[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@ee6b524b252b4f43aaff1f04ff14e8b3?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for Session Fixation**

The insecure practice of retaining the same session cookie value before and after authentication allows for session fixation. When session cookies are used to store state information before login, such as when adding items to a shopping cart before authenticating for payment, this is common.

In the generic exploit of session fixation vulnerabilities, an attacker can obtain a set of session cookies from the target website without first authenticating. The attacker can then employ a variety of methods to force these cookies into the victim's browser. If the victim later authenticates at the target website without refreshing the cookies, the attacker's session cookies will be used to identify the victim. The attacker can then pretend to be the victim.

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