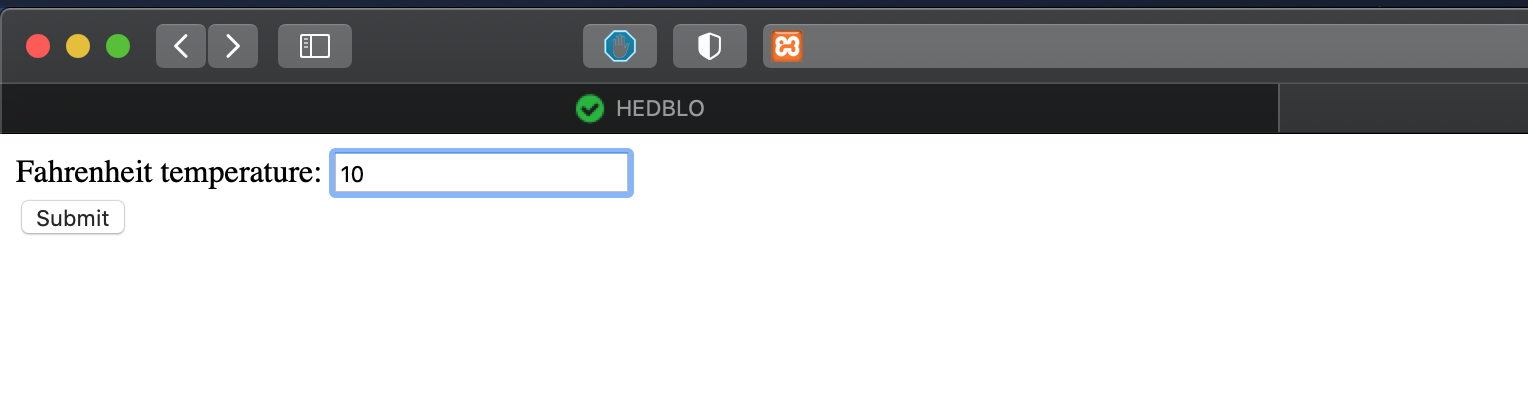
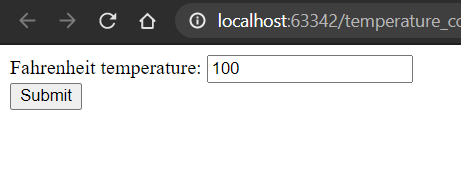
**Báo cáo Lab13**

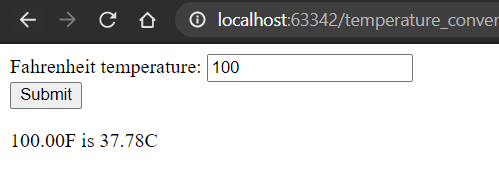
Bài 13.1:. Run the examples in lecture slides

1. Temperature Conversion



2. Sticky form



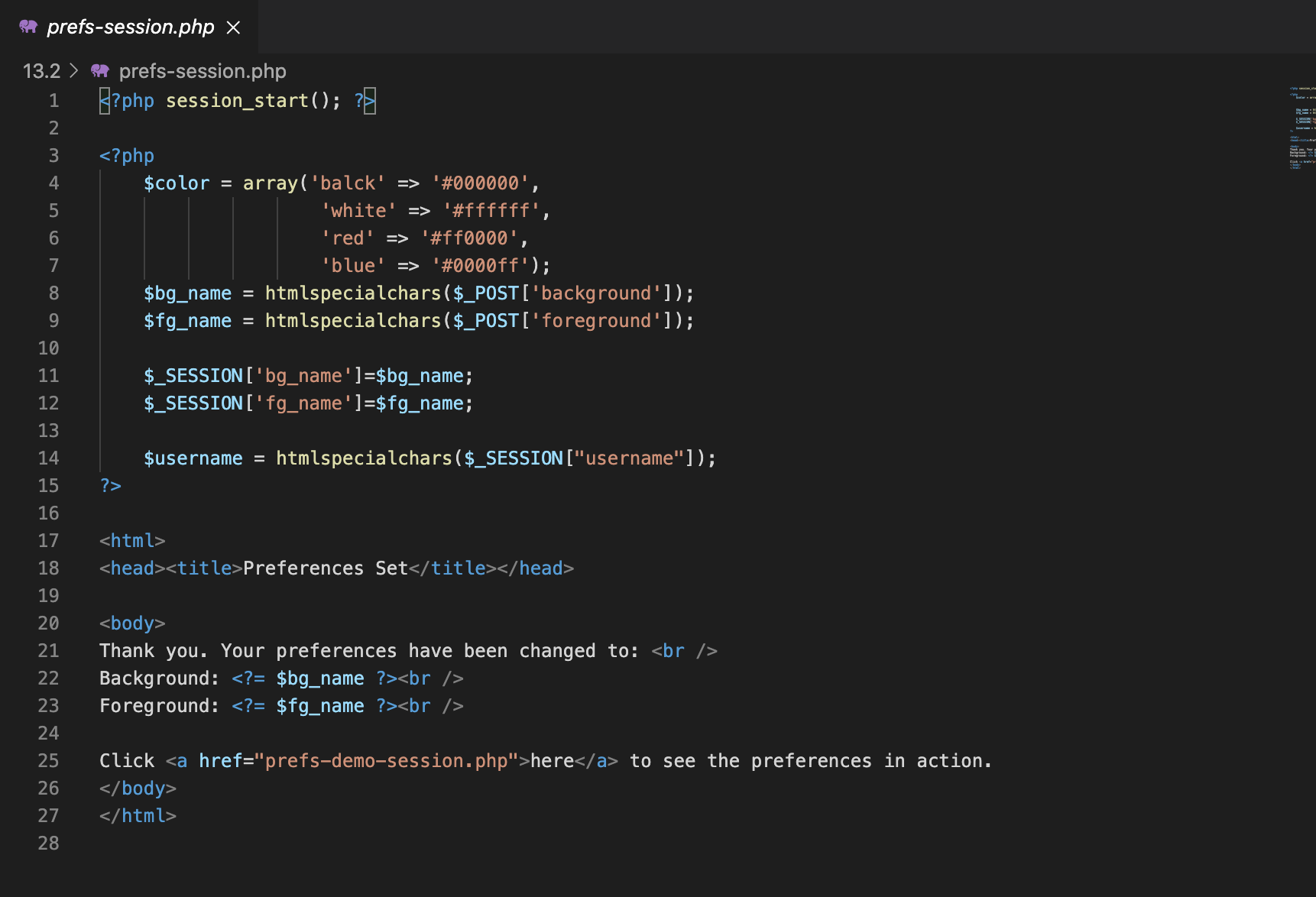


3. Encoding and Escaping



Bài 13.2. Review Lab 10 to make it safer

* Thêm hàm htmlspcialchars() trước $\_POST hoặc $\_SESSION



Bài 13.3. Exercise

1. Cross site scripting:

Tấn công XSS là một đoạn mã độc, để khai thác một lỗ hổng XSS, hacker sẽ chèn mã độc thông qua các đoạn script để thực thi chúng ở phía Client. Thông thường, các cuộc tấn công XSS được sử dụng để vượt qua truy cập và mạo danh người dùng.

Mục đích chính của cuộc tấn công này là ăn cắp dữ liệu nhận dạng của người dùng như: cookies, session tokens và các thông tin khác. Trong hầu hết các trường hợp, cuộc tấn công này đang được sử dụng để ăn cắp cookie của người khác. Như chúng ta biết, cookie giúp đăng nhập tự động. Do đó với cookie bị đánh cắp, hacker có thể đăng nhập bằng các thông tin nhận dạng khác. Và đây là một trong những lý do tại sao XSS được coi là một trong những loại tấn công nguy hiểm nhất.

2. Search web site vulnerabilites with examples for attacker:

1. Broken Authentication

* Ví dụ: các vấn đề liên quan đến xác thực. Nếu code không tốt -> hacker có thể lợi dụng.

1. Lỗ hổng XSS (Cross Site Scripting)

* Ví dụ: như 13.1

1. Insecure Direct Object References

* Ví dụ: chương trình cho phép người dùng truy cập tài nguyên (dữ liệu, file, database) mà không kiểm soát quyền hạn 🡪 có thể bị lợi dụng.

1. Sensitive data exposure (Rò rỉ dữ liệu nhạy cảm)

* Ví dụ: dữ liệu quan trọng được gửi đi mà không được mã hóa 🡪 hacker có thể dễ dàng đọc được.

1. Missing function level access control (lỗi phân quyền)

* Ví dụ: Quá trình phân quyền trên máy chủ không chính xác 🡪 hacker có thể có được quyền admin mà lẽ ra không được phép 🡪 tiến hành phá hoại/lấy dữ liệu.