**ASVS Analysis**

1. **– Password Security Credentials**

5.1.1.2 (not valid): 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)>)

5.1.1.2 (not valid): Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters. ([C6](<https://owasp.org/www-project-proactive-controls/#div-numbering)>)

Unsecure implementation:  
Ein Bild, das Text, Screenshot, Schrift enthält.

Automatisch generierte Beschreibung

Secure implementation:  
Ein Bild, das Text, Screenshot, Schrift, Software enthält.

Automatisch generierte Beschreibung

5.1.1.2 (valid): 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))

5.1.1.2 (valid): Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.

5.1.1.2 (valid): Verify users can change their password.

5.1.1.2 (not valid): Verify that password change functionality requires the user's current and new password.

Unsecure Implementation:  
Ein Bild, das Text, Screenshot, Schrift enthält.

Automatisch generierte Beschreibung

Secure Implementation:  
Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

Automatisch generierte Beschreibung

5.1.1.2 (not valid): 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)>)

Secure Implementation (Added new function to existing password validation:  
Ein Bild, das Text, Screenshot, Software, Schrift enthält.

Automatisch generierte Beschreibung

5.1.1.2 (not valid): Verify that a password strength meter is provided to help users set a stronger password.

Secure Implementation (added functionality of strength meter):  
Javascript function (gets called in php code):  
Ein Bild, das Text, Screenshot, Software, Schrift enthält.

Automatisch generierte Beschreibung

5.1.1.2 (valid): 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))

5.1.1.2 (valid: Verify that there are no periodic credential rotation or password history requirements.

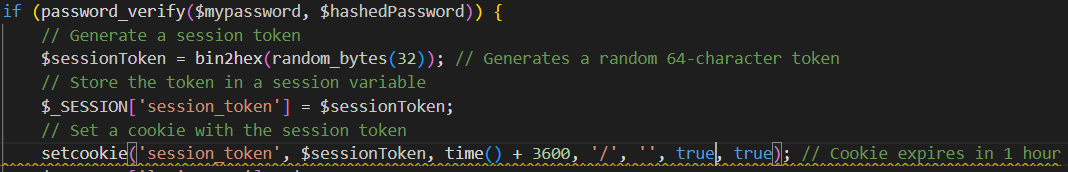
5.1.1.2 (valid): Verify that "paste" functionality, browser password helpers, and external password managers are permitted.

5.1.1.2 (valid): 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.

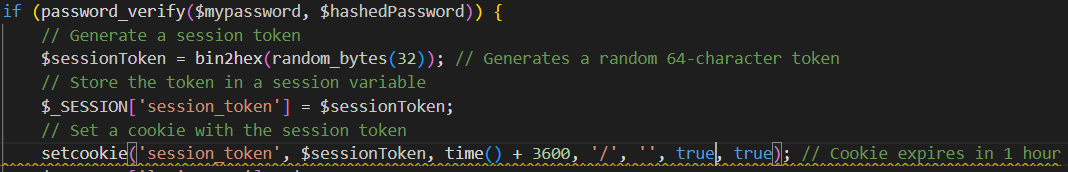
1. **– Session management**

Verify the application never reveals session tokens in URL parameters or error messages. (valid in app\_sec)

7.1 (Non-valid): Verify the application generates a new session token on user authentication. ([C6](https://www.owasp.org/index.php/OWASP\_Proactive\_Controls#tab=Formal\_Numbering))

Secure Implementation (app\_sec/php/login.php):  


7.1 (Non-valid): Verify that session tokens possess at least 64 bits of entropy. ([C6](https://www.owasp.org/index.php/OWASP\_Proactive\_Controls#tab=Formal\_Numbering)

Secure Implementation (app\_sec/php/login.php):  


7.1 (Non-valid): Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.

Secure implementation (app\_sec/php/login.php:56):  


7.1 Verify that session token are generated using approved cryptographic algorithms. ([C6](https://www.owasp.org/index.php/OWASP\_Proactive\_Controls#tab=Formal\_Numbering))

Secure implementation (app\_sec/php/login.php:52):  


7.1 (valid): Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))

7.2 (not valid): If authenticators permit users to remain logged in, verify that re-authentication occurs periodically both when actively used or after an idle period. ([C6](https://owasp.org/www-project-proactive-controls/#div-numbering))

\* L1: 30 days

\* L2: 12 hours or 30 minutes of inactivity, 2FA optional

\* L3: 12 hours or 15 minutes of inactivity, with 2FA"

Secure Implementation (set timeout to 30 minutes):  
Function checkReauthentication() gets called for every page.  
Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

Automatisch generierte Beschreibung