|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**Институт комплексной безопасности и специального приборостроения (ИКБСП)**

**Кафедра КБ-2 «Прикладные информационные технологии»**

**ОТЧЁТ ПО ДИСЦИПЛИНЕ**

**«Разработка безопасного программного обеспечения»**

**Лабораторная работа №1**

**Тема**: «**Безопасность систем аутентификации**»

Студенты: Частов В.В.

Учебная группа: БСБО-01-18

Руководитель: Латыпов И.Т.

Москва 2021 г.

**Постановка задачи**

1. Необходимо разработать переборщик паролей для формы в задании Bruteforce на сайте dvwa.local (Можно использовать [официальный ресурс](https://github.com/digininja/DVWA) или виртуальную машину Web Security Dojo)
2. Проанализировать код и сделать кодревью, указав слабые места

<?php

if( isset( $\_GET[ 'Login' ] ) ) {

// Get username

$user = $\_GET[ 'username' ];

// Get password

$pass = $\_GET[ 'password' ];

$pass = md5( $pass );

// Check the database

$query = "SELECT \* FROM `users` WHERE user = '$user' AND password = '$pass';";

$result = mysqli\_query($GLOBALS["\_\_\_mysqli\_ston"], $query ) or die( '<pre>' . ((is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_error($GLOBALS["\_\_\_mysqli\_ston"]) : (($\_\_\_mysqli\_res = mysqli\_connect\_error()) ? $\_\_\_mysqli\_res : false)) . '</pre>' );

if( $result && mysqli\_num\_rows( $result ) == 1 ) {

// Get users details

$row = mysqli\_fetch\_assoc( $result );

$avatar = $row["avatar"];

// Login successful

$html .= "<p>Welcome to the password protected area {$user}</p>";

$html .= "<img src=\"{$avatar}\" />";

}

else {

// Login failed

$html .= "<pre><br />Username and/or password incorrect.</pre>";

}

((is\_null($\_\_\_mysqli\_res = mysqli\_close($GLOBALS["\_\_\_mysqli\_ston"]))) ? false : $\_\_\_mysqli\_res);

}

?>

1. Разработать свою систему авторизации на любом языке, исключающий взможность подбора паролей разработнным переборщиком паролей в задании 1. Возможно исправление авторизации из dvwa.local

Требования к системе авторизации: Система авторизации должна использовать запросы GET с параметрами, аналогичными из задания bruteforce dvwa

**Ход работы**

1. **Разработка переборщика паролей для формы.**

Все выполнение работы производится в среде разработки Visual Studio 2013 на языке c#.

Дана форма авторизации

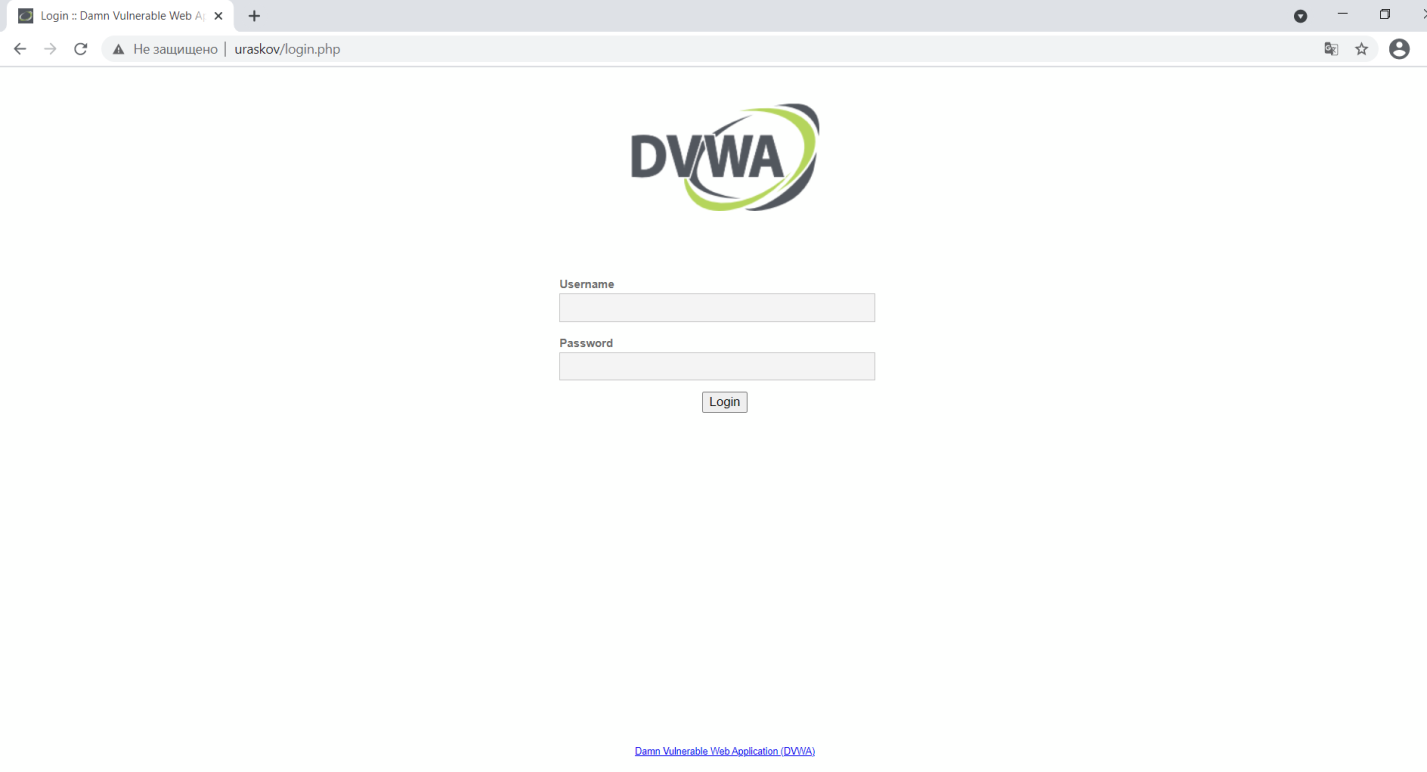


Рис.1 форма авторизации

**Method1** перебирает пароли по алфавиту для заданного логина.

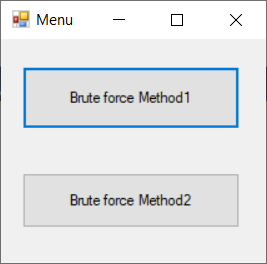


Рис. 2. Главное меню программы

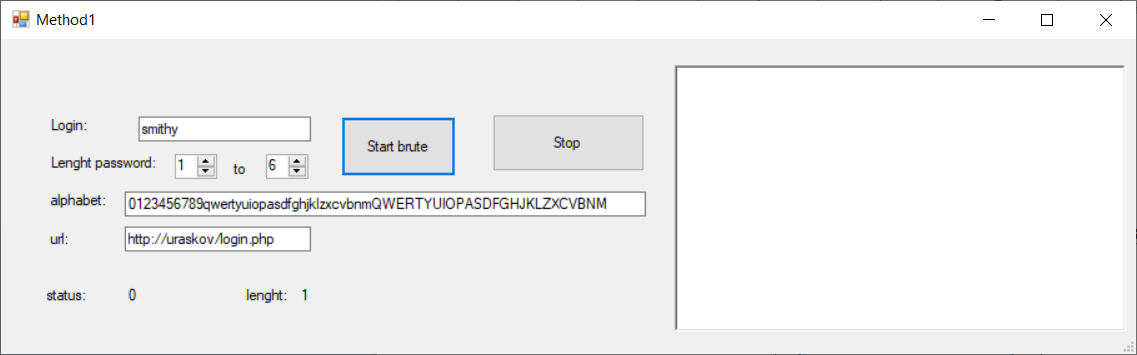


Рис. 3. Метод перебора 1.

В форме первого метода необходимо указать: логин, диапазон длины пароля, алфавит и ссылку на страницу авторизации.

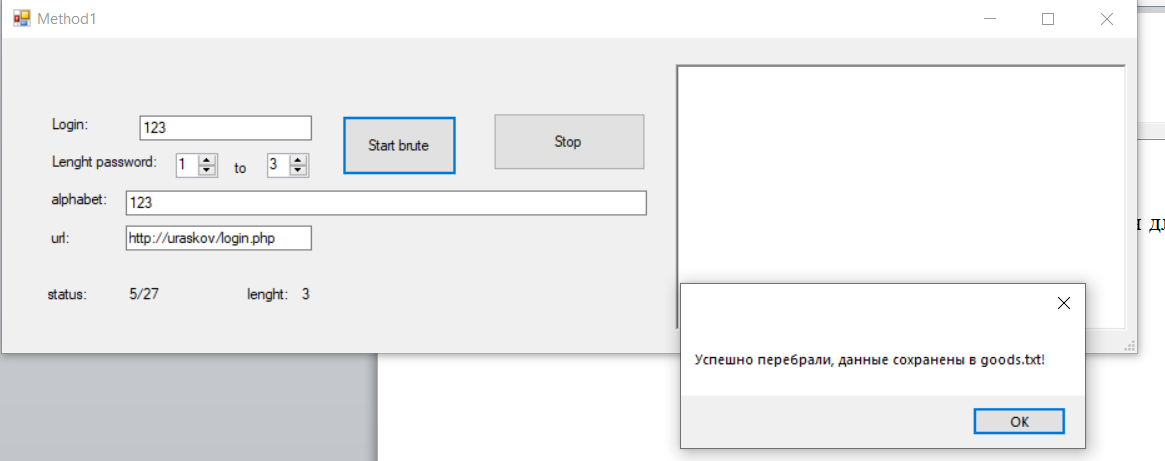


Рис. 4. Перебор паролей методом 1.

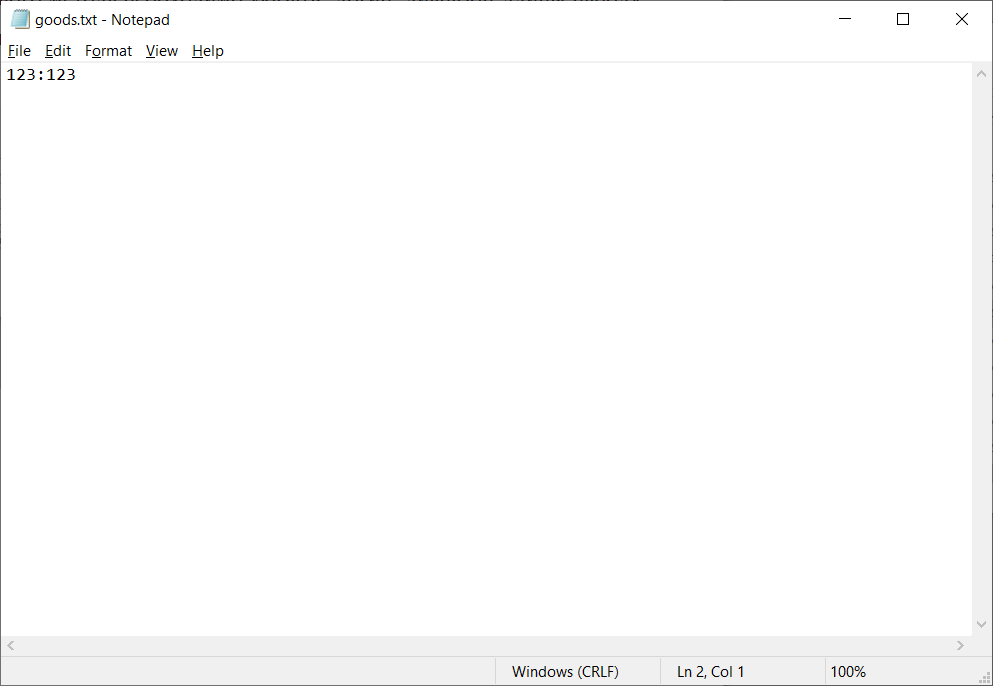


Рис. 5. Вывод в файл валидных данных метода 1.

**Method2** перебирает данные в паре логин-пароль

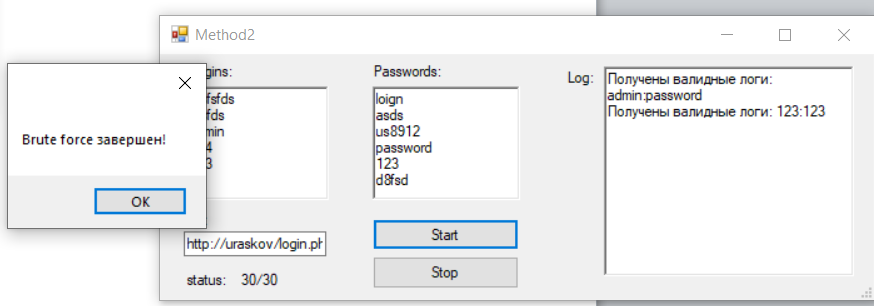


Рис. 6. Пример работы перебора методом 2.

1. **Анализ кода и составление кодревью с указанием слабых мест.**

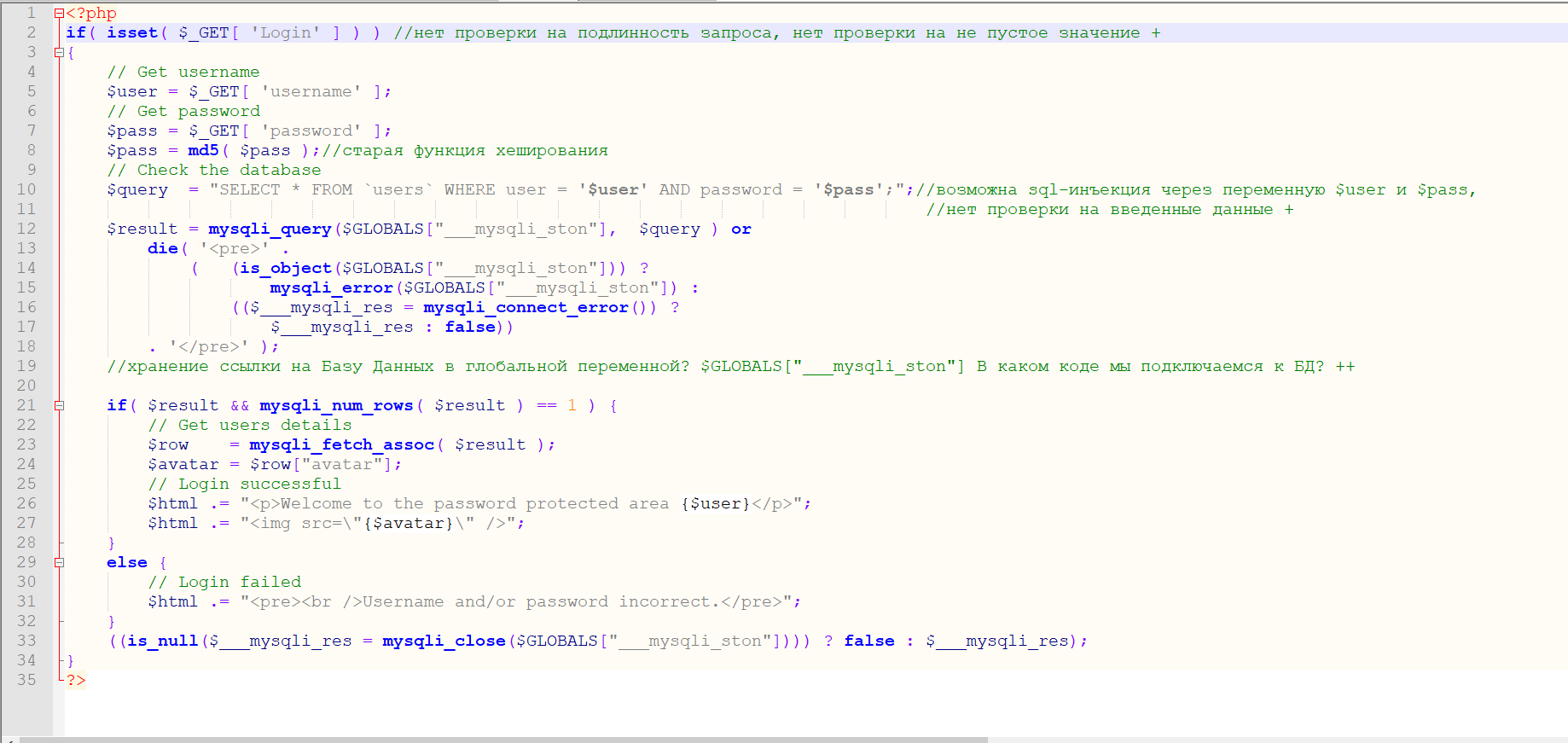


Рис. 6. Указание слабых мест в предложенном коде.

**Выявленные уязвимости:**

CVE-2011-3189 – для функции md5 обход аутентификации с помощью произвольного пароля.

CVE-2016-1927 -  угадывание паролей с помощью метода грубой силы.

CVE-2010-4697 – для функции isset может позволить контекстно-зависимым злоумышленникам вызвать отказ в обслуживании.

CVE-2021-3118 – уязвимость, при которой нет проверки входных параметров на корректность при использовании sql-запросов.

1. **Разработка своей системы авторизации и проверка программы из задания 1.**

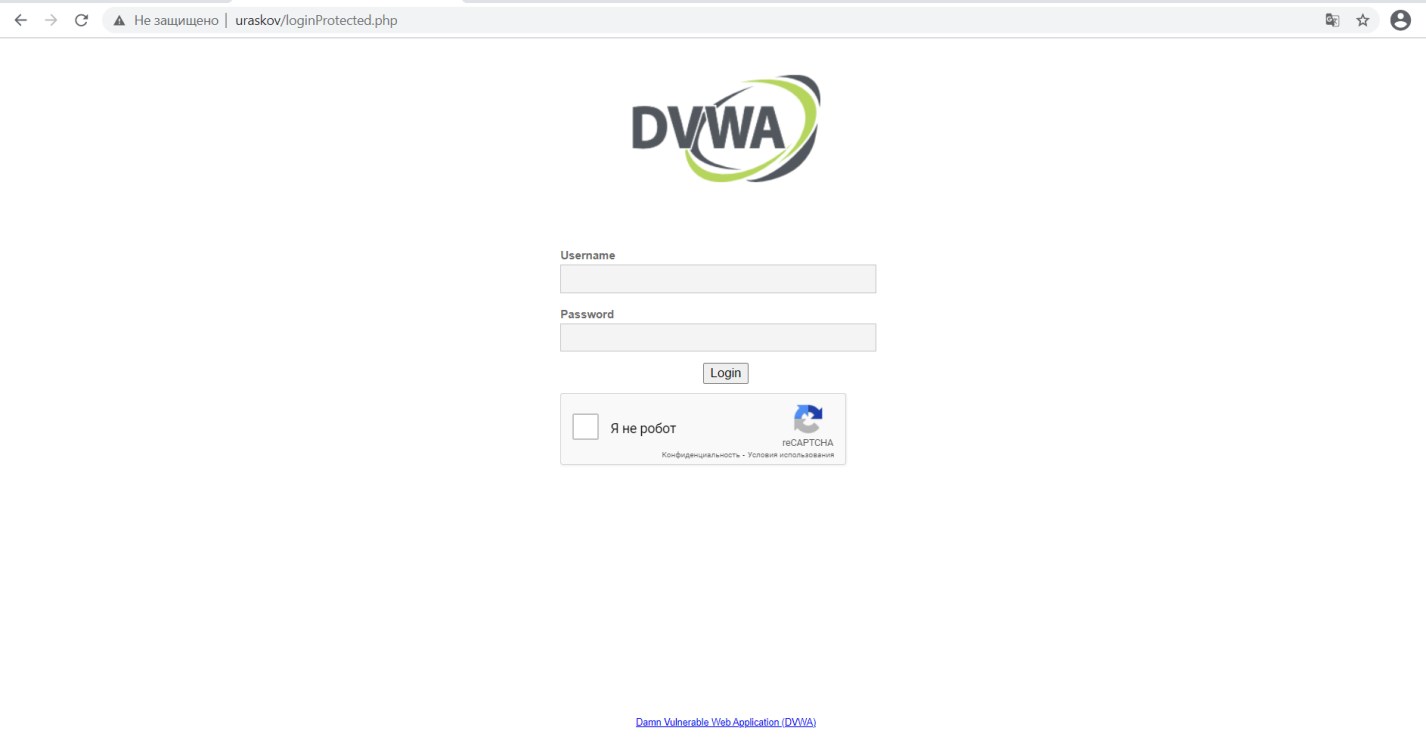
****

Рис. 7. Форма авторизации.

Результаты работы брутфорса:

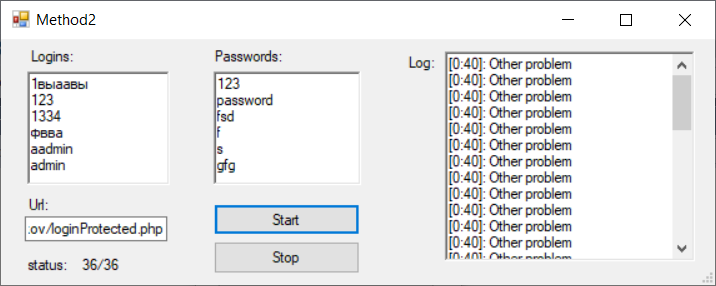


Рис. 8. Результат работы приложения.

Листинг системы авторизации

<?php

define( 'DVWA\_WEB\_PAGE\_TO\_ROOT', '' );

define('link\_auth', 'loginProtected.php');

require\_once DVWA\_WEB\_PAGE\_TO\_ROOT . 'dvwa/includes/dvwaPage.inc.php';

dvwaPageStartup( array( 'phpids' ) );

dvwaDatabaseConnect();

if( isset( $\_POST[ 'Login' ] ) ) {

$antibot=false;

$recaptcha = $\_POST['g-recaptcha-response'];

//Сразу проверяем, что он не пустой

if(!empty($recaptcha))

{

//Получаем HTTP от recaptcha

$recaptcha = $\_REQUEST['g-recaptcha-response'];

//Сюда пишем СЕКРЕТНЫЙ КЛЮЧ, который нам присвоил гугл

$secret = '6LcGw2EaAAAAAOjhkpd4qoHkv-QdPkseMVipf\_sG';

//Формируем utl адрес для запроса на сервер гугла

$url = "https://www.google.com/recaptcha/api/siteverify?secret=".$secret ."&response=".$recaptcha."&remoteip=".$\_SERVER['REMOTE\_ADDR'];

//Инициализация и настройка запроса

$curl = curl\_init();

curl\_setopt($curl, CURLOPT\_URL, $url);

curl\_setopt($curl, CURLOPT\_RETURNTRANSFER, 1);

curl\_setopt($curl, CURLOPT\_TIMEOUT, 10);

curl\_setopt($curl, CURLOPT\_USERAGENT, "Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16");

//Выполняем запрос и получается ответ от сервера гугл

$curlData = curl\_exec($curl);

curl\_close($curl);

//Ответ приходит в виде json строки, декодируем ее

$curlData = json\_decode($curlData, true);

//Смотрим на результат

if($curlData['success'])

{

//Сюда попадем если капча пройдена, дальше выполняем обычные

//действия(добавляем коммент или отправляем письмо) с формой

$antibot=true;

}

else {$antibot=false;}

}

if ($antibot)

{

// Anti-CSRF

if (array\_key\_exists ("session\_token", $\_SESSION)) {

$session\_token = $\_SESSION[ 'session\_token' ];

} else {

$session\_token = "";

}

//echo "test".$session\_token;

checkToken( $\_REQUEST[ 'user\_token' ], $session\_token, link\_auth );

$user = $\_POST[ 'username' ];

$user = stripslashes( $user );

$user = ((isset($GLOBALS["\_\_\_mysqli\_ston"]) && is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_real\_escape\_string($GLOBALS["\_\_\_mysqli\_ston"], $user ) : ((trigger\_error("[MySQLConverterToo] Fix the mysql\_escape\_string() call! This code does not work.", E\_USER\_ERROR)) ? "" : ""));

$pass = $\_POST[ 'password' ];

$pass = stripslashes( $pass );

$pass = ((isset($GLOBALS["\_\_\_mysqli\_ston"]) && is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_real\_escape\_string($GLOBALS["\_\_\_mysqli\_ston"], $pass ) : ((trigger\_error("[MySQLConverterToo] Fix the mysql\_escape\_string() call! This code does not work.", E\_USER\_ERROR)) ? "" : ""));

$pass = md5( $pass );

$query = ("SELECT table\_schema, table\_name, create\_time

FROM information\_schema.tables

WHERE table\_schema='{$\_DVWA['db\_database']}' AND table\_name='users'

LIMIT 1");

$result = @mysqli\_query($GLOBALS["\_\_\_mysqli\_ston"], $query );

if( mysqli\_num\_rows( $result ) != 1 ) {

dvwaMessagePush( "First time using DVWA.<br />Need to run 'setup.php'." );

dvwaRedirect( DVWA\_WEB\_PAGE\_TO\_ROOT . 'setup.php' );

}

$query = "SELECT \* FROM `users` WHERE user='$user' AND password='$pass';";

$result = @mysqli\_query($GLOBALS["\_\_\_mysqli\_ston"], $query ) or die( '<pre>' . ((is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_error($GLOBALS["\_\_\_mysqli\_ston"]) : (($\_\_\_mysqli\_res = mysqli\_connect\_error()) ? $\_\_\_mysqli\_res : false)) . '.<br />Try <a href="setup.php">installing again</a>.</pre>' );

if( $result && mysqli\_num\_rows( $result ) == 1 ) { // Login Successful...

dvwaMessagePush( "You have logged in as '{$user}'" );

dvwaLogin( $user );

dvwaRedirect( DVWA\_WEB\_PAGE\_TO\_ROOT . 'index.php' );

}

// Login failed

dvwaMessagePush( 'Login failed' );

dvwaRedirect( link\_auth );

}

else

{

dvwaMessagePush('error captcha');

}

}

$messagesHtml = messagesPopAllToHtml();

Header( 'Cache-Control: no-cache, must-revalidate'); // HTTP/1.1

Header( 'Content-Type: text/html;charset=utf-8' ); // TODO- proper XHTML headers...

Header( 'Expires: Tue, 23 Jun 2009 12:00:00 GMT' ); // Date in the past

// Anti-CSRF

generateSessionToken();

echo "<!DOCTYPE html>

<html lang=\"en-GB\">

<script src='https://www.google.com/recaptcha/api.js'></script>

<head>

<meta http-equiv=\"Content-Type\" content=\"text/html; charset=UTF-8\" />

<title>Login :: Damn Vulnerable Web Application (DVWA) v" . dvwaVersionGet() . "</title>

<link rel=\"stylesheet\" type=\"text/css\" href=\"" . DVWA\_WEB\_PAGE\_TO\_ROOT . "dvwa/css/login.css\" />

</head>

<body>

<div id=\"wrapper\">

<div id=\"header\">

<br />

<p><img src=\"" . DVWA\_WEB\_PAGE\_TO\_ROOT . "dvwa/images/login\_logo.png\" /></p>

<br />

</div> <!--<div id=\"header\">-->

<div id=\"content\">

<form action=\"".link\_auth."\" method=\"post\">

<fieldset>

<label for=\"user\">Username</label> <input type=\"text\" class=\"loginInput\" size=\"20\" name=\"username\"><br />

<label for=\"pass\">Password</label> <input type=\"password\" class=\"loginInput\" AUTOCOMPLETE=\"off\" size=\"20\" name=\"password\"><br />

<br />

<p class=\"submit\"><input type=\"submit\" value=\"Login\" name=\"Login\"></p>

<div class='g-recaptcha' data-sitekey='6LcGw2EaAAAAAC3d\_-DJOHWHTGvduDDqjAeAH-ED'></div></br>

</fieldset>

" . tokenField() . "

</form>

<br />

{$messagesHtml}

<br />

<br />

<br />

<br />

<br />

<br />

<br />

<br />

<!-- <img src=\"" . DVWA\_WEB\_PAGE\_TO\_ROOT . "dvwa/images/RandomStorm.png\" /> -->

</div > <!--<div id=\"content\">-->

<div id=\"footer\">

<p>" . dvwaExternalLinkUrlGet( 'https://github.com/digininja/DVWA/', 'Damn Vulnerable Web Application (DVWA)' ) . "</p>

</div> <!--<div id=\"footer\"> -->

</div> <!--<div id=\"wrapper\"> -->

</body>

</html>";

?>