GitHub Link: https://github.com/piyushbjadhav/Sandbox

Summary:

The candidate sandbox enforces restrictions on builtins. It whitelist all safe builtins to run untrusted code with limited functionality. Moreover, resource assigned to sandbox are also limited like number of file objects, number of processes, memory space etc.

Program Bugs

The resource limitation RESOURSCELIMIT_NOFILE = (4, 4) is used to set all resource limits whether it's for number of processes or address space.

The program restricts "_" character. Using hex code of underscore can allow attack-1.py to give segmentation fault. These memory errors can result into privilege escalation and other system calls.