**Database Password Storage System**

1. The database are located at the remote place and if one had able to crack it then he would get the all the informations about the usename, password, etc
2. But the more important thing we concern is about the password that we had stored it, If the hacker gets the password than he can miss use it by logging in the system and making the changes
3. But we can make him stop the login in the our system by not storing the exact password in the database but instead storing the hash code of the password in the database
4. This can be done by first changing the password into the hash code by the help of the an hash maker which is an one way function
5. The one way function makes possible to change the password in to the hascode but does not convert the hashcode back in to the password
6. And then we store this hashcode in the our database and when the user login again than we take the password from it and convert it into the hashcode and we also take the hashcode from the database where we stored it and than we store it
7. And by this way the hashcode help us from the hacking of account even if the hacker gets the hashcode
8. And the hashcode changes the whole even if the one character is changed by written else where, hence one cannot imagine the whole password by hascode i.e. even a small change changes the whole hascode
9. But the hackers are also smart they make an table named as **rainbow table** of the many entries suppose like the 3 billion, then if any of the hashcode is matched to that of the database hashcode than he can easily get the password, And that’s why it is advisible to not keep the local password which are used by many or easily thinkable

🡺The concept of the salt

1. Then the new concept came of the salt and in this type of the concept an another random string or keyword is maked and that is made embade to the user’s password and than the hashcode is maded by the help of which the hashcode changes and which is different from that of the hashcode of the original password
2. And this both the password’s hashcode and the salt is stored in the database, Hence if someone tries to to guess the password from the hashcode than that will be wrong as the extra things are added to it and no rainbow table will be helpful
3. And every time the user gives password to the system the system first calls the database and then takes the salt form it than adds that to the user’s password and makes it convert to the hashcode and than matches it with the hashcode in the database
4. Now, it is made hard for the hacker to make the new rainbow table and as the each user has the new salt it will be very difficult to make the new rainbow table with the new salt

🡺The concept of the pepper

1. **Thought the salt is the good concept but it has an drawback** that both the salt and the hashcode(s) are stored in the database and if the database is compromised than the hacker would have both the things, And this is risky
2. And here the new concept of the pepper arrives and the pepper is same for all the users and which is not stored in the database, but it is stored in the backend program and which is an secrete which is not known by anyone
3. By this ways we try to make the security more powerfull
4. And the good things is that we do not need to do this types of the stuff and the js and java provides this type of the functions ready madely
5. Now, For java we use the following way :

