WHERE AND HOW ARE PASSWORD STORED?

HOW MANY SCHEMES

INTRODUCTION:

In the digital realm, where the security of personal information is paramount, the storage of passwords stands as a crucial pillar of safeguarding user accounts. Understanding where and how passwords are stored is essential for developers and users alike to ensure robust security measures are in place. This exploration delves into the various schemes employed for password storage, shedding light on the locations where passwords are stored and the diverse methods used to protect them.

SUMMARY:

The security of passwords relies on where and how they are stored. Passwords are typically stored in databases or storage systems used by applications and websites. To enhance security, various schemes are employed, including hashing, salting, key derivation functions (KDFs), encryption, and access controls. Hashing converts passwords into irreversible hash values, while salting adds random values for extra protection. KDFs introduce computational overhead to deter brute-force attacks. Encryption ensures secure storage, and access controls limit unauthorized access to password databases. Understanding these schemes is crucial for implementing robust security measures and safeguarding user accounts from unauthorized access.

DESCRIPTION:

Passwords serve as the primary means of authentication for accessing online accounts, making their storage a matter of utmost importance. Typically, passwords are stored in databases or other storage systems utilized by applications and websites. However, simply storing passwords as plaintext poses significant security risks, as unauthorized access to the database could compromise user accounts on a massive scale.

To mitigate these risks, various schemes are employed to securely store passwords. Hashing stands as one of the most common techniques, wherein passwords are transformed into irreversible hash values using cryptographic algorithms. Salting, a practice where

random values are added to passwords before hashing, adds an additional layer of security by thwarting common attacks such as rainbow table lookups.

Key Derivation Functions (KDFs) are specifically designed for securely hashing passwords and introduce computational overhead to deter brute-force attacks. Peppering, another method akin to salting, involves adding a secret value to passwords before hashing, further enhancing security. Moreover, passwords should be stored securely using encryption techniques, and access controls should be implemented to restrict unauthorized access to the password database. Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide additional authentication factors alongside their passwords.

CONCLUSION:

The security of passwords hinges on where and how they are stored. By employing a combination of hashing, salting, encryption, and access controls, developers can ensure that passwords are stored securely, mitigating the risk of unauthorized access and data breaches. For users, understanding the security measures implemented by service providers is essential for making informed decisions about the safety of their online accounts. In an era where cyber threats are prevalent, robust password storage mechanisms are indispensable for safeguarding digital identities and maintaining user trust.

Done by,
Name : Mythili S
Dept : B.Tech CSBS 2nd year
Roll No : 22CB38