Vulnerability analysis
The highfashion application lets you set your favourite pose with a cookie, and then it lets you see such a pose again through the "viewfav.php" page. The cookie is something like "favposeid=magnum". Given a pose id (e.g., "magnum"), the "viewfav.php" page retrieves the corresponding pose name and image file name through a MySQL query, which is not injectable. On the other hand, the pose description file name is constructed from the pose id with the following concatenation: "descr/" . $poseid . ".txt". Then, the description si retrieved via the get_file_content() PHP function, and displayed on page. This leaves space for a non-blind path traversal attack.