[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@d8c56729ceee4222935fc5805c755c50?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for Stored Cross-Site Scripting**

The most dangerous type of Cross Site Scripting is Stored Cross-site Scripting (XSS). Web applications that allow users to save data may be vulnerable to this type of attack. The examples in this chapter show stored cross-site scripting injection and related exploitation scenarios.

Stored XSS occurs when a web application collects potentially malicious user input and stores it in a data store for later use. The stored input is not properly filtered. As a result, the malicious data will appear to be part of the website and will run within the user's browser with the web application's privileges. Because this vulnerability usually involves at least two requests to the application, it is also known as second-order XSS.

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