To secure a web server against URL manipulation attacks, it is necessary to keep a watch on vulnerabilities and regularly apply the patches provided by the web server's publisher.

Moreover, a detailed configuration of the web server helps keep users from surfing on pages they are not supposed to have access to. The web server should therefore be configured as follows:

* Prevent the browsing of pages located below the website's root (*chroot*mechanism);
* Disable the display of files present in a directory that does not contain an index file ("Directory Browsing");
* Delete useless directories and files (including hidden files);
* Make sure the server protects access to directories containing sensitive data;
* Delete unnecessary configuration options;
* Make sure the server accurately interprets dynamic pages, including backup files (*.bak*);
* Delete unnecessary script interpreters;
* Prevent HTTP viewing of HTTPS accessible pages.