DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Taller GreyBox Fuzzing

24/10/2022 Ingeniería de Software II

Integrante	LU	Correo electrónico
Schiavinato, Franco	586/14	francocschiavinato@gmail.com
Schiavinato, Mauro	299/19	maurolschiavinato@gmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2610 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (++54 +11) 4576-3300
https://exactas.uba.ar

Introducción

Los tests del ejericio X se encuentran en el archivo *ejercicioX.py*. Al ejercutar el código *magicfuzzer.py* corre el ejercicio 4 y 5 y genera los datos para la tabla.

Aclaraciones

Ejercicio 3

Para el ejericio 3 utilizamos el mapa *_keys* para guardarnos los PathId de cada coverage y en *_frequency* para guardarnos la cantidad de apariciones de un individuo.

Luego para la selección de ruleta, tenemos un puntero que empieza entre 0 y y toda la suma de todas las energías. Y para saber en que individuo cayó de la ruleta vamos restando elemento por elemento las energías hasta que esté dentro del rango de energía de un individuo y quiere decir que cayó inicialmente en ese rango de la ruleta.

Ejercicio 4

Corrimos el fuzzer hasta obtener todo el cubrimiento de lineas múltiples veces y obtuvimos:

#Campaña	#Cantidad de inputs necesarios
1	11233
2	2725
3	1035
4	2575
5	4122

Ejercicio 5

Ahora colocamos un límite de 5000 iteraciones para ejecutar el fuzzer y también habilitamos para que las líneas cubiertas contaran cualquier función y no exclusivamente alguna en particular. Obtuvimos la siguiente tabla:

#Campaña	#Líneas Cubiertas
1	123
2	98
3	123
4	398
5	97