This sandbox starts off with a syntax error ('!' is used instead of 'not'). It uses a blacklist approach with a custom global and local namespace. The input file is searched for any strings in the blacklist, and then run.