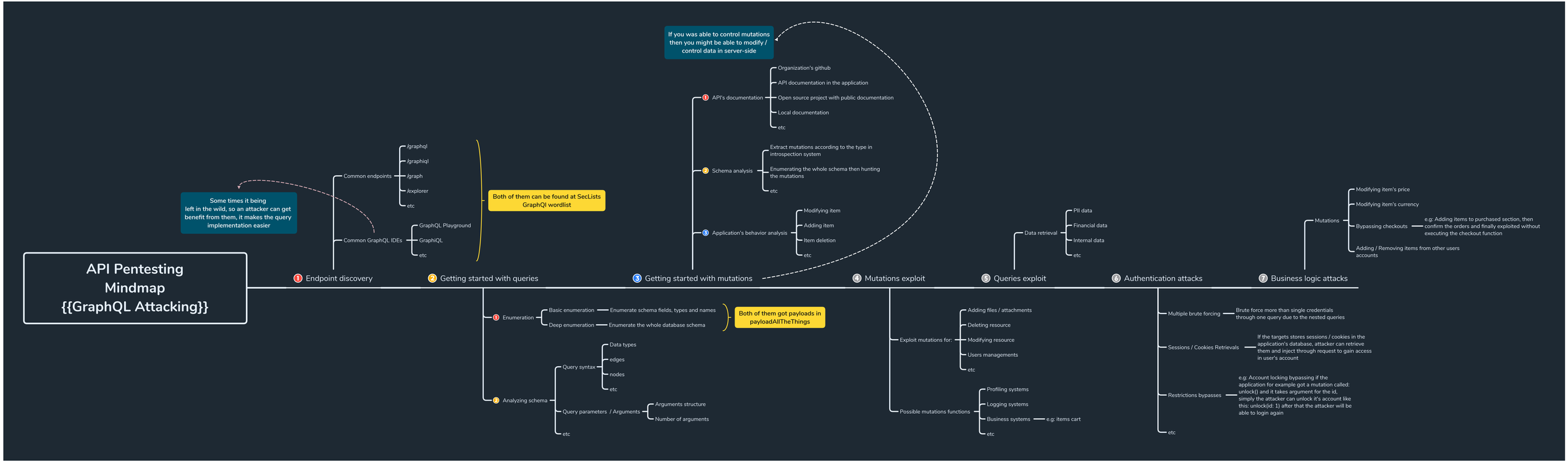
API Pentesting
Mindmap
{{GraphQL Attacking}}
1 Endpoint discovery
Common endpoints
/graphql
/graphiql
/graph
/explorer
etc
Common GraphQL IDEs
GraphQL Playground
GraphiQL
etc
Some times it being left in the wild, so an attacker can get benefit from them, it makes the query implementation easier
2 Getting started with queries
Both of them can be found at SecLists GraphQl wordlist
1 Enumeration
Basic enumeration
Enumerate schema fields, types and names
Deep enumeration
Enumerate the whole database schema
Both of them got payloads in payloadAllTheThings
2 Analyzing schema
Query syntax
Data types
edges
nodes
etc
Query parameters / Arguments
Arguments structure
Number of arguments
etc
3 Getting started with mutations
If you was able to control mutations then you might be able to modify / control data in server-side
1 API's documentation
Organization's github
API documentation in the application
Open source project with public documentation
Local documentation
etc
2 Schema analysis
Extract mutations according to the type in introspection system
Enumerating the whole schema then hunting the mutations
etc
3 Application's behavior analysis
Modifying item
Adding item
Item deletion
etc
4 Mutations exploit
Exploit mutations for:
Adding files / attachments
Deleting resource
Modifying resource
Users managements
etc
Possible mutations functions
Profiling systems
Logging systems
Business systems
e.g: items cart
etc
5 Queries exploit
Data retrieval
PII data
Financial data
Internal data
etc
6 Authentication attacks
Multiple brute forcing
Brute force more than single credentials through one query due to the nested queries
Sessions / Cookies Retrievals
If the targets stores sessions / cookies in the application's database, attacker can retrieve them and inject through request to gain access in user's account
Restrictions bypasses
e.g: Account locking bypassing if the application for example got a mutation called: unlock() and it takes argument for the id, simply the attacker can unlock it's account like this: unlock(id: 1) after that the attacker will be able to login again
etc
7 Business logic attacks
Mutations
Modifying item's price
Modifying item's currency
Bypassing checkouts
e.g: Adding items to purchased section, then confirm the orders and finally exploited without executing the checkout function
Adding / Removing items from other users accounts