 how to store passwords in the database safely.  
   
You can find the link to our YouTube channel at the end of the post.  
   
If you prefer text, you can keep reading:  
   
𝐓𝐡𝐢𝐧𝐠𝐬 𝐍𝐎𝐓 𝐭𝐨 𝐝𝐨  
🔹 Storing passwords in plain text is not a good idea because anyone with internal access can see them.  
🔹 Storing password hashes directly is insufficient because it is pruned to precomputation attacks, such as rainbow tables.   
🔹 To mitigate precomputation attacks, we salt the passwords.   
   
𝐖𝐡𝐚𝐭 𝐢𝐬 𝐬𝐚𝐥𝐭?  
According to OWASP guidelines, “a salt is a unique, randomly generated string that is added to each password as part of the hashing process”.  
   
𝐇𝐨𝐰 𝐭𝐨 𝐬𝐭𝐨𝐫𝐞 𝐚 𝐩𝐚𝐬𝐬𝐰𝐨𝐫𝐝 𝐚𝐧𝐝 𝐬𝐚𝐥𝐭?  
1️⃣ A salt is not meant to be secret and it can be stored in plain text in the database. It is used to ensure the hash result is unique to each password.  
   
2️⃣  The password can be stored in the database using the following format: 𝘩𝘢𝘴𝘩( 𝘱𝘢𝘴𝘴𝘸𝘰𝘳𝘥 + 𝘴𝘢𝘭𝘵).  
   
𝐇𝐨𝐰 𝐭𝐨 𝐯𝐚𝐥𝐢𝐝𝐚𝐭𝐞 𝐚 𝐩𝐚𝐬𝐬𝐰𝐨𝐫𝐝?  
To validate a password, it can go through the following process:  
1️⃣ A client enters the password.  
2️⃣ The system fetches the corresponding salt from the database.  
3️⃣ The system appends the salt to the password and hashes it. Let’s call the hashed value H1.  
4️⃣ The system compares H1 and H2, where H2 is the hash stored in the database. If they are the same, the password is valid.   
   
Over to you: what other mechanisms can we use to ensure password safety?  
   
✅ Subscribe to our Youtube: <https://lnkd.in/eiZENHkB>  
  
[#systemdesign](https://www.linkedin.com/feed/hashtag/?keywords=systemdesign&highlightedUpdateUrns=urn%3Ali%3Aactivity%3A6950474738930479105) [#coding](https://www.linkedin.com/feed/hashtag/?keywords=coding&highlightedUpdateUrns=urn%3Ali%3Aactivity%3A6950474738930479105) [#interviewtips](https://www.linkedin.com/feed/hashtag/?keywords=interviewtips&highlightedUpdateUrns=urn%3Ali%3Aactivity%3A6950474738930479105)  
.

