



## Udvidelse af fuzzer-frameworket sulley:

### Baggrund:

Fuzzer er et relativt nyt begreb indenfor it-sikkerhed. Fuzzing går ud på at sende en række mere eller mindre vilkårlige input til en applikation med henblik på, at få programmet til at fejle. De fejl der findes ved brug af en fuzzer, kan i visse tilfælde udnyttes til at eksekvere arbitrær kode.

### Opgaven:

Der findes i forvejen en række rigtig gode fuzzer-produkter såsom Peach, Spike og Sulley. Sulley er den fuzzer der lader til at have størst potentiale, og derfor ønsker vi at udbygge denne funktionalitet.

- Generelle fejl: Fuzzer-frameworks har ofte til hensigt at finde input der får et program til at lave en segmentation fault. Nogle programmer, så som webapplikationer, fejler programmet ikke ved segmentation faults, men med fejl-sider. Lav en plugin til fuzzeren, der kan finde og genere injektionsstrengte.
- Fuzzer-regler: De fleste fuzzere benytter et sprog til at definere og afgrænse inputtet til den applikation, der skal fuzzes. Disse regler er afgørende for, hvor godt resultatet bliver. Vi ønsker et værktøj, der kan assistere med udarbejdelsen af disse regler. Eksempelvis kunne man forstille sig, at fuzzer-frameworket lytter til den normale brug af programmet og omskrev disse til et regelsæt. Disse regelsæt kunne så videreudvikles til det endelige sæt regler.

### Krav:

Opgaven skal skrives i Python.

Det er et krav fra opgavestillers side at de studerende underskriver en NDA.

### Bidrag:

- Forsvaret bidrager med hostning af opgaven
  - Subversion
  - TracBackup skal selv varetages af de studerende
- Møder med slutbrugere fra Forsvaret