This sandbox uses a blacklist approach. The sandbox is first run and askes for the name of the input file. The file is read in and searched for any strings matching those in the blacklist. The unique thing about this sandbox is that before the code is run code is injected to the beginning to set all sys modules to ‘None’. The code is then run.