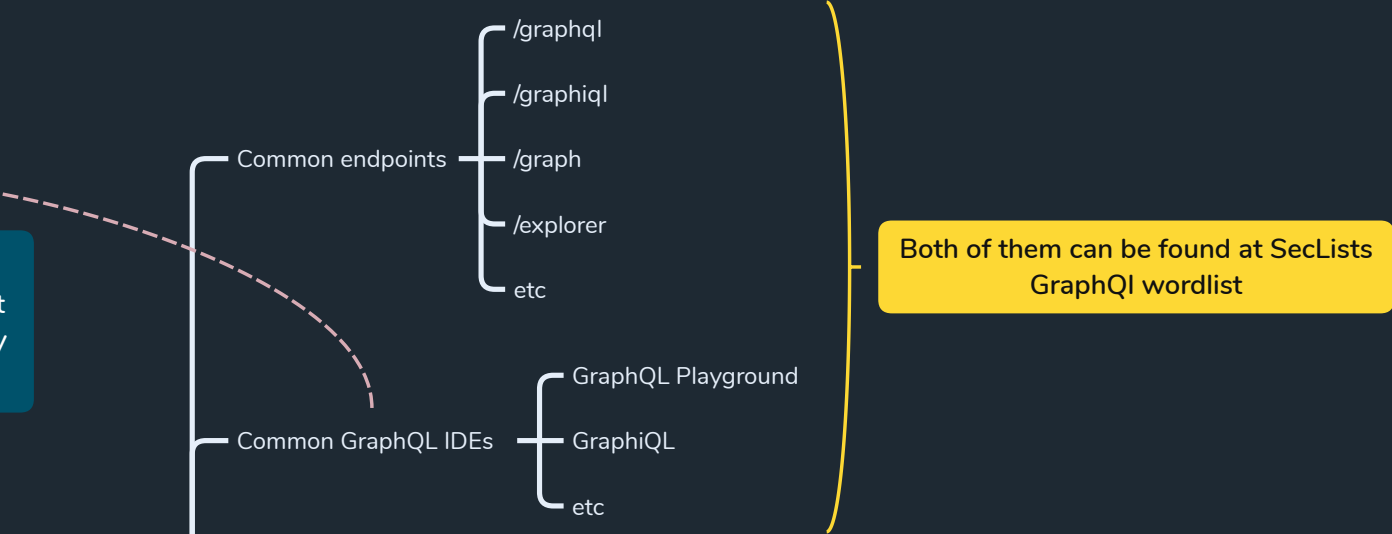


API Pentesting Mindmap

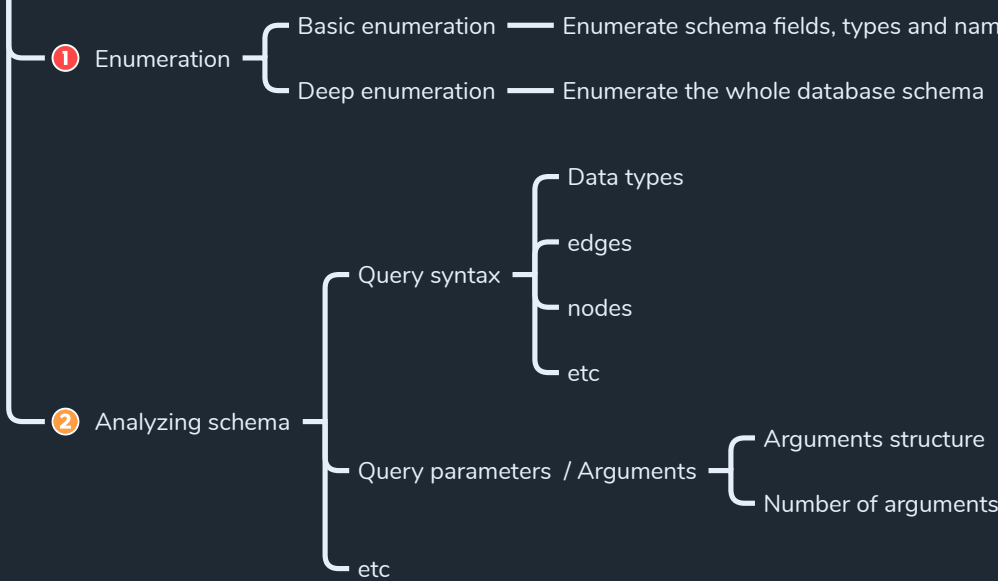
{{GraphQL Attacking}}

Some times it being left in the wild, so an attacker can get benefit from them, it makes the query implementation easier



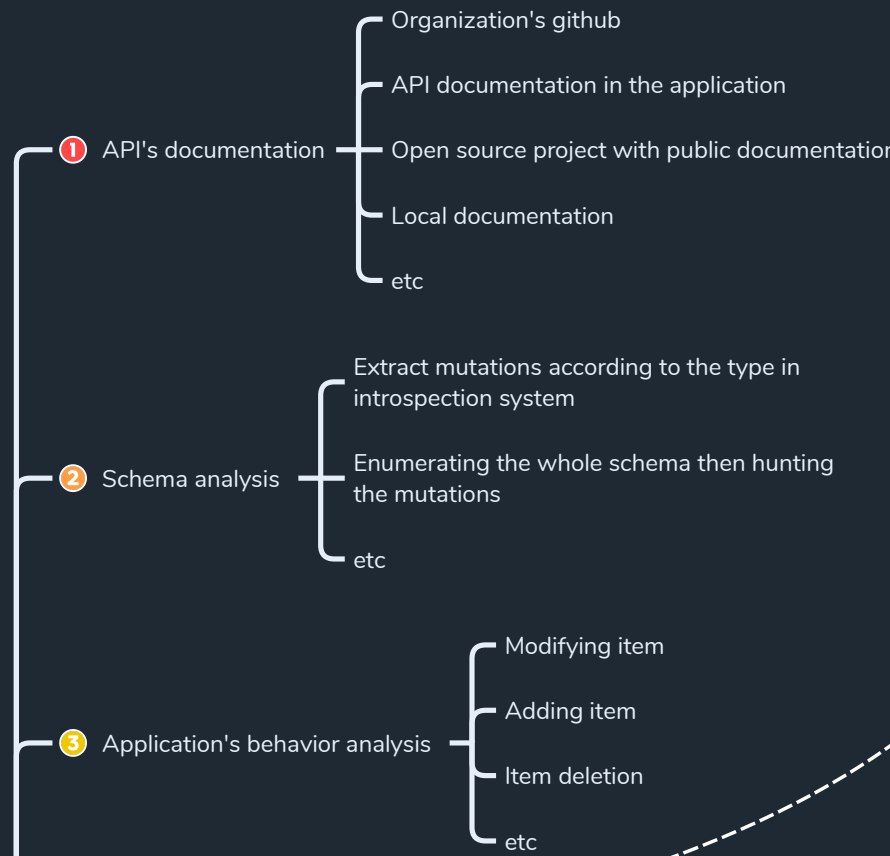
1 Endpoint discovery

2 Getting started with queries



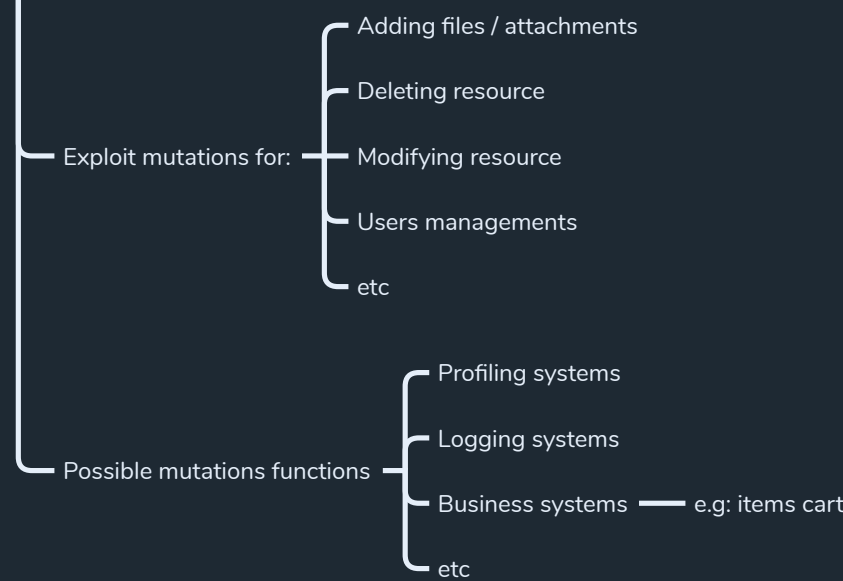
Both of them got payloads in payloadAllTheThings

3 Getting started with mutations



If you was able to control mutations then you might be able to modify / control data in server-side

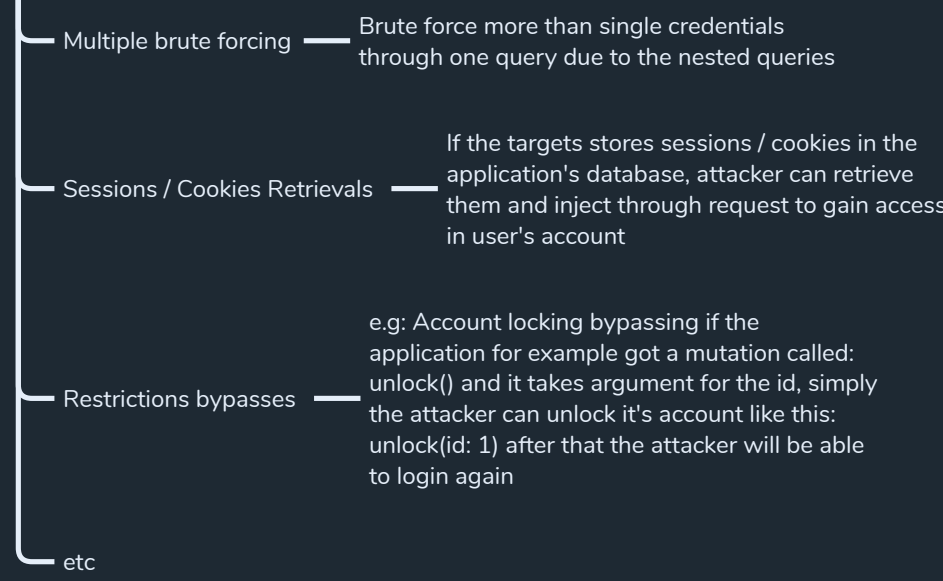
4 Mutations exploit



5 Queries exploit



6 Authentication attacks



7 Business logic attacks

