

Insecure CAPTCHA in *DVWA*

Security & Encryption

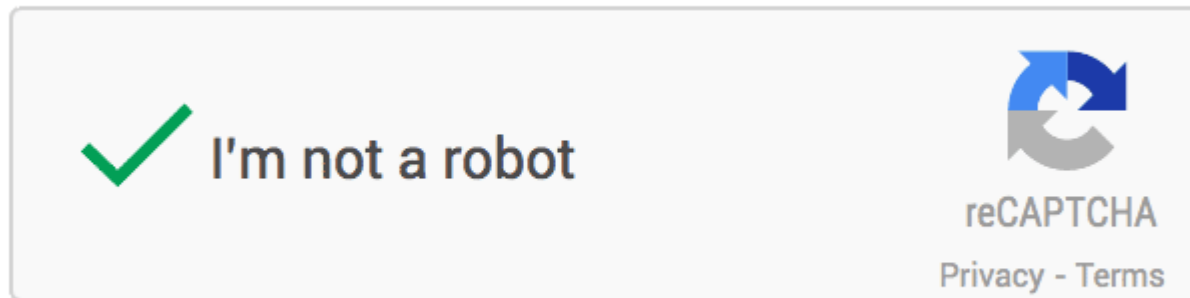
Anastasios Chandrinos

David Alberto Martin Vela

Juan Sanchez Rodriguez

What is a CAPTCHA

- ▶ CAPTCHA is a little protection program that is made to differentiate human web users from bots
- ▶ It prevents bots from abusing and spamming web sites
- ▶ It does this, by using distorted text, or equivalent methods, which bots cannot decode and bypass



Versions of reCAPTCHA

- ▶ reCAPTCHA is a free CAPTCHA security tool that is provided from Google
- ▶ Google shut down their reCAPTCHA v1 API service on March 31, 2018
- ▶ The current versions Google lets developers use is v2(“I am not a robot” checkbox, invisible badge, android) and v3.
- ▶ We will use v2(“I am not a robot” checkbox) for the DVWA hacking
- ▶ V2 checkbox is very easy to implement, using a simple checkbox that has to be clicked with the mouse

DVWA Low Level Security

```
<?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( $_DVWA[ 'recaptcha_private_key' ],
        $_SERVER[ 'REMOTE_ADDR' ],
        $_POST[ 'recaptcha_challenge_field' ],
        $_POST[ 'recaptcha_response_field' ] );

    // Did the CAPTCHA fail?
    if( !$resp->is_valid ) {
        // 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
            $html .= "
                <pre><br />You passed the CAPTCHA! Click the button to confirm your changes.<br /></pre>
                <form action=\"#\" method=\"POST\">
                    <input type=\"hidden\" name=\"step\" value=\"2\" />
                    <input type=\"hidden\" name=\"password_new\" value=\"{$pass_new}\" />
                    <input type=\"hidden\" name=\"password_conf\" value=\"{$pass_conf}\" />
                    <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_
        $pass_new = md5( $pass_new );

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

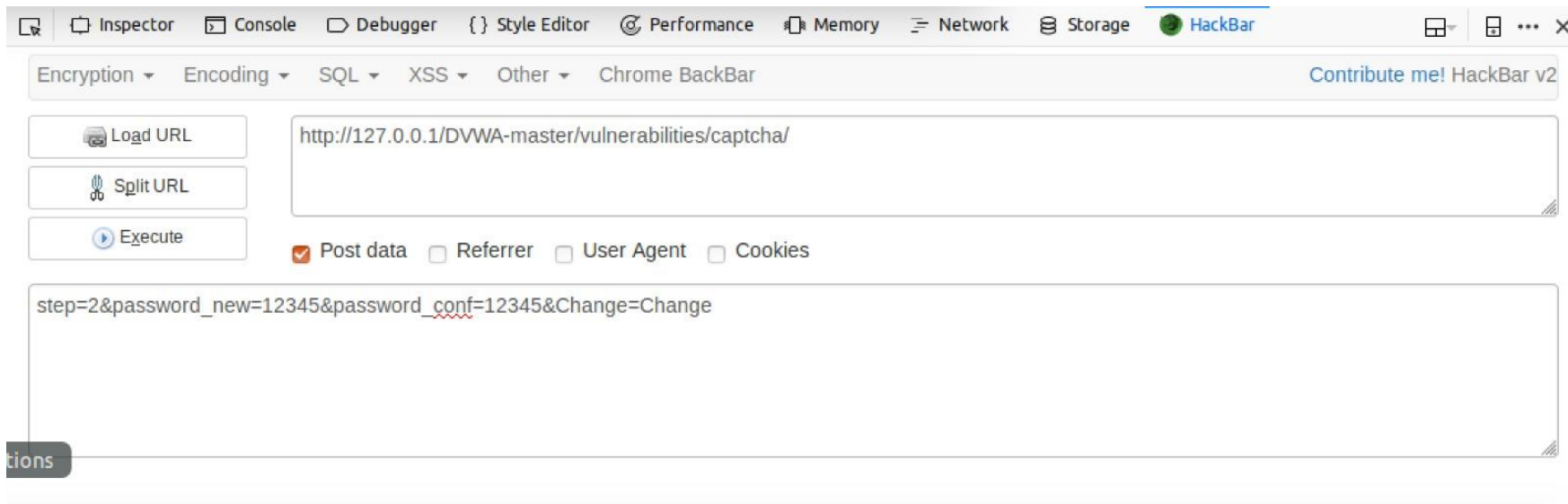
        // Feedback for the end user
        $html .= "<pre>Password Changed.</pre>";
    }
    else {
        // Issue with the passwords matching
        $html .= "<pre>Passwords did not match.</pre>";
        $hide_form = false;
    }

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

?>
```


DVWA Low Level Security

- By using HackBar(free penetration testing tool for the browser) we can make the appropriate post



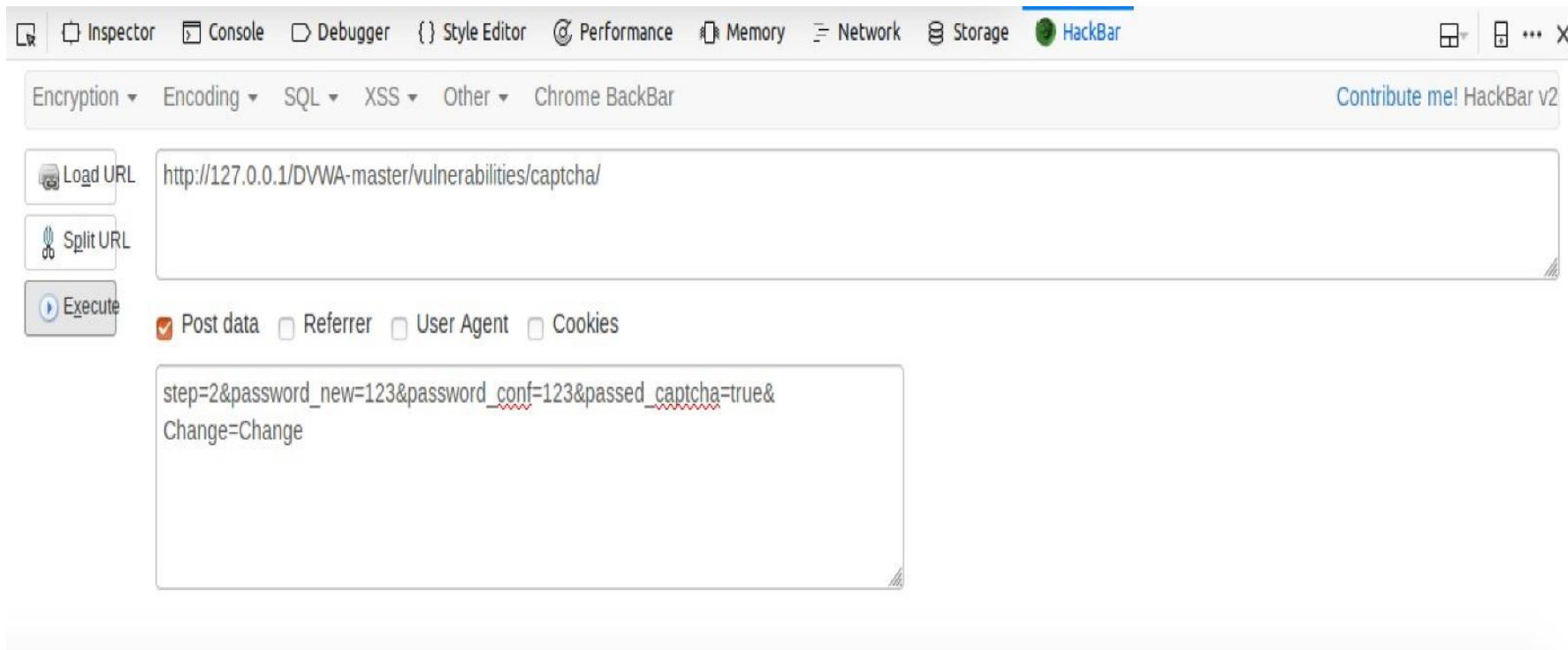
DVWA Medium Level Security

```
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_  
        $pass_new = md5( $pass_new );  
  
        // Update database  
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "'";
```




DVWA Medium Level Security

- By using HackBar(free penetration testing tool for the browser) we can make the appropriate post



DVWA High Level Security

```
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(  
        $_DVWA[ '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"], $pass_new) : addslashes($pass_new));  
            $pass_new = md5( $pass_new );  
        }  
    }  
}
```



DVWA High Level Security

```
// Update database
$insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "' LIMIT 1;";
$result = mysqli_query($GLOBALS["__mysqli_ston"], $insert ) or die( '<pre>' . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : '') );

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

} else {
    // Ops. Password mismatch
    $html .= "<pre>Both passwords must match.</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;
}

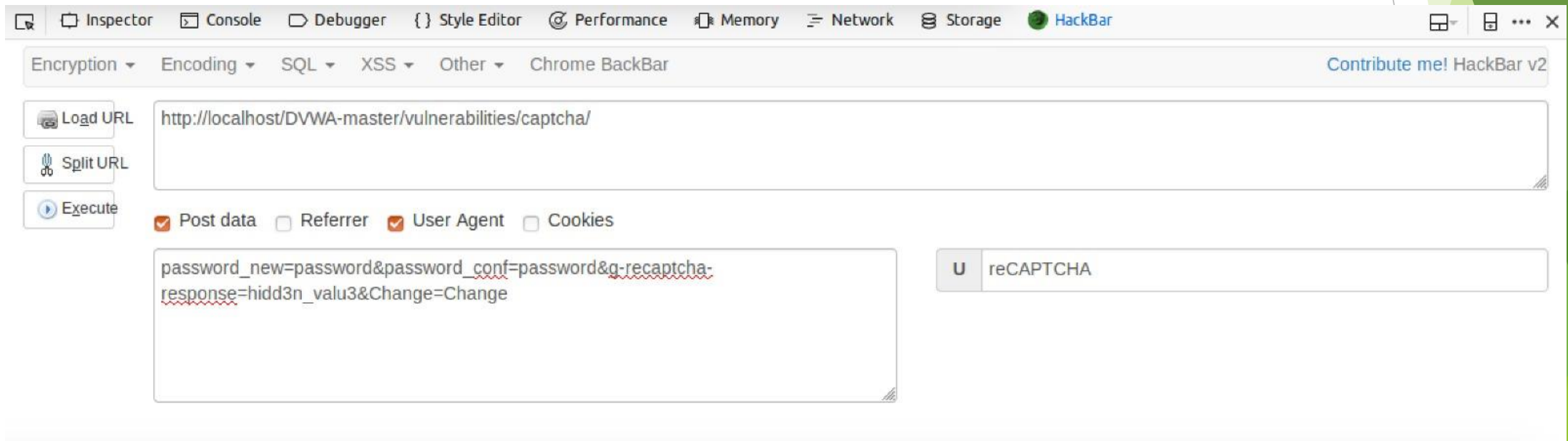
((is_null($__mysqli_res = mysqli_close($GLOBALS["__mysqli_ston"]))) ? false : $__mysqli_res);
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

DVWA High Level Security

- By using HackBar(free penetration testing tool for the browser) we can make the appropriate post and change the user agent



DVWA Impossible Level Security

Vulnerability: Insecure CAPTCHA

Change your password:

Current password:

New password:

Confirm new password:



I'm not a robot



reCAPTCHA
[Privacy](#) - [Terms](#)

Change

DVWA Impossible Level Security



```
<?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)  
[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)  
[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)  
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR) ? "" : "");  
    $pass_curr = md5( $pass_curr );
```

DVWA Impossible Level Security

- ▶ We could not hack it
- ▶ A user_token is asked
- ▶ Also the current password is asked, which only the user knows and exists only on the server