**HRM CODE TUTORIAL COLLECTION**

**Collection By:** R&D Team

Index

[REQUEST POST LARGE DATA JSON – WEB MVC 5](#_Toc23858538)

[Features 5](#_Toc23858539)

[Resolve Exception 5](#_Toc23858540)

[Access to the Code 5](#_Toc23858541)

[How to use 5](#_Toc23858542)

[Example 6](#_Toc23858543)

[Access to the Code 19](#_Toc23858558)

[How to use 19](#_Toc23858559)

[Example 20](#_Toc23858560)

# Cookie

## SameSite Cookies

Một Attribute của Set-Cookie HTTP Response Header là SameSite cho phép chúng ta quản lý việc Cookie nên được giới hạn bởi một First-party hoặc same-site Context

### Values

SameSite Attribute chấp nhận 3 giá trị

#### Lax

Cookies sẽ không được gửi trong một trường hợp Cross-site Subrequests bình thường (ví dụ như một hình ảnh được load từ một Site của Third Party), nhưng sẽ được gửi khi User được điều hướng tới Origin Site (khi follow một liên kết)

Đây là giá trị mặc định của Firefox nếu SameSite không được cài đặt một cách tường minh.

Lax thay thế None trở thành giá trị mặc định để đảm bảo User có một sự bảo về hợp lý và an toàn chống lại việc gặp phải Cross-site Request Forgery (CSRF) Attacks.

#### Strict

Cookies sẽ chỉ được gửi đi tại First-pary Context và sẽ không bao giờ được gửi cùng với Request được phát động bởi Third-party Websites.

#### None

Cookies sẽ được gửi tại mọi Context. Nếu SameSite=None được set, Cookie Secure Attribute phải được set theo (nếu cookie sẽ bị blocked)

## Using the SameSite Cookie Attribute to Prevent CSRP Attacks

### Introduction to Web Cookies

Bởi vì HTTP là một Stateless Protocol, vì vậy nó không có khả năng nhận biết các User internally. Để giải quyết vấn đề này, Cookie đã được tạo ra vào năm 1994. Bằng cách sử dụng Cookies, Server sẽ chỉ dẫn Browsers lưu trữ các Unique Key và sau đó gửi kèm cùng với mỗi Request tới Server.

Khi một Request được gửi từ một Browser tới một Website, Browser sẽ kiểm tra có một Stored Cookie thuộc về Website đó hay không. Trong khi thực hiện quá trình này, nó sẽ kiểm tra các Properties và Flags của Cookies (domain, path, secure) khớp với Data của Website đã được Request không. Nếu match, Browser sẽ gửi các Cookies liên quan cùng với Request

### Cookie Misue can lead to Cross-site Requset Forgery

Behavior này sẽ có có cách lặp lại tương tự cho Requests được tạo bởi Third Parties thông qua Browser.