Cross-Site Scripting

1 min

Cross-site scripting (XSS) is a subtype of injection attack specific to the web. In its most basic form, the user's inputs are displayed in a format where a victim's web browser interprets it as JavaScript, which it executes.

Most types of XSS pass through the web server, but some more advanced types occur entirely within a victim's browser.

The most basic form is Reflected XSS, which can occur when a website displays a page echoing the user's input. Search engines, for example, typically display the string you searched for at the top of the page. If that string is a script and the site is vulnerable, the browser would run that script.

A more dangerous form is Stored XSS. Like Reflected XSS, it involves the user's input being displayed as part of a webpage, but stored XSS occurs when that user's input is stored on the server. For example, a vulnerable social media site could show a post with XSS embedded in it to many people.

DOM-based XSS is entirely client-side and involves hijacking a browser's Document Object Model (DOM), which is used to parse webpages. It is considered the most complicated form to understand, and details are beyond the scope of this lesson.

Regardless of the type, the basic way to prevent XSS is the same as any other type of injection – don't trust the user's input. Sanitize it, use language-specific features to ensure it doesn't get interpreted as code, etc.