# CWE Detail – CWE-1022

## Description

The web application produces links to untrusted external sites outside of its sphere of control, but it does not properly prevent the external site from modifying security-critical properties of the window.opener object, such as the location property.

## Extended Description

When a user clicks a link to an external site ("target"), the target="\_blank" attribute causes the target site's contents to be opened in a new window or tab, which runs in the same process as the original page. The window.opener object records information about the original page that offered the link. If an attacker can run script on the target page, then they could read or modify certain properties of the window.opener object, including the location property - even if the original and target site are not the same origin. An attacker can modify the location property to automatically redirect the user to a malicious site, e.g. as part of a phishing attack. Since this redirect happens in the original window/tab - which is not necessarily visible, since the browser is focusing the display on the new target page - the user might not notice any suspicious redirection.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2022-4927: Library software does not use rel: "noopener noreferrer" setting, allowing tabnabbing attacks to redirect to a malicious page

## Modes of Introduction

**•** Architecture and Design: This weakness is introduced during the design of an application when the architect does not specify that a linked external document should not be able to alter the location of the calling page.

**•** Implementation: This weakness is introduced during the coding of an application when the developer does not include the noopener and/or noreferrer value for the rel attribute.

## Common Consequences

**•** Impact: Alter Execution Logic — Notes: The user may be redirected to an untrusted page that contains undesired content or malicious script code.

## Potential Mitigations

**•** Architecture and Design: Specify in the design that any linked external document must not be granted access to the location object of the calling page. (Effectiveness: N/A)

**•** Implementation: When creating a link to an external document using the <a> tag with a defined target, for example "\_blank" or a named frame, provide the rel attribute with a value "noopener noreferrer". If opening the external document in a new window via javascript, then reset the opener by setting it equal to null. (Effectiveness: N/A)

**•** Implementation: Do not use "\_blank" targets. However, this can affect the usability of the application. (Effectiveness: N/A)

## Applicable Platforms

**•** JavaScript (Class: None, Prevalence: Often)

## Demonstrative Examples

**•** There are two ways that this weakness is commonly seen. The first is when the application generates an <a> tag is with target="\_blank" to point to a target site: