[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@7906180aeb114030baa2ea359c9ff2aa?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for DOM-Based Cross-Site Scripting.**

DOM-based cross-site scripting is the de facto term for XSS bugs caused by active browser-side content on a page, typically JavaScript, obtaining user input and then doing something dangerous with it, resulting in the execution of injected code. This document only covers JavaScript bugs that result in XSS.

The DOM, or Document Object Model, is the structural format used in browsers to represent documents. The DOM allows dynamic scripts such as JavaScript to refer to document components such as a form field or a session cookie. The DOM is also used by the browser for security purposes, such as preventing scripts from obtaining session cookies for other domains. A DOM-based XSS vulnerability can occur when active content, such as a JavaScript function, is modified by a specially crafted request, allowing an attacker to control a DOM element.

Please click on this URL to perform this lab <http://wstg.alnafi.com/>