e) Directory Traversal

Directory traversal makes it possible for the client to access files outside of the www-path directory. This is commonly done by using the / character. Some clients has added prevention to this directly in their browser. We tried to access a file just outside the root by adding /../../ in the address bar, it worked when using postman, but did not work in a browser like opera.

Since this is an obvious vulnerability, it must be patched, since not doing so can let the attacker easily access password and other important files on the server.

One way of doing so can be to filter out paths that contains the sequence /../ . Also, we must think to alternative ways of writing / or \. '%255c' is a Unicode-encoding of \. So the sequence %255c..%255c must also be filtered.

A different way of blocking access to other files is to constrain the access to a list of known paths. The server must then check if the requested file is one of them. If it is not, simply block the request.