[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@e5f255ac90b24c9ab0c9f41af8e3c1ad?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for JavaScript Execution**

A JavaScript injection vulnerability is a subtype of cross-site scripting (XSS) that allows the attacker to inject arbitrary JavaScript code into the victim's browser. This vulnerability can have a variety of consequences, such as the disclosure of a user's session cookies, which could be used to impersonate the victim, or, more broadly, it can allow the attacker to modify the page content or application behavior seen by the victims.

JavaScript injection vulnerabilities can occur when the application does not properly validate user-supplied input and output. Because JavaScript is used to dynamically populate web pages, the injection takes place during the content processing phase and thus affects the victim.

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

Here’s an example of Testing for JavaScript Execution

