

[SOC] Cyberchef

Introduction

Cyberchef est un outil pour décoder, formater etc très utile en CTF ou dans les tâches quotidiennes.



Sources

- <https://gchq.github.io/CyberChef/>
- <https://kravensecurity.com/cyberchef-guide/#CyberChef>

Cyberchef API

Un projet a été réalisé, permettant d'exécuter des recettes via des call API (très pratique pour de l'automatisation :

- <https://github.com/gchq/CyberChef-server>

Pour l'installer (docker requis) :

```
git clone https://github.com/gchq/CyberChef-server && cd CyberChef-server && docker build -t cyberchef-server .
```

Pour lancer le serveur :

```
docker run -it --rm --name=cyberchef-server -p 3000:3000 cyberchef-server
```

Ensuite, par exemple, vous pourriez extraire des IPv4 d'un texte brut avec une simple requête curl :

```
curl -X POST -H "Content-Type: application/json" -d '{"input":"120[.]89[.]71[.]226 120[.]89[.]71[.]226:9090 aa",  
"recipe":[{"op":"Fang URL", "args":[true, false]}, {"op":"Extract IP addresses", "args":["IPv4", false]}]}'  
http://localhost:3000/bake
```

Revision #1

Created 16 June 2025 14:41:58 by Elieroc

Updated 16 June 2025 14:48:29 by Elieroc