ossfuzz

ossfuzz

> *Catalogue généré le 2026-05-11*

En une phrase

OSS-Fuzz est un service gratuit de Google qui fait tourner du fuzzing 24h/24 sur les projets open source critiques pour trouver des bugs avant les hackers.

Quand l'utiliser

- Inscrire un projet open source important dans le programme de fuzzing continu de Google.
- Mettre en place une infrastructure de fuzzing continu pour ton équipe.
- Quand un projet est utilisé par beaucoup de monde et mérite un audit continu (curl, OpenSSL, etc.).
- Pour automatiser le fuzzing dans un pipeline CI/CD.
- Pour publier des coverage reports automatiques.

Comment l'invoquer

- **Slash command** : `/ossfuzz`
- **Phrases déclencheurs (texte)** : "continuous fuzzing", "OSS-Fuzz enrollment", "Google fuzzing service"
- **Auto-invocation** : Sur demande explicite

Description détaillée

OSS-Fuzz est un service open source de Google qui fournit gratuitement une infrastructure massive (des milliers de cœurs CPU) pour faire tourner du fuzzing en continu sur les projets open source qui acceptent de s'inscrire. L'idée : les projets critiques pour internet (curl, OpenSSL, SQLite, Linux kernel…) tournent 24h/24 sur les serveurs Google, et dès qu'un bug est trouvé, Google notifie les mainteneurs en privé pour corriger avant que ce soit public.

Pour rejoindre OSS-Fuzz, tu dois préparer trois fichiers : un `project.yaml` (metadata du projet), un `Dockerfile` (l'image avec les dépendances de build) et un `build.sh` (le script qui compile les fuzzers). Google fait passer tes harnesses à travers libFuzzer, AFL++, Honggfuzz et les sanitizers (ASan, UBSan, MSan). Si quelque chose crashe, tu reçois un rapport détaillé.

Les projets acceptés sont évalués selon leur "criticality score" (importance pour l'écosystème). Tu peux aussi héberger ton propre instance d'OSS-Fuzz pour tes projets privés — le code de base est open source. C'est devenu LE standard de l'industrie pour le fuzzing continu sérieux.

Pour aller plus loin

Pour les exemples concrets, options de configuration et patterns avancés, voir le SKILL.md original.

Source

- **Plugin** : `trailofbits/testing-handbook-skills`
- **Nom interne** : `ossfuzz`
- **Fichier** : `/home/thymon/.claude/plugins/cache/trailofbits/testing-handbook-skills/1.0.1/skills/ossfuzz/SKILL.md`

Revision #2
Created 2026-05-11 21:19:49 UTC by thymon
Updated 2026-05-11 21:37:24 UTC by thymon