Introduction

The Docker in the RESOURCE section contains a default installation of an Apache 2.4 HTTP server on Ubuntu Linux. No configuration for hardening has been made so far.

You do not have direct access to the Docker's file system. However, calling the URL xxx [URL and Port, depends on integration in HL] in your browser returns a simple graphical interface of an editor, in which the configuration of the web server can be extended. Within this editor you can

- view the enabled and loaded modules
- edit the configuration file
- save the configuration, which triggers a syntax check by running apachectl checkconfig
- view the output of the syntax check
- revert changes you have made
- download the configuration file for submission

Goal and Tasks

The web server must now be hardened. Expand the configuration in the scope of the pre-configured virtual host to meet the requirements below. Please comment your edits in the configuration file with the respective requirement number. Hardening Requirement

- R1 - For better protection against DoS attacks, the maximum number of header fields in HTTP requests must be limited to 50. In addition, the maximum size for one header field must be limited to 1024 bytes.
- R2 - The maximum size for the request body must be limited to 2 MB.
- R3 - The timeout for TCP packets when reading requests from clients must be limited to 20 seconds.
- R4 - There must be a scope with the URL /admin and access to this URL must be restricted to private IP ranges (A/B/C class) only.
- R5 - Client-side MIME type sniffing must be avoided by setting a response header indicating that type settings in Content-Type headers should be followed.
- R6 - Client-side click-jacking attacks must be prevented by setting a response header instructing browsers to restrict content framing to frames from the same origin as the page itself only.
- R7 - The already enabled module mod evasive increases DoS protection. For testing purposes, the localhost should be excluded from the settings of this module. However, this configuration must be conditional on the presence of the module.
- R8 - Support of HTTP request methods must be limited to GET, POST, HEAD and OPTIONS for directory /var/www/html.
- R9 - Support of HTTP 1.0 protocol must be disabled to prevent session hijacking.

Submission

Download the configuration with your edits in the integrated editor, check that it is the version with your latest changes and submit the configuration file.