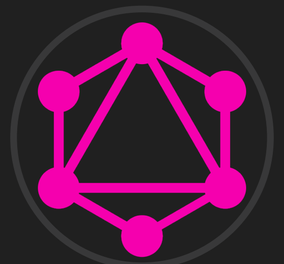
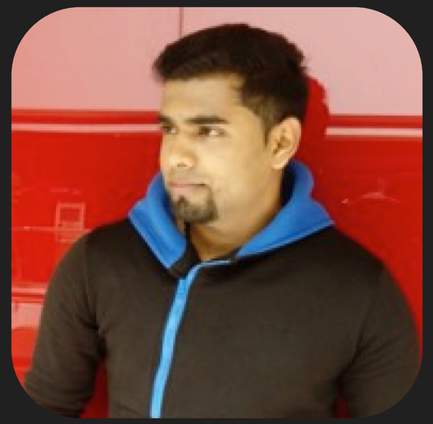


OFFENSIVE GRAPHQL API EXPLOITATION

ARUN.S

whoami



Query whoami {
Arun.S
Senior Security Consultant @ IBM India Software Labs.
Speaker at Conferences and Communities like c0c0n Bsides Delhi, Null/OWASP.
Null Bangalore Chapter Lead, Member of OWASP & BSides Bangalore.
Certified – OSCP, eWPT,ECSA etc.,
}

Howtographql.com

GraphQL

- GraphQL is open sourced by Facebook.
- GraphQL is a query language for APIs - not databases.
- GraphQL is often confused with being a database technology.
- GraphQL server only exposes a single endpoint.

GraphQL Schema

SDL - GraphQL has its own type system that's used to define the *schema* of an API.
The syntax for writing schemas is called Schema Definition Language (SDL).

Queries

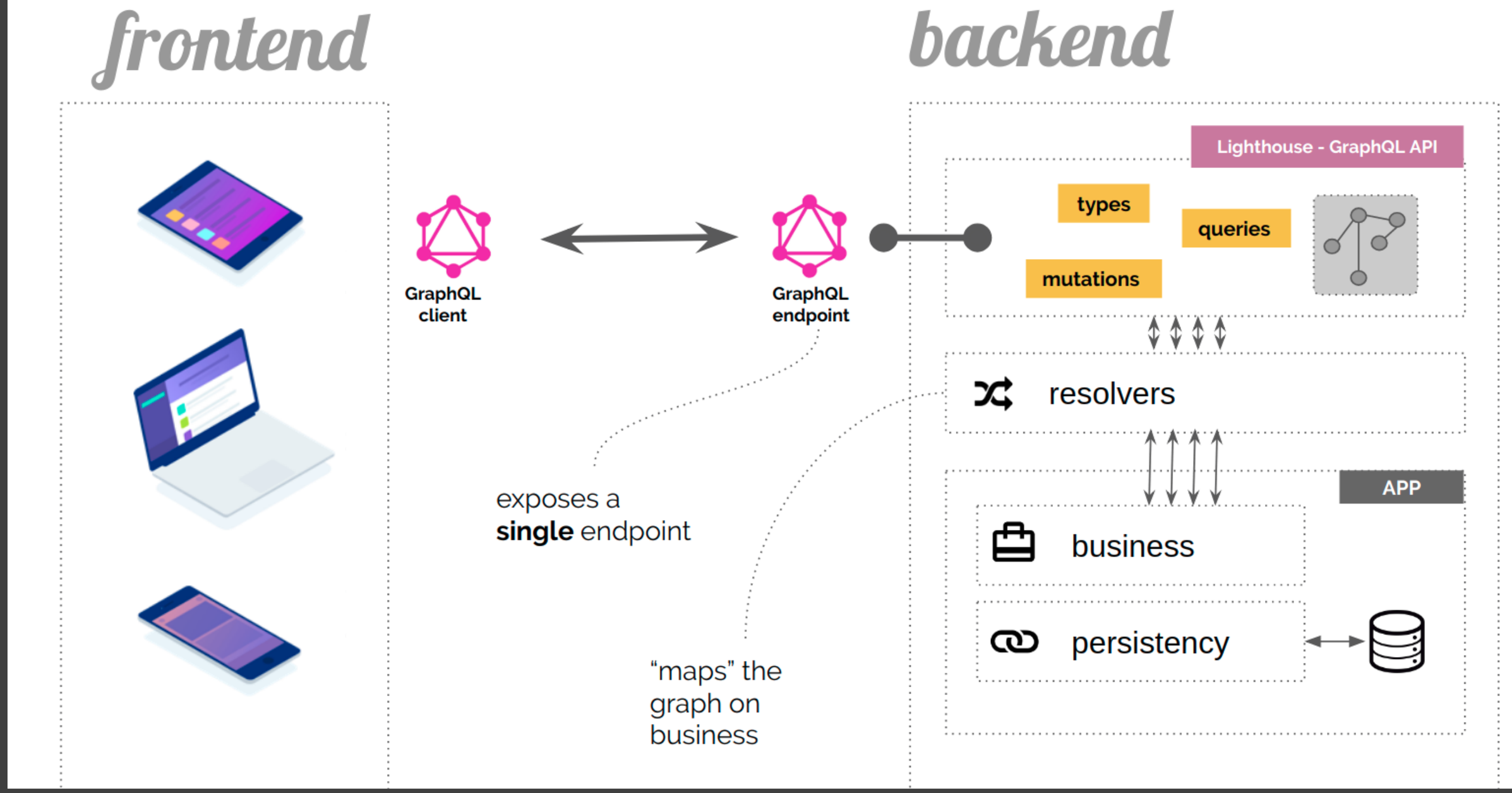
- **Used for retrieving data/results.**
- **Similar to GET in REST.**

Mutation

- **Used for some state changing activities.**
- **Similar to POST/PUT/DELETE.**

Subscriptions

- **Used for Events/Realtime Updates.**



Link: https://lighthouse-php.com/tutorial/#what-is-graphql

S

STRENGTHS

Strengths

GraphQL Architecture is gaining more popularity in the recent days. Some of the reasons I can think of are;

- No More Over & UnderFetching.
- Simple & Efficient to Use.
- Evolve APIs without versioning issues.
- Schema Introspection
- Adapts to different requirements for different clients.
- No Wonder that big Facebook, Shopify, Pinterest, HackerOne etc.,

S

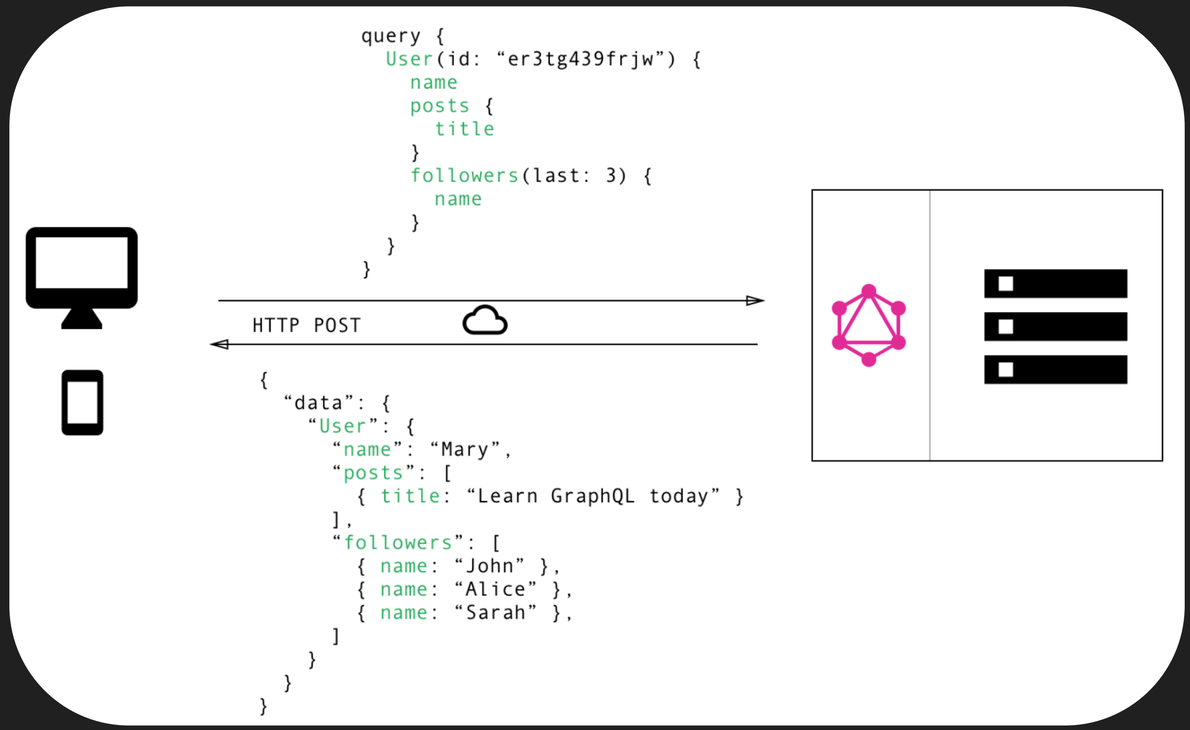
STRENGTHS

REST

S

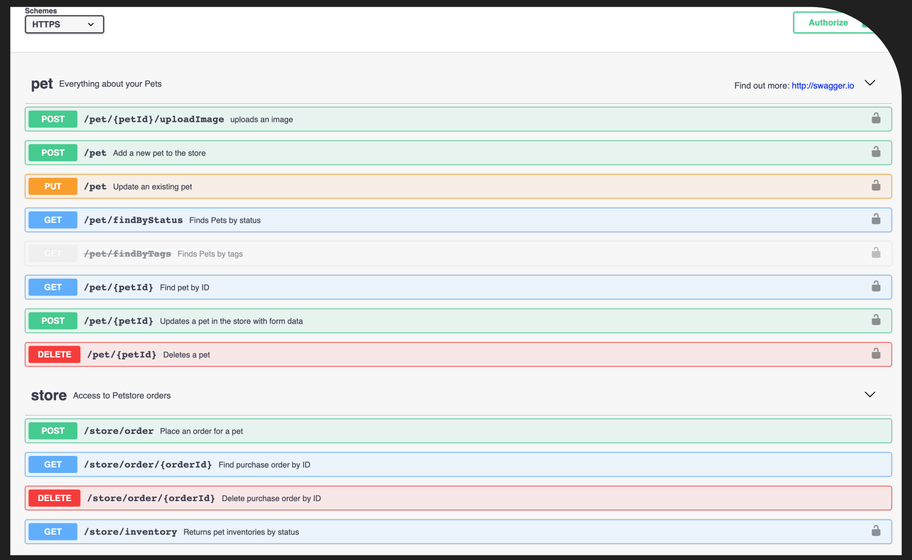
STRENGTHS

GraphQL



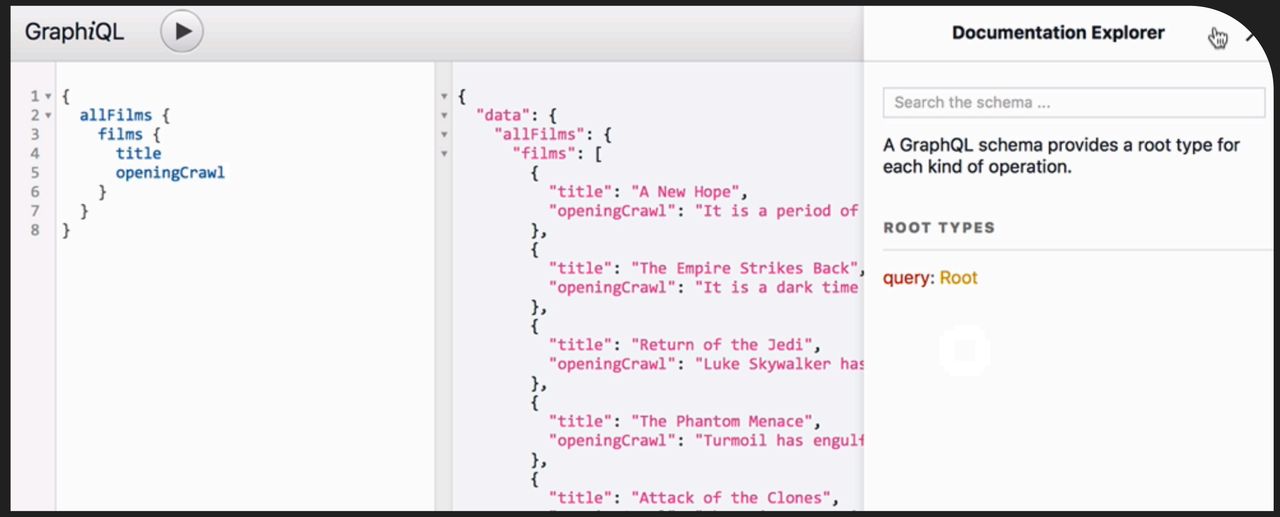
S

STRENGTHS



REST

GraphQL



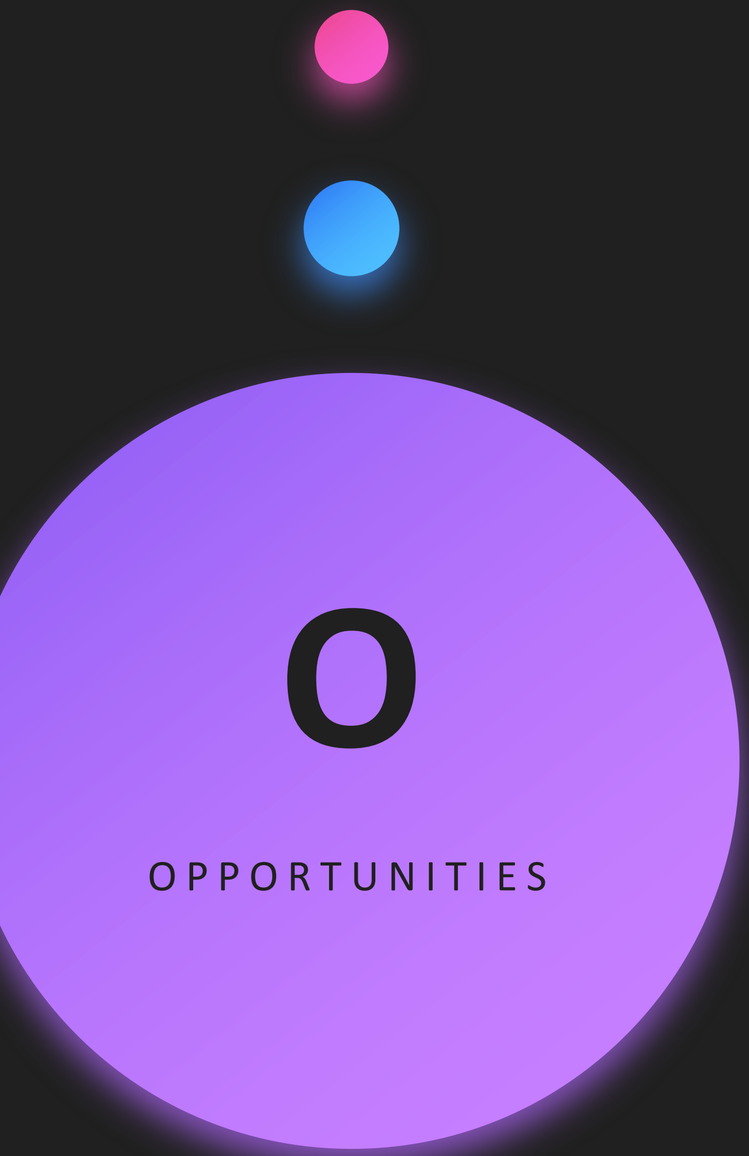
W

WEAKNESSES

Weaknesses

Every technology has some disadvantages, and Graphql do have few disadvantages.

- Query Complexity & Depths.
- Rate Limiting & Timeouts.
- Caching.

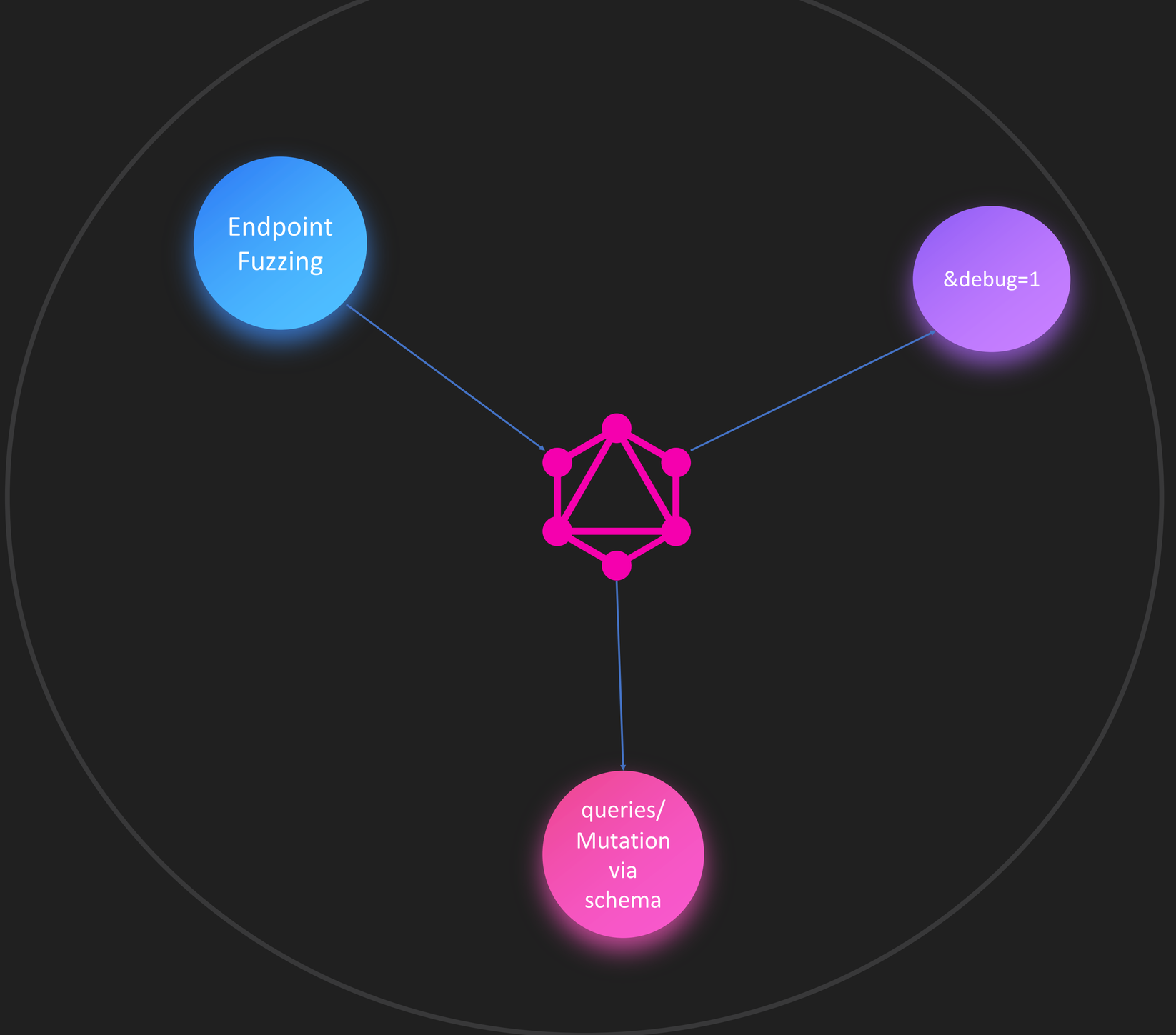


Opportunity for Hackers

- There is a wide scope for the pentesters & bug bounty hunters on GraphQL.
- The GraphQL Endpoints like /graphql or /graphiql are still publicly available out there due missing security best practices.

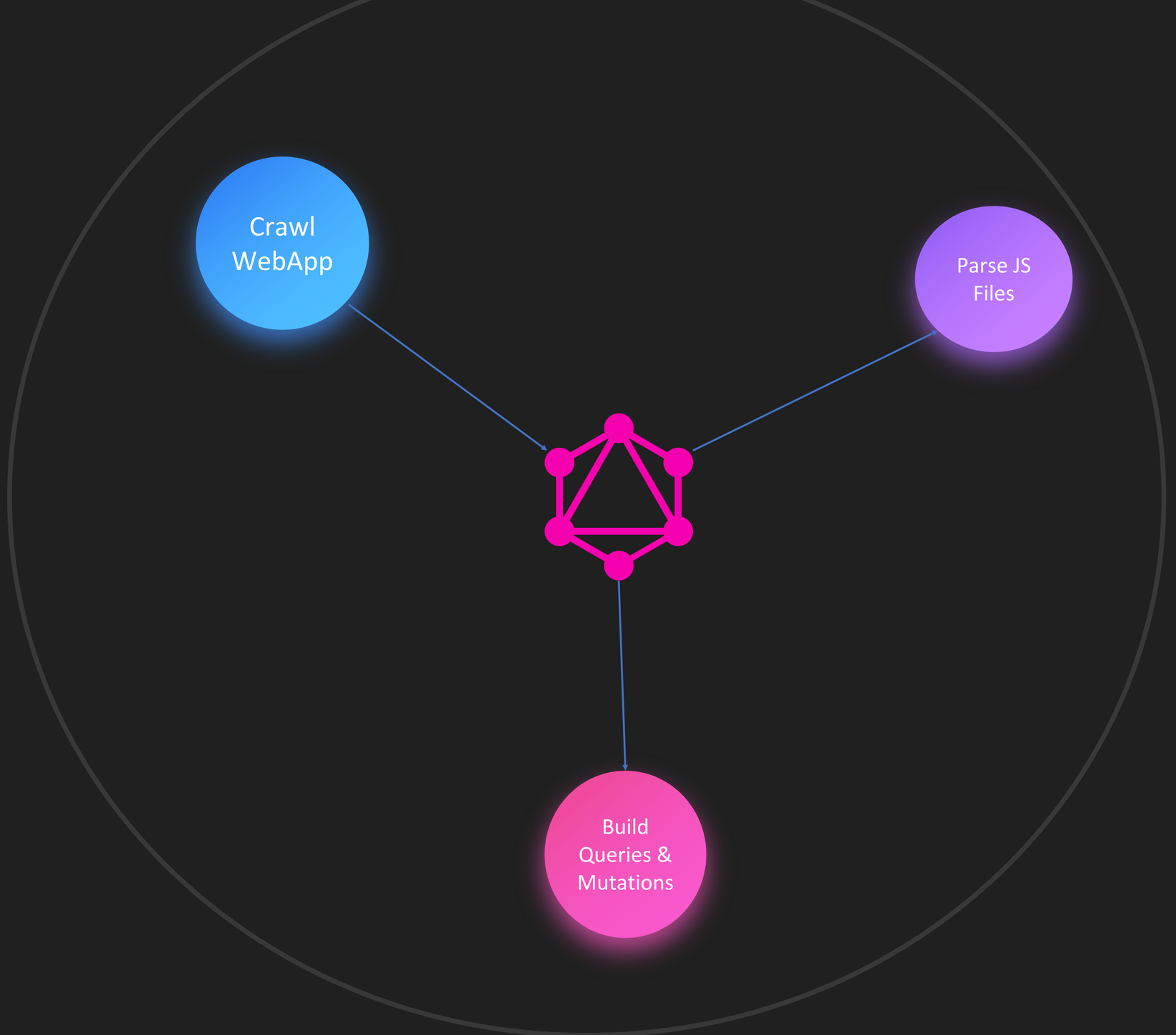
0

RECON - INTROSPECTION ALLOWED



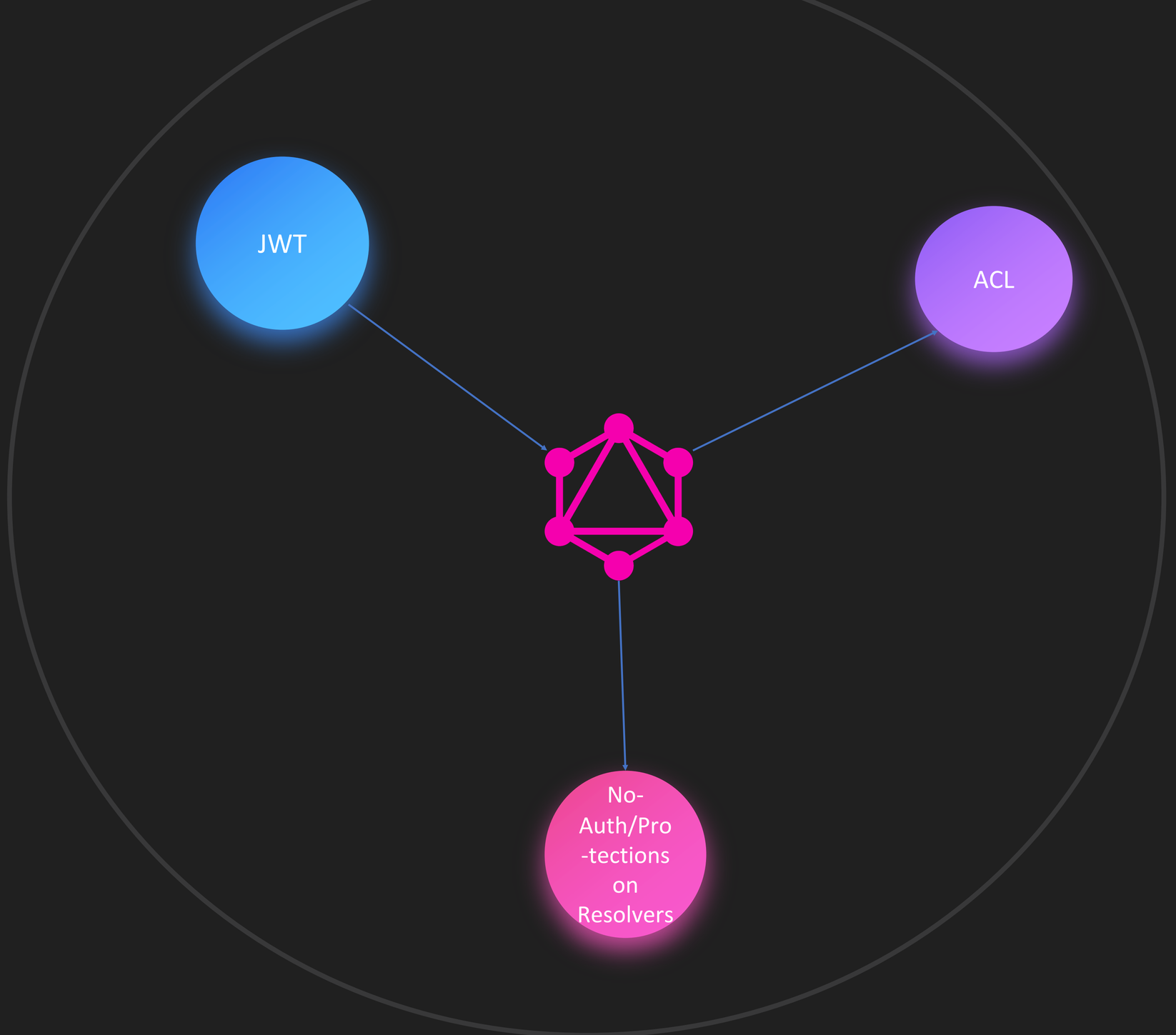
O

RECON TO RESCUE WHEN INTROSPECTION DISABLED



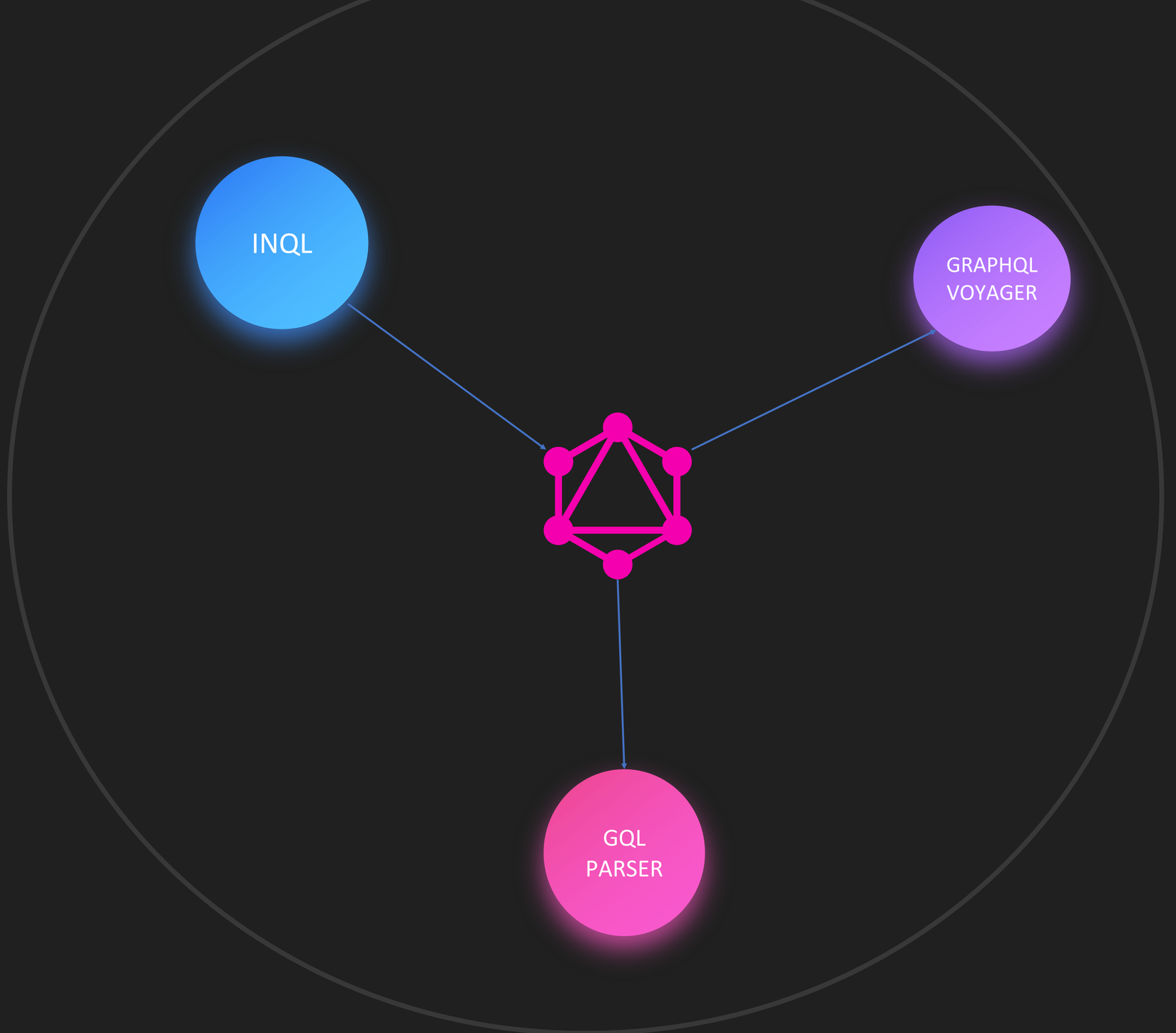
0

LOOK FOR THE AUTHENTICATION



0

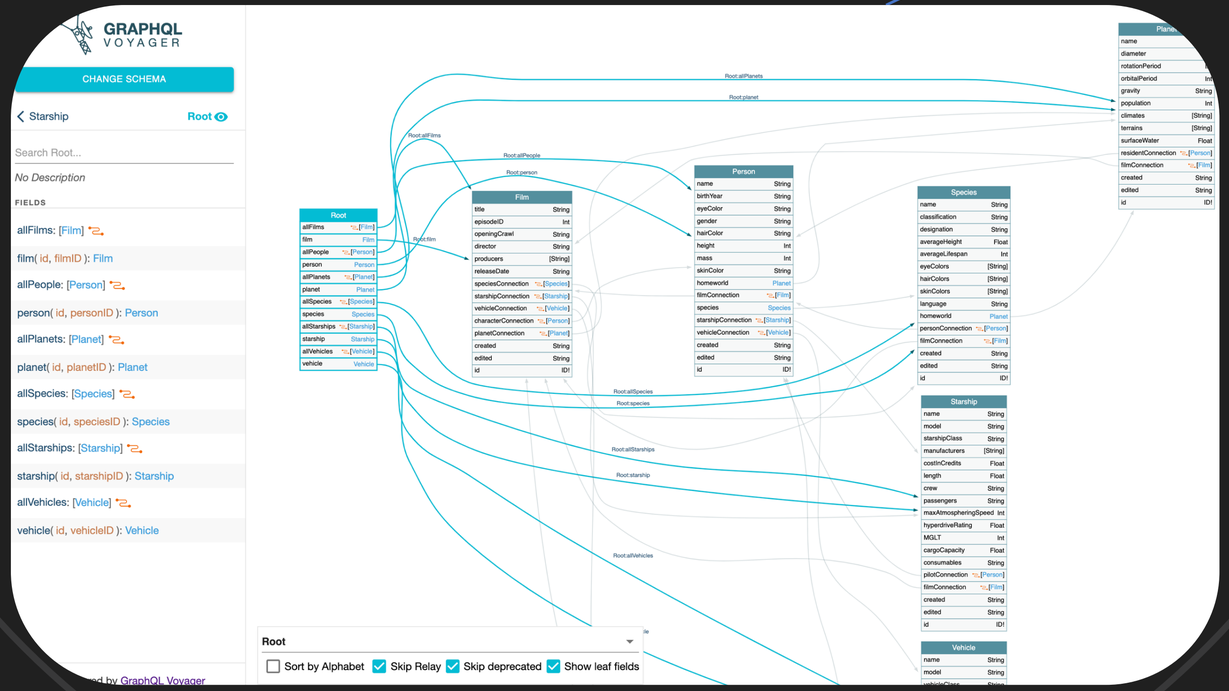
TOOLS TO RESCUE



O

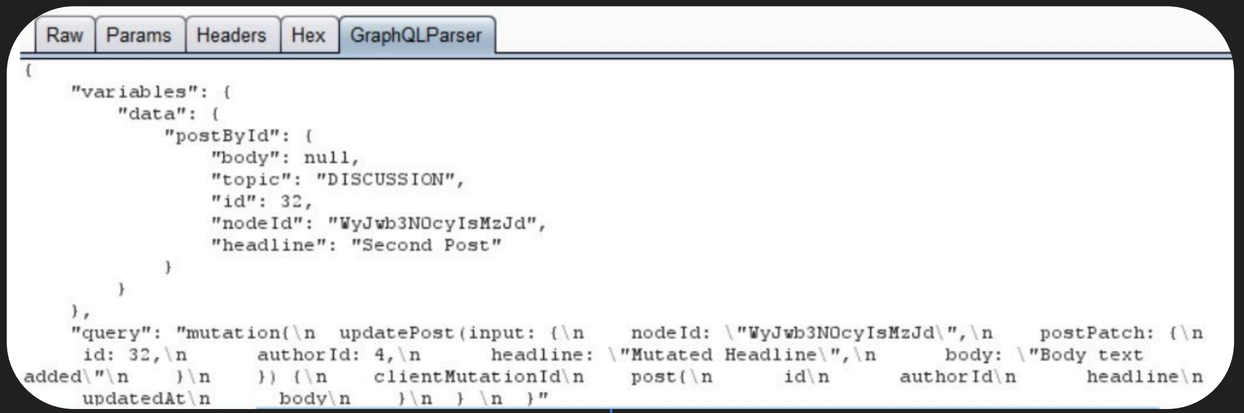
TOOLS TO RESCUE

GRAPHQL VOYAGER



0

TOOLS TO RESCUE



GQL
PARSER

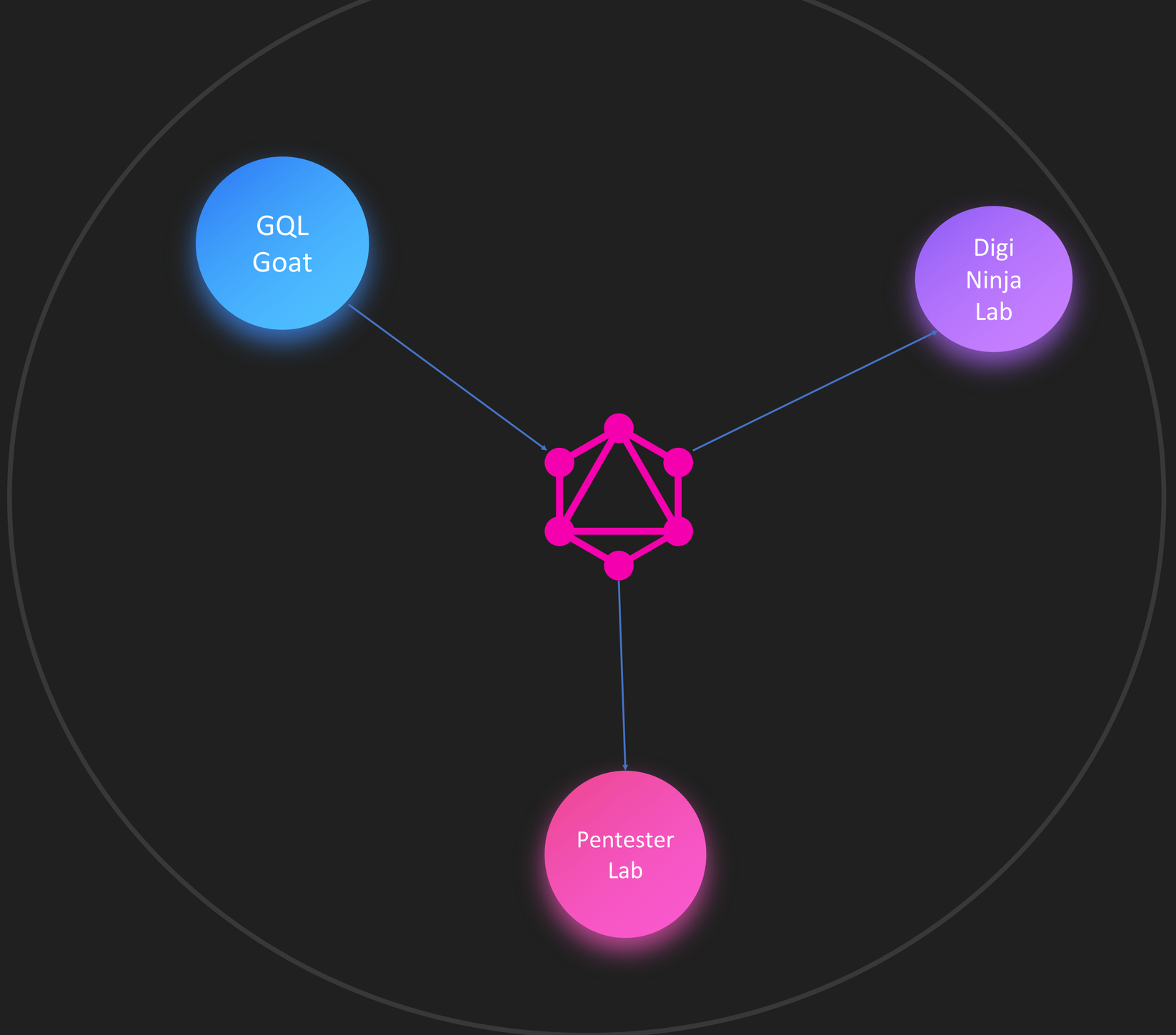
0

TOOLS TO RESCUE

INQL

0

LABS TO PRACTICE



Threats!!!

GraphQL gives enormous power to clients.
But with great power come great responsibilities !!!

Vulnerabilities!!!

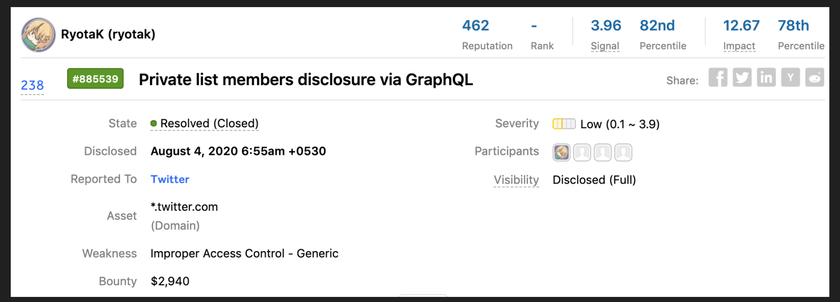
Most of all vulnerabilities related to REST APIs & WebApp are applicable for GraphQL as well.

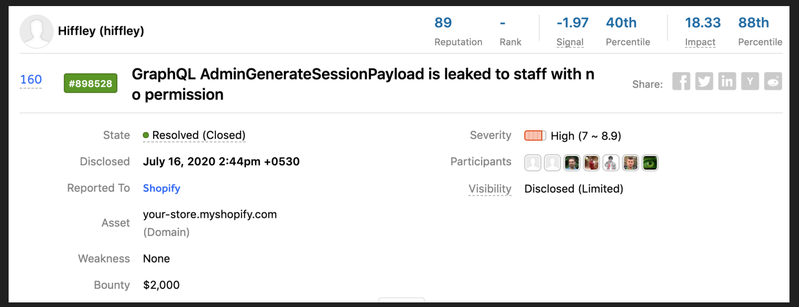
- SQL Injection
- NoSQL Injection
- Access Control Related Issues.
- Mass Assignment
- IDOR
- Bypassing 2FA/BruteForce Attacks.
- DOS Attacks etc.,

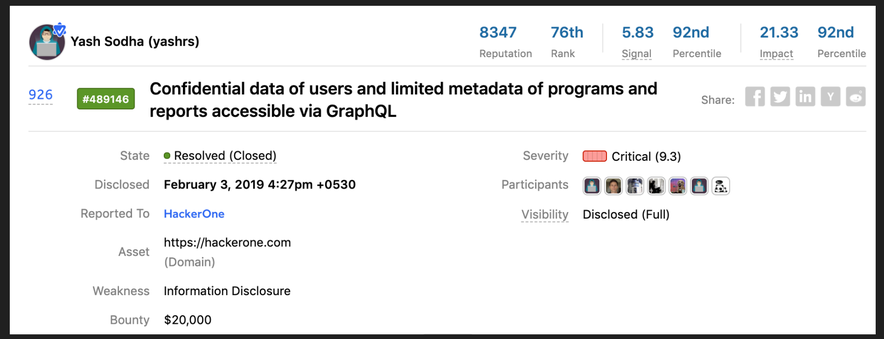

STOP TALKING
SHOW ME A DEMO !!!

Threats!!!

GraphQL is great, because it gives client so much more power. But if not used properly it could cost them more they can imagine.







Threats!!!

There are many approaches to secure your GraphQL server against these queries, but none of them is bullet proof. It’s important to know what options are available and know their limits and take best decisions out of it!.

- Disable well known /graphql & /graphiql endpoints from the domain.
- Craft your own schema and avoid using autogenerated SDL which creates queries and mutations.
- Input validation, Authentication & Authorization should never be forgotten.
- Never trust user inputs.
- Enforce a limit on maximum query depth(~<10), Query complexity, timeouts & enabled throttling based on the server time & query complexity.

References

Labs:

- https://github.com/CarveSystems/vulnerable-graphql-api
- https://graphqlab.digi.ninja/
- https://pentesterlab.com/exercises/graphql/online
- https://www.hackerone.com/blog/graphql-week-hacker101-capture-flag-challenges

Tools:

- https://github.com/doyensec/inql
- https://github.com/br3akp0int/GQLParser

Credits

Slide Template Credit:

https://hislide.io/

Demo App Credit:

https://carvesystems.com/

Thank you☺