|  |  |
| --- | --- |
| SEESIONS | COOKIES |
| * Lưu trữ thông tin sever | * Lưu trữ thông tin trên client |
| * Phiên làm việc tối đa là 1440s | * Phải thiết lập thời gian phiên |
| * Trước khi sử dụng session phải khởi động sesion\_start | * Không cần phải khởi động cookies |
| * Seesion lưu trữ tối đa được 128MB | * Cookies lưu trữ tối đa được 4K |
| * Phiên làm việc kết thúc khi bạn đóng trình duyệt | * Kết thúc phụ thuộc vào thời gian sống mà bạn thiết lập |
| * Hủy session dùng lệnh session\_destroy() | * Không có chức năng hủy cookie mà muốn hủy cookie phụ thuộc vào thời gian sống mà bạn thiết lập cho nó. |

**SQL injection** là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,… trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

Cách phòng chống

* Nhận dữ liệu kiểu INT: Khi bạn nhận dữ liệu ID trên URL thì cách tốt nhất bạn nên ép kiểu, chuyển nó về kiểu số INT, sau đó chuyển về kiểu STRING

Sử dụng hàm **addslashes** để nó tự động thêm ký tự \ vào trước dấu ‘ (nháy đơn), ” (nháy kép) như thế sẽ không phá vỡ cấu trúc câu lệnh SQL