Forum:Hack Forums

Thread: Security Breach Notification

Omniscient - *September 16, 2011, 12:38 am*
This is to notify members that one of our staff has been compromised today. Rusty_v had his password reset earlier today without his knowledge or consent. About an hour ago I found this out and I've begun forensics to access all the damage.

Luckily it doesn't appear much was done. Most of their actions was reputation related. They had rep fucked 3 members and removed many reps on individual members. They did spent some time reading staff section which is boring trust me.

This appears to have been a direct attack toward the user Legitti. His account was rep fucked and after reviewing some other activity I think it's someone who held a grudge against this particular user.

The access was for about 5 hours. I have full logs of actions but they did view many threads and profiles. I'm notifying everyone now and alerting you that your accounts are secured. Staff cannot see or edit your pms/password/emails but they can view your IPs in posts. Please be aware.

I have some suspects but if any members know something and wish to share please PM me. It will be confidential. You can even use the contact form as "Other" as a guest.

Thank you.

Laggings - *September 16, 2011, 12:40 am*
Thank you for making this public. Whilst you could've kept it without letting anyone know, this puts more minds at ease because of it.

SIM-524734 - *September 16, 2011, 12:40 am*
Oh well, Legitti, wasn't he a scammer 0.o (He sure has a shitton of scam reports) Maybe one of those who got scammed did it.

Chamomile Tea - *September 16, 2011, 12:43 am*
Thanks for the sharing this with us Omni. I'm glad not a lot of damage was done.

cY?eRteRR?Ri?t - *September 16, 2011, 12:47 am*
I think Anyone want To Take Revenge With Leggiti Thats Why He Repfucked Him .

C??????I - *September 16, 2011, 12:48 am*
Thanks for the Information Omni.
O.o Legitti's Neg and Neutral reps and his given negative reps are also got deleted.
I Hope you will find that guy soon who have done this.

chimpy - *September 16, 2011, 12:48 am*
If you could list the other members rep-fucked, that would be great.

SIM-524734 - *September 16, 2011, 12:49 am*
(Sep 16, 2011 12:48 AM)???J???? Wrote: *[CITE]* Thanks for the Information Omni.

O.o Legitti's Neg and Neutral reps are also got deleted.
I Hope you will find that guy soon who have done this.
Lol really? He had so much reps calling him scammer.

!!* Alone Vampire *!! - *September 16, 2011, 12:49 am*
Well I guess it's done by someone whom Legitti scammed.
Bad news that Rusty's account was compromised.

Omniscient - *September 16, 2011, 12:49 am*
If more obvious damage was being done it would have probably been noticed much quicker.
Everyone is watching everyone around here.

cc100 - *September 16, 2011, 12:50 am*
thanks for tracking down this ! this is usefull informtion !

(R)e1gn - *September 16, 2011, 12:52 am*
I saw the ban page.

That really sucks, hope all gets well.

Unknown fo securi reasons - *September 16, 2011, 12:52 am*
Well Cant we get some kind of extra security ? Like facebook has?

My idea is taken from facebook.

But here it is : Well for security reasons we could connect our telephone number to HF and get some kind of verification number to enter it. Or we could make a kind of app like wow where there is a authenticator that allows you to access HF And the authenticator generates a unique pw with 7-8 diggits that you have to enter everytime you login to hf. But the app makes a new pw each 1 min.

What do you think omni ?

SIM-524734 - *September 16, 2011, 12:54 am*
(Sep 16, 2011 12:52 AM)Starhawk Wrote: *[CITE]* Well Cant we get some kind of extra security ? Like facebook has?

My idea is taken from facebook.

But here it is : Well for security reasons we could connect our telephone number to HF and get some kind of verification number to enter it. Or we could make a kind of app like wow where there is a authenticator that allows you to access HF And the authenticator generates a unique pw with 7-8 diggits that you have to enter everytime you login to hf. But the app makes a new pw each 1 min.

What do you think omni ?
Or, there could be a formula and a number, the staff has a formula and the forum has one, when the staff enters they're account they need to enter a number, but with each login that number will increase depending on the formula.

But this is all dreamer's talk :?

(° ? °) - *September 16, 2011, 12:56 am*
On future note, I suggest to make passwords have at least one uppercase character and one

non-alphanumeric character, to make it more secure.

Volim te - *September 16, 2011, 12:57 am*
Oh so I probably did get DDoS'd offline before? when I though I did ? (since no one else knows my IP)
 Thanks for letting us know a lot of admins would not have ?

The GRim - *September 16, 2011, 12:59 am*
Who Were The Other Two Members That Got Repfucked?

Omniscient - *September 16, 2011, 1:00 am*
 (Sep 16, 2011 12:56 AM)Subotai Wrote: *[CITE]* On future note, I suggest to make passwords have at least one uppercase character and one non-alphanumeric character, to make it more secure.
 That's how it is now but that's not going to help if your email is stolen and a PW reset occurs. Which is what happened here.

Legitti - *September 16, 2011, 1:00 am*
That sucks for me, i dont know then. Gotta talk to rusty i guess

 I almost hit 900 reps

(R)e1gn - *September 16, 2011, 1:01 am*
Maybe something like a pin code staff has to enter when they preform extreme actions such as repfucks?

 Like LR's pin to log in.

loki` - *September 16, 2011, 1:02 am*
Philly basically took the words out of my mouth except for the fact I haven't been scammed personally.

 I think karma did infact slap him today.

 I can prove it wasn't me if you think it was tho, don't take this like I'm saying it was me. Cuz it wasn't.

  (Sep 16, 2011 01:01 AM)Ron Paul Wrote: *[CITE]* Maybe something like a pin code staff has to enter when they preform extreme actions such as repfucks?

 Like LR's pin to log in.
 Good idea actually

Androctonus - *September 16, 2011, 1:05 am*
This is unfortunate. Hope the guy who did it is caught soon.

 @ people saying "this wasn't me". I'd just like to throw in that you have absolutely nothing to worry about if it wasn't your or if you had nothing to do with it. No need to be paranoid. :)

Rippin™ - *September 16, 2011, 1:06 am*
Oh well, rep is just a number people can survive..

C??????l - *September 16, 2011, 1:06 am*

(Sep 16, 2011 01:00 AM)Omniscient Wrote: [CITE] That's how it is now but that's not going to help if your email is stolen and a PW reset occurs. Which is what happened here.
That's why i use only gmail with 2 Step verification ;P
That's secure as hell

?Love - *September 16, 2011, 1:06 am*
(Sep 16, 2011 01:00 AM)Omniscient Wrote: [CITE] That's how it is now but that's not going to help if your email is stolen and a PW reset occurs. Which is what happened here.
Maybe do a certain amount of numbers for pin verification on top of the email and pass login. Might be a little much but something i think is to be considered..

Philly - *September 16, 2011, 1:08 am*
(Sep 16, 2011 01:01 AM)Ron Paul Wrote: [CITE] Maybe something like a pin code staff has to enter when they preform extreme actions such as repfucks?

Like LR's pin to log in.
Thats a really good idea! I am going to try something like this on my own site even. Its a really smart idea.

(Sep 16, 2011 01:05 AM)?Pink ?Floyd Wrote: [CITE] This is unfortunate. Hope the guy who did it is caught soon.

@ people saying "this wasn't me". I'd just like to throw in that you have absolutely nothing to worry about if it wasn't your or if you had nothing to do with it. No need to be paranoid. :)
I am not paranoid at all. I was just stating a simple fact.

spikebites - *September 16, 2011, 1:09 am*
Well I think someone should find a way to contact Rusty_V and have him check his computer for any RATs/keyloggers. If he is ratted, then at least he will be able to find the IP of the person ratting him, then you can use that to cross verify if that IP has ever logged onto HF and to whom it belongs to.

If he's not infected, then it must be a friend of Rusty's to be able to find out his email password and then to reset it.

Legitti - *September 16, 2011, 1:10 am*
(Sep 16, 2011 01:02 AM)+Glaze Wrote: [CITE] Philly basically took the words out of my mouth except for the fact I haven't been scammed personally.

I think karma did infact slap him today.

I can prove it wasn't me if you think it was tho, don't take this like I'm saying it was me. Cuz it wasn't.

Good idea actually
I dont think it was karma, i dont believe in such a thing. This was obiviosly out of my hands and there for i couldnt do anything about it.

And other thing is that i dont really care about rep, i havent been so active on the marketplace or any other sections lately becouse of some personal things, and i think i get get back up on my feet again

Condoms - *September 16, 2011, 1:13 am*

Can't you just compare ip addresses? To see who it matches with?

Volim te - *September 16, 2011, 1:15 am*
(Sep 16, 2011 01:13 AM)Condoms Wrote: [CITE] Can't you just compare ip addresses? To see who it matches with?Because they probably used a VPN/Proxy? ?

BreastMilk - *September 16, 2011, 1:20 am*
What A Little Bitch Gaining Access To A Staff Account. Thanks For Informing Us Omni. :)

nitrateoxide - *September 16, 2011, 1:20 am*
You should do some background on his IP. There's a few ways to narrow down an ip. But yeah, good that it's all under control.

xViper - *September 16, 2011, 2:07 am*
This user had sent me a PM asking if I needed an exchange done.

Thanks for the warning Omni.

TehShrink - *September 16, 2011, 2:08 am*
That's unfortunate. Gladly the person didn't do much else.

Invincible Light - *September 16, 2011, 2:38 am*
Damn, sux for the repfucked people

hope you all get your rep back soon :)

Esix - *September 16, 2011, 2:50 am*
How was Rusty account compromise? Was he infected or was it logged?

Riggs - *September 16, 2011, 2:56 am*
The fact someone gained access to a staff account for 5 hours and only used the additional privileges for such a small vendetta gains them a little respect from me (not a lot). It shows their motives were not to harm the community, but rather a select few individuals for what appeared to be personal reasons. I'd really like to know why the hacker chose the three people he did. My guess is that Legitti probably knows the person responsible, even if he says he doesn't.

And before anyone rages at me, I do not encourage nor support any attempts to breach HF security. I'm just voicing my opinion regarding the statements made public.

Ramsay448 - *September 16, 2011, 3:00 am*
I have some Information as to who this might be. I will PM you the Details.

As for Legitti, he deserved the Rep Fuck IMO, but receiving it from a Compromised Staff Account is out of order.

Volim te - *September 16, 2011, 3:08 am*
(Sep 16, 2011 02:56 AM)Riggs Wrote: [CITE] The fact someone gained access to a staff account for 5 hours and only used the additional privileges for such a small vendetta gains them a little respect from me (not a lot). It shows their motives were not to harm the community, but rather a select few individuals for what appeared to be personal reasons. I'd really like to know why the hacker chose the three people he did. My guess is that Legitti probably knows the person responsible, even if he says he doesn't.

And before anyone rages at me, I do not encourage nor support any attempts to breach HF security. I'm just voicing my opinion regarding the statements made public.That's true, in 5 HOURS s/he could have banned/rep'd fucked a lot of HF but they did not thankful.

Burn Notice - *September 16, 2011, 3:14 am*
Rusty should check his "Recent Activity" on his gMail account. It should show who logged in and their IP Address.

Sun Tzu - *September 16, 2011, 4:12 am*
Well thanks for the tip, people are watching around others these days.

-Revolution- - *September 16, 2011, 5:19 am*
Thanks omni.
I am really sad about what happened to Legitti.!

Legitti - *September 16, 2011, 5:28 am*
It was fun to contrubute for the community. With various things, but now.. like everything at some point.. my jorney has come to an end.

https://hackforums.net/showthread.php?tid=1729319

Gyarados - *September 16, 2011, 5:30 am*
(Sep 16, 2011 05:28 AM)Legitti Wrote: *[CITE]* https://hackforums.net/showthread.php?tid=1729319
Was going to comment on your theard but it is locked :(

Anyways I'm not sure if your a scammer or not you seem legitii
Enough :p but it sucks to see you go I hope you have the best future possible
!

Legitti - *September 16, 2011, 5:35 am*
(Sep 16, 2011 03:14 AM)Burn Notice Wrote: *[CITE]* Rusty should check his "Recent Activity" on his gMail account. It should show who logged in and their IP Address.
And how u know that it was gmail account? ?

danbirk - *September 16, 2011, 5:36 am*
How come my messages keep getting deleted :/
Staff dont like me.
Omni, answer my PM.

daman123 - *September 16, 2011, 5:45 am*
Thanks for the info man :) hopefully no one else is hurt

Fucking Idiots - *September 16, 2011, 5:50 am*
(Sep 16, 2011 01:00 AM)Omniscient Wrote: *[CITE]* That's how it is now but that's not going to help if your email is stolen and a PW reset occurs. Which is what happened here.
Honestly, I think staff accounts should be IP secured or something similar. Or get texted each time they log in from a different IP with the option to answer and cancel + reset pw instantly.

bourd - *September 16, 2011, 5:57 am*
I feel that staff shouldn't have a password reset option. They should instead talk to Omni to get it changed. It would be safer that way.

Hydra - *September 16, 2011, 6:09 am*
Its gonna be really hard to find this guy.. A lot of people hate Legitti.. Anyways, glad the account is secure and no further damage has been made.
Thanks for the Notice.

SoMuchMudkip - *September 16, 2011, 6:54 am*
That explains why he ignored my PMs.

g0dspeak - *September 16, 2011, 7:25 am*
Man that sucks. Well, now Rusty will find out how hard it is to use the contact form huh?

!!* Alone Vampire *!! - *September 16, 2011, 7:38 am*
Well, he's in a bad condition atm.
His Gmail account, and live have also been hacked together with his Liberty Reserve account.

Tobbi - *September 16, 2011, 9:09 am*
Thanks for the share omni :)
Glad not much damage was don but this should not have happened to a staff..
I hope the person behind this gets caught soon...

Anubis - *September 16, 2011, 9:22 am*
Who would say that it could happen to Rusty_v :((

BullShooter - *September 16, 2011, 9:29 am*
Yeah Rusty last night asked for my youtube credentials for 3 very important youtube accounts, and I was like bro, you have to be hacked to him! LOL!

Guess Who Is Back - *September 16, 2011, 11:28 am*
I'm so sorry for rusty and the peoples who repfucked and banned?
Anyway i hope this dosen't happens in the future.
(Sep 16, 2011 01:13 AM)Condoms Wrote: [CITE] Can't you just compare ip addresses? To see who it matches with?
Proxy, Aol, VPN, VPS? ? ?

Xerotic - *September 16, 2011, 11:54 am*
I PM'd Rusty about something yesterday. I can only wonder if it was while he was compromised.. Fuck sakes. I feel for Rusty, it can happen to anyone. Same happened to me in May. Email taken because of Gmail support. Resolved issue now, though.

Good luck Rusty.

Guess Who Is Back - *September 16, 2011, 11:56 am*
(Sep 16, 2011 11:54 AM)xerotic Wrote: [CITE] I PM'd Rusty about something yesterday. I can only wonder if it was while he was compromised.. Fuck sakes. I feel for Rusty, it can happen to anyone. Same happened to me in May.
Maybe they have the email from the HF database that was leaked/?

BritishKitten - *September 16, 2011, 12:02 pm*
(Sep 16, 2011 11:56 AM)Guess Who Is Back Wrote: [CITE] Maybe they have the email from the HF database that was leaked/?
Surely if he was on the names on the list, how comes he wasn't hacked sooner then? ?

?Screamo - *September 16, 2011, 12:11 pm*
(Sep 16, 2011 12:02 PM)Red™ Wrote: [CITE] Surely if he was on the names on the list, how comes he wasn't hacked sooner then? ?
Because he like everyone else changed their password :P

Vexna - *September 16, 2011, 12:29 pm*
@ Omniscient, Really sad to hear this, I just saw your message on Twitter.

St. Jiberish - *September 16, 2011, 12:31 pm*
(Sep 16, 2011 12:38 AM)Omniscient Wrote: [CITE] Staff cannot see or edit your pms/password/emails but they can view you
Oh thank god, also I had a new IP, yet I matched it on my IP with my iPod.

VIRUZ™ - *September 16, 2011, 12:38 pm*
(Sep 16, 2011 12:52 AM)Starhawk Wrote: [CITE] Well Cant we get some kind of extra security ? Like facebook has?

My idea is taken from facebook.

But here it is : Well for security reasons we could connect our telephone number to HF and get some kind of verification number to enter it. Or we could make a kind of app like wow where there is a authenticator that allows you to access HF And the authenticator generates a unique pw with 7-8 diggits that you have to enter everytime you login to hf. But the app makes a new pw each 1 min.

What do you think omni ?Why not do it like we add a phone number to our account upon creation if we login from a different country we live in, they give the option to call us an verification code to verify we are who we say we are or even without the phone option still better security as not everyone knows where people live.

Wolves - *September 16, 2011, 12:51 pm*
Hmmm, what an interesting turn of events.
As far as Legitti being targeted, he was on a lot of people's shitlist, so it doesn't really narrow down the users very much.
Kind of goes without saying here, but Staff positions do bring a lot of unwanted attention to themselves as well as enemies.
Thankfully the damage wasn't more severe, is there no way to implement some safety features as far as if Staff log in with an unapproved IP?
Not sure if that is possible with MyBB, but if so, sounds like a rather good plugin to prevent these kind of incidents.

Nostre - *September 16, 2011, 12:51 pm*
Well I changed my password once again just in case.

Thanks for the notice.

Scooter - *September 16, 2011, 1:11 pm*
Thanks for notifying us Omniscient, I think that this hacker's primary motive was to attack people he didn't like. I'm guessing that the hacker went for whomever staff member was the easiest to get - in this case it was Rusty unfortunately. I too think that this was a case of karma, and Legitti got what was coming to him... It's a shame that a hacker had to do this though.

However, there is a silver lining to all of this: Legitti has permanently left and the Marketplace just

got rid of 1 scammer.

Good Luck to Rusty on trying to get his e-mail/LR/HF Account/ and other things sorted out.

Minnesota Nice - *September 16, 2011, 1:20 pm*
Could have been a lot worse haha. Thanks for the heads up.

Zach - *September 16, 2011, 2:43 pm*
Weird, I had a convo with rusty last night on HF. He wasn't acting normal.

Wolves - *September 16, 2011, 2:49 pm*
(Sep 16, 2011 02:43 PM)Zach Wrote: [CITE] Weird, I had a convo with rusty last night on HF. He wasn't acting normal.
More than likely the person that held his account knew you from somewhere else and couldn't resist the humor of talking to you on Rusty's account.

? Lollipop ? - *September 16, 2011, 2:58 pm*
(Sep 16, 2011 02:43 PM)Zach Wrote: [CITE] Weird, I had a convo with rusty last night on HF. He wasn't acting normal.
Message omni about this you must have some idea who would contact you if they had a staff account.

Zach - *September 16, 2011, 3:27 pm*
Doubt it would help, however they did know my hosting very well. Control panel links when not on thread and no where mentioned.

I confirmed I was talking to the hacker, he was trying to get access to mskeys.in. Rusty's site.

He stole rusty's LR account also, $400. With his live account.

Scincid - *September 16, 2011, 4:37 pm*
Could've been worse, they could have went on a scamming spree. Looks like they were after some good ole revenge on some people.

clectric - *September 16, 2011, 4:45 pm*
What if staff were to PM Omni the IPs they would be logging in with as a whitelist, all other IPs be blacklisted...
Therefore the breach would not be able to log-in, only the whitelisted IPs gain access. There should be some way to create this filter in PHP or Java.

Kappah - *September 16, 2011, 4:47 pm*
(Sep 16, 2011 12:56 AM)Subotai Wrote: [CITE] On future note, I suggest to make passwords have at least one uppercase character and one non-alphanumeric character, to make it more secure.
He said the password was reset, not guessed or bruted.

Even if they did have that security, people could still reset, keylog, and rat, so it wouldn't do all so much.

Zach - *September 16, 2011, 4:56 pm*
(Sep 16, 2011 04:45 PM)clectric Wrote: [CITE] What if staff were to PM Omni the IPs they would be logging in with as a whitelist, all other IPs be blacklisted...
Therefore the breach would not be able to log-in, only the whitelisted IPs gain access. There should be some way to create this filter in PHP or Java.

Wouldn't work. A lot of staff have dynamic always changing IPs.

g0dspeak - *September 16, 2011, 7:10 pm*
(Sep 16, 2011 04:56 PM)Zach Wrote: [CITE] Wouldn't work. A lot of staff have dynamic always changing IPs.
True, and I myself have a dynamic IP, it's always in the 71.210.xxx.xxx range, so maybe he could make something for just the IP range and the ISP. Not sure if it would do any good though.

Positive - *September 16, 2011, 7:12 pm*
Sorry to hear this.
I have PMed you with a user that has directly messaged me via skype.
Please message back when you have a second.

Threadlocks - *September 16, 2011, 7:16 pm*
Legeti.. Well we can't say that he did not have it coming, although I am outraged they had to hack a admins account and could not settle this another way.

Milky Gum Shot - *September 16, 2011, 7:17 pm*
Wow. Legitti is really nice and shit, why would people rage him? Anyways for whatever reason, thank you for posting this Omni, great job! Keep it up bro!

Phenomenal - *September 16, 2011, 7:39 pm*
I feel bad for Rusty/ Are there going to be any repercussions for him, or does he get staff right back?

Taserz - *September 16, 2011, 7:54 pm*
Well I know a user I -repped got thre -rep removed. I am not aware of who removed it as it does not break any rule but it was just RECENTLY removed. If you have logs of what they did and one was a removal of one of my -rep's then I would like to know. Just wondering as a -rep I gave to a user was removed without a staff member notifying me.

Grammar Rays - *September 17, 2011, 9:45 am*
His own fault for letting his account get compromised.

No offence, but this is the attitude I would have to any member, being staff doesn't excuse you, if anything it makes the situtation worse.
Glad it is sorted now, a lesson can be learned also.

Greyersting - *September 17, 2011, 8:00 pm*
Wait I thought staff CAN view PMs

RUS7Y - *September 17, 2011, 10:28 pm*
It was my fault I must admit.

I recently lost my old mobile number so I was tend to remove that number from "2 step gmail verification" and hotmail too, I thought I'll add the new number sometime soon but by luck you can say my live account was connected to my gmail and hf, He retrieved the pass and got access to my Gmail, live and libertyreserve. Sigh

I'm sorry for the problems anyone has faced due to my compromisation.

? Lollipop ? - *September 17, 2011, 10:30 pm*
(Sep 17, 2011 10:28 PM)Rusty_v Wrote: [CITE] This is my fault I must admit.

I recently lost my old mobile number so I was tend to remove that number from "2 step gmail verification" and hotmail too, I thought I'll add the new number sometime soon but by luck you can say my live account was connected to my gmail and hf, He retrieved the pass and got access to my Gmail, live and libertyreserve. Sigh

I'm sorry for the problems anyone has faced due to my compromisation.
Are you not staff anymore ? D:

you should use a email provider that isn't used much.

PM me for the one i use hardly anyone knows about it.

Warlexx - *September 18, 2011, 12:13 am*
I am glad this scamming fuck Legitti got his rep removed and account closed.Should of happened a long time ago.

ByteNull - *September 18, 2011, 8:28 am*
Hey, ive lost my neg rep, Thank you who did this..

Bigandrewgold - *September 18, 2011, 8:38 am*
(Sep 18, 2011 08:28 AM)Gone 4 Ever Wrote: [CITE] Hey, ive lost my neg rep, Thank you who did this..
That probably has nothing to do with this.

Valence - *September 18, 2011, 2:04 pm*
That's unfortunate. I'm glad to see no real damage was done, other than the unfortunate tampering of reputations.

New_York_City - *September 18, 2011, 2:17 pm*
I'm so happy that Legitti got his payback.