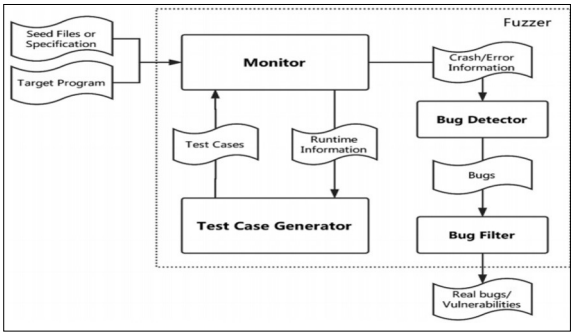

Danusan PREMANANTHAN


Aynkaran SUNDRALINGAM

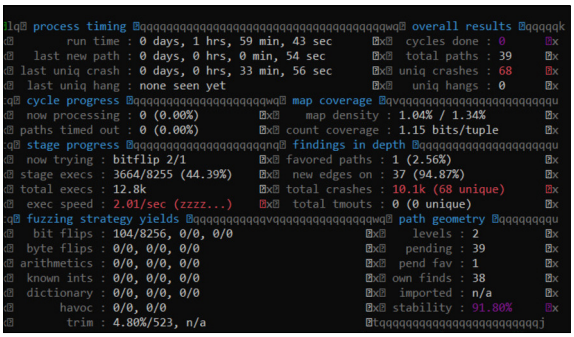

Kevin Moro

Fuzzing .NET

XML-Parser Fuzzing



Fuzzing Prozess
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8371326



AFL Screen
Eigene Darstellung

Einleitung: Fuzzing ist eine Form von Software-Testing bei dem ein Programm mit zufällig generierten Daten gefüttert wird. Das Ziel dieser Tests ist es ein abnormales Verhalten des Programmes zu finden das man mit anderen Testmethoden nicht finden würde. Diese Technik ist für das Testen eines XML-Parsers sehr hilfreich, da man so auf Testszenarien/Programminputs kommt, die man sonst nicht in Betracht ziehen würde.

Ziel der Arbeit: Das Ziel dieser Arbeit ist es, verschiedene Fuzzing Tools mit den dazugehörigen Tool-Chains für die .NET Plattform zu recherchieren und danach auch zu evaluieren, mit besonderer Aufmerksamkeit auf die Eignung der Tools für das Testen von einem XML-Parser, welchen wir von nxt Engineering zur Verfügung gestellt bekommen haben. Ebenfalls ein Teil der Arbeit ist die Evaluation des neuen, von Microsoft entwickelten, Tool OneFuzz.

Ergebnis: Um dieses Ziel zu erreichen, wurden zuerst die theoretischen Eigenschaften verschiedener Fuzzing-Tools analysiert. In einem zweiten Schritt wurden die vielversprechendsten Tools in Betrieb genommen und praktisch an einem XML-Parser getestet.
Ein Resultat dieser Arbeit ist die Tool-Chain die sich besonders gut eignet, um XML-Parser auf .NET Umgebung zu testen und auf was man bei der Einrichtung sowie dem Testen besonders achten muss. Des Weiteren wurden während dem Testen des XML-Parsers von nxt Engineering nur wenige kleine Programmierfehler gefunden.