# CWE Detail – CWE-1275

## Description

The SameSite attribute for sensitive cookies is not set, or an insecure value is used.

## Extended Description

The SameSite attribute controls how cookies are sent for cross-domain requests. This attribute may have three values: 'Lax', 'Strict', or 'None'. If the 'None' value is used, a website may create a cross-domain POST HTTP request to another website, and the browser automatically adds cookies to this request. This may lead to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-24045: Web application for a room automation system has client-side JavaScript that sets a sensitive cookie without the SameSite security attribute, allowing the cookie to be sniffed

## Related Attack Patterns (CAPEC)

* CAPEC-62

## Modes of Introduction

**•** Implementation: This weakness occurs during implementation when the coder does not properly set the SameSite attribute.

## Common Consequences

**•** Impact: Modify Application Data — Notes: If the website does not impose additional defense against CSRF attacks, failing to use the 'Lax' or 'Strict' values could increase the risk of exposure to CSRF attacks. The likelihood of the integrity breach is Low because a successful attack does not only depend on an insecure SameSite attribute. In order to perform a CSRF attack there are many conditions that must be met, such as the lack of CSRF tokens, no confirmations for sensitive actions on the website, a "simple" "Content-Type" header in the HTTP request and many more.

## Potential Mitigations

**•** Implementation: Set the SameSite attribute of a sensitive cookie to 'Lax' or 'Strict'. This instructs the browser to apply this cookie only to same-domain requests, which provides a good Defense in Depth against CSRF attacks. When the 'Lax' value is in use, cookies are also sent for top-level cross-domain navigation via HTTP GET, HEAD, OPTIONS, and TRACE methods, but not for other HTTP methods that are more like to cause side-effects of state mutation. (Effectiveness: High)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** Since the sameSite attribute is not specified, the cookie will be sent to the website with each request made by the client. An attacker can potentially perform a CSRF attack by using the following malicious page: