GitHub: https://github.com/Justinvalcarcel/CS9163

Summary:

The candidate sandbox use blacklisting approach to remove dangerous builtins. This approach is not effective for running untrusted code in sandbox. With this approach, there is a possibilty to leave certain builtin functions which can cause undesirable behaviour of sandbox when running untrusted code.

Vulnerability:

The candidate sandbox blacklists very few builtins. Upon close scrutiny an attacker can figure out what other builtins are allowed by checking with dir() method. Moreover attacker can run exec and eval functions if found in any of builtin dictionaries.

‘attack-1’.py - The candidate sandbox is not able manage memory over usage. The memory management is poor. Using attack1.py program crashes and causes segmentation fault. These type of memory errors can result into privilege escalation and other system level attacks