burpsuite-project-parser

burpsuite-project-parser

> *Catalogue généré le 2026-05-11*

En une phrase

Permet de fouiller en ligne de commande dans les fichiers de projet de Burp Suite (un outil de test d'intrusion web très répandu chez les pentesters), pour retrouver des requêtes HTTP, des en-têtes ou des réponses suspectes.

Quand l'utiliser

- Tu as réalisé un audit de sécurité d'un site web avec Burp Suite et tu veux extraire des trouvailles précises de ton fichier `.burp`.
- Tu veux chercher un motif spécifique (mot-clé, regex) à travers des milliers de requêtes capturées.
- Tu prépares un rapport et tu dois retrouver toutes les réponses qui contiennent un certain en-tête (par exemple : `Set-Cookie` sans `Secure`).
- Tu veux automatiser l'exploration du trafic HTTP sans cliquer manuellement dans l'interface graphique de Burp.

Comment l'invoquer

- **Slash command** : `/burpsuite-project-parser` (ou `/burp-search`).
- **Phrases déclencheurs (texte)** : "search Burp project", "analyze .burp file", "extract findings from Burp", "dump proxy history".
- **Auto-invocation** : Sur demande explicite.

Description détaillée

Burp Suite est l'outil de référence pour auditer la sécurité des applications web : il se positionne comme un proxy entre ton navigateur et le serveur, et capture toutes les requêtes et réponses qui passent. À la fin d'une session, tu te retrouves avec un fichier `.burp` qui peut peser plusieurs giga-octets et contenir des dizaines de milliers d'échanges. Impossible à explorer à la main.

Ce skill ne lit pas le fichier directement (le format est propriétaire), mais s'appuie sur Burp Suite Professional et une extension officielle appelée `burpsuite-project-file-parser`. Une fois cette extension installée, le skill fournit un script wrapper qui te permet de lancer des recherches ciblées depuis le terminal — par exemple : « donne-moi toutes les réponses dont le code de statut est 500 », ou « trouve-moi toutes les requêtes qui contiennent le mot `password` dans leur corps ».

Le skill insiste fortement sur les filtres : récupérer l'historique complet d'un projet Burp peut renvoyer plusieurs giga-octets de texte qui saturent la console. Il préconise donc de toujours commencer par les en-têtes (petits, rapides à scanner) et de ne charger les corps de réponses qu'après avoir identifié les URLs intéressantes. Idéal pour extraire automatiquement des éléments de preuve à coller dans un rapport d'audit.

Pour aller plus loin

Pour les détails techniques, exemples et patterns spécifiques, voir le SKILL.md original.

Source

- **Plugin** : `trailofbits/burpsuite-project-parser`
- **Nom interne** : `burpsuite-project-parser`
- **Fichier** : `/home/thymon/.claude/plugins/cache/trailofbits/burpsuite-project-parser/1.0.0/skills/SKILL.md`

Revision #2
Created 2026-05-11 21:19:28 UTC by thymon
Updated 2026-05-11 21:37:06 UTC by thymon