МИНОБРНАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Ижевский государственный технический университет

имени М.Т. Калашникова»

Факультет «Информатика и вычислительная техника»

Кафедра «Защита информации в компьютеризованных системах»

Отчет по лабораторной работе №2

по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности»

на тему «Разработка системы парольной авторизации сайта»

Выполнил:

студент группы С07-361-1

Дангыт А.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверил:

к.т.н, доцент Вдовин А.Ю.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ижевск 2017

Оглавление

[Цель лабораторной работы 3](#_Toc508535445)

[Задание 3](#_Toc508535446)

[Исходный код 4](#_Toc508535447)

[Результат работы системы 18](#_Toc508535448)

[Вывод 19](#_Toc508535449)

# Цель лабораторной работы

Изучить систему парольной авторизации для сайта и организацию политики безопасности системы.

# Задание

Разработка системы парольной авторизации для сайта. Предусмотреть несколько категорий пользователя (не менее 2) различными правами доступа. Категория администраторов должна обладать возможностью редактирования списка пользователей. Для всех категорий реализовать возможность закрытия текущей сессии.

# Исходный код

Index.php

<head>

<?php

require "db.php";

?>

<style type="text/css" media="all">

<?php include "style/style.css" ?>

</style>

</head>

<body id="telo3">

</body>

<?php

?>

<a href="/aut.php" style="color: white;">Авторизоваться</a> <br>

<a href="/signup.php" style="color: green;">Регистрация</a> <br>

Signup.php -регистрация

<head>

<?php

require "db.php";

?>

<style type="text/css" media="all">

<?php include "style/style.css" ?>

</style>

</head>

<body id = "telo1">

</body>

<?php

require "db.php";

$data=$\_POST;

if(isset($\_COOKIE['login']))

{

header('Location: auth.php');

}

if(isset($data['do\_signup']))

{

$username = mysqli\_real\_escape\_string($dbc, trim($data['Login']));

$password1 = mysqli\_real\_escape\_string($dbc, trim($data['Password']));

$password2 = mysqli\_real\_escape\_string($dbc, trim($data['Password2']));

$errors=array();

if(trim($data['Login'])=='')

{

$errors[]='Введите логин';

}

if($data['Password']=='')

{

$errors[]='Введите пароль';

}

if ($data['Password2']!=$data['Password'])

{

$errors[]='Введите пароль еще раз' ;

}

if(!empty($username) && !empty($password1) && !empty($password2) && ($password1 == $password2))

{

$query = "SELECT \* FROM `signup` WHERE login = '$username'";

$data1 = mysqli\_query($dbc, $query);

if(mysqli\_num\_rows($data1) != 0)

{

$errors[]='Логин уже существует';

}

}

if(empty($errors))

{

$pwrd=crypt('$password2','r1');

$dbc->query("INSERT INTO signup(login, password,role) VALUES ('$username','$pwrd', 'user')");

//$dbc->query("INSERT INTO signup(login, password) VALUES ('$username','$password2')");

echo '<div style="color: green;">Вы зарегистрированы <br/> Go to home list <a href="/"HOME>glavnaya</div><hr>';

}

else

{

echo '<div style="color: red;">'.array\_shift($errors).'</div><hr>';

}

}

if(isset($data['do\_before']))

{

header('Location:/ ');

}

?>

<form action="/signup.php" method="POST">

<p>

<p><strong style="color:white">Введите логин:</strong>:</p>

<input type="text" name="Login" value="<?php echo @$data['

Login'];?>">

<p><strong style="color:white">Введите пароль:</strong>:</p>

<input type="password" name="Password" value="<?php echo @$data[

'Password'];?>">

<p><strong style="color:white">Введите пароль еще раз:</strong>:</p>

<input type="password" name="Password2">

<button style="color:green" type="submit" name="do\_signup">Зарегистрироваться</button> </p>

<p>

<button style="color:green" type="submit" name="do\_before">На главную</button>

</p>

</form>

Aut.php - авторизация

<head>

<?php

require "db.php";

?>

<style type="text/css" media="all">

<?php include "style/style.css" ?

</style>

</head>

<body id = "telo4">

</body>

<?php

require "db.php";

$data=$\_POST;

$cook=$\_COOKIE;

if(isset($\_COOKIE['login']))

{

header('Location: auth.php');

}

if(!isset($\_COOKIE['login']))

{

if(isset($data['do\_aut']))

{

$username\_aut = mysqli\_real\_escape\_string($dbc, trim($data['Login']));

$password\_aut = mysqli\_real\_escape\_string($dbc, trim($data['Password']));

$errors=array();

if(trim($data['Login'])=='')

{

$errors[]='Введите логин';

}

if($data['Password']==''&& $data['Password']==' ')

{

$errors[]='Введите пароль';

}

$pwrd=crypt('$password\_aut', 'r1');

$query = "SELECT login FROM `signup` WHERE login = '$username\_aut'";

$data1 = mysqli\_query($dbc, $query);

if(mysqli\_num\_rows($data1)== 0)

{

$errors[]='ТАКОГO ПОЛЬЗОВАТЕЛЯ НЕТ';

}

$query11 = "SELECT password FROM `signup` WHERE password = '$pwrd'";

$data12 = mysqli\_query($dbc, $query11);

if(mysqli\_num\_rows($data12)== 0)

{

$errors[]='Не правильный пароль';

}

if(!empty($username\_aut) && !empty($password\_aut))

{

$pwrd=crypt('$password\_aut','r1');

//$log=$data['Login'];

//$pas=$data['Password'];

$query="SELECT \* FROM `signup` WHERE login='$username\_aut' AND password='$pwrd'";

$query2="SELECT id\_user,login, role FROM `signup` WHERE login='$username\_aut' ";

$data1=mysqli\_query($dbc, $query);

if(mysqli\_num\_rows($data1)!=0)

{

$row=mysqli\_fetch\_assoc($data1);

setcookie('id\_user', $row['id\_user'], time() +(60\*60\*24\*30));

setcookie('login', $row['login'], time() +(60\*60\*24\*30));

setcookie('password', $row['password'], time() +(60\*60\*24\*30));

setcookie('role', $row['role'], time() +(60\*60\*24\*30));

}

else

{

$errors[]='Такого пользователя нет';

printf("%s", $username\_aut);

printf("%s", $password\_aut);

}

}

if(empty($errors))

{

header('Location: auth.php');

}

else

{

echo '<div style="color: red;">'.array\_shift($errors).'</div><hr>';

}

}

}

?>

<form action="/aut.php" method="POST">

<p>

<p><strong style="color:white">Введите логин:</strong>:</p>

<input type="text" name="Login" value="<?php echo @$data['

Login'];?>">

</p>

<p>

<p><strong style="color:white">Введите пароль:</strong>:</p>

<input type="password" name="Password" value="<?php echo @$data[

'Password'];?>">

</p>

<p><p>

<button style="color:green" type="submit" name="do\_aut">Войти</button>

</p></p>

<div style="color: green;">Вы зарегистрированы <br/><a href="/"HOME>На главную страницу</div><hr>

</form>

Signup\_adm.php-регистрация пользователя администратором

<head>

<?php

require "db.php";

?>

<style type="text/css" media="all">

<?php include "style/style.css" ?>

</style>

</head>

<body id = "">

</body>

<?php

require "db.php";

$data=$\_POST;

if(isset($data['do\_signup']))

{

$username = mysqli\_real\_escape\_string($dbc, trim($data['Login']));

$password1 = mysqli\_real\_escape\_string($dbc, trim($data['Password']));

$password2 = mysqli\_real\_escape\_string($dbc, trim($data['Password2']));

$errors=array();

if(trim($data['Login'])=='')

{

$errors[]='Введите логин';

}

if($data['Password']=='')

{

$errors[]='Введите пароль';

}

if ($data['Password2']!=$data['Password'])

{

$errors[]='Введите пароль еще раз' ;

}

if(!empty($username) && !empty($password1) && !empty($password2) && ($password1 == $password2))

{

$query = "SELECT \* FROM `signup` WHERE login = '$username'";

$data1 = mysqli\_query($dbc, $query);

if(mysqli\_num\_rows($data1) != 0)

{

$errors[]='Логин уже существует';

}

}

if(empty($errors))

{

$pwrd=crypt('$password2',rl);

$dbc->query("INSERT INTO signup(login, password,role) VALUES ('$username','$pwrd', 'user')");

//$dbc->query("INSERT INTO signup(login, password) VALUES ('$username','$password2')");

echo '<div style="color: green;">Новый пользователь зарегистрирован <br/> Назад <a href="auth.php"HOME>glavnaya</div><hr>';

}

else

{

echo '<div style="color: red;">'.array\_shift($errors).'</div><hr>';

}

}

?>

<form action="/signup.php" method="POST" >

<fieldset> <legend>Регистрация пользователя</legend>

<p>

<p><strong style="color:white">Введите логин:</strong>:</p>

<input type="text" name="Login" value="<?php echo @$data['

Login'];?>">

<p><strong style="color:white">Введите пароль:</strong>:</p>

<input type="password" name="Password" value="<?php echo @$data[

'Password'];?>">

<p><strong style="color:white">Введите пароль еще раз:</strong>:</p>

<input type="password" name="Password2">

<button style="color:green" type="submit" name="do\_signup">Зарегистрировать</button>

<button style="color:green" type="submit" name="do\_adm">Назад</button>

</p>

</fieldset>

</form>

Auth\_user.php – авторизация юзера

<head>

<?php

require "db.php";

?>

<style type="text/css" media="all">

<?php include "style/style.css" ?>

</style>

</head>

<body id = "telo2">

</body>

<?php

if(isset($\_COOKIE['login']))

{

echo '<div style="color: green;">Здравствуйте</div><hr>';

}

else

{

header('Location: /aut.php');

}

?>

<p><a href="exit.php">Выйти(<?php echo $\_COOKIE['login']; ?>)</a></p>

Auth\_admin-авторизация админа

<head

<?php

require "db.php";

?>

<style type="text/css" media="all">

<?php include "style/style.css" ?>

</style>

</head>

<body id = "telo2">

</body>

<?php

echo '<div style="color: green;">Здравствуйте</div><hr>';

echo $\_COOKIE['login'];

echo "<br/>";

if($\_COOKIE['role']=='admin')

{

if ($result = mysqli\_query($dbc,'SELECT id\_user, login, password, role FROM signup'))

{

$row\_cnt=$result->num\_rows;

printf("rows %d \n", $row\_cnt);

print("данные:\n <br>");

/\* Выборка результатов запроса \*/

echo '<table border="1" >';

echo '<thead>';

echo '<tr>';

echo '<th align="center">id\_user</th>';

echo '<th align="center">login</th>';

echo '<th align="center">password</th>';

echo '<th align="center">role</th>';

echo '<th align="center">Delete this user</th>';

echo '<th align="center" colspan="2">Изменить роль</th>';

echo '</tr>';

echo '</thead>';

echo '<tbody>';

// выводим в HTML-таблицу все данные клиентов из таблицы MySQL

while($row = mysqli\_fetch\_array($result))

{

echo '<tr>';

echo '<td align="center">' . $row['id\_user'] . '</td>';

echo '<td >' . $row['login'] . '</td>';

echo '<td >' . $row['password'] . '</td>';

echo '<td align="center">' . $row['role'] . '</td>';

echo "<td> <a name=\"delete\" href=\"auth.php?del=".$row["id\_user"]."\">Удалить</a></td>\n";

// echo '<td align="center">' .'<input type="text" name="text" >'. '</td>';

/\* echo '<td align="center">'

.'<select> method="GET" name="sel\_role" size="1"

<option selected value="null"></option>

<option value="admin">admin</option>

<option value="user">user</option>

</select> '. '</td>';\*/

echo "<td> <a name=\"rewrite\_role\" href=\"auth.php?rewrite=".$row["id\_user"]."\">admin</a></td>\n";

echo "<td> <a name=\"rewrite\_role2\" href=\"auth.php?rewrite2=".$row["id\_user"]."\">user</a></td>\n";

echo '</tr>';

//<input type="submit" name="delete" value="Ok">

//<input type="checkbox" name="check">

}

echo '</tbody>';

echo '</table>';

// $del=$\_GET['del'];

// $query="DELETE signup WHERE id\_user=$del";

}

}

else

{

header('Location: auth\_user.php');

}

if(isset($\_GET['del']))

{

$delete=(int) $\_GET['del'];

$query="DELETE FROM `signup` WHERE `id\_user`=$delete";

mysqli\_query($dbc, $query);

}

if(isset($\_GET['rewrite2']))

{

$rewrite\_role2=(int) $\_GET['rewrite2'];

$query="UPDATE `signup` SET `role`='admin' WHERE `id\_user`=$rewrite\_role2";

mysqli\_query($dbc, $query);

}

?>

<p><a href="exit.php">Выйти(<?php echo $\_COOKIE['login']; ?>)</a></p>

<p><a href="signup\_adm.php">Добавить пользователя(<?php echo $\_COOKIE['login']; ?>)</a></p>

Db.php – подключение БД

<?php

$dbc=mysqli\_connect('localhost','root','encrypt1719','lab1');

?>

Exit.php

<?php

require "db.php";

unset($\_COOKIE['id\_user']);

unset($\_COOKIE['login']);

unset($\_COOKIE['password']);

unset($\_COOKIE['role']);

setcookie('id\_user', '', -1, '/');

setcookie('login', '', -1, '/');

setcookie('password', '', -1, '/');

setcookie('role', '', -1, '/');

header('Location: /');

?>

# Результат работы системы

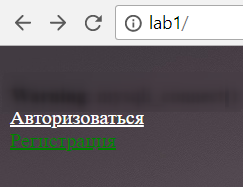


Рисунок 1 – Вход в систему

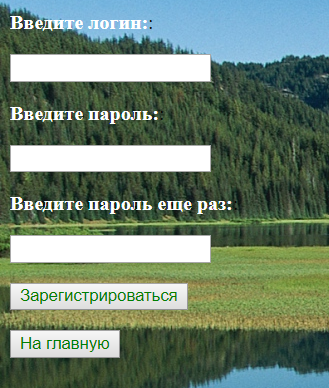


Рисунок 2 – Регистрация в системе

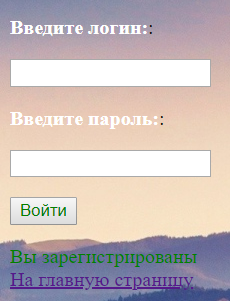


Рисунок 3 – Авторизация в системе

# Вывод

В ходе выполнения лабораторной работы была изучена и разработана система парольной авторизации для сайта с политикой безопасности. После авторизации администратор может редактировать БД, а обычные пользователи нет.