[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@c034a0e350044319a5fbfcf1f3109132?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Testing for HTTP Splitting Smuggling**

This section shows examples of attacks that take advantage of specific features of the HTTP protocol, either by exploiting weaknesses in the web application or by exploiting differences in how different agents interpret HTTP messages. This section will look at two attacks that target specific HTTP headers:

1. HTTP smuggling
2. HTTP splitting

The first attack takes advantage of a lack of input sanitization, allowing an intruder to insert CR and LF characters into the application response headers and split that response into two separate HTTP messages. The attack's goal can range from cache poisoning to cross-site scripting.

The attacker uses the fact that some specially crafted HTTP messages can be parsed and interpreted differently depending on the agent that receives them in the second attack. HTTP smuggling necessitates some understanding of the various agents that handle HTTP messages (web server, proxy, firewall), and will thus be included only in the gray-box testing section.

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