethro Gibbs - May 8, 2016, 2:58 am

As of 5AM CST 5/8/2016, it still takes a good 30 seconds to load a webpage.

I'm not stressing it too much. I don't mind not getting on HF for a while until it gets fixed.

ahemokay - May 8, 2016, 3:52 am

(May 8, 2016 02:58 AM)Leroy Jethro Gibbs Wrote: [\[CITE\]](#) As of 5AM CST 5/8/2016, it still takes a good 30 seconds to load a webpage.

I'm not stressing it too much. I don't mind not getting on HF for a while until it gets fixed.

Not for me anymore, doesnt even take 5 sec to load a page.