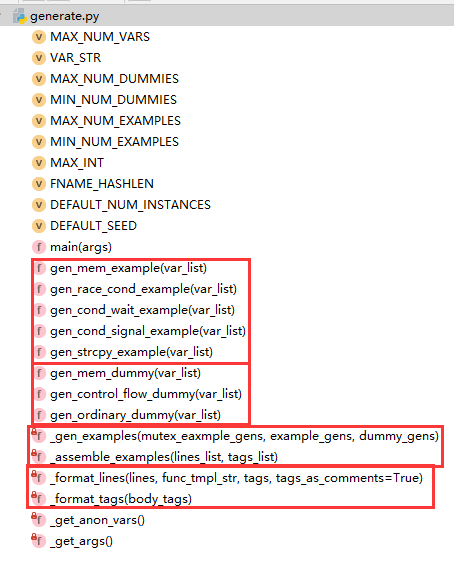
# Generate C files with designed flaws

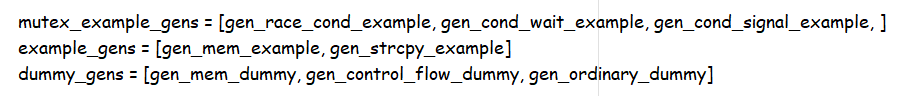
### Code refactoring redesign code logic

For generating c files with new designed flaws, the generate.py is the most important file. Using the method of multiway merging, refactor the main process of generating code files. The code outline is as follows:



For each gen\_xx\_example or gen\_xx\_dummy function, return a list of code blocks and a coresponding list of tag blocks. The code lines in each block are inseparable.

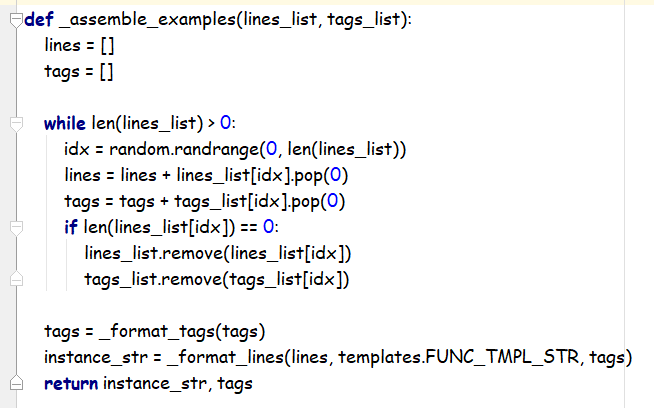
In the main function, three generator lists are created with those gen functions – mutex\_example\_gens, example\_gens and dummy\_gens.



Then it calls the function gen\_examples, using these generator lists to randomly generate the two lists of code blocks and tag blocks.



The lists are transmitted to assemble\_example function in which the blocks are assembled and formatted into one c file. While assembled, the blocks are mixed logically into one block by multiway merging.

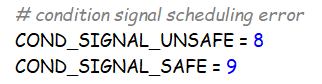


By this way, the templates of vulnerabilities and dummy statements are easy to add and modify, implementing mixed generation of multiple vulnerabilities and dummy statements as well as realizing the interpolation of multiple vulnerabilities and dummy statements on the premise of logical conformity.

### The details of each flaw template

#### Signal scheduling

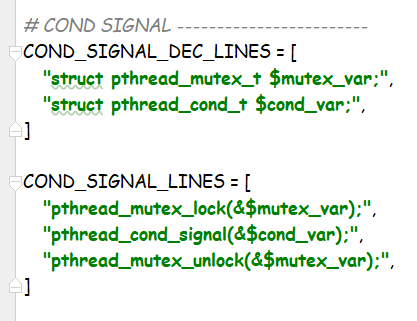
Tag



Generate function

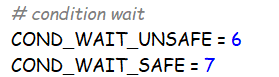


Template



#### Conditional var wait with while-loop

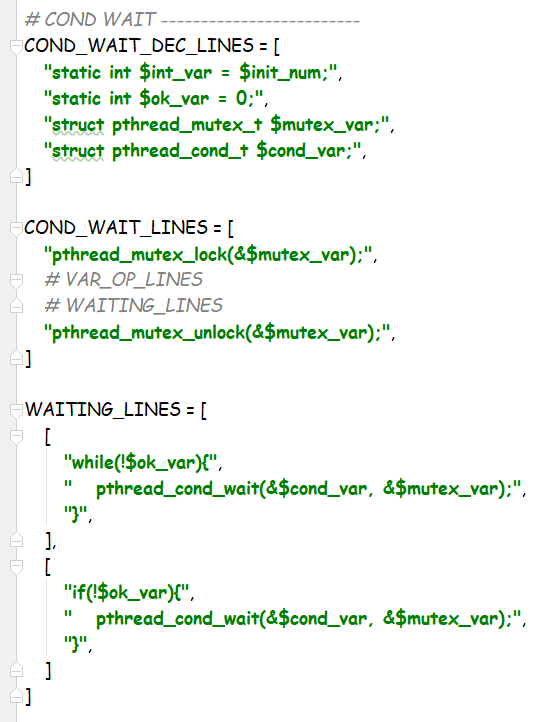
Tag



Generate function

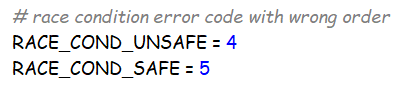


Template



#### Mutex lock

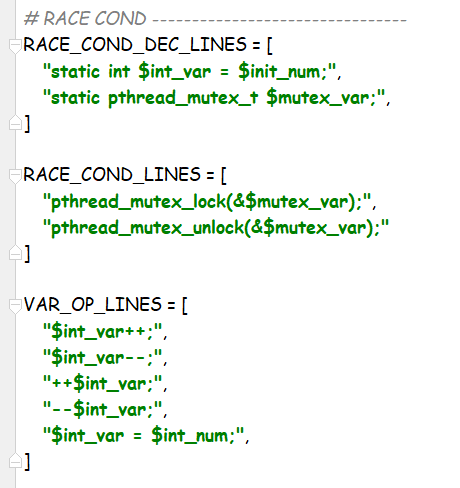
Tag



Generate function

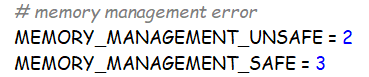


Template



#### Malloc

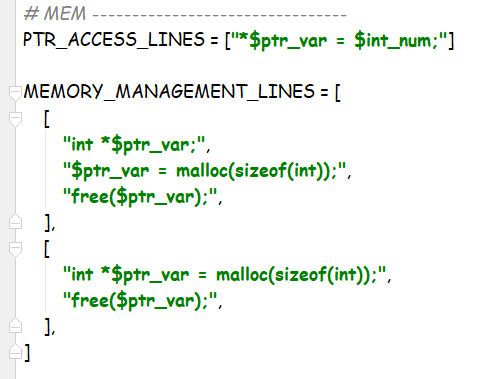
Tag



Generate function

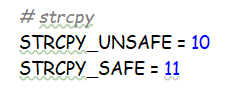


Template



#### String copy buffer overflow

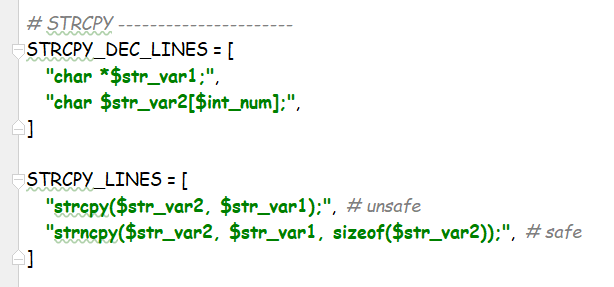
Tag



Generate function



Template



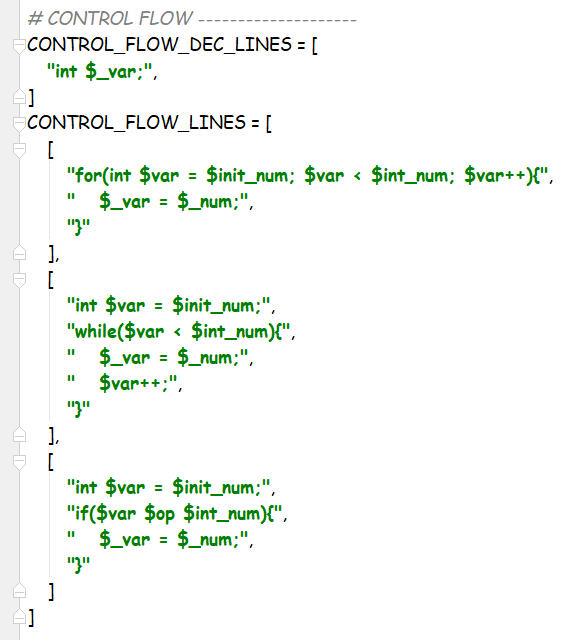
### Dummy templates

#### Control flow dummy

Generate function



Template

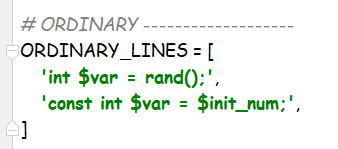


#### Ordinary dummy

Generate function

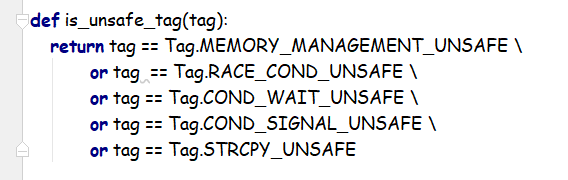


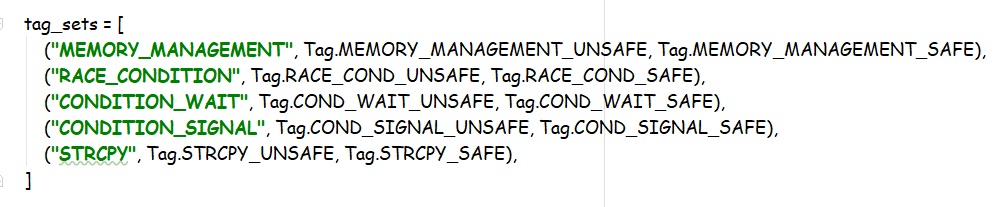
Template



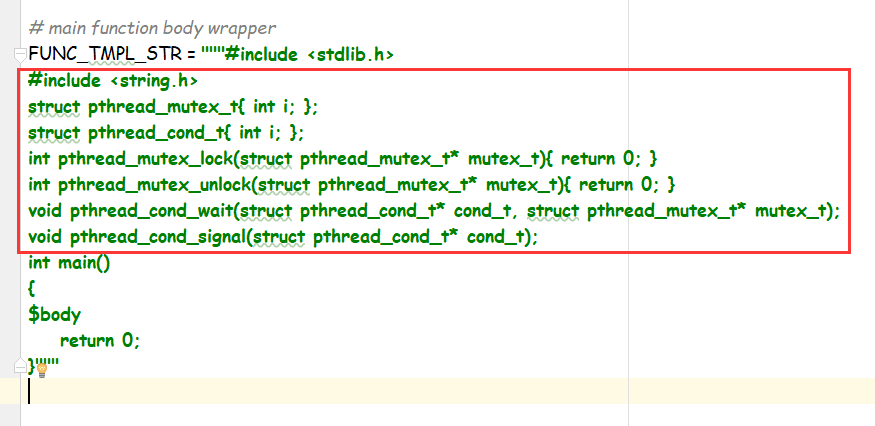
### Other

Change corresponding functions in other python files





For static check tools, there are no available thread module, for which declarations and definitions are added to make it through.



### Result example

