1

Lab

ÔN TẬP KIẾN THỨC CƠ BẢN

Ứng dụng web

(HTML, Javascript, PHP, CSDL)

Thực hành Bảo mật web và ứng dụng

Lưu hành nội bộ

A. TỔNG QUAN

A.1 Giới thiệu

Ôn tập kiến thức cơ bản về web (các ngôn ngữ HTML, Javascript, PHP…) để chuẩn bị kiến thức cho phần bảo mật.

A.2 Mục tiêu

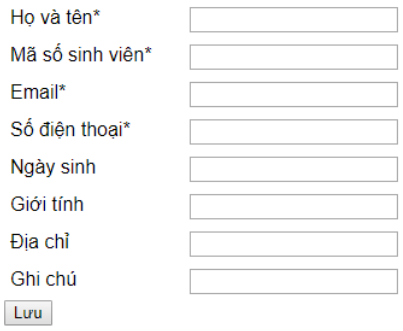
Giúp sinh viên có được kiến thức thao tác với JavaScript (như validation, Ajax, …), PHP và Cơ sở dữ liệu.

B. CHUẨN BỊ MÔI TRƯỜNG

B.1 Các tập tin được cung cấp sẵn

Để thuận tiện cho quá trình thực hành và tập trung vào những phần quan trọng, GVTH cung cấp sẵn cho sinh viên một số tập tin như sau:

- **SimpleForm.html** tạo một form đơn giản, trong đó bao gồm:
  - Đoạn mã HTML để tạo form đơn giản gồm **8** trường ***Họ và tên, Mã số sinh viên, Email, Số điện thoại, Ngày sinh, Giới tính, Địa chỉ*** và ***Ghi chú***.
  - Đoạn mã Javascript bắt sự kiện nhấn nút **Lưu** của form.
  - Import tập tin jQuery hỗ trợ cho **Phần C.3**.



Hình B.1 Form thông tin mẫu

- **submit_form.php** xử lý yêu cầu submit form được gửi từ **SimpleForm.html**. Tập tin này sẽ thực hiện kết nối đến MySQL server để lưu thông tin.
- **login.php** xử lý yêu cầu đăng nhập và có kết nối với MySQL server, tuy nhiên không có mã nguồn để gọi nó từ tập tin HTML.

B.2 Triển khai Web server

B.2.1 Chuẩn bị môi trường

Sinh viên có thể thực hiện cài đặt, tạo máy và cấu hình máy ảo trên **VMware Workstation**, **Virtual Box**, …

Sinh viên có thể tải image Ubuntu tại http://mirror.bizflycloud.vn/ubuntu-releases/20.04/.

Khuyến cáo: Sinh viên nên thiết lập cấu hình máy ảo như bảng bên dưới (hoặc có thể thay đổi tùy vào cấu hình của mỗi sinh viên. Tuy nhiên, card mạng vẫn phải giữ nguyên)

Máy ảo	Ubuntu
Dung lượng RAM	2 GB
Vi xử lý	1 Processor, 4 Core
Dung lượng ổ cứng	20 GB
Card mạng	NAT (VMnet8)

B.2.2 Cài đặt Web server

Sinh viên có thể thực hiện cài đặt và triển khai một web server: Apache hoặc Nginx.

```
sudo apt-get install apache2 -y
```

hoặc

```
sudo apt-get install nginx -y
```

Sau khi cài, web server Apache hay Nginx đều tự hoạt động và có thể kiểm tra bằng cách truy cập vào đường dẫn **http://<ip_web_server>**.

B.2.3 Cài đặt Cơ sở dữ liệu MySQL

Trong bài thực hành này, phần hướng dẫn được thực hiện với cơ sở dữ liệu MySQL. Sinh viên tiến hành cài đặt MySQL, có thể tham khảo đường dẫn Hướng dẫn cài đặt MySQL.

Một số câu lệnh để cài đặt MySQL trên Ubuntu:

```
sudo apt-get install mysql-server -y
sudo mysql_secure_installation
```

Sau khi cài đặt, truy cập vào MySQL với lệnh:

```
mysql -u root -p
```

B.2.4 Cài đặt PHP

Cần cài đặt PHP để có thể thực thi các file xử lý **.php** được cung cấp sẵn.

```
sudo apt install php-fpm php-mysql -y
```

B.2.5 Chạy trang web

Sau khi cài đặt web server và các gói cần thiết, sao chép 2 tập tin được cung cấp vào thư mục tương ứng của web server ở đường dẫn ***/var/www/html/.*** Trên trình duyệt, truy cập vào đường dẫn sau **http://<IP>:<port>/SimpleForm.html**, nếu thấy hiện form thì bước đầu đã cấu hình thành công.

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 bên dưới.

Dùng thuộc tính mặc định của HTML, hiện thực các ràng buộc sau:

- 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.

Gợi ý: Trường **Email** đổi type khác, tham khảo các thuộc tính của thẻ *<input>*.

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.

Gợi ý: Sinh viên có thể kiểm tra lúc nhấn nút **Submit** hoặc dùng các sự kiện keypress để kiểm tra lúc nhập cho trường ***Họ và tên***.

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.

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.

Sinh viên có thể lựa chọn 1 trong 3 cách kết nối cơ sở dữ liệu đã được học, ghi rõ mình đang sử dụng kiểu kết nối nào.

- MySQLi hướng đối tượng
- MySQLi dùng hàm
- PDO

Tham khảo thêm ở đường dẫn:
https://www.w3schools.com/php/php_mysql_connect.asp

Gợi ý: Cần đảm bảo:

- Nút **Lưu** có type là **submit**.
- Đường dẫn xử lý của form đã trỏ đến **submit_form.php**
- Thông tin kết nối CSDL đúng với MySQL đã xây dựng.
- Lấy được các tham số đã nhập trong form và tạo được SQL Command đúng.

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

Gợi ý: Cần đảm bảo:

- Sử dụng nút **Lưu** mới với type là **button**.
- Bắt sự kiện click của nút này và xử lý JavaScript với Ajax để gửi form đến URL của **submit_form.php**.
- Có thể sử dụng jQuery.

Tham khảo thêm ở đường dẫn: https://www.w3schools.com/xml/xml_http.asp hoặc https://api.jquery.com/jquery.ajax/

> **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**

Gợi ý: Dùng sự kiện **onload** của body để submit form tự động. Có thể tự động gửi bằng chức năng input có type "submit" hoặc bằng Ajax.

C.4 Vọc một chút

Trong các tập tin được cung cấp, có 1 file **login.php** là file không được gọi từ file HTML, tuy nhiên có thể sử dụng để đăng nhập.

> **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**.

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

Cần đảm bảo: *Thay đổi chỉ có thể tạo ra lúc đang chạy file SimpleForm.html, nội dung của file trên ổ đĩa chỉ cho phép thêm button Click me và tên file JavaScript.*

Gợi ý: mã nguồn JavaScript có thể thêm form mới hoặc thay nội dung form ở **Yêu cầu 1.1** bằng một form đăng nhập khi có sự kiện click nút.

D. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm**.
- Sinh viên có thể báo cáo theo 2 hình thức:
  - Báo cáo trực tiếp trên lớp: Sinh viên báo cáo và vấn đáp trực tiếp với GVTH.
  - Nộp báo cáo kết quả trên website môn học theo thời gian quy định: gồm **Code, CSDL được export** và chi tiết những việc (**Report**) đã thực hiện, kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
    - File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
    - Đặt tên theo định dạng: **[Mã lớp]-LabX_NhomX_MSSV1-MSSV2**.

      Ví dụ: [NT213.L21.ATCL.1]-Lab1_Nhom1_1852xxxx-1852yyyy.
    - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

E. THAM KHẢO

[1] W3Schools – JavaScript, https://www.w3schools.com/js/default.asp
[2] W3Schools – HTML Form Element, https://www.w3schools.com/html/html_forms.asp
[3] W3Schools – PHP, https://www.w3schools.com/php/php_syntax.asp

HẾT