## HTTP Request Smuggling Prevention

Preventing HTTP request smuggling attacks generally is no easy task, as the issues causing request smuggling vulnerabilities often live within the web server software itself. Thus, it cannot be prevented from within the web application. Furthermore, web application developers might be unaware of underlying quirks that exist in the web server which might cause HTTP request smuggling vulnerabilities, such that they have no chance of preventing them. However, there are some general recommendations we can follow when configuring our deployment setup to ensure that the risk of HTTP request smuggling vulnerabilities is as minimal as possible, or at least the impact is reduced:

* Ensure that web server and reverse proxy software are kept up-to-date such that patches for security issues are installed as soon as possible
* Ensure that client-side vulnerabilities that might seem unexploitable on their own are still patched, as they might become exploitable in an HTTP request smuggling scenario
* Ensure that the default behavior of the web server is to close TCP connections if any exception or error occurs on the web server level during request handling or request parsing
* If possible, configure HTTP/2 usage between the client and web server and ensure that lower HTTP versions are disabled. We will discuss in the upcoming sections why this is beneficial