

Csrf Token

1. Khái niệm.

- Token CSRF là 1 chuỗi ký tự ngẫu nhiên được tạo ra bởi máy chủ và gửi cho người dùng .Khi người dùng gửi yêu cầu đến web,token CSRF sẽ được đính kèm vào yêu cầu.Máy chủ sẽ kiểm tra Token CSRF và chỉ thực yêu cầu nếu Token CSRF hợp lệ.
- token CSRF thường được sử dụng ở 1 số form, header hoặc request body của người dùng.

2. hoạt động.

Bước 1 : thực hiện GET giao diện.

Bước 2 : server nhận yêu cầu get trả về giao diện và có chèn vào csrf token vào form cần csrf xác thực.có thể ở html hoặc trong header cookie.

Bước 3 : sử dụng method POST để đẩy dữ liệu kiểm csrf.

Bước 4 : kiểm tra csrf xem có trùng khớp với csrf nói trả cho bạn đầu không nếu trùng khớp thực hiện xử lý yêu cầu.

3. mục đích.

- ngăn chặn yêu cầu giả mạo
- xác thực nguồn gốc yêu cầu
- bảo vệ hành động nhạy cảm
- bảo vệ niềm tin người dùng

4. cấu hình.