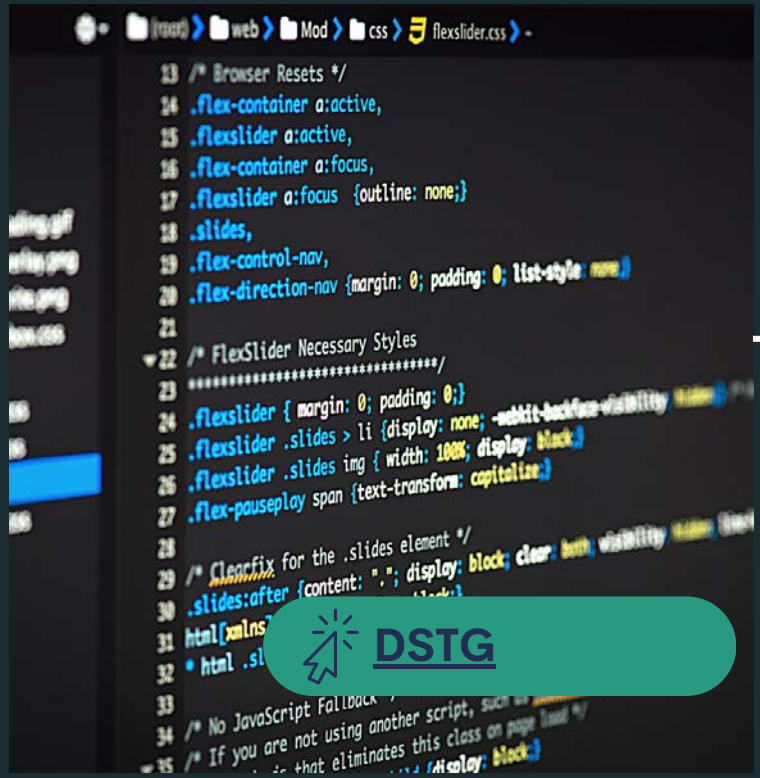
PROBLEM 6



A NOVEL TOOL TO DETECT SOFTWARE VULNERABILITIES

Race conditions are severe software vulnerabilities that tend to be highly non-deterministic and chaotic. Due to these complexities, locating race conditions with dynamic techniques such as fuzzing can be challenging. Furthermore, since they can cause application and system crashes and inadvertent data poisoning, experimenting with race-condition vulnerabilities on active Defence platforms can be undesirable. Can we develop a new software tool and source code package capable of ingesting a compiled binary and outputting identified problematic statements within the program alongside a comparison to existing approaches?