SecurityRules

fopen

3 reasons to not use fopen to read urls:

- if the url is not syntax-checked, one can read local files
- if the websever is behind a firewall (intranet) and restricted to use a proxy, it does simply not work (don't think that this is a rare case!)
- if the websever is behind or part of a firewall (intranet or dmz) one can read contents of the internal network (http://localhost:631 to get cups managemnent for example).

exec, system & others

Calls to execute external programs should be avoided if possible. If it is not possible to avoid them, all parameters, input and output should be checked for consistency.
Example attack:
{CODE(ln=>0,colors=>phpsource),wrap=>0,wiki=>1}
$a=$_REQUEST'input';
passthru("/bin/echo $a");
{CODE}
if someone adds ?input=bla;/bin/ls to the url, then he can read the local directory.