**Question about hash password**

by [Jingjiao Ni](https://eclass.srv.ualberta.ca/user/view.php?id=187851&course=31986) - Wednesday, 16 November 2016, 4:34 PM

For security reason, I know it is better to just store the hash value of the user's password in the database.

But since in the api example there  is a requirement for post api

http://service/author/{AUTHOR\_ID}/posts (all posts made by {AUTHOR\_ID} visible to the **currently authenticated user**)

It seems we need to send the auth based on the user, so we need to send the base64 encode for username and password, so we need to know the plain text of the user's password. Then is it Ok for me to store the plain text of user's password in the database?

[Reply](https://eclass.srv.ualberta.ca/mod/forum/post.php?reply=1944551#mformforum)

**Re: Question about hash password**

by [Abram Hindle](https://eclass.srv.ualberta.ca/user/view.php?id=1001&course=31986) - Wednesday, 16 November 2016, 9:48 PM

Password hashes: You don't have to worry too much about that, but if you really want to do passwords by hand to avoid this weakness you can store the username:password hash. The other alternative is to store encrypted passwords and then decrypt them. The fact is that the USERS of your website don't use the basic auth API so you don't have to worry about it that much.

Node 2 Node communication is via basic auth.

Client 2 Node communication is whatever you want.