



Danusan
PREMANAN
THAN

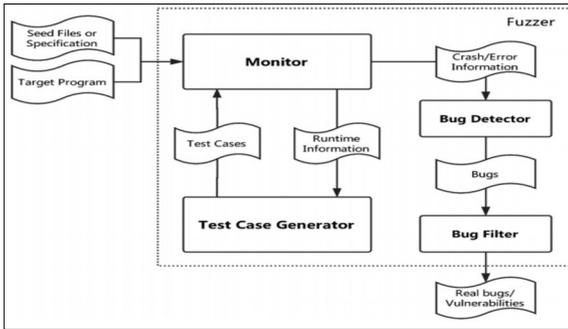


Aynkaran
SUNDRALIN
GAM



Kevin
Moro

Fuzzing .NET XML-Parser Fuzzing



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 Testscenarien/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.

Fuzzing Prozess

<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8371326>

```

|a| process timing |a| overall results |a|
|  run time : 0 days, 1 hrs, 59 min, 43 sec |  cycles done : 0 |  |
|  last new path : 0 days, 0 hrs, 0 min, 54 sec |  total paths : 39 |  |
|  last uniq crash : 0 days, 0 hrs, 33 min, 56 sec |  uniq crashes : 68 |  |
|  last uniq hang : none seen yet |  uniq hangs : 0 |  |
|a| cycle progress |a| map coverage |a|
| now processing : 0 (0.00%) |  map density : 1.04% / 1.34% |  |
| paths timed out : 0 (0.00%) |  count coverage : 1.15 bits/tuple |  |
|a| stage progress |a| findings in depth |a|
| now trying : bitflip 2/1 |  favored paths : 1 (2.56%) |  |
| stage execs : 3664/8255 (44.39%) |  new edges on : 37 (94.87%) |  |
| total execs : 12.8k |  total crashes : 10.1k (68 unique) |  |
| exec speed : 2.01/sec (zzzz...) |  total touts : 0 (0 unique) |  |
|a| fuzzing strategy yields |a| path geometry |a|
| bit flips : 104/8256, 0/0, 0/0 |  levels : 2 |  |
| byte flips : 0/0, 0/0, 0/0 |  pending : 39 |  |
| arithmetics : 0/0, 0/0, 0/0 |  pend fav : 1 |  |
| known ints : 0/0, 0/0, 0/0 |  own finds : 38 |  |
| dictionary : 0/0, 0/0, 0/0 |  imported : n/a |  |
| havoc : 0/0, 0/0 |  stability : 91.80% |  |
| trim : 4.88%/523, n/a |  |  |
  
```

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.

AFL Screen

Eigene Darstellung