[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@2a9d73c8daeb41758a4fdbf65f774453?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Web Fingerprinting**

Web server fingerprinting is the process of determining the type and version of the web server on which a target is running. While automated testing tools frequently include web server fingerprinting, researchers must understand the fundamentals of how these tools attempt to identify software and why this is useful.

Accurately determining the type of web server on which an application runs allows security testers to determine whether the application is vulnerable to attack. Servers running older versions of software without up-to-date security patches, in particular, are vulnerable to known version-specific exploits.

Banner grabbing, eliciting responses to malformed requests, and using automated tools to perform more robust scans that use a combination of tactics are all techniques used for web server fingerprinting. All of these techniques operate on the same fundamental premise. They are all attempting to elicit some sort of response from the web server, which can then be compared to a database of known responses and behaviors and thus matched to a known server type.

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

Here’s A Picture showcasing the results of a typical Network Fingerprinting Command

