

Password Security & Authentication Analysis

Objective: To demonstrate password hashing and security using a simple application (CyberChef).

Step 1: Weak Password Hashing (MD5)

The password 'password' was hashed using MD5 to demonstrate weak hashing.

The screenshot shows the CyberChef interface with two main sections. The top section is titled "CyberChef - Input Password" and contains a single input field with the text "password". The bottom section is titled "CyberChef - MD5 Hash Output" and displays the resulting hash value: "MD5 Output 5f4dcc3b5aa765d81d8327deb882cf99".

Step 2: Strong Password Hashing (bcrypt)

bcrypt hashing produces salted and slow hashes, improving security.

CyberChef - bcrypt Hash Output

bcrypt Output: \$2y\$10\$examplehash

Conclusion: Weak passwords and fast hashes are insecure. Strong hashing and MFA are recommended.