|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| **Институт комплексной безопасности и специального приборостроения** | | |
|  |  |  |

Кафедра КБ-2 «Прикладные информационные технологии»

**Отчет**

по выполнению практического задания «Ренцензия кода»

по дисципилне «Основы создания безопасного программного обеспечения»

Выполнил:

Студент 4 курса

Группа БСБО-02-18

Шифр 18Б0354

Поспелов Пётр Михайлович

Преподаватель:

Латыпов И. Т.

Москва, 2021

# Исходный код

<?php

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

// Get username

//Не проверяется значение, полученное от пользователя

// https://cwe.mitre.org/data/definitions/20.html

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

// Get password

//Не проверяется значение, полученное от пользователя

// https://cwe.mitre.org/data/definitions/20.html

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

$pass = md5( $pass );

// Использование уязвимого хэша

// https://cwe.mitre.org/data/definitions/327.html

// Check the database

// Непроверенные данные в запросе, возможна SQL инъекция

// https://cwe.mitre.org/data/definitions/89.html

$query = "SELECT \* FROM `users` WHERE user = '$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);

}

?>