[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@e3cc13c5a7b54c0293d490cc7754173d?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for HTML Injection**

HTML injection is a type of injection vulnerability in which a user has control over an input point and can inject arbitrary HTML code into a vulnerable web page. This vulnerability can have a variety of consequences, such as exposing a user's session cookies, which could be used to impersonate the victim, or, more broadly, allowing the attacker to modify the page content seen by the victims.

When user input is not properly sanitized and the output is not encoded, this vulnerability occurs. With an injection, an attacker can send a malicious HTML page to a victim. Because the targeted browser is unable to distinguish (trust) legitimate from malicious parts of the page, it will parse and execute the entire page in the victim's context.

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

Here's an example of Testing for HTML Injection:

