Password Policy Requirements:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verify that user set passwords are at least 12 characters in length (after multiple spaces are combined). ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | | | | | | | | |
| Verify that passwords of at least 64 characters are permitted, and that passwords of more than 128 characters are denied. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | | | | | | | | |
| Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | | | | | | | | |
| Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords. | | | | | | | | |
| Verify users can change their password. | | | | | | | | |
| Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | | | | | | | | |
| Verify that a password strength meter is provided to help users set a stronger password. | | | | | | | | | | |  | |  | |  | |  | |  | |  |
| Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | | | | | | |  | | |  | |  | |  | |  | |  | |
| Verify that there are no periodic credential rotation or password history requirements. | | | | | | |  | | |  | |  | |  | |  | |  | |
| Verify that "paste" functionality, browser password helpers, and external password managers are permitted. | | | | | | |  | | |  | |  | |  | |  | |  | |
| Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as built-in functionality. | | | | | | |  | | |  | |  | |  | |  | |  | |
|  |  |  |  |  |  |  | |

Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))

|  |  |
| --- | --- |
| Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | |
| Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | |
| Verify that if bcrypt is used, the work factor SHOULD be as large as verification server performance will allow, with a minimum of 10. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) | |
| Verify that a system generated initial activation or recovery secret is not sent in clear text to the user. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) |  |
| Verify password hints or knowledge-based authentication (so-called "secret questions") are not present. |  |
| Verify password credential recovery does not reveal the current password in any way. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) |  |
| Verify shared or default accounts are not present (e.g. "root", "admin", or "sa"). |  |
| Verify that if an authentication factor is changed or replaced, that the user is notified of this event. |  |
| Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as time-based OTP (TOTP) or other soft token, mobile push, or another offline recovery mechanism. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering)) |  |
| Verify that intra-service secrets do not rely on unchanging credentials such as passwords, API keys or shared accounts with privileged access. |  |
| Verify that if passwords are required for service authentication, the service account used is not a default credential. (e.g. root/root or admin/admin are default in some services during installation). |  |
| Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access. |  |
| Verify passwords, integrations with databases and third-party systems, seeds and internal secrets, and API keys are managed securely and not included in the source code or stored within source code repositories. Such storage SHOULD resist offline attacks. The use of a secure software key store (L1), hardware TPM, or an HSM (L3) is recommended for password storage |  |

Verify storing of a user ID, passwords and sensitive PII in a database in a hash or encrypted format or Verify there is no request from frontend directly connecting backend database.