INFO M227 Analyse de programmes pour la cybersécurité

Assistant : Gonzague Yernaux (gonzague.yernaux@unamur.be)

Travail individuel : Fuzzing

Aperçu général du travail

Dans ce travail, il vous est demandé de construire un petit *fuzzer* qui soit capable d'attaquer un programme ou une fonction de votre choix. La contrainte est que le *fuzzer* doit utiliser une approche basée sur une grammaire et des mutations. Le but est de démontrer l'utilité du *fuzzing* en pratique pour la cybersécurité.

Délivrables

Il est attendu de vous que vous délivriez sur WebCampus, dans l'espace prévu à cet effet, une archive en format standard (`.zip`, `.rar`, `.7z` ou autre) contenant :

- d'une part, **le code source de votre *fuzzer*** ;
- d'autre part, **un rapport au format PDF ou écrit à la main.**

Le rapport explicitera, de façon claire, formelle, précise et non-ambigüe la marche à suivre pour exécuter votre programme, ainsi que toute information utile que vous souhaiteriez nous communiquer : fonctionnalités supplémentaires, techniques utilisées, chapitres du *fuzzing book* lus de votre côté et utilisés, bugs éventuels trouvés, …

Cotation

Ce travail vaudra pour 25 % de la note du cours. Les éléments principaux de cotation sont : la précision et l'adéquation du programme fourni, l'utilité du *fuzzer* dans un contexte de sécurisation d'un programme, l'élégance des solutions apportées, le taux d'investissement dans le travail (allant du minimum requis au dépassement des attentes).

Échéance

Le travail est à rendre pour le 15 janvier 2024 **à 23h59**.

Consignes plus précises

Votre programme devra être réalisé sur base du code Python fourni par le *Fuzzing Book*. Vous pouvez choisir d'utiliser une autre librairie de *fuzzing* ; dans ce cas, prévenez Gonzague qui validera votre choix avec vous.

Votre *fuzzer* doit utiliser une approche à base d'une grammaire et de mutations. Le programme à attaquer est de votre choix : à vous de choisir une API, un serveur Web, ou simplement une fonction à tester. Les tests peuvent être *white*, *grey* ou *black* box, au choix (à documenter dans le rapport) !

Des questions ?

Privilégiez le forum Questions-réponses sur WebCampus.

Bon travail !