Secure Programming execirses lesson 1 excersise 2

B.L.Schopman

November 2019

1 Introductie

Dit zijn de uitwerkingen van de oefening 2 van Secure Programming les 1.

2 Change password

2.1 Probleem

$if(passwordisnotNoneandpwhash! = argon2.argon2_hash(password = str(password), salt =$
$"XQEXFggkPcw9BtuGkn4ELm4a7r7MUKTjBW2fjaVv6ou8mJ9ZrfEQBYhiGqQ6LzRz", t =$
$16, m = 8, p = 1, buflen = 128, argon_type = argon2.Argon2Type.Argon2_i)) :$
$returnrender_template('password.html', result =' Passwordisnotcorrect')iflen(new) <$
$16 : returnrender_template('password.html', result =' Passwordslengthistooshort(min16characters)')if($
$repeat) : returnrender_template('password.html', result =' Newpasswordsarenotthesame')$
$new = request.form.get('new')repeat = request.form.get('repeat')$
$if(passwordisnotNoneandpwhash! = argon2.argon2_hash(password = str(password), salt =$
$"XQEXFggkPcw9BtuGkn4ELm4a7r7MUKTjBW2fjaVv6ou8mJ9ZrfEQBYhiGqQ6LzRz", t =$
$16, m = 8, p = 1, buflen = 128, argon_type = argon2.Argon2Type.Argon2_i)) :$
$returnrender_template('password.html', result =' Passwordisnotcorrect')iflen(new) <$
$16 : returnrender_template('password.html', result =' Passwordslengthistooshort(min16characters)')if($
$repeat) : returnrender_template('password.html', result =' Newpasswordsarenotthesame')$
Het probleem is in deze code is dat de code niet kijkt naar de naar:

- *het oude wachtwoord om te kijken of het klopt. Password is een te generieke test.*
- *het kan alleen maar te kort zijn de lengte van het password. Niet te lang*

2.2 Bewijzen

De code kijkt alleen naar het wachtwoord ***password****. Dat is te zien in de volgende code:*
$if(passwordisnotNoneandpwhash! = argon2.argon2_hash(password = str(password), salt =$
$"XQEXFggkPcw9BtuGkn4ELm4a7r7MUKTjBW2fjaVv6ou8mJ9ZrfEQBYhiGqQ6LzRz", t =$
$16, m = 8, p = 1, buflen = 128, argon_type = argon2.Argon2Type.Argon2_i)) :$

De code kijkt alleen naar het te kort zijn voor de lengte van het password

2.3 Oplossing

De code zo maken:
$new = request.form.get('new')repeat = request.form.get('repeat')password =$
$request.form.get('password')if$ (*password is not None and pwhash !=* $argon2.argon2_hash(password =$
$str(password), salt = "XQEXFggkPcw9BtuGkn4ELm4a7r7MUKTjBW2fjaVv6ou8mJ9ZrfEQBYh$
$16, m = 8, p = 1, buflen = 128, argon_type = argon2.Argon2Type.Argon2_i)) :$
$returnrender_template('password.html', result =' Passwordisnotcorrect')iflen(new) <$
$16len(new) > 30 : returnrender_template('password.html', result =' Passwordslengthistooshort(min16ch$
$repeat) : returnrender_template('password.html', result =' Newpasswordsarenotthesame')$