Subject: Re: Dont use Atomix forums!
Posted by a000clown on Thu, 08 Apr 2010 05:02:31 GMT
View Forum Message <> Reply to Message

Xpert wrote on Wed, 07 April 2010 23:43Trojan
Does THAT constitute hacking a password off IRC to make himself feel a bit better about his feeble self.

Again another lie. I didn't use IRC. Infact, I don't even know his password. If I used IRC, raven would know since he is a NetAdmin on my network and he can see the services channel.

Xpert wrote on Wed, 07 April 2010 23:43So I'm gonna say it again, I can't read pms on these forums. And password stealing? I don't have that either. So you can hop off of me for that. If you want proof, look up IPB stuff on it. I came across this while googling:

Quote:
to generate the passwords, ipb generates an md5 hash of it, "salts" it, and then re-hashes the salt. the salt i beleive is stored in ibf_members_extra, but i am not sure. note: it is unique for each user knowing what my own password was, i tried this via the SQL toolkit thing in IPB admin... just to see if i could get it to match. i ran the following query: SELECT md5(concat(md5('abcdefgh'),'#####'))
where 'abcdefgh' was my password that i knew and '#####' was the salt stored in the members_converge.converge_pass_salt field.
it did not match either the members.member_login_key or the members_converge.converge_pass_hash fields for my user...
ugh, i figured this would be a simple hash or hash and salt that i could duplicate, didn't expect to not be able to discover this...

Just to clarify a few things:

1) Whether he has a modification/plugin for IPB to read private messages is irrelevant. Any site administrator can simply go into the SQL database itself and read from there.
I am not saying Xpert or any of his admins do this, I am simply stressing the fact nothing on the internet is really private, it's all a matter of how willing the administrators are to protect your data.

2) Although most web application protect your passwords by hashing it (and hopefully with a salt as well) to make it near impossible to crack for the average person, that only means it is safe from prying eyes going through the SQL database.
It does not prevent malicious administrators from altering the PHP code (or whatever other language the software is written in) to log the passwords you input, email them, or even remove the hashing method entirely.
This is one of the reasons I don't like all these solutions like "OpenID" or "Facebook Connect", they depends too heavily on mutual trust.
Again, I am stating this to enlighten people about security, not to imply Xpert or his admins do this.

3) When Anope IRC Services is set to no hash method (which it is by default afaik) it stores the

passwords in a simple text file anyone can read. Using the getpass command while connected is unnecessary. Additionally, the getpass command does not work when the passwords are set to use a hash such as md5.
Most IRC networks tend to use the name services.example.com which makes it easy for you to check how they're saving your passwords.
If I type /quote version services.* it gives me this on Atomix's IRC.
Quote:Anope-1.7.21 (1341) services.atomix-gaming.net UnrealIRCd 3.2.x -  M (enc_none) -- build #1, compiled Oct  2 2009 11:19:16
Notice the (enc_none) which indicates the passwords are saved as plain-text.
My point is not that anyone is reading your passwords, because honestly I doubt they care. My point is you are putting your trust in the network administrators, on this site, on Atomix's site, and every other site you're registered on.

To sum up my 3 points above: Use different passwords and don't put anything on the internet that you wouldn't want to be made public.

Ralph wrote on Thu, 08 April 2010 00:29I hope Xpert the best for his new community ...
It's the same community with a few people missing tbh... At least, from what I can tell in my few hours of playing in the server.

---