[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@0a9090f25e4945c7879bb0d00c1696bb?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for CSS Injection**

A CSS Injection vulnerability allows an attacker to inject arbitrary CSS code into the context of a trusted website, which is then rendered inside the victim's browser. The severity of this type of vulnerability varies depending on the CSS payload supplied. This could result in cross-site scripting or data exfiltration.

This vulnerability occurs when the application allows user-supplied CSS to interfere with the legitimate stylesheets of the application. Injecting code into the CSS context may give an attacker the ability to execute JavaScript or extract sensitive values using CSS selectors and functions that can generate HTTP requests. Allowing users to customize pages by supplying custom CSS files is a significant risk in general.

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

Here’s an example of testing for CSS Injection:

