

Markdown Autogeneration from a GraphQL Schema

Author:

Alessandro BUONERBA

Supervisor:

Dr Konstantin KAPINCHEV

A dissertation submitted in fulfillment
of the requirements for the degree of
BSc (Hons) Computer Science (Cybersecurity)

Department of Computing & Mathematical Sciences
Liberal Arts & Sciences



University of Greenwich
London, United Kingdom

May 2022

Markdown Autogeneration from a GraphQL Schema, © May 2022

Author:

Alessandro BUONERBA

Supervisor:

Dr Konstantin KAPINCHEV

Institute:

University of Greenwich, London, United Kingdom

CONTENTS

List of Figures	v
Abstract	vi
Acknowledgments	vii
1 INTRODUCTION	1
1.1 Aims	1
1.2 Objectives	1
2 ETHICAL CONSIDERATIONS	2
3 LITERATURE REVIEW	3
3.1 Introduction	3
3.2 GraphQL Security	3
3.3 GraphQL vs REST	3
3.3.1 Introspection	4
3.3.2 N+1 Problem	5
3.4 Exploring GraphQL API	6
3.5 Framework Agnostic	6
3.6 GraphQL Schema	6
3.7 MD and MDX	7
3.8 Conclusion	8
4 UX DESIGN AND AGILE METHODOLOGIES	9
4.1 Ways of Working	9
4.2 Kanban vs Scrum	9
4.3 Agile Project Management	10
4.3.1 Epics	10
4.3.2 Spikes	10
5 IMPLEMENTATION	11
5.1 Design	11
5.2 Proof of Concept	11
5.3 Refactoring	17
5.4 Frontend	18
5.5 Version Control System	18

6	TESTING	19
6.1	Unit Tests	19
6.2	End to End	19
6.3	Accessibility	19
7	CONCLUSIONS	20
7.1	Reflection	20
7.2	Future ideas	20
	BIBLIOGRAPHY	i
A	APPENDIX	1
A.1	Project Proposal	1
B	APPENDIX	5
B.1	Frontend Screenshots	5
B.2	Code Screenshots	5

LIST OF FIGURES

Figure 3.1	Introspection Query	4
Figure 3.2	GraphQL N+1 Problem	5
Figure 3.3	Object Type	7
Figure 3.4	Wizard Query Result	7
Figure 4.1	Ready for Development Agile Board	10
Figure 5.1	High-Level Architecture	11
Figure 5.2	Handlebars Template Language	12
Figure 5.3	PoC Imports	13
Figure 5.4	PoC Type Guards	13
Figure 5.5	PoC Scalar Path	14
Figure 5.6	PoC Scalar Path Markdown	14
Figure 5.7	PoC Format Type Lambda Function	14
Figure 5.8	PoC Print AST Node	15
Figure 5.9	PoC Empty Structure	15
Figure 5.10	PoC Full Structure	16
Figure 5.11	PoC Nested Loop	16
Figure 5.12	PoC Output Folder	17
Figure A.1	REST API vs GraphQL API	1
Figure A.2	GraphQL N+1 Problem	2
Figure A.3	JAMstack Workflow	3
Figure A.4	High-Level Architecture	4

ABSTRACT

Since GraphQL was publicly released in 2015, many developers adopted it to create new public faced APIs, but these are often poorly documented. Writing well-structured documentation requires time and manual work, and the tooling currently available at the time of this paper would require technologies and frameworks lock-in. This project aims to generate markdown files that can then be parsed in any framework of choice. Since the output will be in markdown, the user can then use his parser to manipulate the documents and produce static files for their frontend.

ACKNOWLEDGMENTS

This project required a lot of time and the minimum I can do is to thanks the support of my friends and family. *Thank You for everything!*

Also, a huge thank you to supervisor **Dr Konstantin Kapinchev** for support me throughout this year. I have been lucky to have you!

INTRODUCTION

Generating an up-to-date documentation from a specific source of truth such as a schema, is a very important aspect of documenting an Application Programming Interface (API) for a large corporate company and not only. The absence of a tool to generate such documentation, more specifically a tool to generate Markdown files. Even more importantly, one that could generate a file with a support for syntax aimed at custom components such as Markdown for the component era (MDX). The modern world is building the majority of their web in React, and it is very important and relevant that a file supports both Markdown (MD) and JavaScript XML (JSX) and MDX does just that. This would certainly mean and resolve one of the biggest issues developers are finding when working with GraphQL APIs, which is Introspection. Introspection is a GraphQL query that allows developers to navigate and discover the traits of an entire Schema from the external world, which is something we all want to avoid at all cost for a security perspective. This project has been designed and researched and discussed with my supervisor to be the solution at the above problems while keeping it framework agnostic.

1.1 AIMS

This project will not only generate the markdown files but also give examples on how to integrate them in a frontend framework of choice.

1.2 OBJECTIVES

Chapter 2 will explain the legal, social, and ethical aspects of the project.

Chapter 3 will give an overview of the literature review.

Chapter 4 will give an overview of the user experience and agile methodologies.

Chapter 5 will give an overview of the implementation.

Chapter 6 will give an overview of the testings.

Chapter 7 will give an overview of the conclusions.

ETHICAL CONSIDERATIONS

The data that will be used to generate the documentation and used within the software is not connected anyhow to any individual or company. The source of truth will be a schema that is a representation of the data that could be used to auto-generate the documentation and might point bad actors to write malicious queries, hence why it is suggested to have schema and the documentation private. If by any chance there might be data into field descriptions that could be used, it will be processed securely as it will not be stored in any database and directly served to the end user locally without traversing the web, following the Data Protection Act-1998 (Legislation.gov.uk, [2022](#)).

LITERATURE REVIEW

3.1 INTRODUCTION

Documentation is a crucial aspect of the development of software. It is so important that every developer building a GraphQL API should be aware of it and keeping their Schemas documented to enable and facilitate consumers to understand how to use the API (Derks, 2021). A very good way to document such APIs is not to be locked in with any vendor-specific that generates documentation on the fly given a specific schema but building static documentation that automatically updates on the fly when a change is made to it (ibid). The following literature review will point the differences between different APIs, analyse and critically evaluate the options developers have to reach the same goal and why the software implementation of the tool used in the project gives the producers better results, freedom and save them money. Security implications are also another important aspect of the lifecycle and this paper will dive into analysis and confrontation to understand this.

3.2 GRAPHQL SECURITY

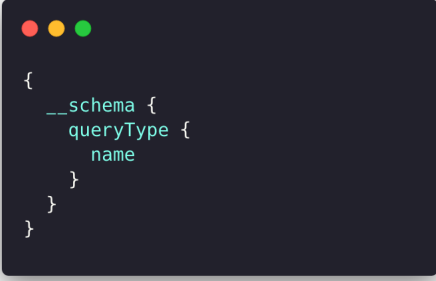
3.3 GRAPHQL VS REST

Before diving in, context needs to be added on why the projects build solutions for GraphQL instead of REST. REST has become the common choice to build and design APIs in the past years (Brito and Valente, 2020), but as the developers needed more flexibility on evolution, a sharp decouple between the backend and frontend and a gateway to access all the data they needed through a single point of access. GraphQL came to the rescue of such developers wanting a better way to build API. While REST usually have multiple endpoints to fetch different type of data, GraphQL unifies everything through a single query to the server with a simple JSON return with the data requested by the consumer. One of the biggest problems of REST is overfetching. Designing an API that returns exactly what the consumer wants in REST requests is impossible (Seabra, Nazário, and Pinto, 2019).

GraphQL solved the overfetching problem as the user can write a specific query with the data needed. As previously mentioned, GraphQL - differently from REST - is decoupled from the backend. That means the front end can change its UI without changing the back end for adjustments. Not only for the same reason, but the backend also has instrumental analytics on the data requested by the consumer since everything will be requested through a specific query. That leads to supporting graceful deprecation of specific fields that are not mainly used. That is alluring, but how does a consumer know which query to write to gather his data? This is when Introspection comes in handy, but it has some critical drawbacks and security implications that makes it unusable in production. Contrary to all the advantages previously explained, the team at Kernel (2021) also emphasised many disadvantages. One of that is that every query always returns a state of 200 even if the query was not successful. It is very accurate and changes the way of monitoring and measuring errors from how everyone is used with REST. GraphQL is also very bad at handling caching which is also very complex to implement and manage, but one thing that has not been mentioned from Kernel (2021) is that it is also fairly simple to wrap the whole API in a Content Delivery Network (CDN) that would be the first point of contact between the server and the consumer. There are many very viable techniques that would make this solution not only a patch to what GraphQL does badly, but also to generally improve the API. A CDN could fully cache any document and not only small pieces of it, making it very fast, secure, scalable and on edge, which is always a great addition to services such as an API.

3.3.1 Introspection

Introspection is a GraphQL feature that, if enabled, grant access to a query that returns any possible query and updates as the schema evolves overtime. A bad actor could easily access sensitive information, types, and operations supported with such a tool.



```
{
  __schema {
    queryType {
      name
    }
  }
}
```

Figure 3.1: Introspection Query

Introspection enables users to query a GraphQL API and discover its schema structure, giving bad actors a chance to find potentially malicious operations (Khalil, 2021) quickly and disrupt the availability of the API. However, it is also a requirement for tools such as *GraphiQL* and *Playground*. This is a severe dilemma for producers who want to keep their APIs as secure as possible, away from indiscreet eyes, and closed to potential threats but still have documentation tooling. If the attackers have access to the whole schema through introspection, it will be effortless to find and exploit API calls meant for internal use and debugging purposes (Rizwan, 2021). Through the same technique, the attackers could also get access to mutations and API calls intended to add, edit or delete specific data on the database, making it a real threat. Many other security issues are linked to the activation of the introspection and misconfiguration; some are information disclosure, insecure direct object references, and inexistent Access Control List (ACL) (YesWeHack, 2021).

3.3.2 *N+1 Problem*

By design, GraphQL has a fetching inefficiency known as *N+1 Problem* where the number of queries executed against the database (or other upstream services) can be as large as the number of nodes in the resulting graph (GraphQL by PoP, 2020).



```
query {  
  students(first: N) {  
    name  
    friends (first: M) {  
      name  
    }  
  }  
}
```

Figure 3.2: GraphQL N+1 Problem

In the example above, the query against the schema would make a single call to the database to retrieve the first N students, and then for each of these N s students it would make a separate query to the same database to fetch M friends details (N calls), hence $N+1$. Having introspection disabled is the right choice looking at a security perspective, and this project will help solve the downside of not having tools to help document the API and more.

3.4 EXPLORING GRAPHQL API

There are different tools which lock-in both producers and consumers that aims to explore a specific GraphQL API. The problem with those tools is that the producer does not ever have the freedom and the flexibility to have a static documentation running on a machine. Not only, most of the time the GraphQL server needs to be communicating with the service, with introspection enabled. Apollo Studio is a great tool to explore GraphQL APIs with just registering a schema but it is a paid tool and does not come cheap. Also, in order to use most of the tooling offered from Apollo, the server must be built with Apollo server and this hugely lock the company or developer of the project to a single vendor with huge implications in terms of flexibility and ownership of the whole ecosystem that will be built around it. In practical terms, if a producer do want to create a GraphQL API in Elixir using Absinthe (Hexdocs, [2022](#)), it will be impossible for the developer to utilise any of the Apollo tooling.


3.5 FRAMEWORK AGNOSTIC

As previously mentioned, the end goal is to build a framework agnostic tool, meaning that using a single GraphQL schema as a source of truth, the tool will generate a well structured set of markdown files to document the API and utilise those files in any way the developer wants. This would boost productivity and flexibility as the developers can utilise the deep knowledge they already have on a framework of their choice, with the language of their choice (Stefan, [2018](#)).

3.6 GRAPHQL SCHEMA

A GraphQL schema is a set of structured rules that express requirements for an application. It might be easy with a simple UI but it can easily become difficult as the interface of the application grows and evolves. It is to keep in mind that most of the benefits that GraphQL brings to the table are attributed to the schema itself as it enabled most of the features that GraphQL provides such as code generation, parsing, validation and type checking. For this exact reason, many developers couple GraphQL with a strong typed language such as TypeScript to have an ecosystem of tools at their disposal that can help them catch errors at runtime through the IDE or editor itself, rather than at compile time. The GraphQL schema is also a graph because not only is a representation of data graph but also a definition of relationships between entities (Karthic, [2020](#)). That are few in-built types that are covered in GraphQL which are Object, Scalar, Query and Mutation. The Scalar types that GraphQL supports are Int, Float, String, Boolean and ID. All these specs

will be covered and supported in the project as it is very important to support all the types that are built-in GraphQL or the documentation would fail to be procued as the schema could have types not supported. An example of object type below.



```
type Wizard {  
  name: String!  
  age: Int!  
}
```

Figure 3.3: Object Type

In this object type there are also two scalar type as field which represent the decoration of their entities. In this case both fields are both non-nullable fields, which means that the field cannot be null and is mandatory. Meaning that if a consumer performs a query on a non-nullable field, he will never be able to receive a response like the one below.



```
{  
  wizard: {  
    name: null,  
    age: null  
  }  
}
```

Figure 3.4: Wizard Query Result

3.7 MD AND MDX

As Gruber (2020) explains in his article, Markdown is intended to be simple to read and simple to write. It is important to have a an output text that is easy to read so that the end consumer does not have to know anything related to coding to make things as simple as possible. In this case, though, we also want to embed and integrate components in our markdown files, hence the use of the MDX. It is fair to say that MDX is a superset of MD that blends both markdown and JSX syntax to build an hybrid to power the most modern frameworks such as React, Vue and Angular, but still leave the choice to the developers building the project.

3.8 CONCLUSION

Developers are not only interested in building an API but also in continuously document it and provide a way for their consumers to have a better understanding of the API. Even though GraphQL could have some downsides, the advantages of using it are just far too greater to ignore. A tool to create documentation while keeping the schema and the structure of the API secure and keeping everything framework agnostic is something that this project will try to achieve. After some research it is easy to say that it will be unique and could be interesting to see how it could expand after making it open-source.

4

UX DESIGN AND AGILE METHODOLOGIES

4.1 WAYS OF WORKING

During the early stage of the project, many things needed to be decided, such as the language, the agile framework, testing, and how to document everything. The best agile frameworks that would be fit for purpose during the development process were Kanban and Scrum. It is essential to have a good understanding of how to work Agile. Agile is an approach very well known in the industry that facilitates the management of a project by an individual or a group of developers, designers and managers of the same team. It provides a rigorous methodology, depending on which framework, to self-organise work and not deviate from the end goal the team did impose themselves (or their company). While working on this project, an Agile framework will be chosen and used as one of the main requirements to simulate the working of a team of one or more, working for a company or themselves. The goal is to have a simulated experience, create a habit, and document the process, the decisions, and the steps taken from the initial thoughts to the end product. Two main two frameworks will be discussed and evaluated: Kanban and Scrum.

4.2 KANBAN VS SCRUM

Scrum is fast and has ceremonies split into sprint planning, review, retrospective, and daily standups. With Scrum, the team wants to ship a piece of functionality by the end of each sprint and each sprint usually last two weeks. Kanban on the other hand is much more flexible and based on continuous delivery on the idea of having a backlog where the team can park their future work and then move it next as soon as it is unblocked from other tickets. In Kanban new feature and pieces of code are released when ready and one do not need to be too worried of the deadlines given by the sprint such as in the Scrum framework.

4.3 AGILE PROJECT MANAGEMENT

As previously mentioned, there must always be a tool and techniques to keep track of the work must has been done and the progress in general. For this specific project, a Kanban board has been used to keep track of the work, while still retaining some aspects of Scrum, which gives the framework a more flexible approach that is more recognised as a Scrumban approach. Below an example of tickets created in a Kanban board that makes it so visually appealing and easy to work with.

Ready for Development		Reporter	Problem/Opportunity	Priority
[Spike]	Which packet manager?	A		High
	Import GraphQL utilities	A		
+ Add Feature				

Figure 4.1: Ready for Development Agile Board

The Ready for Development board is used for all the tickets that have been through the whole initial lifecycle that comprehend creation, refinement, estimation, and ready to start. This approach is used throughout the project ceremonies but for the sake of the speed have been reduced to a single evaluation in the backlog as in this project there is only one working developer.

4.3.1 Epics

When a huge pieces of functionality needs more than a ticket, a new epic is created where all the moving parts of the new functionality are put together. The epic usually have a description that summarise the whole functionality, what needs to be done to reach the end goal and the members involved.

4.3.2 Spikes

When an investigation is required to find a solution which is unknown to the team, a spike is created. A spike is a ticket that is used to gather information and answering questions instead of producing a piece of functionality or solution. The outcome of a spike is usually documented in the ticket itself and it usually blocks other tickets from being moved to Ready to Development. This project has a spike for starting points such as language to use, tools, and frameworks.

IMPLEMENTATION

5.1 DESIGN

Before diving into implementing the code, it is always imperative to have a whiteboard and design the architecture of the tool being built. The tool that will be made will have a single source of truth for a schema that will then be taken and processed through the logic of the application and transformed into structured folders containing files that represent each living part of the source. The mark-down will support framework-agnostic plug-in and integration, meaning that any JSX framework can parse it and build HTML static files that any browser can read. It is vital to support as many types and Scalars as possible to consistently generate the files from any schema, regarding their complex tree structure and the scalars used by the producer. The diagram below visually explores the solution that will be chased for the end goal.

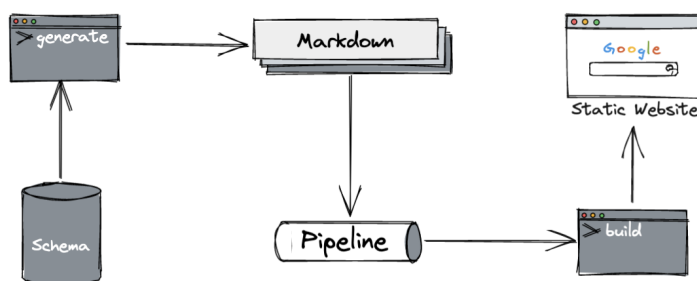
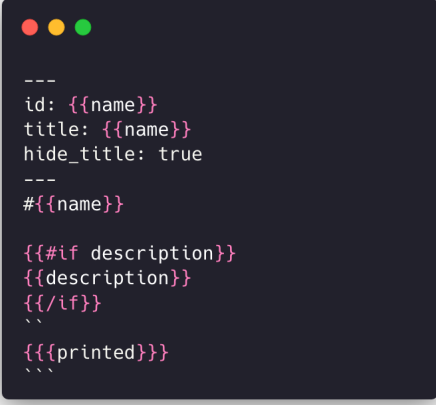


Figure 5.1: High-Level Architecture

5.2 PROOF OF CONCEPT

This section will discuss the first iteration of the project as Proof of Concept (PoC). This will be the initial implementation stage of the project used for discovery and testing. The PoC is a software development methodology that helps the project developers implement the initial logic and validate their hypothesis on the project's feasibility. This specific PoC will be coded in JavaScript using Node as a backend

runtime. In a perfect world, the tool should be written using a more robust programming language and ecosystem such as Scala to have the advantage of an effective, high-performance in pure functional programming. This would massively improve concurrency with the use of IO, which facilitates Fibers as a replacement for native OS threads and allows for the benefit of millions of concurrent processes without the need for a thread manager. In this use case, the PoC is using JavaScript to keep things simple, without looking too much at the performances that it would have in a production environment as it will be only used to demonstrate how feasible the project is. Since JavaScript does not support the concept of template literals, a templating language named Handlebars will be used to generate the inside structure of the markdown files. Handlebars use expressions that are evaluated and replaced with the evaluation results. An example of this can be seen below.



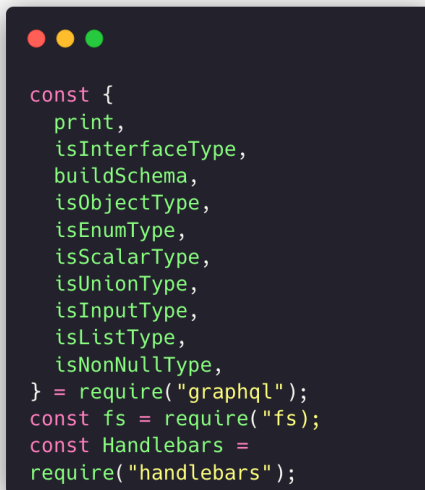
```
---
id: {{name}}
title: {{name}}
hide_title: true
---
#{{name}}

{{#if description}}
{{description}}
{{/if}}
`

{{{printed}}}
```

Figure 5.2: Handlebars Template Language


The imports for the PoC will be kept at the very minimal. Below is shown the start of the index file with the imported tools to complete and reach the end goal.



```
const {
  print,
  isInterfaceType,
  buildSchema,
  isObjectType,
  isEnumType,
  isScalarType,
  isUnionType,
  isInputType,
  isListType,
  isNonNullType,
} = require("graphql");
const fs = require("fs");
const Handlebars =
  require("handlebars");
```

Figure 5.3: PoC Imports

In order for it to work, we need to install the GraphQL library and import all the type guards that are implemented in it to be able to check the types while navigating in the complex nested structure of the Abstract Syntax Tree (AST) generated by the reading the schema given in the folder. An example on how the type guards are implemented is shown in the image below.



```
const createPath = (type) => {
  if (isListType(type) || isNonNullType(type)) {
    return createPath(type.ofType);
  }
  if (isScalarType(type)) {
    return `/scalars/${typename}`;
  }
}
```

Figure 5.4: PoC Type Guards

Since in the markdown file, there are places where it would be nice to have hyperlinks that point the user to the right page when navigating the relationship between the fields, there is a need of the type guards to be able to place the right path into the object of a specific formatted data structure used to group the data. An example of the object related to the image above is shown below.



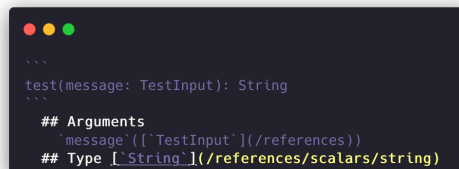
```

mutations: [
  {
    name: 'test',
    description: undefined,
    type: String,
    printed: 'test(message: TestInput): String',
    arguments: [Array],
    fields: [],
    path: '/scalars/string',
    isRootType: true
  }
]

```

Figure 5.5: PoC Scalar Path

As shown in the image above, the field has a type of String and the path to the scalar is /scalar/string. The type guard is implemented as a way to recursively navigate the AST and find the right path to the each specific hyperlink case.



```

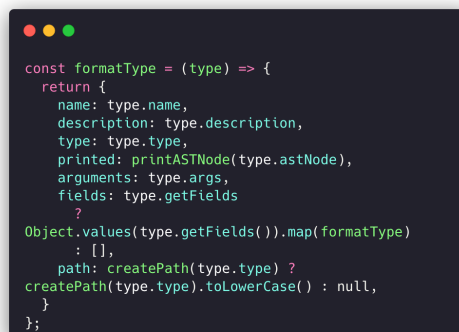
'''
test(message: TestInput): String
'''
## Arguments
`message`(['TestInput'])(/references))
## Type ['String'](/references/scalars/string)

```

Figure 5.6: PoC Scalar Path Markdown

The image above shows the exact same mutation but in a generated markdown format, completely done by the tool.

In order to have a great structure of the data we are going to manipulate for the generation, a special lambda function has been created which return an object with all the properties each type has to offer, it goes and traverse the AST and places the information in the right properties available for later use.



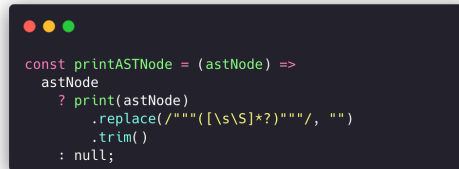
```

const formatType = (type) => {
  return {
    name: type.name,
    description: type.description,
    type: type.type,
    printed: printASTNode(type.astNode),
    arguments: type.args,
    fields: type.getFields
    ?
    Object.values(type.getFields()).map(formatType)
      : [],
    path: createPath(type.type) ?
    createPath(type.type).toLowerCase() : null,
  }
};

```

Figure 5.7: PoC Format Type Lambda Function

It is important to note there is another function operating in the body format-Type which is used to pull out the printed version taken from the schema. This is useful to have so that the documentation can have an original representation of the piece of schema that is being discussed. The image below represent the function written to achieve the printed version of the schema in the formatted structure.



```
const printASTNode = (astNode) =>
  astNode
  ? print(astNode)
    .replace(/""([\s\S]*)""/, " ")
    .trim()
  : null;
```

Figure 5.8: PoC Print AST Node

It is again a lambda function that is used to traverse the AST till it reaches a specific node and then surgically extract the printed version of it, making sure it doesn't have any unwanted literal strings, characters or whitespace in it, so that it can directly be used without any further manipulation in the templating system previously described.

One of the last pieces of the puzzle is a wrapper that groups all types in a last and single object, done used the previously described functions recursively for any type in the AST. This prints out a massive object that is then used in a nested loop to again recursively generate the markdown files for each type, while accessing the Handlebars templating for valuating the expressions.

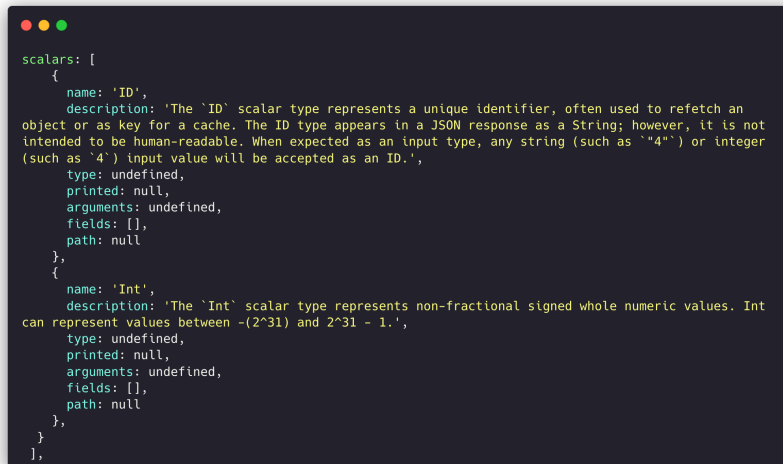
The structure of the final, but empty, data structure is as shown below.



```
{
  queries: [],
  mutations: [],
  subscriptions: [],
  objects: [],
  enums: [],
  scalars: [],
  interfaces: [],
  unions: [],
  inputs: [],
  directives: [],
}
```

Figure 5.9: PoC Empty Structure

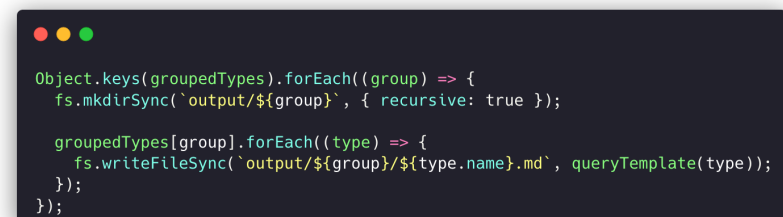
The structure is being shown as empty because it would be too much to show in a single image. In order to facilitate the understanding, below also an image representing a single type with its full array structure.



```
scalars: [  
  {  
    name: 'ID',  
    description: 'The `ID` scalar type represents a unique identifier, often used to refetch an  
    object or as key for a cache. The ID type appears in a JSON response as a String; however, it is not  
    intended to be human-readable. When expected as an input type, any string (such as `"4"`) or integer  
    (such as `4`) input value will be accepted as an ID.',  
    type: undefined,  
    printed: null,  
    arguments: undefined,  
    fields: [],  
    path: null  
  },  
  {  
    name: 'Int',  
    description: 'The `Int` scalar type represents non-fractional signed whole numeric values. Int  
    can represent values between  $-(2^{31})$  and  $2^{31} - 1$ .',  
    type: undefined,  
    printed: null,  
    arguments: undefined,  
    fields: [],  
    path: null  
  },  
]
```

Figure 5.10: PoC Full Structure

And as previously mentioned, the final structure is then used in a nested function shown below.



```
Object.keys(groupedTypes).forEach((group) => {  
  fs.mkdirSync(`output/${group}`, { recursive: true });  
  
  groupedTypes[group].forEach((type) => {  
    fs.writeFileSync(`output/${group}/${type.name}.md`, queryTemplate(type));  
  });  
});
```

Figure 5.11: PoC Nested Loop

The nested loop makes sure that all the types are accounted for and uses the templating system to generate the markdown files for each type.

The final output is an output folder with all the markdown files generated, and the goal of the PoC has been validated and the code is ready to be used and refactored for better improvements and use cases.

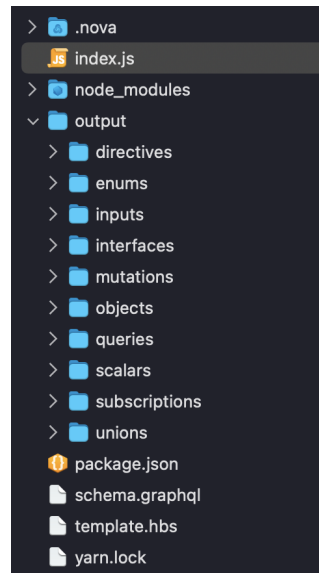


Figure 5.12: PoC Output Folder

Each folder has multiple md files that can be used by any framework that can parse the markdown files and build static generated pages in HTML.

Now that the proof of concept has been completed and resulted in a successful experiment, the next step is to refactor the code and removing unnecessary steps such as Handlebars templating, which will be redundant with TypeScript. It is always good to keep the dependencies as minimum as possible in order to keep the code clean and easy to maintain. Easy to maintain because deprecation of functionalities are always behind the corner and it means that the code needs to be migrated to a new version of the library which would require time, effort and money.

5.3 REFACTORING

For the same reasons explained before, the code will be then refactored in TypeScript removes the templating system and utilises the one in-built with the language. The template literals types will produce the same result shown and achieved in the JavaScript PoC, making it much more succinct, readable and powerful as the code will not be decoupled in different files and folders. It will also keep the code much more DRY with a single source of truth, which the language itself tries to doctrine.

5.4 FRONTEND

In this part I will show how I produced the frontend part that generates the website.

5.5 VERSION CONTROL SYSTEM

GitHub etc

TESTING

6.1 UNIT TESTS

This section will cover the unit tests done with Jest

6.2 END TO END

This section will cover the end to end tests done with Cypress

6.3 ACCESSIBILITY

This section will cover the accessibility tests done with Axe-core

CONCLUSIONS

7.1 REFLECTION

This section will contain my reflection

7.2 FUTURE IDEAS

This section will contain my future ideas

BIBLIOGRAPHY

- Brito, Gleison and Marco Tulio Valente (Mar. 2020). "REST vs GraphQL: A Controlled Experiment". In: *2020 IEEE International Conference on Software Architecture (ICSA)*, pp. 81–91. doi: [10.1109/ICSA47634.2020.00016](https://doi.org/10.1109/ICSA47634.2020.00016).
- Derks, Roy (2021). *Documenting GraphQL APIs* | HackerNoon. URL: <https://hackernoon.com/documenting-graphql-apis> (visited on 03/19/2022).
- Fan, Qiang, Yue Yu, Tao Wang, Gang Yin, and Huaimin Wang (Jan. 2021). "Why API Documentation Is Insufficient for Developers: An Empirical Study". In: *Science China Information Sciences* 64.1, p. 119102. ISSN: 1674-733X, 1869-1919. doi: [10.1007/s11432-019-9880-8](https://doi.org/10.1007/s11432-019-9880-8). URL: <http://link.springer.com/10.1007/s11432-019-9880-8> (visited on 10/09/2021).
- Freeman, Adam (2021). "Understanding TypeScript". In: *Essential TypeScript 4: From Beginner to Pro*. Ed. by Adam Freeman. Berkeley, CA: Apress, pp. 35–41. ISBN: 978-1-4842-7011-0. doi: [10.1007/978-1-4842-7011-0_2](https://doi.org/10.1007/978-1-4842-7011-0_2). URL: https://doi.org/10.1007/978-1-4842-7011-0_2 (visited on 10/09/2021).
- Gagliardi, Valentino (2021). "Django REST Meets Next.js". In: *Decoupled Django : Understand and Build Decoupled Django Architectures for JavaScript Front-ends*. Ed. by Valentino Gagliardi. Berkeley, CA: Apress, pp. 113–132. ISBN: 978-1-4842-7144-5. doi: [10.1007/978-1-4842-7144-5_8](https://doi.org/10.1007/978-1-4842-7144-5_8). URL: https://doi.org/10.1007/978-1-4842-7144-5_8.
- GraphQL by PoP (2020). *Suppressing the N+1 Problem* | GraphQL by PoP. URL: <https://graphql-by-pop.com/docs/architecture/suppressing-n-plus-one-problem.html#what-is-the-n-1-problem> (visited on 10/11/2021).
- Gruber, John (2020). *38 Markdown: Syntax*. URL: http://scholar.googleusercontent.com/scholar?q=cache:VSqALECcGQYJ:scholar.google.com/+markdown&hl=en&as_sdt=0,5 (visited on 03/19/2022).
- Helmold, Marc (2020). "Lean Management KPI and OKR". In: *Lean Management and Kaizen: Fundamentals from Cases and Examples in Operations and Supply Chain Management*. Ed. by Marc Helmold. Management for Professionals. Cham: Springer International Publishing, pp. 113–122. ISBN: 978-3-030-46981-8. doi: [10.1007/978-3-030-46981-8_12](https://doi.org/10.1007/978-3-030-46981-8_12). URL: https://doi.org/10.1007/978-3-030-46981-8_12 (visited on 10/09/2021).
- Hexdocs (2022). *Overview — Absinthe v1.7.0*. URL: <https://hexdocs.pm/absinthe/overview.html> (visited on 03/19/2022).
- Karthic, Rao (2020). *Designing GraphQL Schemas* - Dgraph Blog. URL: <https://dgraph.io/blog/post/designing-graphql-schemas/> (visited on 03/19/2022).
- Kernel, Stable (2021). *Advantages and Disadvantages of GraphQL* | Stable Kernel. URL: <https://stablekernel.com/article/advantages-and-disadvantages-of-graphql/> (visited on 03/20/2022).
- Khalil, Stemmler (2021). *Why You Should Disable GraphQL Introspection In Production* – GraphQL Security. URL: <https://www.apollographql.com/blog/graphql/security/why-you-should-disable-graphql-introspection-in-production/> (visited on 10/09/2021).
- Koren, István and Ralf Klamma (2018). "The Exploitation of OpenAPI Documentation for the Generation of Web Frontends". In: *Companion Proceedings of the the Web Conference 2018*. International World Wide Web Conferences Steering Committee. ISBN: 978-1-4503-5640-4. doi: [10.1145/3184558.3188740](https://doi.org/10.1145/3184558.3188740). URL: <https://doi.org/10.1145/3184558.3188740>.
- Legislation.gov.uk (Jan. 2022). *Data Protection Act 1998*. Text. URL: <https://www.legislation.gov.uk/ukpga/1998/29/contents> (visited on 03/19/2022).
- Pratap Yadav, Mahendra, Nisha Pal, and Dharmendra Kumar Yadav (2021). "A Formal Approach for Docker Container Deployment". In: *Concurrency and Computation: Practice and Experience* 33.20, e6364. ISSN: 1532-0634. doi: [10.1002/cpe.6364](https://doi.org/10.1002/cpe.6364). URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.6364> (visited on 10/09/2021).
- Rizwan, Bilal (Feb. 2021). *GraphQL — Common Vulnerabilities & How to Exploit Them*. URL: <https://the-bilal-rizwan.medium.com/graphql-common-vulnerabilities-how-to-exploit-them-464f9fdce696> (visited on 10/09/2021).
- Seabra, Matheus, Marcos Felipe Nazário, and Gustavo Pinto (Sept. 2019). "REST or GraphQL? A Performance Comparative Study". In: *Proceedings of the XIII Brazilian Symposium on Software Components, Architectures, and Reuse*. SBCARS '19. New York, NY, USA: Association for Com-

- puting Machinery, pp. 123–132. ISBN: 978-1-4503-7637-2. DOI: [10.1145/3357141.3357149](https://doi.org/10.1145/3357141.3357149). URL: <https://doi.org/10.1145/3357141.3357149> (visited on 03/19/2022).
- Stefan, Nieuwenhuis (2018). *3 Reasons Why I Went Framework Agnostic and Why You Should Do That Too* | by Stefan Nieuwenhuis | Medium. URL: <https://stefannhs.medium.com/3-reasons-why-i-went-framework-agnostic-and-why-you-should-do-that-too-f39ba81c6001> (visited on 03/19/2022).
- Wittern, Erik, Alan Cha, and Jim A. Laredo (2018). “Generating GraphQL-Wrappers for REST(-like) APIs”. In: *Web Engineering*. Ed. by Tommi Mikkonen, Ralf Klamma, and Juan Hernández. Cham: Springer International Publishing, pp. 65–83. ISBN: 978-3-319-91662-0.
- YesWeHack (Mar. 2021). *How to Exploit GraphQL Endpoint: Introspection, Query, Mutations & Tools*. URL: <https://blog.yeswehack.com/yeswehackers/how-exploit-graphql-endpoint-bug-bounty/> (visited on 10/09/2021).
- Yu, Liang, Emil Alégroth, Panagiota Chatzipetrou, and Tony Gorshek (Jan. 2020). “Utilising CI Environment for Efficient and Effective Testing of NFRs”. In: *Information and Software Technology* 117, p. 106199. ISSN: 0950-5849. DOI: [10.1016/j.infsof.2019.106199](https://doi.org/10.1016/j.infsof.2019.106199). URL: <https://www.sciencedirect.com/science/article/pii/S095058491930206X> (visited on 10/09/2021).
- Zammetti, Frank (2020). “What Is JAMstack All About?” In: *Practical JAMstack: Blazing Fast, Simple, and Secure Web Development, the Modern Way*. Ed. by Frank Zammetti. Berkeley, CA: Apress, pp. 1–17. ISBN: 978-1-4842-6177-4. DOI: [10.1007/978-1-4842-6177-4_1](https://doi.org/10.1007/978-1-4842-6177-4_1). URL: https://doi.org/10.1007/978-1-4842-6177-4_1 (visited on 10/09/2021).
- Zayat, Wael and Ozlem Senvar (June 2020). “Framework Study for Agile Software Development Via Scrum and Kanban”. In: *International Journal of Innovation and Technology Management* 17.04. doi: [10.1142/S0219877020300025](https://doi.org/10.1142/S0219877020300025), p. 2030002. ISSN: 0219-8770. DOI: [10.1142/S0219877020300025](https://doi.org/10.1142/S0219877020300025). URL: <https://www.worldscientific.com/doi/epdf/10.1142/S0219877020300025> (visited on 10/06/2021).

APPENDIX

A.1 PROJECT PROPOSAL

INTRODUCTION

This project aims at solving the choice between security and programmatically generated documentation in the world of the GraphQL Application Programming Interface (API). API documentation is an essential part of the software development process as it improves the dev experience — making it easier to integrate — enhancing maintainability and conveniently enables versioning with indication on deprecated fields (Fan et al., 2021). Working with API documentation is not always straightforward, especially when working with gateway and federation, as it would require much effort from all the developers involved in the process. Swagger makes documentation for Representational state transfer (REST) APIs very uncomplicated, as it automatically generates HyperText Markup Language (HTML) based visualisation and interaction out of the box for any consumer of the API (Koren and Klamma, 2018). Since Facebook released GraphQL to the mass in 2015, many individual developers and companies are switching and converting to it to build their APIs, as it enables them to have a much more flexible and efficient way of building their APIs (Brito and Valente, 2020). GraphQL gives to the consumer only the data that he needs, solve the overfetching and underfetching problem related to the traditional REST APIs (Wittern, Cha, and Laredo, 2018).

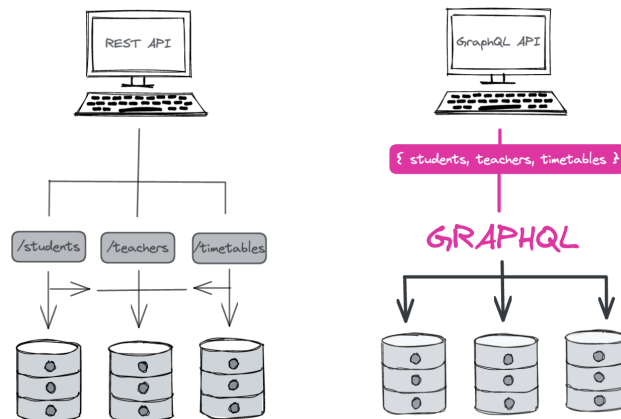


Figure A.1: REST API vs GraphQL API

Querying the API the way users want enables flexibility but can also threaten security if not appropriately handled. This project aims to facilitate API producers

to build secure GraphQL APIs without reachable introspection on the endpoint while still counting on a tool that can generate framework-agnostic structured documentation.

PROBLEM DOMAIN

When working on such a problem, there are many complications in keeping constantly automated and updated documentation for GraphQL APIs. One of them is security. Introspection enables users to query a GraphQL API and discover its schema structure, giving bad actors a chance to find potentially malicious operations (Khalil, 2021) quickly and disrupt the availability of the API. However, it is also a requirement for tools such as *GraphiQL* and *Playground*. This is a severe dilemma for producers who want to keep their APIs as secure as possible, away from indiscreet eyes, and closed to potential threats but still have documentation tooling. If the attackers have access to the whole schema through introspection, it will be effortless to find and exploit API calls meant for internal use and debugging purposes (Rizwan, 2021). Through the same technique, the attackers could also get access to mutations and API calls intended to add, edit or delete specific data on the database, making it a real threat. Many other security issues are linked to the activation of the introspection and misconfiguration; some are information disclosure, insecure direct object references, and inexistent Access Control List (ACL) (YesWeHack, 2021). By design, GraphQL has a fetching inefficiency known as *N+1 Problem* where the number of queries executed against the database (or other upstream services) can be as large as the number of nodes in the resulting graph (GraphQL by PoP, 2020).



```
query {  
  students(first: N) {  
    name  
    friends (first: M) {  
      name  
    }  
  }  
}
```

Figure A.2: GraphQL N+1 Problem

In the example above, the query against the schema would make a single call to the database to retrieve the first N students, and then for each of these Ns students it would make a separate query to the same database to fetch M friends details (N calls), hence N+1. Having introspection disabled is the right choice looking at a security perspective, and this project will help solve the downside of not having tools to help document the API and more.

METHODOLOGY

The project will be divided into two main parts, one being the package to build the structure and generate the documentation from a single source of truth, in this case is a GraphQL schema, and the other is the implementation of a statically generated website that renders the previously generated file in HTML format (Gagliardi, 2021). NodeJS will be used as the backend runtime for the backend to generate the documentation that will then be served to the frontend. The frontend will use NextJS as a React framework to generate the static HTML files parsing previously generated markdowns. A JAMstack (Javascript, API and Markup) with Headless CMS (Content Management System) the approach will be used throughout this project, with additional content outside the generation scope, being decoupled from the whole Versioning Control System (VCS) and being fetched on build time through API queries (Zammetti, 2020).

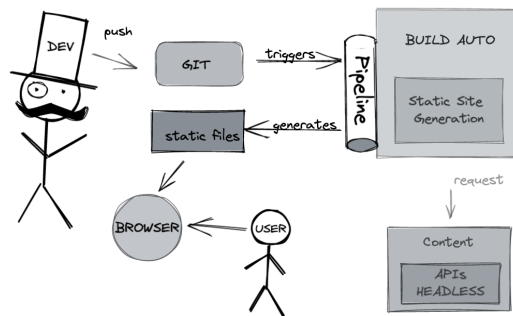


Figure A.3: JAMstack Workflow

A Kanban board will be used to maximise efficiency and visualise the workload and limit the WIP of the project. Kanban has been chosen over Scrum as it is more flexible and does not require running ceremonies, including daily standups. Also, Scrum is overkill for a team of one developer as it would take much time lost on stories, refinements, pointing, spikes and epics while also managing them over different sprints (Zayat and Senvar, 2020). On the other hand, Kanban will focus much more on delivery and is more suited for a small team or individual developers.

The programming language will be JavaScript for the Proof of Concept (PoC) that will then be refactored in TypeScript to make the development process more efficient with its powerful type system saving developers time (Freeman, 2021). The architecture will be managed with popular tools such as GitHub for versioning control and a single source of truth for input files, CircleCI for continuous integration, Vercel for deployment and hosting. To increase package flexibility, the project will also be containerised building an image through Docker that can run on Amazon Web Services (AWS) such as Amazon Elastic Compute (ECS) with a virtual remote machine (EC2) (Pratap Yadav, Pal, and Kumar Yadav, 2021).

EVALUATION

A goal-setting methodology will be used to evaluate the project; the initial goal and key results will be set up at the start of the project with fortnightly updates. To see

if the progress towards the goal is not on the decline, key performance indicators (KPIs) will be set to monitor any gaps and focus the attention on the previously set Objectives and Key Results (OKRs). This will help adjust the goals based on the progress and be able to evaluate if the project reaches a complete state at the end of the deadlines (Helmold, 2020). On the technical side, testing will ensure that the end product is performant, accessible and meets the expectations set at the start of the development process. The project will be tested through a mixture of Unit and End to End (E2E) tests integrated into the previously stated CircleCI pipeline before shipping and deploying the code in production environments. This will ensure that bugged code is only present in non-production environments, and the last deploy step is reached only when the whole project is ready for production (Yu et al., 2020). The development process will be evaluated as successful if the OKRs reaches green metrics and the final project complies with the specifications that have been set (Helmold, 2020). The final product will generate a structured folder with markdown files that document the references of a GraphQL schema and are rendered with a JAMstack philosophy.

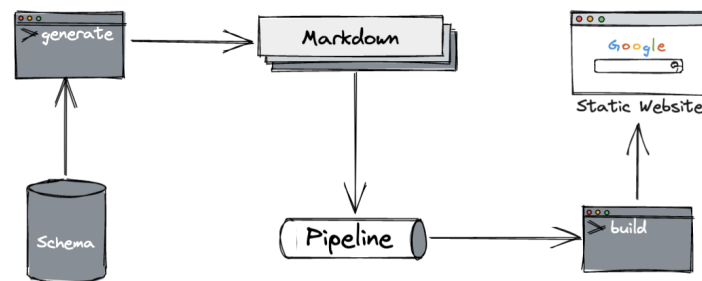


Figure A.4: High-Level Architecture

B

APPENDIX

B.1 FRONTEND SCREENSHOTS

Screenshots Here

B.2 CODE SCREENSHOTS

Screenshots Here