1. Password Length.

- Minimum password length should be 8 characters.

2. Password Complexity.

Password must contain:

- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 number
- At least 1 special character
- This rule should be enforced during:
- Registration
- Password change
- Password reset

3. Password Masking.

Password input should be masked (i.e., hidden) when the user types it, so it is not visible on the screen.

4. Password Encryption.

Passwords should be encrypted or hashed, not stored or transmitted in plain text.

Test this by:

Logging in and capturing the request in Burp Suite

If the password is seen in clear text, it's a vulnerability

5. Password Replay Attack. Protection

Passwords (and related tokens) should be randomized.

During login, if you capture the request and see the same password/token reused, it's a vulnerability.

Ensure hashed passwords are used and do not repeat.

6. Old Password Requirement.

When changing the password, the system should ask for the old password.

If this step is skipped, someone with physical access can easily change the password.

7. Login Bypass.

Be cautious of response manipulation that might allow bypassing login mechanisms.

8. Source Code Exposure.

Never expose username or password in the HTML source code.

You can check this by:

Opening the website

Pressing Ctrl + U to view source

If any sensitive info (username/password) is visible, it's a security flaw

9. Autocomplete Off.

Autocomplete for sensitive fields (username, password) should be disabled.

If clicking on the username field shows previous inputs, it can be a security issue.

Ensure autocomplete="off" is set in the HTML.