

## BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Kỳ báo cáo: Buổi 01 (Session 01)

Tên chủ đề: Lập trình và build trên môi trường docker (docker-compose)

GV: Nghi Hoàng Khoa

Ngày báo cáo: 15/03/2023

**Nhóm: 01**

### 1. THÔNG TIN CHUNG:

Lớp: NT213.N21.ATCL

STT	Họ và tên	MSSV	Email
1	Trần Quốc Đạt	20521179	20521179@gm.uit.edu.vn
2	Nguyễn Minh Huy	20520545	20520545@gm.uit.edu.vn
3	Hoàng Thanh Lâm	20521513	20521513@gm.uit.edu.vn

### 2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Viết một trang html đơn giản có một form điền thông tin username/password	100%	20520545 20521179 20521513
2	Viết code Javascript kiểm tra điều kiện của username/password được nhập	100%	20520545 20521179 20521513
3	Sử dụng PHP/MySQL để hoàn thiện bài tập tạo form đăng nhập/ đăng ký đơn giản	100%	20520545 20521179 20521513

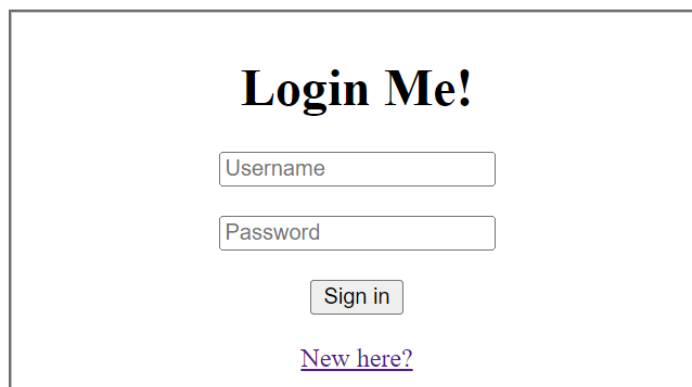
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

## BÁO CÁO CHI TIẾT

### 1. Viết một trang html đơn giản có một form điền thông tin username/password

- Tài nguyên:
- Mô tả/mục tiêu:
- Các bước thực hiện/ Phương pháp thực hiện (Ảnh chụp màn hình, có giải thích)

Giao diện form đăng nhập:



The screenshot shows a web form with a title "Login Me!". Below the title are two text input fields labeled "Username" and "Password". Under the "Password" field is a button labeled "Sign in". At the bottom of the form is a link labeled "New here?".

Code:

```
<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>Login me!</title>
    <link rel="stylesheet" href="style.css"></link>

  </head>
  <body>
    <form action="./login.php" method="POST">
      <fieldset>
        <h1>Login Me!</h1>
        <input class="username" type="text" name="txtUsername" placeholder="Username"/><br><br>
        <input class="password" type="password" name="txtPassword" placeholder="Password"><br><br>
        <input type="submit" id="btnSubmit" name="btn-submit" value="Sign in"><br><br>
        <a href='register.html'>New here?</a>
      </fieldset>
    </form>
  </body>
  <script src="login.js"></script>
</html>
```

Giao diện form đăng ký:

# Register Me!

  
  
  
[Already have account?](#)

Code:

```
<!DOCTYPE html>
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <title>Register me!</title>
    <link rel="stylesheet" href="style.css"></link>
  </head>
  <body>
    <h1></h1>
    <body>
      <form action="./register.php" method="POST">
        <fieldset>
          <h1>Register Me!</h1>
          <input class="username" type="text" name="txtUsername" placeholder="Username"/><br><br>
          <input class="password" type="password" name="txtPassword" placeholder="Password"><br><br>
          <input type="submit" id="btnSubmit" name="btn-submit" value="Sign up"><br><br>
          <a href='login.html'>Already have account?</a>
        </fieldset>
      </form>
    </body>
    <script src="register.js"></script>
  </body>
</html>
```

## 2. Viết code Javascript kiểm tra điều kiện của username/password được nhập

- Tài nguyên:
- Mô tả/mục tiêu:
- Các bước thực hiện/ Phương pháp thực hiện (Ảnh chụp màn hình, có giải thích)

- Khi nhập sai định dạng username và nhấn nút "Sign in":

**3. Sử dụng PHP/MySQL để hoàn thiện bài tập tạo form đăng nhập/ đăng ký đơn giản**

- Tài nguyên:
- Mô tả/mục tiêu:
- Các bước thực hiện/ Phương pháp thực hiện (Ảnh chụp màn hình, có giải thích)

**\*Mô tả hệ thống:**

Hệ thống dịch vụ web services sử dụng php, mysql thông qua phpmyadmin để đăng ký và đăng nhập người dùng, đồng thời xây dựng trên Docker để dễ dàng cài đặt.

- Các file cài đặt cho docker:

**Dockerfile:**

Cập nhật và cài đặt các package cần thiết cho web services.

```
FROM php:8.0-apache

# Set the working directory to /var/www/html
WORKDIR /var/www/html
COPY ./src /var/www/html/

# Install any necessary dependencies
RUN apt-get update -y && docker-php-ext-install pdo pdo_mysql mysqli
RUN apt-get install -y libmariadb-dev
RUN apt-get install -y nginx
RUN rm /etc/nginx/sites-enabled/default
RUN mkdir -p /etc/nginx/sites-enabled/
COPY ./nginx/* /etc/nginx/sites-enabled/

EXPOSE 80
```

**docker-compose.yaml** để lấy các image cần dùng cho web services là php, mysql, phpmyadmin(công cụ dùng để tạo GUI hỗ trợ cho người dùng).

Map các port của dịch vụ với các port của localhost. Khai báo image muốn pull về và các thông số và giá trị cho hệ thống.

```
version: '3.9'

services:
  php-env:
    build: .
    ports:
      - "9000:80"
    volumes:
      - ./src:/var/www/html
    depends_on:
      - mysql_db
  mysql_db:
    image: mysql:latest
    restart: always
    command: --default-authentication-plugin=mysql_native_password
    environment:
      MYSQL_DATABASE: users
      MYSQL_ROOT_PASSWORD: root
    volumes:
      - ./src/init.sql:/docker-entrypoint-initdb.d/dump.sql
    ports:
      - "9906:3306"
  phpmyadmin:
    image: phpmyadmin:latest
    restart: always
    ports:
      - "9001:80"
    environment:
      - PMA_ARBITRARY=1
```

**cmd.sh:**

Lệnh chạy để pull các image trong docker-compose và điều chỉnh DNS resolver do trong quá trình cài đặt package trong Dockerfile bị lỗi phân giải tên miền mặc dù trình duyệt có thể truy cập được tên miền đó.

```
$ cmd.sh
1  # Fixing Temporary Failure resolving at deb.debian.org:
2
3  # Update docker json daemon DNS resolver by : `{
4  #   "dns": ["8.8.8.8", "8.8.4.4"]
5  # }`
6
7  ifconfig /flushdns
8
9  docker-compose up --build
10
11
```

ifconfig /flushdns hoặc ipconfig /flushdns dùng để xóa cache dns.

Kiểm tra thông tin bằng js:

```
var username = document.querySelector(".username");
var password = document.querySelector(".password");
var form = document.querySelector("form");
form.addEventListener("submit", function(e) {
    e.preventDefault();
    var check = false;
    // check username/password is null
    if (username.value == '')
    {
        alert("Missing username!");
    } else if (password.value == '')
    {
        alert("Missing password!");
    }
    else if (!check)
    {
        // check username
        const username_regex = /^[a-zA-Z0-9._-]+$/;
        if (!username_regex.test(username.value))
        {
            alert("Username must not contain special characters beside - and _!. Never");
        }
        else
        {
            // send form data to server
            var xhr = new XMLHttpRequest();
            xhr.open("POST", "login.php");
            xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
            xhr.onreadystatechange = function() {
                if (xhr.readyState == XMLHttpRequest.DONE)
                {
                    if (xhr.status == 200) {
                        // Load the HTML response in the current page
                        document.documentElement.innerHTML = xhr.responseText;
                    }
                    else {
                        // Handle error response
                        alert("Request failed. Returned status of " + xhr.status);
                    }
                }
            };
            xhr.send("txtUsername=" + username.value + "&txtPassword=" + password.value);
        }
    }
});
```

Đoạn code lấy thông tin từ form trên, sử dụng event handler để bắt submit và thêm các điều kiện kiểm tra giá trị của form. Sau đó dùng XMLHttpRequest() để gửi data cho file \*.php xử lý bên server. Thông báo sử dụng alert() để hiển thị sai sót cho người dùng.



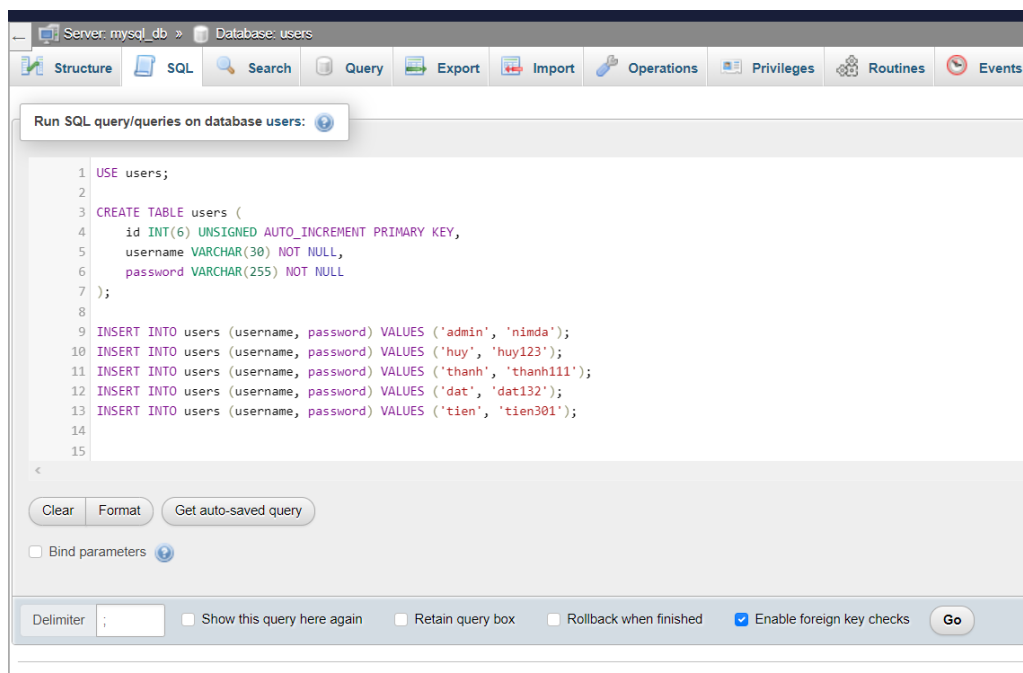


## Login Me!

[New here?](#)

Hiện thị thông báo khi người dùng nhập sai.

**\*Khởi tạo databases ban đầu (init.sql) sử dụng phpmyadmin:**



Sau khi khởi tạo thông tin, ta sẽ có những người dùng mặc định:

Showing rows 0 - 4 (5 total, Query took 0.0006 seconds.)

```
SELECT * FROM `users`
```

☐ Profiling [ Edit ]

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

Extra options

					id	username	password
<input type="checkbox"/>	Edit	Copy	Delete		1	admin	nimda
<input type="checkbox"/>	Edit	Copy	Delete		2	huy	huy123
<input type="checkbox"/>	Edit	Copy	Delete		3	thanh	thanh111
<input type="checkbox"/>	Edit	Copy	Delete		4	dat	dat132
<input type="checkbox"/>	Edit	Copy	Delete		5	tien	tien301

☐ Check all | With selected: Edit Copy Delete Export

### \* Trang đăng ký:

Khi điền thông tin đăng ký và nhấn nút “Sign up” thì hiện thông tin sau trên trình duyệt:

## Register Me!

  
  
  
[Already have account?](#)

Nếu chưa tồn tại người dùng:

## Registered successfully!

Nếu đã tồn tại người dùng:

## User already exists!

Code giải thích:

register.php

```
<?php
$host = 'mysql_db';
$username = 'root';
$password = 'root';
$dbname = 'users';
if(isset($_COOKIE['user']))
{
    echo("<meta http-equiv='Refresh' content='2; url=index.php'>");
}
try
{
    $conn = mysqli_connect($host, $username, $password, $dbname);
    if ($conn->connect_error)
    {
        die("Connection failed: ". $conn->connect_error);
    }
}
catch (Exception $e)
{
    echo($e->getMessage());
}
if($_SERVER['REQUEST_METHOD']=="POST")
{
    //receive data from file register.html
    $username = $_POST['txtUsername'];
    $password = $_POST['txtPassword'];
}
else
{
    die("<h1>Wrong method!</h1>");
}
try
{
    $query = "SELECT * FROM users WHERE username = '$username'";
    $result = mysqli_query($conn, $query);
    if (mysqli_num_rows($result) > 0)
    {
        echo "<h1>User already exists!</h1>";
        die();
    }
    $query = "INSERT INTO users (username, password) VALUES ('$username', '$password')";
    if ($conn->query($query)===TRUE)
    {
        echo "<h1>Registered successfully!</h1>";
        sleep(3);
        echo("<meta http-equiv='Refresh' content='2; url=login.html'>");
    }
}
catch(Exception $e)
```

Trước khi kết nối với CSDL, code sẽ kiểm tra bằng isset() để xem người dùng có đang đăng nhập hay không. Sau đó, lấy tham số từ phương thức POST và truy vấn SELECT để kiểm tra xem có người dùng này tồn tại trong CSDL không. Sau đó mới thực hiện INSERT để ghi người dùng mới này vào CSDL. Sau khi đăng kí, trang sẽ điều hướng sang login page để đăng nhập.

### Luồng xử lý kết quả:

Tại trang chủ, nếu chưa đăng nhập sẽ hiển thị kết quả:

**You are not login yet. Redirecting to login page.**

[Log Out](#)

Sau khi người dùng đã đăng nhập:

**Welcome, admin**

[Log Out](#)

Giải thích code:

- Code sử dụng isset() và cookie để quản lí phiên đăng nhập của người dùng. Nút Log Out gọi hàm xóa cookie và load lại page để xác định phiên đăng nhập. sleep để làm chậm lại chữ để người dùng dễ theo dõi thông báo. Nếu không có phiên đăng nhập hiện tại, file sẽ redirect sang trang đăng nhập.

index.php

```
<!DOCTYPE html>
<html Lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Index</title>
</head>
<body>
  <?php
  if(!isset($_COOKIE["user"]))
  {
    echo("<h1>You are not login yet. Redirecting to login page.</h1>");
    sleep(3);
    echo("<meta http-equiv='Refresh' content='2; url=login.html'>");
    //exit(header("Location: login.html"));
  }
  else
  {
    echo("<h1>Welcome, ".$_COOKIE['user']."</h1>");
    echo("<a href='\"javascript:void(0);\" onclick='\"deleteAllCookies();\"' >Log Out</a>");

  }
  ?>

</body>
<script>
function deleteAllCookies()
{
  const cookies = document.cookie.split(";");

  for (let i = 0; i < cookies.length; i++) {
    const cookie = cookies[i];
    const eqPos = cookie.indexOf("=");
    const name = eqPos > -1 ? cookie.substr(0, eqPos) : cookie;
    document.cookie = name + "=;expires=Thu, 01 Jan 1970 00:00:00 GMT";
  }
  window.location.href= "index.php";
}
</script>
</html>
```

Tại trang đăng nhập:

Khi nhập username không tồn tại, nhập sai password hoặc username:

**Username or password is not correct, please enter again!**

Khi nhập đúng username và password:

# Login successfully!

Và trang sẽ redirect sang trang chủ với tên người dùng đã đăng nhập

Giải thích:

Code sẽ kết nối với database, kiểm tra người dùng đã đăng nhập chưa. Nếu đã đăng nhập, sẽ điều hướng sang trang chủ. Nếu chưa sẽ lấy các tham số thông qua phương thức POST để thực hiện truy vấn đăng nhập. Nếu người dùng nhập không đúng thông tin so với database, kết quả trả về từ chối đăng nhập. Nếu nhập đúng thông tin, trang sẽ ghi cookie, hiện thông báo và điều hướng sang trang chủ.

```
<?php
$host = 'mysql_db'; //server name
$username = 'root';
$password = 'root';
$dbname = 'users'; //database name
$conn = mysqli_connect($host, $username, $password, $dbname);
if(isset($_COOKIE['user']))
{
    echo("<meta http-equiv='Refresh' content='2; url=index.php'>");
}
if($_SERVER['REQUEST_METHOD']=='POST')
{
    //receive data from file register.html
    $username = $_POST['txtUsername'];
    $password = $_POST['txtPassword'];
    // Compare input vs database
    $query = "SELECT * FROM users WHERE username='$username' AND password='$password'";
    $result = mysqli_query($conn,$query);
    // Inform login success or failed
    if (mysqli_num_rows($result) >= 1)
    {
        {
            setcookie("user",$username,0,"/");
            echo("<h1>Login successfully!</h1>");
            sleep(3);
            echo("<meta http-equiv='Refresh' content='2; url=index.php'>");
        }
    }
    else
    {
        echo("<h1>Username or password is not correct, please enter again!</h1>");
        sleep(3);
        echo("<meta http-equiv='Refresh' content='2; url=index.php'>");
    }

    // //echo '<br><a href='.'index.html?name='.'>Back to Login page</a>';

    $conn->close();
}
else
die();
?>
```



---HẾT