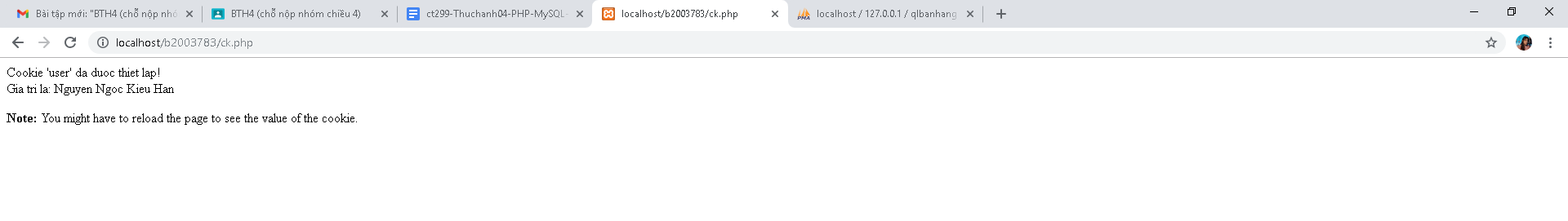
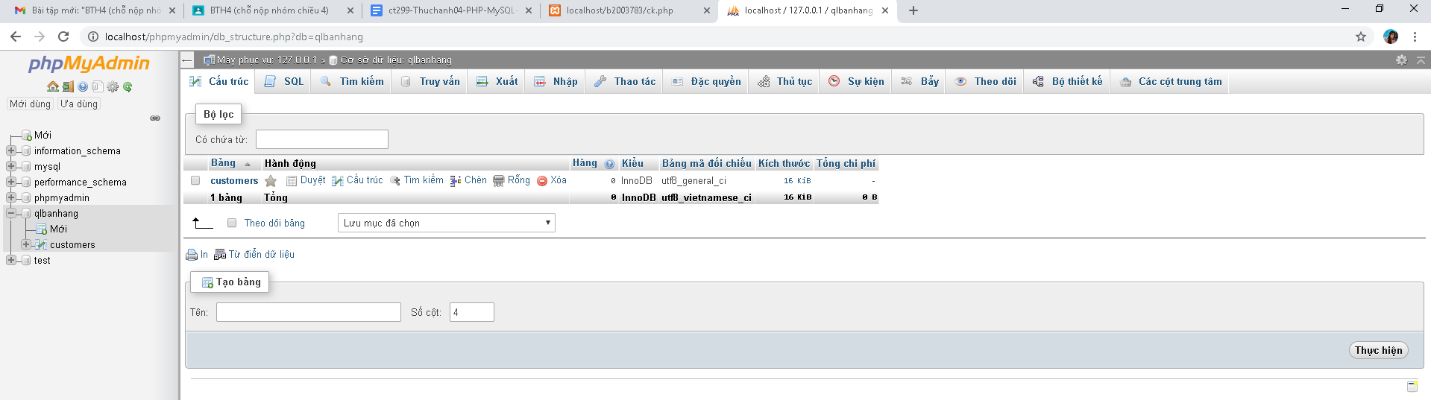
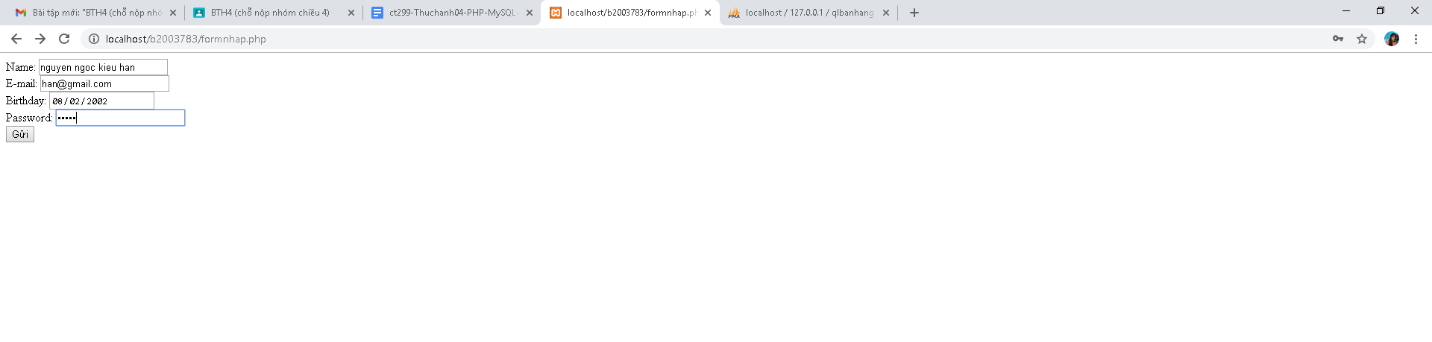
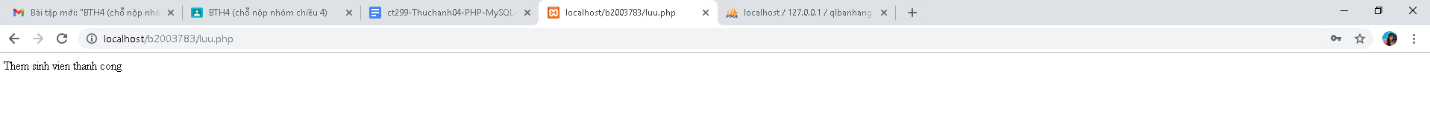
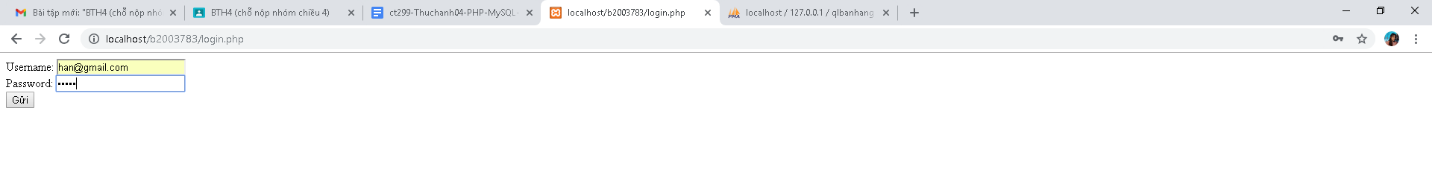
1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

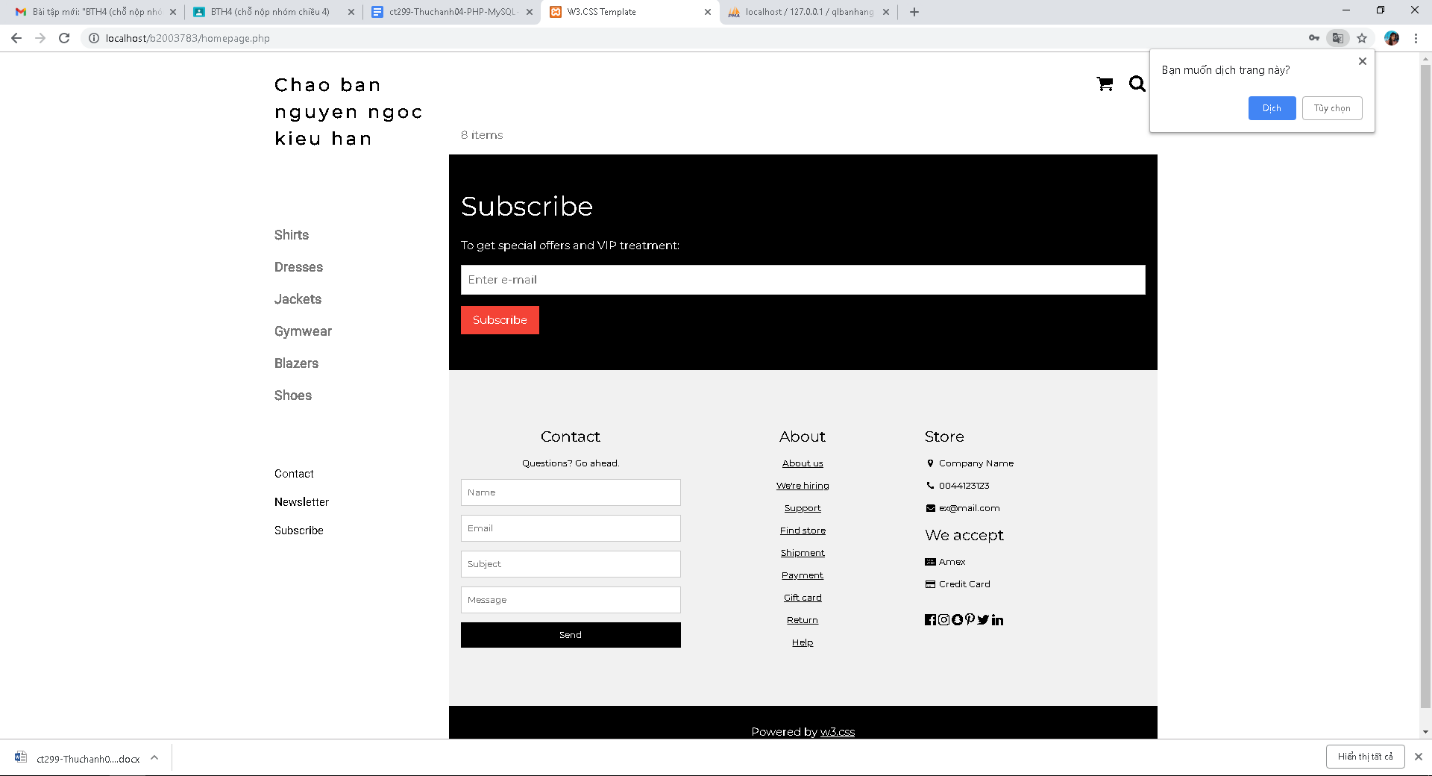
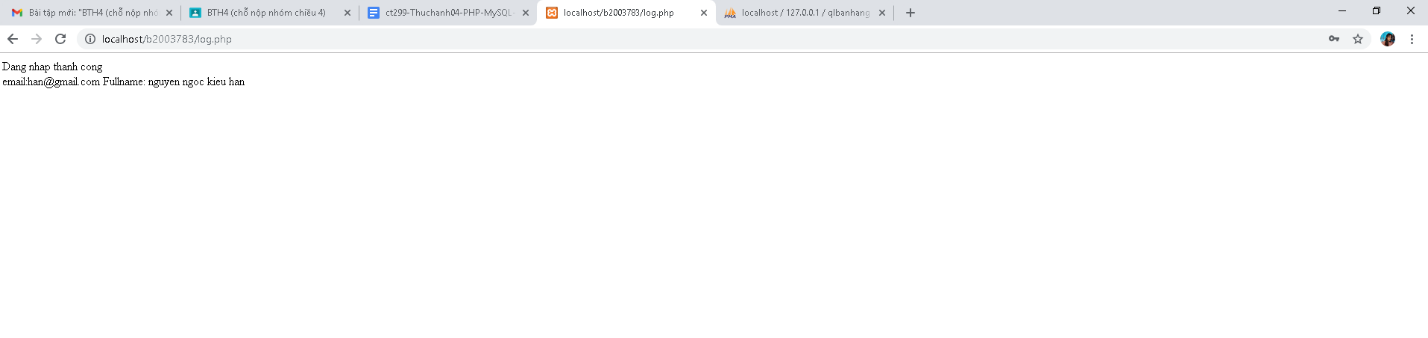


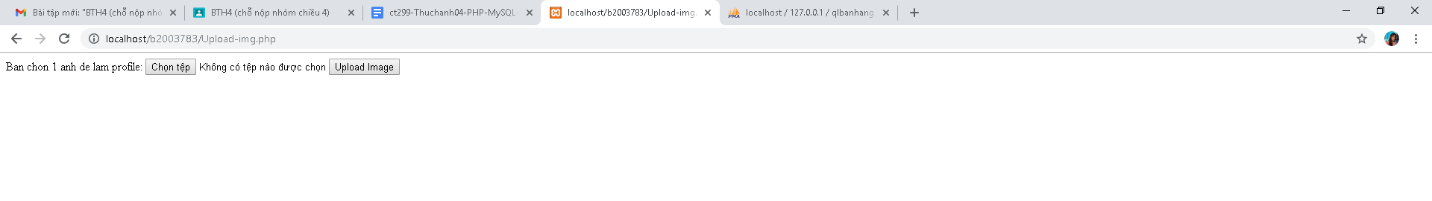


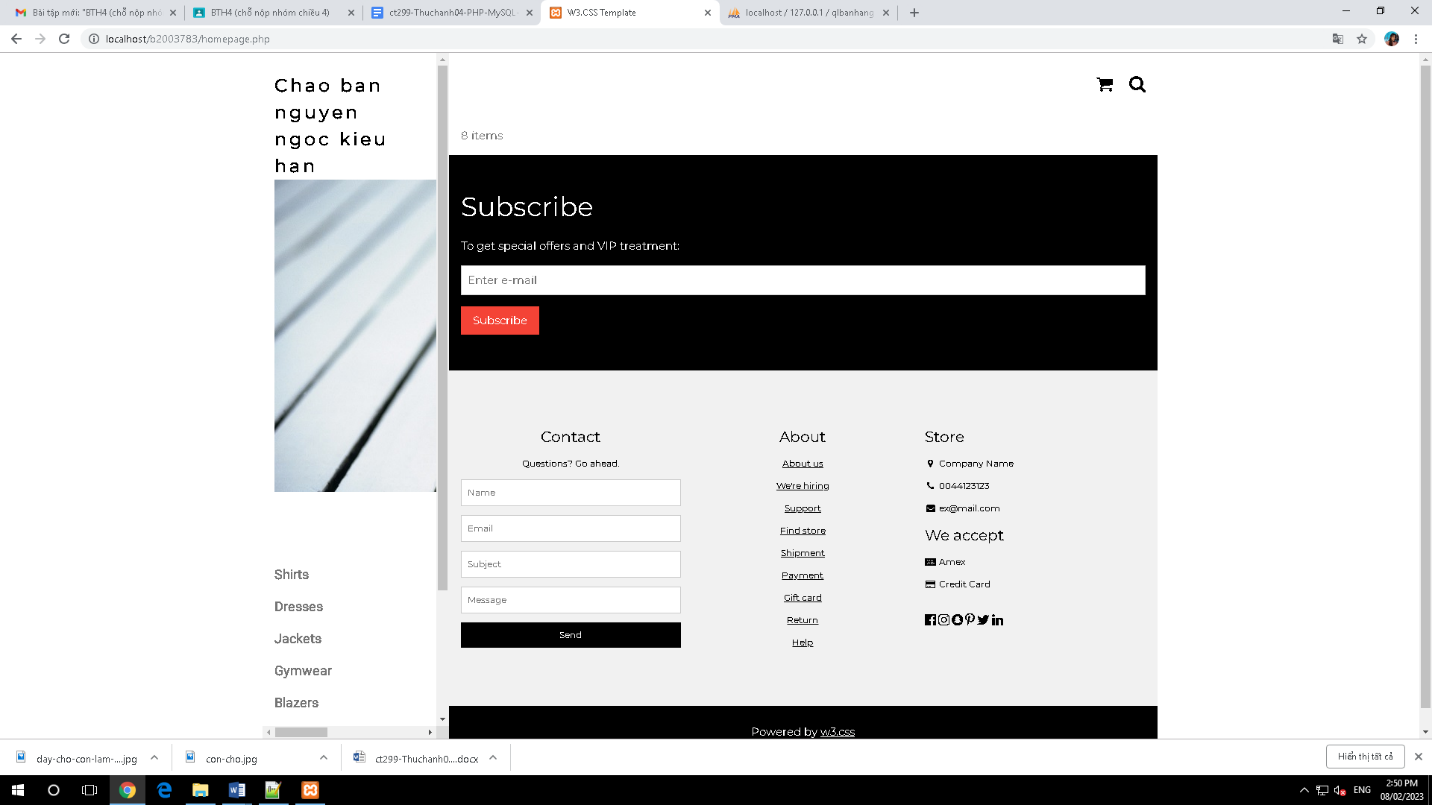
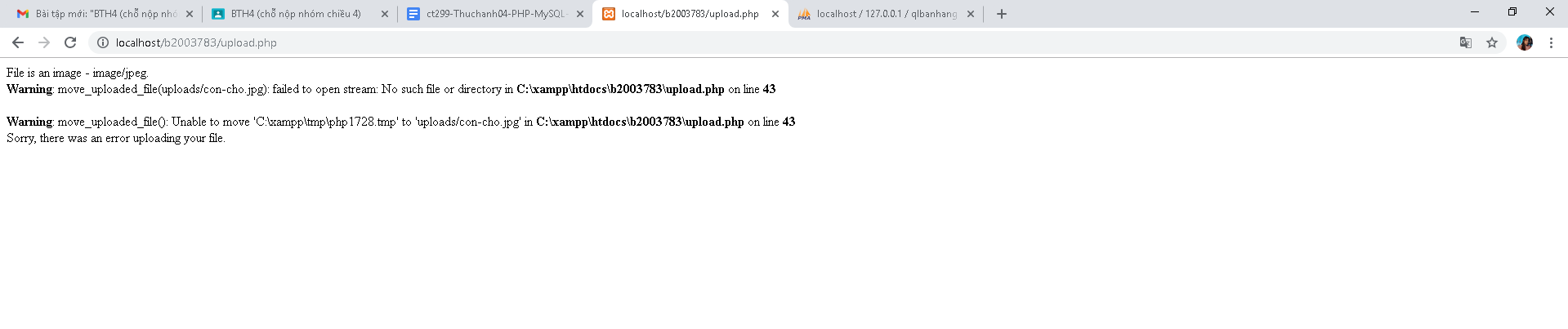


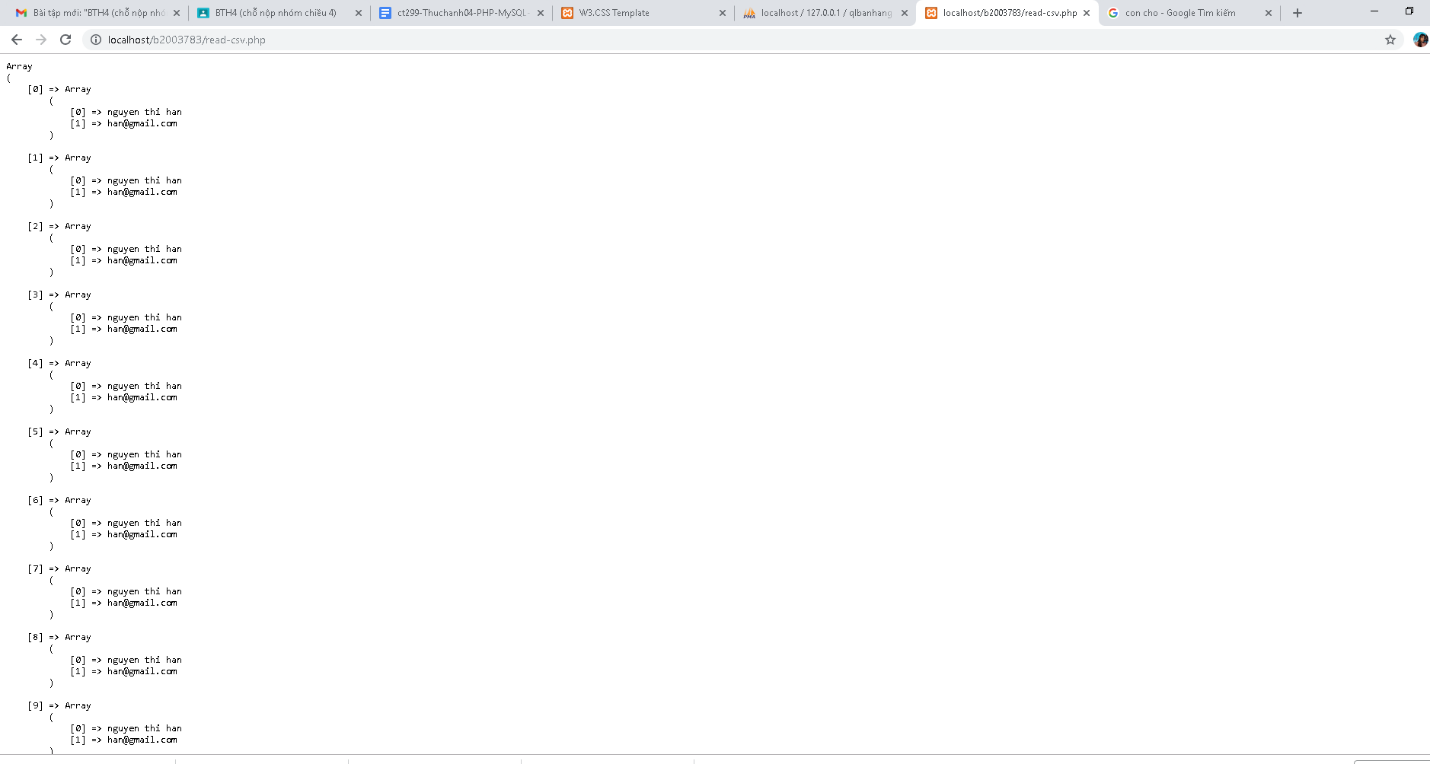












1. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong [[1]](#footnote-1). Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

SQL injection là một kỹ thuật chèn mã có thể phá hủy cơ sở dữ liệu của bạn.

SQL injection là một trong những kỹ thuật hack web phổ biến nhất.

SQL injection là vị trí của mã độc hại trong câu lệnh SQL, thông qua đầu vào trang web.

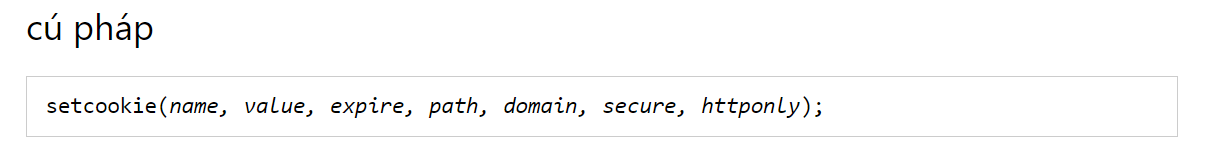
SQL trong các trang web

SQL injection thường xảy ra khi bạn yêu cầu người dùng nhập dữ liệu, chẳng hạn như tên người dùng/userid của họ và thay vì tên/id, người dùng cung cấp cho bạn một câu lệnh SQL mà bạn sẽ **vô tình** chạy trên cơ sở dữ liệu của mình.

1. Dựa vào link[[2]](#footnote-2), bạn hãy cho biết Cookie là gì, diễn giải ý nghĩa các tham số trong setcookie(). Cách lưu, lấy, xóa giá trị trong cookie.

Cookie là một tệp nhỏ mà máy chủ nhúng vào máy tính của người dùng. Mỗi khi cùng một máy tính yêu cầu một trang bằng trình duyệt, nó cũng sẽ gửi cookie.

Một cookie được tạo bằng setcookie()chức năng.



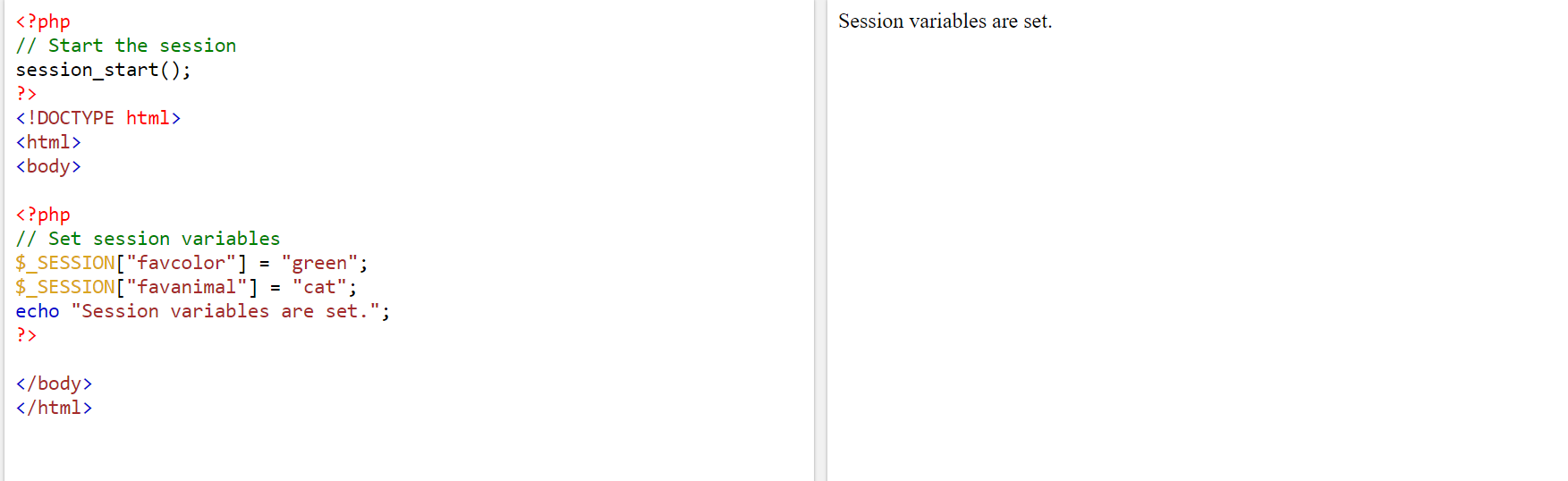


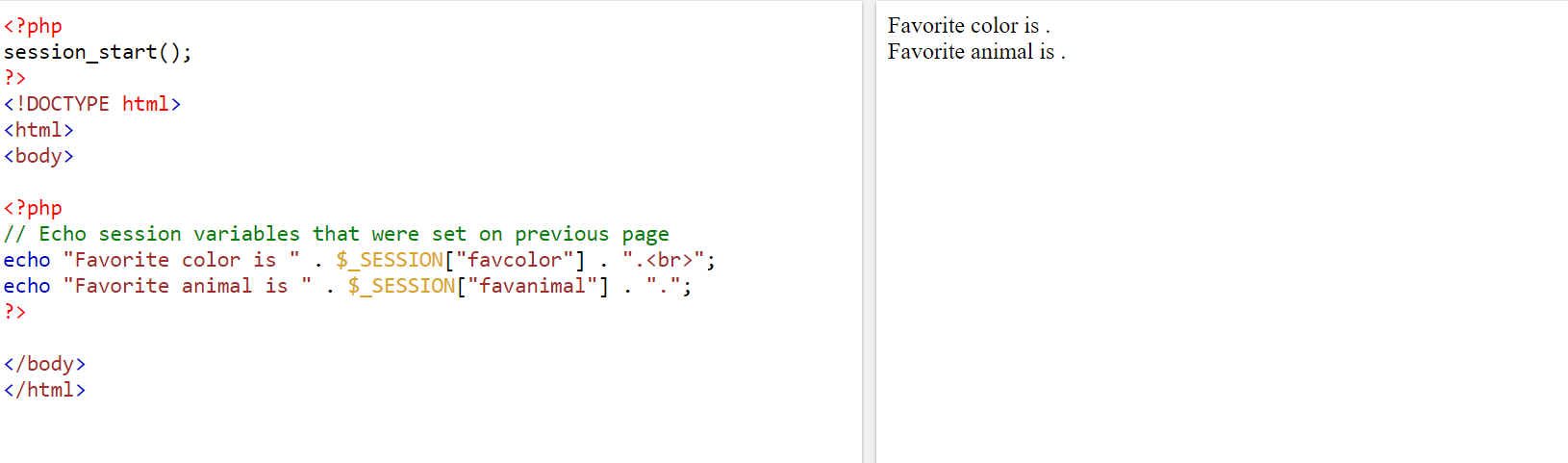
Chỉ có tham số tên là bắt buộc. Tất cả các tham số khác là tùy chọn.

1. Dựa vào link[[3]](#footnote-3), bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

Session là một cách để lưu trữ thông tin (trong các biến) sẽ được sử dụng trên nhiều trang.

Không giống như cookie, thông tin không được lưu trữ trên máy tính của người dùng.





1. Bạn hãy so sánh Cookie và Session.

Về khái niệm, Cookie cũng có nét tương đồng với khái niệm Session là gì. Tuy nhiên, giữa chúng có ba điểm khác biệt nổi bật giữa phải kể đến như sau:

* **Nơi lưu trữ:**Session không được lưu trữ trên trình duyệt, còn Cookie được lưu trữ.
* **Nơi lưu trữ dữ liệu:** Dữ liệu Session được lưu trữ ở phía server, còn dữ liệu Cookie được lưu trữ ở phía client.
* **Tính linh hoạt:** Dữ liệu session không dễ dàng được sửa đổi vì chúng được lưu trữ ở phía máy chủ. Trong khi đó, dữ liệu Cookie sẽ dễ dàng hơn vì được lưu trữ ở phía client.

Sau khi lập trình viên đã tạo ra được một tập tin Session trên máy chủ để có thể lưu trữ dữ liệu tạm thời của người dùng. Thì bạn vẫn phải phân biệt được Session nào của người dùng nào. Để có thể làm được việc này, đối với mỗi một session thì cần phải tạo ra được 1 cookie trên trình duyệt của người dùng tương ứng với nó.

Tuy cookie có thể tạo ra mà không bắt buộc phải tạo một session trên máy chủ tương ứng với nó. Tuy nhiên, mỗi session tạo ra thì bắt buộc cần phải có một cookie tương ứng với nó để xác định. Nhờ có cookie mà chúng ta có thể phân biệt được session khác nhau của các trình duyệt khác nhau.

1. Chỉnh sửa các đoạn gán, khởi tạo, lấy giá trị cookie trong log.php và homepage.php thay bằng cách dùng Session. Tạo tập tin thoat.php để xóa các giá trị trong session, cookie thực hiện chức năng log out khỏi hệ thống.
2. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô cho phép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với nhau và không giống với mật khẩu cũ, nếu đáp ứng điều kiện thì tiến hành băm mật khẩu với md5 và lưu mật khẩu mới vào CSDL.
3. Bạn đọc trong[[4]](#footnote-4) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.
4. Bạn hãy đọc[[5]](#footnote-5), mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).
5. Bạn hãy tạo 1 tập tin csv ít nhất 10 dòng dữ liệu với các cột dữ liệu như bảng customer trong csdl qlbanhang. Tạo tập tin upload-csv.php với giao diện cho phép upload các tập

1. <https://www.w3schools.com/sql/sql_injection.asp> [↑](#footnote-ref-1)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-2)
3. <https://www.w3schools.com/php/php_sessions.asp> [↑](#footnote-ref-3)
4. <https://www.w3schools.com/php/php_file_upload.asp> [↑](#footnote-ref-4)
5. <https://www.w3schools.com/php/func_filesystem_file.asp> [↑](#footnote-ref-5)