



1

Lab

ÔN TẬP KIẾN THỨC CƠ BẢN

Ứng dụng web

(HTML, Javascript, PHP, CSDL)

Thực hành Bảo mật web và ứng dụng

Học kỳ I – Năm học 2020 - 2021

Lưu hành nội bộ

(Ng nghiêm cấm đăng tải trên internet dưới mọi hình thức)

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

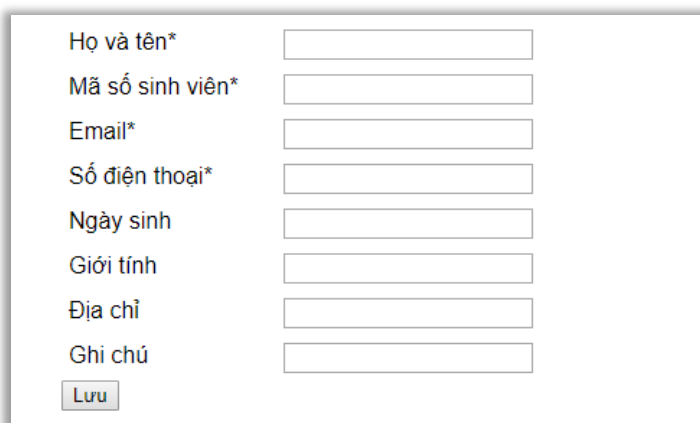
Giúp sinh viên có được kiến thức thao tác với JavaScript (như validation, Ajax,...), PHP và Cơ sở dữ liệu.

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 **Yêu cầu 3.4**.



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

Sinh viên sẽ thực hiện cài đặt và triển khai một web server. Tùy vào hệ điều hành của máy, cần cài đặt sẵn phần mềm **Web server** phù hợp:

- Đối với máy chạy Linux: Apache hoặc Nginx.
- Đối với máy chạy Windows: nên cài phần mềm Xampp.

Sau khi cài đặt web server, sao chép 2 tập tin được cung cấp vào thư mục tương ứng của web server.

- Đối với máy chạy Linux: Apache dùng **/var/www/html/**

- Đối với máy chạy Windows: Xampp dùng `xampp\htdocs\`

Truy cập thông qua đường dẫn sau **http://<IP>:<port>/SimpleForm.html**. Điều chỉnh IP và Port theo cấu hình khi cài đặt.

B.3 Cơ sở dữ liệu

Trong bài thực hành này, phần hướng dẫn được thực hiện với cơ sở dữ liệu MySQL. Sinh viên tiến hành cài đặt MySQL.

- Nếu sử dụng Xampp: đã được tích hợp sẵn.
- Ngược lại, có thể tham khảo đường dẫn [Hướng dẫn cài đặt MySQL](#).

Sau khi cài đặt, cần điều chỉnh các thông số trong **submit_form.php** và **login.php** cho phù hợp.

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 các mã nguồn **Javascript** (có thể ở trong hoặc ngoài tập tin cung cấp) thực hiện các yêu cầu bên dưới.

- 1.2a.** Viết mã nguồn JavaScript thực hiện kiểm tra trường **Họ và tên** chỉ cho nhập chữ và khoảng trắng.

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

- 1.2b.** Viết mã nguồn JavaScript thực hiện tạo cookie (với key và value tùy chọn), xem và xóa cookie. Hãy cho biết Cookie không được gán thời gian hết hạn và cookie được gán khác nhau như thế nào?

Yêu cầu 1.3 Dùng JavaScript thay nội dung form ở **Yêu cầu 1.1** bằng một form đăng nhập có 2 trường: **Tên đăng nhập** và **Mật khẩu** khi có một sự kiện cụ thể, ví dụ click một nút.

C.2 PHP và Cơ sở dữ liệu

Yêu cầu 2.1 Tạo cơ sở dữ liệu bằng 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 Điều chỉnh mã nguồn trong tập tin **submit_form.php** để nhận các giá trị được submit và lưu vào CSDL dùng MySQL theo 3 dạng kết nối cơ sở dữ liệu.

- MySQLi hướng đối tượng
- MySQLi dùng hàm
- PDO

Tham khảo thêm ở đường dẫn:

https://www.w3schools.com/php/php_mysql_connect.asp

Yêu cầu 2.3 Thêm mã nguồn PHP để tạo cookie.

C.3 Kết hợp form và Cơ sở dữ liệu

Yêu cầu 3.1 Viết mã nguồn thực hiện lưu giá trị được nhập vào CSDL khi nhấn nút submit và hiển thị thông báo thành công/thất bại cho người dùng.

Gợi ý: Sử dụng nút **Lưu** với type là **submit**.

Yêu cầu 3.2 Viết mã nguồn Ajax thực hiện khi nhấn vào một nút thì gửi giá trị để lưu vào CSDL và hiển thị thông báo thành công/thất bại cho người dùng.

Gợi ý: Sử dụng nút **Lưu** mới với type là **button**, bắt sự kiện click của nút này.

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

Yêu cầu 3.3 Viết một tập tin tương tự khác, trong đó khi mở lên thì tự động gửi một giá trị với các trường tham số như **Yêu cầu 1.1**.

Gợi ý: dùng sự kiện **onload** của body để submit form tự động.

Yêu cầu 3.4 Viết lại **Yêu cầu 3.2** dùng jQuery.

C.4 Vọc một chút (optional)

Tạo một bảng chứa thông tin người dùng đơn giản trong MySQL, gồm ít nhất 2 trường là **tên đăng nhập** và **mật khẩu**. Không sửa mã nguồn HTML trong tập tin **SimpleForm.html**, 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.

Gợi ý: Xem lại **Yêu cầu 1.3**.

D. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm từ 2 – 3 SV**.
- Nộp báo cáo kết quả gồm **Code, CSDL được export** và chi tiết những việc (**Report**) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-LabX_MSSV1-MSSV2-MSSV3**.

Ví dụ: [NT213.K11.ANTN.1]-Lab1_1452xxxx-1652yyyy-1452zzzz.

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá: Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.

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