C'est vrai que Burp est devenu un monstre à tout faire avec scanner de vulnérabilités, fuzzer, crawler, extensions... Y'a aussi Charles Proxy que j'aime bien mais qui pèse dans les 100 Mo et nécessite une JVM complète. Et même mitmproxy , pourtant réputé léger, a accumulé tellement de fonctionnalités qu'il faut lire 50 pages de doc pour comprendre comment l'utiliser.

Avec HTTP Breakout Proxy, il y a moins de features c'est vrai mais ça va plus vite et c'est gratuit. Maintenant, au niveau technique, le projet utilise l'interception MITM classique. Vous installez le certificat racine fourni par le proxy, et il peut déchiffrer le trafic HTTPS qui passe par lui. Ensuite, l'interface web affiche tout en temps réel via Server-Sent Events. Vous avez du filtrage par regex, du color-coding configurable pour repérer visuellement les requêtes importantes, et même des charts Gantt pour visualiser le timing des connexions...etc.

Que demande le peuple ? Ah oui, y'a aussi l'export vers curl ou Python requests, ce qui est pratique quand vous voulez rejouer une requête dans un script. Et bien sûr la possibilité de mettre la capture en pause pour analyser tranquillement ce qui s'est passé.

Voilà, c'est minimaliste mais ça marche hyper bien et quand on est pas un pro de la sécurité, c'est bien d'avoir des outils de ce style pour explorer un truc vite fait. Et merci à Lorenper pour le partage !

A découvrir ici !

Cet article peut contenir des images générées à l'aide de l'IA - J'apporte le plus grand soin à chaque article, toutefois, si vous repérez une boulette, faites-moi signe !

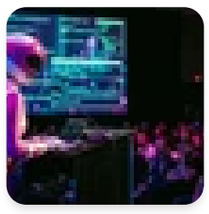
Articles récents

HA-Animated-cards – 67 cartes animées pour...

La Freebox HD complètement pwned...

Transformez votre Steam Deck en mini borne...

CrossPaste - Le presse-papier universel qui se...



Une hacktiviste déguisée en Pink Ranger suppri...

La clé magique qui déverrouille tous les...

Les métiers de la Cybersécurité et de l'Intelligence Artificielle