

Password Security & Authentication Analysis Report

1. Introduction

Passwords are one of the most commonly used methods for protecting digital accounts. They are used in email services, social media platforms, banking systems, and organizational networks. Despite their importance, many users still choose weak or predictable passwords, which makes systems vulnerable to attacks.

This report focuses on how passwords are stored, how attackers attempt to crack them, and what security measures can be used to protect authentication systems effectively.

2. Password Storage: Hashing vs Encryption

Passwords should never be stored in plain text because anyone who gains access to the database can see them. Instead, systems use **hashing**.

Hashing is a one-way process that converts a password into a fixed-length value. When a user logs in, the entered password is hashed and compared with the stored hash. Since hashing cannot be reversed, it provides strong protection.

Encryption, on the other hand, is a two-way process that can be reversed using a key. Because encrypted passwords can be decrypted, encryption is not recommended for password storage.

3. Common Hashing Algorithms

Different hashing algorithms provide different levels of security:

- **MD5:** Very fast and insecure
- **SHA-1:** No longer considered safe
- **SHA-256:** Strong but still fast
- **bcrypt:** Secure, slow, and salted
- **Argon2:** Modern and highly secure

Slower hashing algorithms are more secure because they make password cracking attempts more difficult and time-consuming.

4. Hash Identification and Generation

Hash types can be identified using tools such as **Hashcat**, **John the Ripper**, or online hash identifiers.

Example:

Password: password123

MD5 Hash:

482c811da5d5b4bc6d497ffa98491e38

This example shows how a common password produces a predictable hash that attackers can easily target.

5. Password Cracking Techniques

Attackers use several methods to crack passwords:

Dictionary Attack

This method uses a list of commonly used passwords. It is fast and very effective because many users choose simple passwords.

Brute Force Attack

This method tries every possible password combination. It is slower but will succeed if the password is short.

Hybrid Attack

This attack combines dictionary words with numbers or symbols.

6. Tools Used

Hashcat is a GPU-based password cracking tool known for its speed and wide hash support.

John the Ripper is a CPU-based tool that is easy to use and popular for security testing.

7. Why Weak Passwords Fail

Weak passwords fail because they are short, predictable, and commonly reused. Many of them are already available in leaked password databases. Examples include 123456, password, admin, and qwerty. These passwords can often be cracked within seconds.

8. Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an extra layer of security by requiring additional verification such as a one-time password, biometric data, or a hardware token. Even if a password is compromised, MFA can prevent unauthorized access.

9. Security Recommendations

- Use long and unique passwords
- Avoid common words and patterns
- Use bcrypt or Argon2 for hashing

- Enable Multi-Factor Authentication
- Use password managers
- Avoid password reuse

10. Conclusion

Weak passwords remain one of the main causes of security breaches. By understanding how passwords are stored and attacked, better security practices can be applied. Strong passwords, secure hashing algorithms, and multi-factor authentication together provide effective protection against modern password attacks.

Final Outcome

This analysis provides a clear understanding of password security concepts, attack techniques, and modern authentication defenses.

Prepared by:

MEGARAJ S