Bộ môn An toàn Thông tin – Khoa MMT&TT
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO THỰC HÀNH

Bảo mật web và ứng dụng - NT213.M21.ANTN

Lab 1: Ôn tập kiến thức cơ bản ứng dụng web
(html, javascript, php, csdl)

GVHD: Đỗ Hoàng Hiển

Nhóm thực hiện: 08

Ngày báo cáo: 17/03/2022

STT	Tên	MSSV
1	Nguyễn Mỹ Quỳnh	19520241
2	Trần Huỳnh Quốc Đạt	19520459

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

BÁO CÁO CHI TIẾT

A. TỔNG QUAN

B. CHUẨN BỊ MÔI TRƯỜNG

C. THỰC HÀNH

C.1 HTML và JavaScript:

> **Yêu cầu 1.1** Điều chỉnh tập tin mã nguồn **SimpleForm.html** để thỏa mãn các yêu cầu:

- Bắt buộc phải nhập **04** trường ***Họ và tên, Mã số sinh viên, Email*** và ***Số điện thoại*** trước khi lưu.
- Trường ***Email*** cần kiểm tra người dùng có nhập đúng định dạng email không.
- ***Số điện thoại*** và ***Mã số sinh viên*** có độ dài tối đa 15 ký tự.

Trả lời:

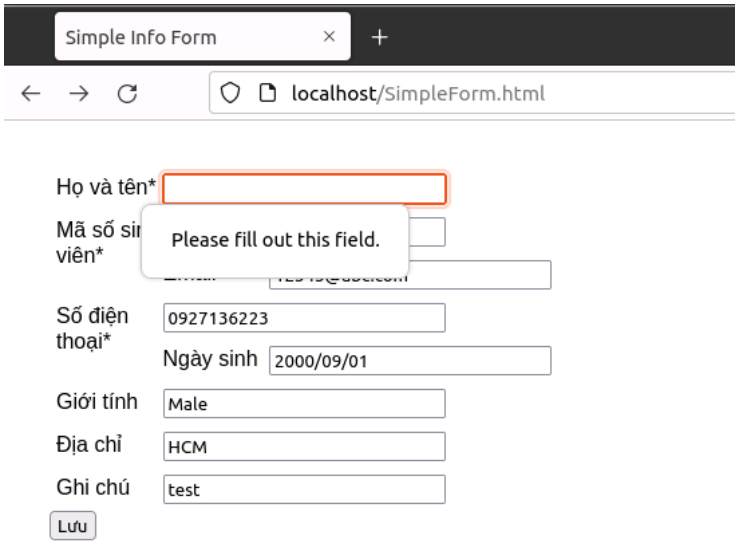
```
d="simple-form" action="./submit_form.php" method="POST">
 <div class="info">
        <div class="label">Họ và tên*</div>
        <input type="text" id="name" name="name" required></input><br>
 </div>
 <div class="info">
        <div class="label">Mã số sinh viên*</div>
        <input type="text" name="student_id" pattern=".{1,15}" required></input><br>
 </div>
 <div class="info">
        <div class="label">Email*</div>
        <input type="email" name="email" pattern="[a-z0-9._%+-]+@[a-z0-9.-]+\.[a-z]{2,}$" required></inp
 </div>
 <div class="info">
        <div class="label">Số điện thoại*</div>
        <input type="text" name="phone" pattern=".{1,15}" required></input><br>
```

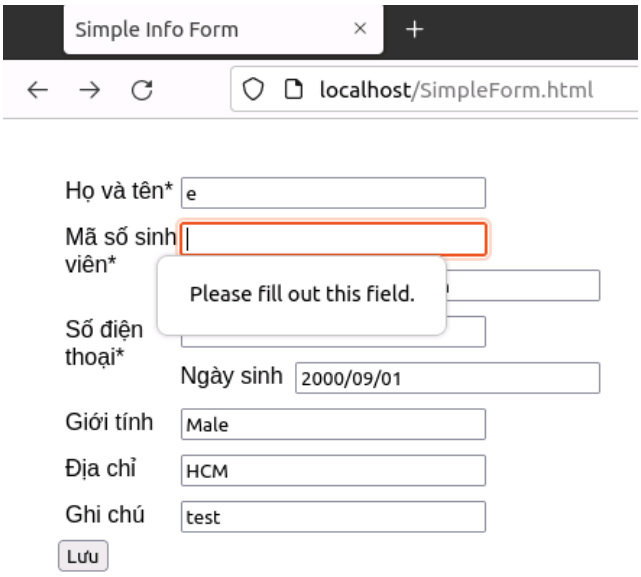
- Để bắt buộc phải nhập **04** trường ***Họ và tên, Mã số sinh viên, Email*** và ***Số điện thoại*** trước khi lưu, ta thêm thuộc tính **required** vào thẻ input 4 trường đó.

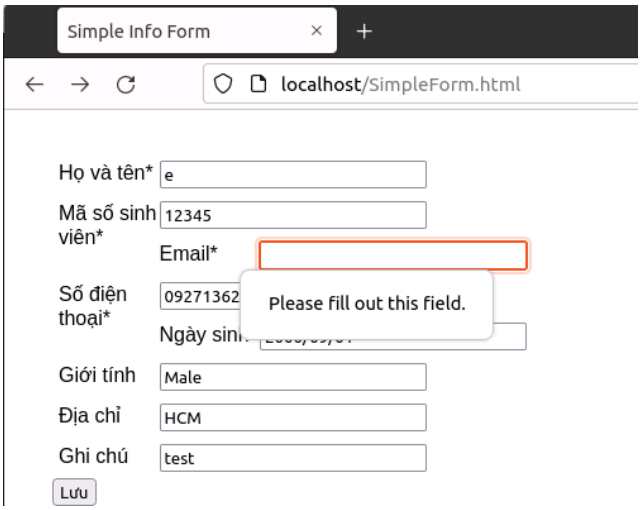
- Trường ***Email*** cần kiểm tra người dùng có nhập đúng định dạng email không:
  - ✓ Đổi type từ "text" thành **"email"**.
  - ✓ Đồng thời dùng thuộc tính pattern để chỉ định nhập đúng format dạng email(characters1@characters2.domain): pattern="[a-z0-9._%+-]+@[a-z0-9.-]+\.[a-z]{2,}$" : Characters1 có thể là một trong các kí tự thuộc [a-z0-9._%+-], tiếp đến là dấu "@", character2 Characters1 có thể là một trong các kí tự thuộc [a-z0-9.-], tiếp đến là dấu ".", domain có thể là một trong các kí tự thuộc [a-z] và có từ 2 kí tự trở lên.

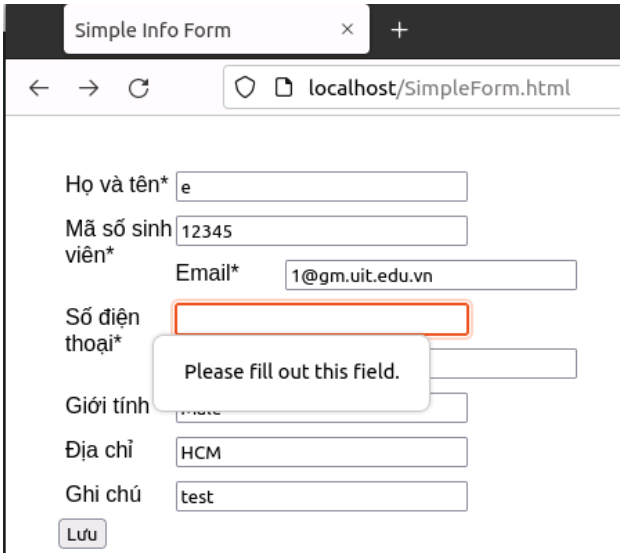
- ***Số điện thoại*** và ***Mã số sinh viên*** có độ dài tối đa 15 ký tự: dùng thuộc tính pattern=".{1,15}" cho thẻ input 2 trường đó, **pattern=".{1,15}"** mang ý nghĩa chỉ đinh nhập 1 đến 15 kí tự bất kì (match chuỗi bất kì từ 1 đến 15 kí tự, tối đa 15).

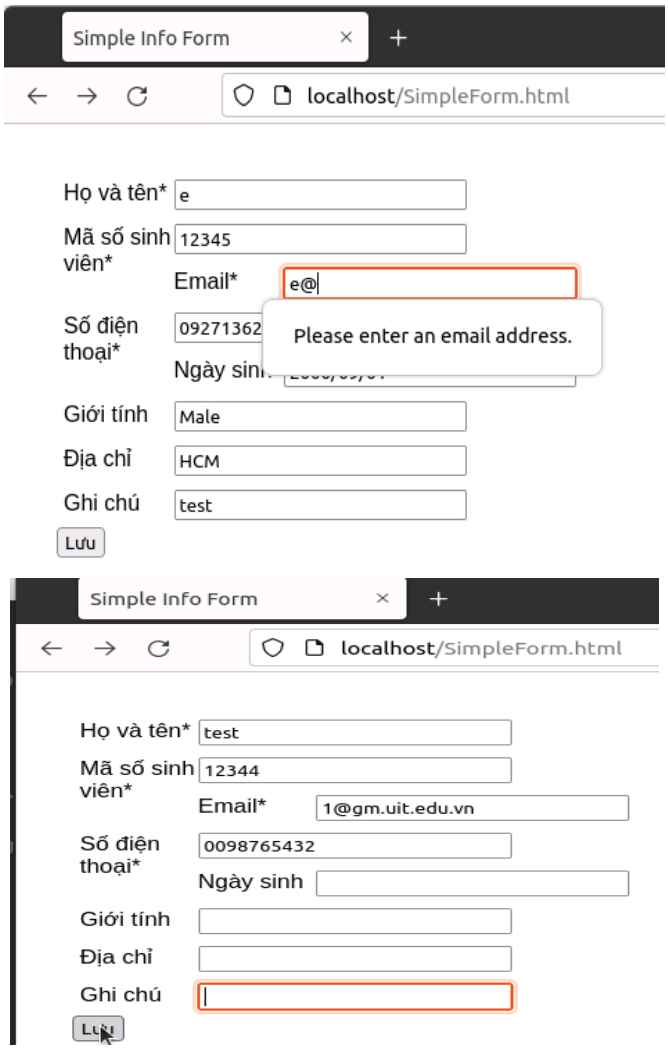
Kiểm tra:

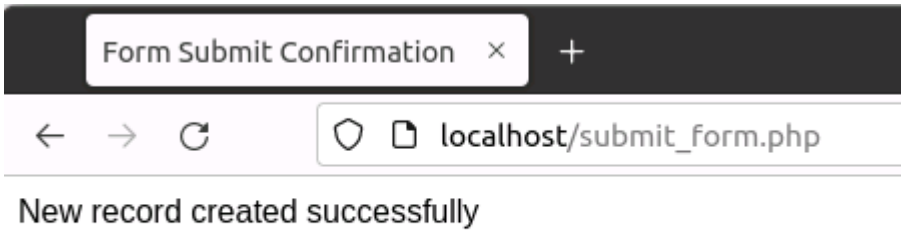



Simple Info Form
localhost/SimpleForm.html
Họ và tên* e
Mã số sinh viên*
Please fill out this field.
Số điện thoại*
Ngày sinh 2000/09/01
Giới tính Male
Địa chỉ HCM
Ghi chú test
Lưu


Simple Info Form
localhost/SimpleForm.html
Họ và tên* e
Mã số sinh viên* 12345
Email*
Số điện thoại* 09271362
Please fill out this field.
Giới tính Male
Địa chỉ HCM
Ghi chú test
Lưu


Simple Info Form
localhost/SimpleForm.html
Họ và tên* e
Mã số sinh viên* 12345
Email* 1@gm.uit.edu.vn
Số điện thoại*
Please fill out this field.
Giới tính
Địa chỉ HCM
Ghi chú test
Lưu





Yêu cầu 1.2 Viết mã nguồn **Javascript** (có thể ở trong hoặc ngoài tập tin HTML) thực hiện kiểm tra trường ***Họ và tên*** chỉ cho nhập chữ và khoảng trắng.

Trả lời:

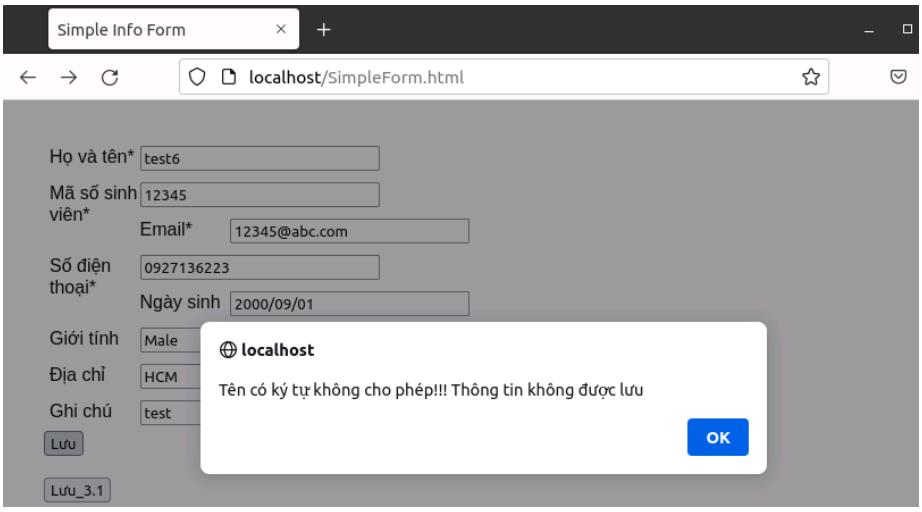
Nhóm thực hiện viết mã nguồn Javascript trong tập tin HTML bên trong cặp thẻ <script></script>, viết function kiểm tra lúc nhấn submit form:

- Tiến hành lấy element Họ và tên của form thông qua name property của nó(câu lệnh dòng 173) và gán vào biến Name.
- Từ dòng 177 đến dòng 199 tiến hành duyệt qua từng kí tự chuỗi Name, nếu không là chữ hoặc khoảng trắng return false; ngay lập tức

  Sau khi đã kiểm tra toàn chuỗi thỏa chỉ toàn nhập chữ và khoảng trắng thì return true;

```
169     form.onsubmit = function(){
170         // Do something to verify inputs
171         // To get an element, use its name property, for example student_id field:
172         form.elements["student_id"].value;
173         var Name = form.elements["name"].value;
174         //var Dob = form.elements["dob"].value;
175         //alert(Dob);
176         // alert(Name.length);
177         len = Name.length;
178         for (let i=0; i<len; i++)
179         {
180             if(Name[i] != ' ')
181             {
182                 if(Name[i] < 'A')
183                 {
184                     alert("Tên có ký tự không cho phép!!! Thông tin không được lưu");
185                     return false;
186                 }
187                 else if(Name[i] > 'Z' && Name[i] < 'a')
188                 {
189                     alert("Tên có ký tự không cho phép!!! Thông tin không được lưu");
190                     return false;
191                 }
192                 else if(Name[i] > 'z')
193                 {
194                     alert("Tên có ký tự không cho phép!!! Thông tin không được lưu");
195                     return false;
196                 }
197             }
198         }
199         return true;
```

- Kiểm tra:



C.2 Xử lý yêu cầu với PHP và Cơ sở dữ liệu

Yêu cầu 2.1 Tạo một bảng trong cơ sở dữ liệu MySQL với các trường tương ứng ở **Yêu cầu 1.1** thỏa mãn các yêu cầu sau.

- Cơ sở dữ liệu có thể lưu chữ dạng **UTF-8**.
- Các trường tương ứng ở **Yêu cầu 1.1** với ***Họ và tên***, ***MSSV***, ***Số điện thoại*** và ***Email*** không được bỏ trống. ***Số điện thoại*** và ***MSSV*** có độ dài tối đa 15 ký tự.

Trả lời:

- Kiểm tra các database trước khi tạo dung lệnh ***show DATABASE;***

```
mysql> show DATABASE
    -> show DATABASE;
ERROR 1064 (42000): You have an error in your SQL syntax; ch
syntax to use near 'DATABASE
show DATABASE' at line 1
mysql> SHOW DATABASE;
ERROR 1064 (42000): You have an error in your SQL syntax; ch
syntax to use near 'DATABASE' at line 1
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.16 sec)
```

- Tiến hành tạo database mới tên ***mydatabase*** lưu chữ dạng UTF-8 dùng câu lệnh cú pháp:

  CREATE DATABASE <tên_database> CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

```
mysql> CREATE DATABASE mydatabase CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0.02 sec)

mysql> show DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mydatabase         |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)

mysql> USE mydatabase;
Database changed
```

- Kiểm tra thấy database đã tạo thành công:

```
mysql> show DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mydatabase         |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

- Dùng lệnh **USE <tên_database>;** để sử dụng database vừa tạo:

```
mysql> USE mydatabase;
Database changed
```

- Tiến hành tạo bảng thỏa mãn yêu cầu 1.1 tên **student** và ***Họ và tên***, ***MSSV***, ***Số điện thoại*** và ***Email*** không được bỏ trống. ***Số điện thoại*** và ***MSSV*** có độ dài tối đa 15 ký tự theo cú pháp sau:

```
mysql> CREATE TABLE student(
    -> HOVATEN VARCHAR(50) NOT NULL,
    -> MSSV VARCHAR(15) NOT NULL,
    -> SDT VARCHAR(15) NOT NULL,
    -> EMAIL VARCHAR(50) NOT NULL,
    -> NGAYSINH DATE,
    -> GIOITINH VARCHAR(5),
    -> DIACHI VARCHAR(50),
    -> GHICHU VARCHAR(100));
Query OK, 0 rows affected (0.04 sec)
```

- Kiểm tra bảng vừa tạo dùng lệnh **DESCRIBE <tên_bảng>;**

```
mysql> DESCRIBE student;
+----------+--------------+------+-----+---------+-------+
| Field    | Type         | Null | Key | Default | Extra |
+----------+--------------+------+-----+---------+-------+
| HOVATEN  | varchar(50)  | NO   |     | NULL    |       |
| MSSV     | varchar(15)  | NO   |     | NULL    |       |
| SDT      | varchar(15)  | NO   |     | NULL    |       |
| EMAIL    | varchar(50)  | NO   |     | NULL    |       |
| NGAYSINH | date         | YES  |     | NULL    |       |
| GIOITINH | varchar(5)   | YES  |     | NULL    |       |
| DIACHI   | varchar(50)  | YES  |     | NULL    |       |
| GHICHU   | varchar(100) | YES  |     | NULL    |       |
+----------+--------------+------+-----+---------+-------+
8 rows in set (0.00 sec)

mysql>
```

Yêu cầu 2.2 **Thực hiện:**

1. Điều chỉnh mã nguồn trong tập tin **submit_form.php** để nhận các giá trị được submit và lưu vào CSDL dùng MySQL.
2. Điền và submit thử một form để kiểm tra hoạt động của mã nguồn đã điều chỉnh.

Trả lời:

1. **Điều chỉnh mã nguồn trong tập tin submit_form.php để nhận các giá trị được submit và lưu vào CSDL dùng MySQL:**

- Tạo một user mới với username là "nhom" và password là "password" sử dụng câu lệnh sau:

```
mysql> create user 'nhom'@'localhost' identified by 'password';
Query OK, 0 rows affected (0.02 sec)
```

- Thiết lập tất cả quyền cho user:

```
mysql> grant all on dbname.* to nhom@localhost;
Query OK, 0 rows affected (0.01 sec)
```

- Điều chỉnh Thông tin kết nối CSDL đúng với MySQL đã xây dựng:

var > www > html > submit_form.php

```php
<?php
    session_start();
    //Change these configs according to your MySQL server
    $servername = "localhost";
    $username = "nhom";
    $password = "password";
    $database = "mydatabase";
    $table = "student";
```

- Lấy các trường của form và gán vào các biến tương ứng:

```php
    // Create connection
    $conn = mysqli_connect($servername, $username, $password, $database);
    //$_SESSION['msg'] = "abc";
        // Check connection
        if ($conn->connect_error) {
            $_SESSION['msg'] = "Connection failed";
            //die("Connection failed: " . $conn->connect_error);
        }
        else{
            $_SESSION['msg'] = "Connected";
            // 2 ways to get fields in form, the later is more secure
            $name = $_POST['name'];
            $student_id = $_POST['student_id'];
            $email = $_POST['email'];
            $phone = $_POST['phone'];
            $dob = $_POST['dob'];
            $gender = $_POST['gender'];
            $address = $_POST['address'];
            $note = $_POST['note'];
            $_SESSION['dob'] = $dob;
            // $name = mysqli_real_escape_string($conn, $_POST['name']);
```

- Tạo SQL Command để nhận các giá trị được submit và lưu vào CSDL

```php
        //Create SQL command to insert data to database
        if (ord($dob) === 0)
            $sql_command = "INSERT INTO student (HOVATEN, MSSV, SDT, EMAIL, NGAYSINH, GIOITINH, DIACHI, GHICHU)
            VALUES ('$name', '$student_id', '$phone', '$email', NULL, '$gender', '$address', '$note')";
        else
            $sql_command = "INSERT INTO student (HOVATEN, MSSV, SDT, EMAIL, NGAYSINH, GIOITINH, DIACHI, GHICHU)
            VALUES ('$name', '$student_id', '$phone', '$email', '$dob', '$gender', '$address', '$note')";

        if ($conn->query($sql_command) === TRUE)
            $_SESSION['msg'] = "New record created successfully";
        else
            $_SESSION['msg'] = $conn->error;
            //$_SESSION['msg'] .= ord($dob);
            //$_SESSION['msg'] .= "a";
        mysqli_close($conn);
    }
//mysqli_close($conn);
?>
```

2. Điền và submit thử một form để kiểm tra hoạt động của mã nguồn đã điều chỉnh:

- Truy cập vào mysql với user vừa tạo phía trên:

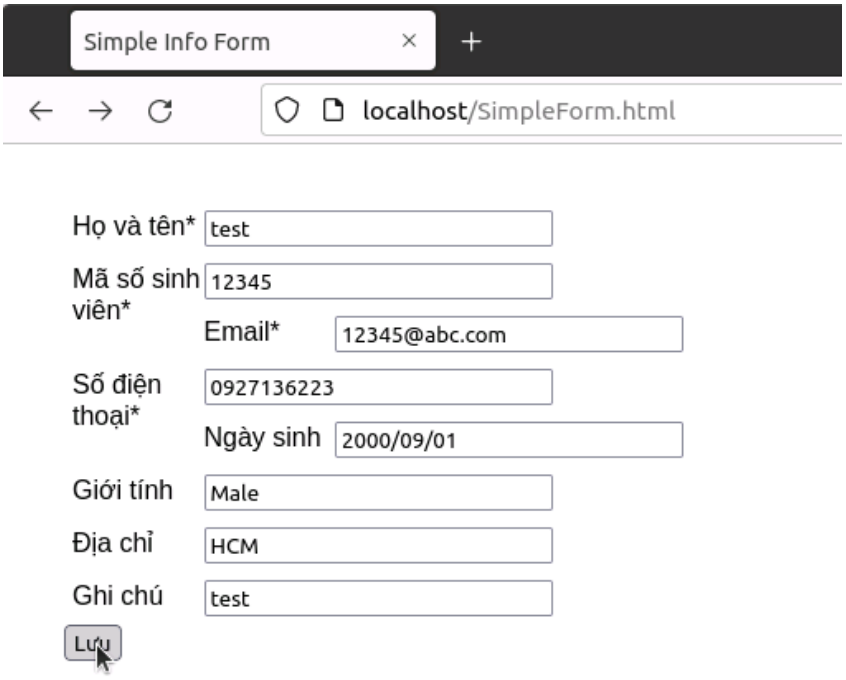
```
ubuntu@s-24c4056819214a80956a79d25fe7abde8-server:~$ mysql -u nhom -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 50
Server version: 8.0.28-0ubuntu0.20.04.3 (Ubuntu)
```

- Kiểm tra các giá trị của bảng student:

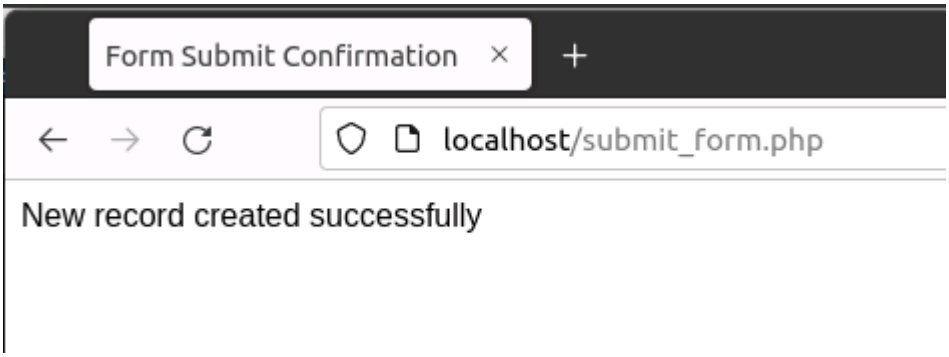
```
mysql> select * from student;
+---------------+------+-----------+----------------+-----------+----------+--------+--------+
| HOVATEN       | MSSV | SDT       | EMAIL          | NGAYSINH  | GIOITINH | DIACHI | GHICHU |
+---------------+------+-----------+----------------+-----------+----------+--------+--------+
| abc           | abc  | 123       | 1@gm.com       | 2000-01-01 | abc      | abc    | abc    |
| abc           | abc  | 123       | 1@gm.com       | 2000-01-01 | abc      | abc    | abc    |
| abc           | abc  | 123       | 1@gm.com       | 2000-01-01 | abc      | abc    | abc    |
+---------------+------+-----------+----------------+-----------+----------+--------+--------+
96 rows in set (0.14 sec)

mysql>
```

- Điền và submit thử một form:



- Nhận được thông báo thành công:



- Kiểm tra thấy dữ liệu đã có trong bảng:

```
| abc            | abc   | 123        | 1@gm.com        | 2000-01-01 | abc     | abc    | abc    |
| abc            | abc   | 123        | 1@gm.com        | 2000-01-01 | abc     | abc    | abc    |
| abc            | abc   | 123        | 1@gm.com        | 2000-01-01 | abc     | abc    | abc    |
| test           | 12345 | 0927136223 | 12345@abc.com   | 2000-09-01 | Male    | HCM    | test   |
+----------------+-------+------------+-----------------+------------+---------+--------+--------+
97 rows in set (0.01 sec)

mysql>
```

C.3 Tuỳ chỉnh kết hợp giữa form và cơ sở dữ liệu

> **Yêu cầu 3.1** Điều chỉnh form và viết mã nguồn Ajax để gửi thông tin form lưu vào CSDL qua Ajax và hiển thị thông báo thành công/thất bại cho người dùng

Trả lời:

- Bắt sự kiện onclick của nút để gọi hàm Send() và xử lý JavaScript với Ajax để gửi form đến URL của submit_form.php.

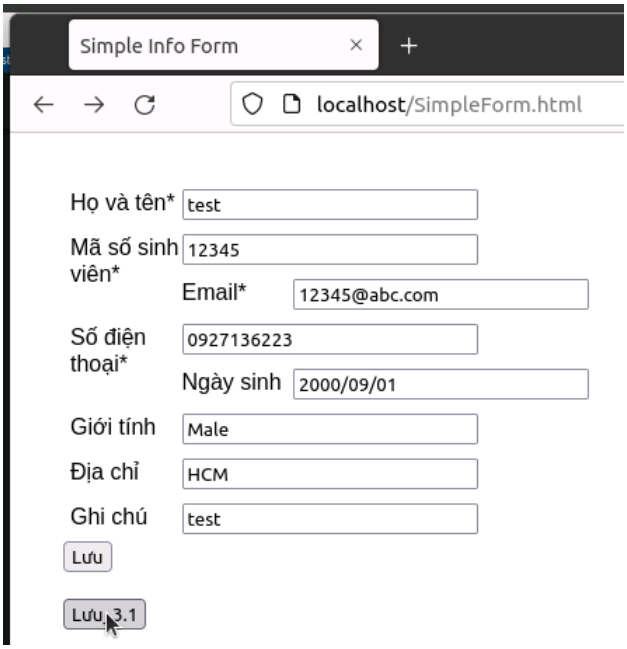
```
67          <input type="button" name="submit1" onclick="Send()" value="Lưu_3.1"></input>
68          <br>
```

- Chi tiết giải thích các câu lệnh có trong hình bên dưới:

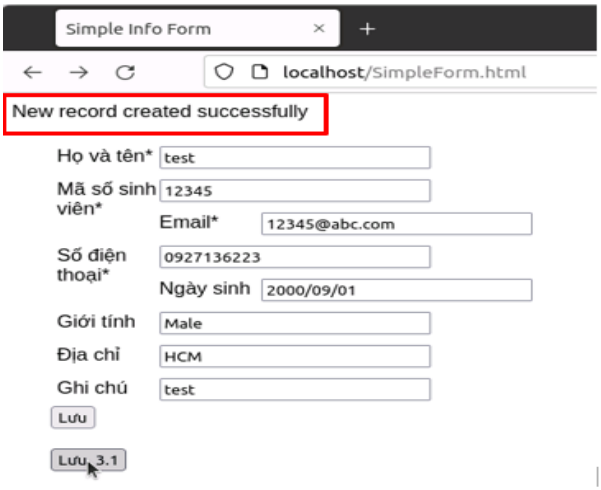
```
142     function Send() {
143     // Tạo đối tượng XMLHttpRequest
144     var request = new XMLHttpRequest();
145
146     // Khởi tạo đối tượng yêu cầu
147     request.open("POST", "submit_form.php");
148
149     request.onreadystatechange = function() {
150         // Kiểm tra xem yêu cầu đã hoàn thành và thành công chưa
151         if(this.readyState === 4 && this.status === 200) {
152             // Chèn phản hồi từ máy chủ vào một phần tử HTML
153             //document.getElementById("simple-form").visibility = "hidden";
154             document.getElementById("result").innerHTML = this.responseText;
155
156         }
157     };
```

```
158
159
160     // Truy xuất dữ liệu biểu mẫu
161     var myForm = document.getElementById("simple-form");
162     var formData = new FormData(myForm);
163
164     // Gửi yêu cầu đến máy chủ
165     request.send(formData);
166 }
```

- Điền và submit thử một form:



- Hiển thị thông báo thành công cho người dùng:



Yêu cầu 3.2 Viết một tập tin tương tự khác, trong đó khi mở lên thì tự động gửi một form với các trường tham số như **Yêu cầu 1.1** đến **submit_form.php**

Trả lời:

- Sử dụng hàm Send() tương tự câu 3.1 nhưng lần này sẽ dùng sự kiện onload của body để submit form tự động như hình sau:

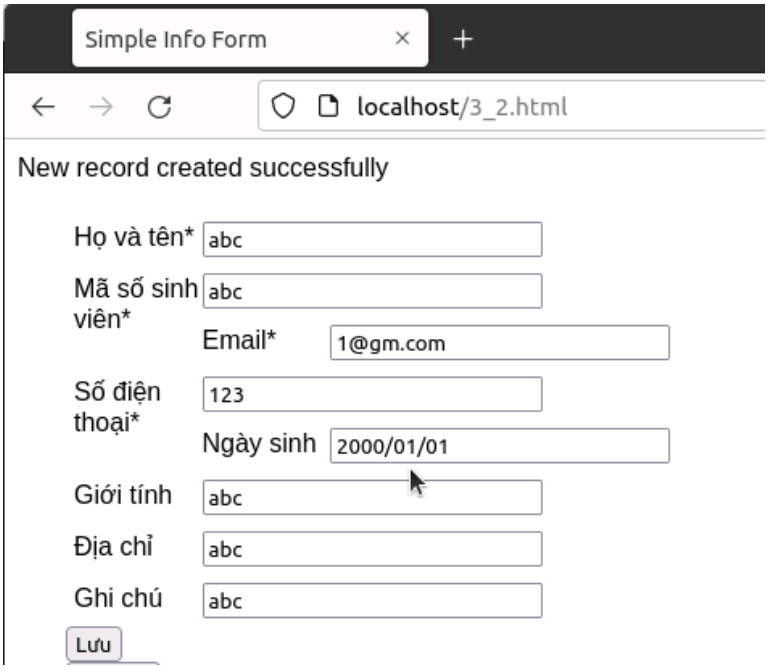
```
26  <body onload="Send()">
27      <div id="result">
28      <p></p>
29      </div>
30      <br>
31      <form id="simple-form" action="./submit_form.php" method="POST">
32          <div class="info">
33              <div class="label">Họ và tên*</div>
34              <input type="text" id="name" name="name" required value="abc"></
35          </div>
36          <div class="info">
37              <div class="label">Mã số sinh viên*</div>
38              <input type="text" name="student_id" pattern=".{1,15}" required
39          </div>
40          <div class="info">
41              <div class="label">Email*</div>
42              <input type="text" name="email" pattern="[a-z0-9._%+-]+@[a-z0-9
43          </div>
44          <div class="info">
45              <div class="label">Số điện thoại*</div>
46              <input type="text" name="phone" pattern=".{1,15}" required valu
47          </div>
48          <div class="info">
49              <div class="label">Ngày sinh</div>
50              <input type="text" name="dob" value="2000/01/01"></input><br>
```

- Chi tiết giải thích các câu lệnh có trong hình bên dưới:

```
142     function Send() {
143     // Tạo đối tượng XMLHttpRequest
144     var request = new XMLHttpRequest();
145
146     // Khởi tạo đối tượng yêu cầu
147     request.open("POST", "submit_form.php");
148
149     request.onreadystatechange = function() {
150         // Kiểm tra xem yêu cầu đã hoàn thành và thành công chưa
151         if(this.readyState === 4 && this.status === 200) {
152             // Chèn phản hồi từ máy chủ vào một phần tử HTML
153             //document.getElementById("simple-form").visibility = "hidden";
154             document.getElementById("result").innerHTML = this.responseText;
155
156         }
157     };
```

```
158
159
160     // Truy xuất dữ liệu biểu mẫu
161     var myForm = document.getElementById("simple-form");
162     var formData = new FormData(myForm);
163
164     // Gửi yêu cầu đến máy chủ
165     request.send(formData);
166 }
```

- Kiểm tra form tự submit khi mở lên:



C.4 Vọc một chút

> **Yêu cầu 4.1** Phân tích file **login.php,** sinh viên thực hiện các yêu cầu bên dưới.

4.1a. Tạo một bảng chứa thông tin người dùng đơn giản trong MySQL, với các trường phù hợp dựa trên phân tích file **login.php**.

Trả lời:

```
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
        // Check connection
        if ($conn->connect_error) {
                $_SESSION['msg'] = "Connection failed";
            //die("Connection failed: " . $conn->connect_error);
        }
        else{
                $username = $_POST['username'];
                $password = $_POST['password'];
                //print $username;
                $sql_command = "SELECT * FROM ".$table." WHERE username='".$username."' and password='".$password."'"

                $result = mysqli_query($conn, $sql_command);
                if (mysqli_num_rows($result) > 0)
                {
                        //print "inside";
                        $row = mysqli_fetch_assoc($result);
                        $_SESSION['name'] = $row['username'];//$result[0]['username'];
                }
                else
                {
                        $_SESSION['name'] = null;
```

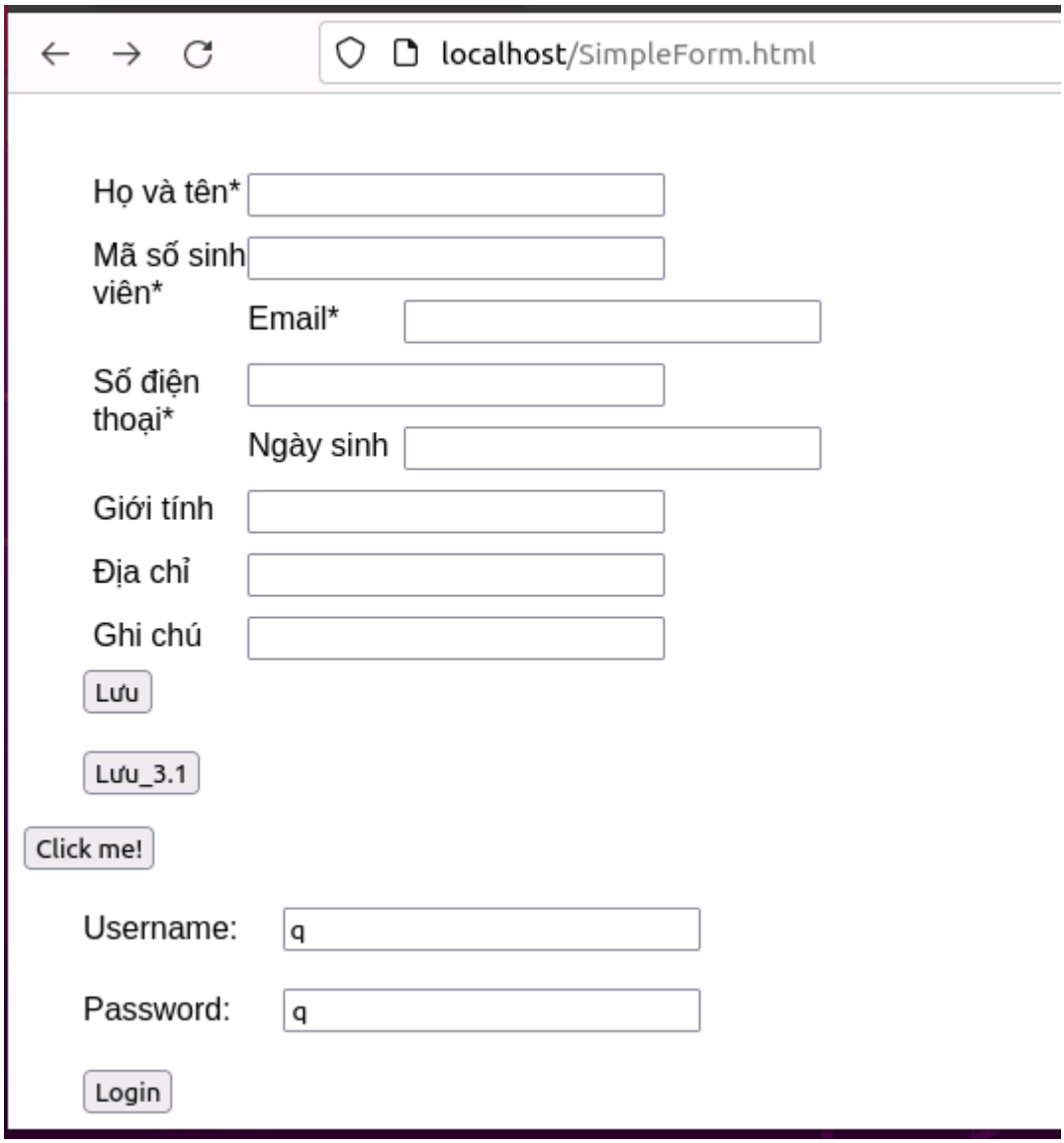
```
mysql> CREATE TABLE USERINFO(
    -> username VARCHAR(50),
    -> password VARCHAR(100));
Query OK, 0 rows affected (0.19 sec)
```

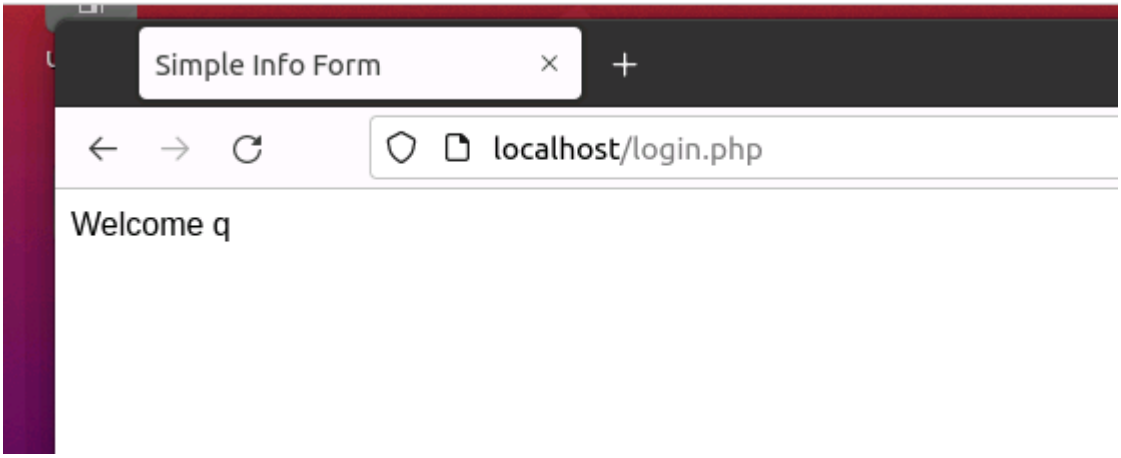
```
mysql> Describe USERINFO;
+----------+--------------+------+-----+---------+-------+
| Field    | Type         | Null | Key | Default | Extra |
+----------+--------------+------+-----+---------+-------+
| username | varchar(50)  | YES  |     | NULL    |       |
| password | varchar(100) | YES  |     | NULL    |       |
+----------+--------------+------+-----+---------+-------+
2 rows in set (0.31 sec)

mysql>
```

4.1b. Chỉ thêm 1 button **Click me** trong mã nguồn HTML của tập tin **SimpleForm.html** đã chỉnh sửa xong ở **Phần 3**, hãy sử dụng Javascript để tìm cách tạo một form cho phép nhập tài khoản và gọi tập tin xử lý **login.php** để đăng nhập.

Trả lời:





HẾT