□□ Index — 05 — Testing & Fuzzing (Trail of Bits)

05 — Testing & Fuzzing (Trail of Bits)

> Index des skills regroupés dans ce livre. Clique sur un skill pour ouvrir sa fiche.

16 skills documentés.

Skill	En une phrase
address-sanitizer	AddressSanitizer (ASan) est un "détecteur de fumée" qu'on greffe au code C/C++ pour repérer en temps réel les bugs mémoire…
aflpp	AFL++ est un "fuzzer" (machine à tester) qui bombarde un programme C/C++ avec des milliers d'entrées aléatoires en parallèle sur…
atheris	Atheris est un fuzzer pour Python : il bombarde ton code Python avec des entrées aléatoires pour faire surgir les exceptions non…
cargo-fuzz	cargo-fuzz est l'outil officiel pour fuzzer un projet Rust : il bombarde tes fonctions Rust avec des entrées aléatoires pour…
constant-time-testing	Le constant-time testing vérifie qu'une opération cryptographique met toujours exactement le même temps à s'exécuter — sinon un…
coverage-analysis	L'analyse de couverture mesure quelles lignes de ton code ont vraiment été exécutées par les tests/fuzzers — pour repérer les…
fuzzing-dictionary	Un dictionnaire de fuzzing, c'est une liste de "mots magiques" qu'on donne au fuzzer pour qu'il sache de quoi il parle (mots-clés…

Skill	En une phrase
fuzzing-obstacles	Recueil de techniques pour contourner les "blocages" qui empêchent un fuzzer d'avancer (checksums, horloges aléatoires,...
harness-writing	Le harness (ou "harnais") c'est la petite fonction d'entrée qu'on écrit pour brancher un fuzzer à son code : un mauvais harness =...
libafl	LibAFL est une "boîte à outils" en Rust pour construire ton propre fuzzer sur mesure quand les fuzzers tout faits (libFuzzer,...
libfuzzer	libFuzzer est un "fuzzer" intégré au compilateur LLVM qui bombarde une fonction C/C++ avec des milliers d'entrées aléatoires pour...
ossfuzz	OSS-Fuzz est un service gratuit de Google qui fait tourner du fuzzing 24h/24 sur les projets open source critiques pour trouver...
property-based-testing	Le property-based testing teste des **propriétés universelles** ("encoder puis décoder doit redonner la valeur d'origine") au...
ruzzy	Ruzzy est un fuzzer pour Ruby (créé par Trail of Bits) : il bombarde ton code Ruby et tes extensions C de Ruby avec des entrées...
testing-handbook-generator	Méta-skill qui lit le "Testing Handbook" de Trail of Bits (appsec.guide) et génère automatiquement de nouvelles skills Claude...
wycheproof	Wycheproof est une énorme collection de "pièges crypto" maintenus par Google : des entrées tordues, déjà connues pour casser les...

Revision #2
Created 2026-05-11 21:17:47 UTC by thymon
Updated 2026-05-11 21:36:00 UTC by thymon