[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@e905d907bb6349fcbf7951a24015beb3?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Testing for Weak Transport Layer Security.**

Information sent between the client and the server must be encrypted and protected to prevent an attacker from reading or modifying it. This is most commonly accomplished through the use of HTTPS, which employs the Transport Layer Security (TLS) protocol, which is a replacement for the older Secure Socket Layer (SSL) protocol. TLS also allows the server to show the client that they have connected to the correct server by displaying a trusted digital certificate.

Over the years, a large number of cryptographic flaws in the SSL and TLS protocols, as well as the ciphers they employ, have been discovered. Furthermore, many of these protocols' implementations have been found to have serious flaws. As a result, it is critical to ensure that sites not only implement TLS, but that they do so securely.

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

Here’s an example of a Test for Weak Transport Layer Security.  
