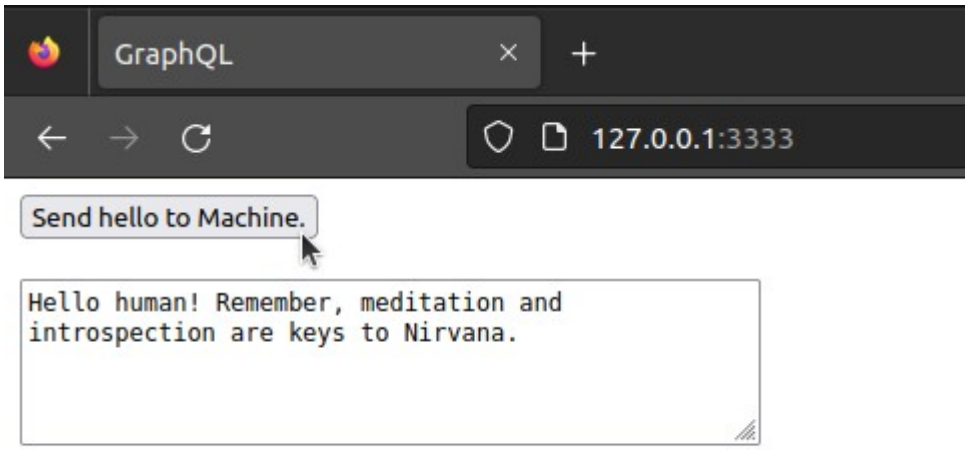
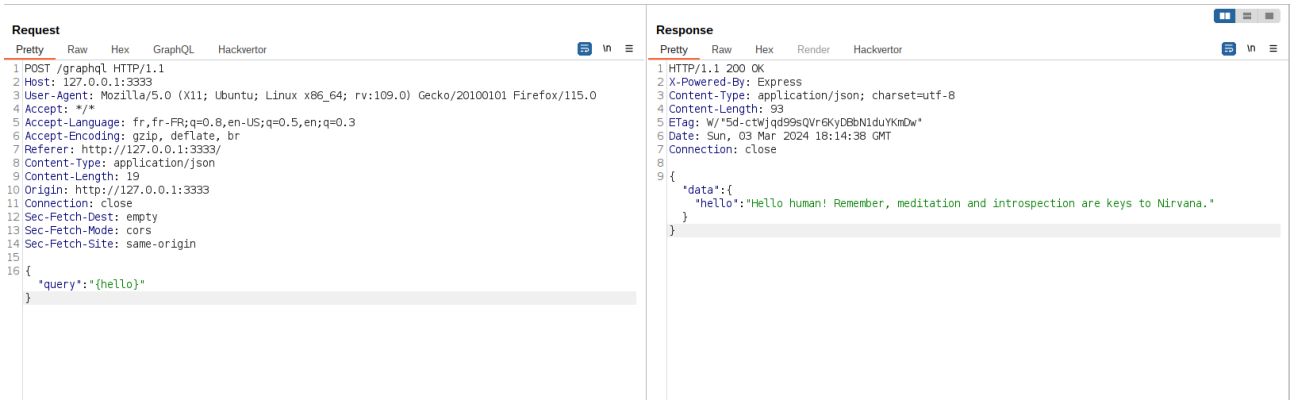
API Part 1

#1 Repérage

La page principale du challenge propose de dire bonjour à la machine. En cliquant sur la bouton, nous remarquons un message s'afficher dans la zone de texte.



Si l'on intercepte la requête en utilisant BurpSuite, nous voyons une requête **POST** vers */graphql*.



Le message de la machine contient le mot clef « **Introspection** » qu'il fallait réussir à relier à la techno de l'API qu'est **GraphQL**. Puis se renseigner sur le principe et ce que permet l'introspection d'une API GraphQL.

Ressources utiles :
- GraphQL.org
- Hacktricks – GraphQL
- PortSwigger – Use BurpSuite for GraphQL APIs
- YesWeHack - Exploiting GraphQL APIs

#2 Exploitation

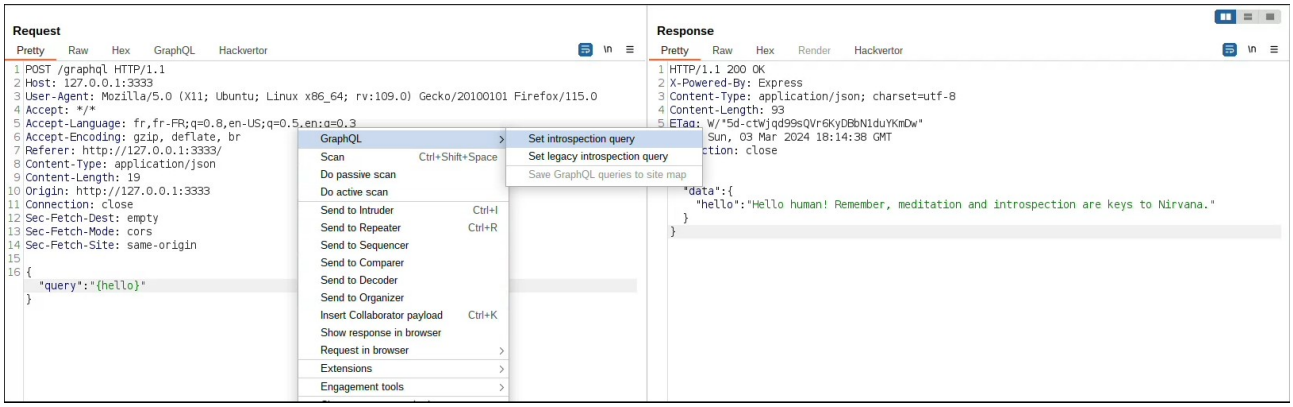
En fonction de vos recherches, plusieurs options s'offrent à vous. La première étant d'utiliser les fonctionnalités de BurpSuite liées à GraphQL. L'autre étant de copier une requête d'introspection et de la formater correctement dans votre requête.

Dans le cas d'une requête d'introspection sur plusieurs lignes, qui n'est pas pris en charge par l'argument *query* vous auriez pu utiliser la commande : ***echo 'payload' | tr -d '\n'*** avec payload étant la requête d'introspection.

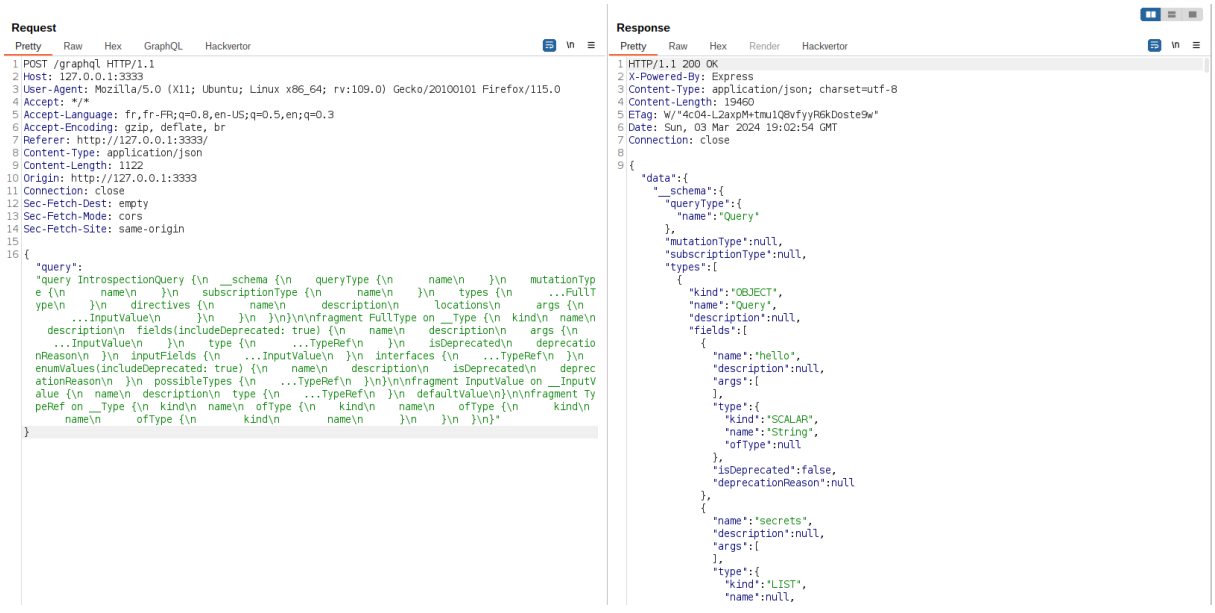
Exemple 1

La ressource suivante présente comment utiliser les nouvelles fonctionnalités de BurpSuite concernant les APIs GraphQL (fonctionnalités dispo dans la version gratuite Community).

Sur la requête vers */graphql*, un clique droit permet d'afficher le menu contextuel en rapport avec GraphQL. Il suffisait de sélectionner « Set Introspection Query » afin d'obtenir la requête d'introspection.

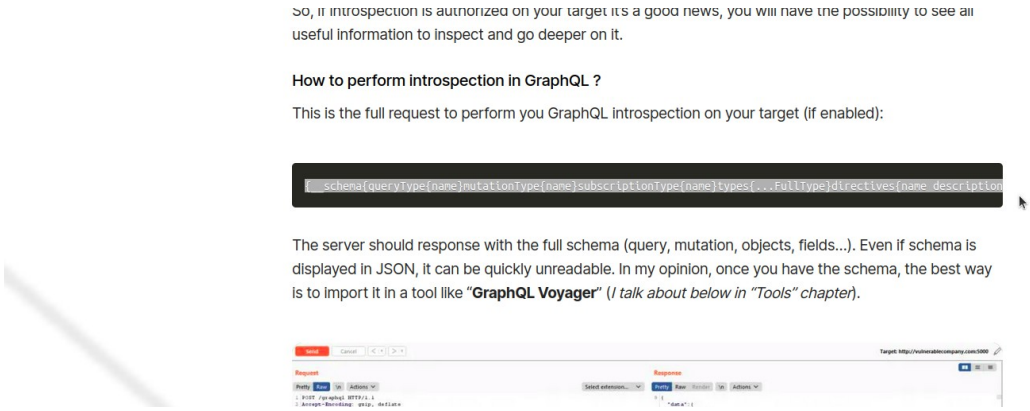


Une fois envoyée, vous obtenez le schéma complet utilisé par l'API.

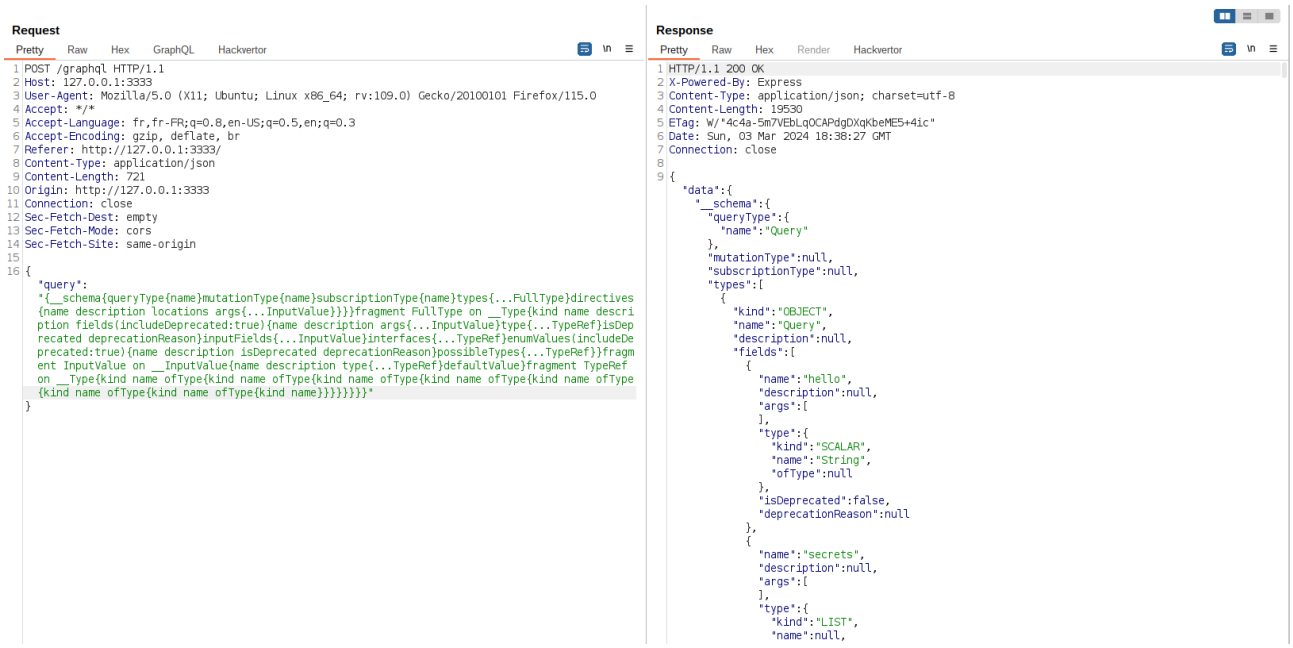


Exemple 2

La [ressource suivante] présente une requête facilement utilisable. Elle est donnée en une seule ligne et est compactée.



Une fois collée dans BurpSuite vous obtenez le schéma complet utilisé par l'API.



#3 Flag

Pour obtenir le flag, il fallait s'intéresser au schéma retourné par l'API et surtout aux parties qui étaient spécifique aux données gérée par l'instance GraphQL.

La méthode la plus simple était d'effectuer une recherche par mot clef en utilisant la fonctionnalité de BurpSuite. On cherche « Flag » et tada !