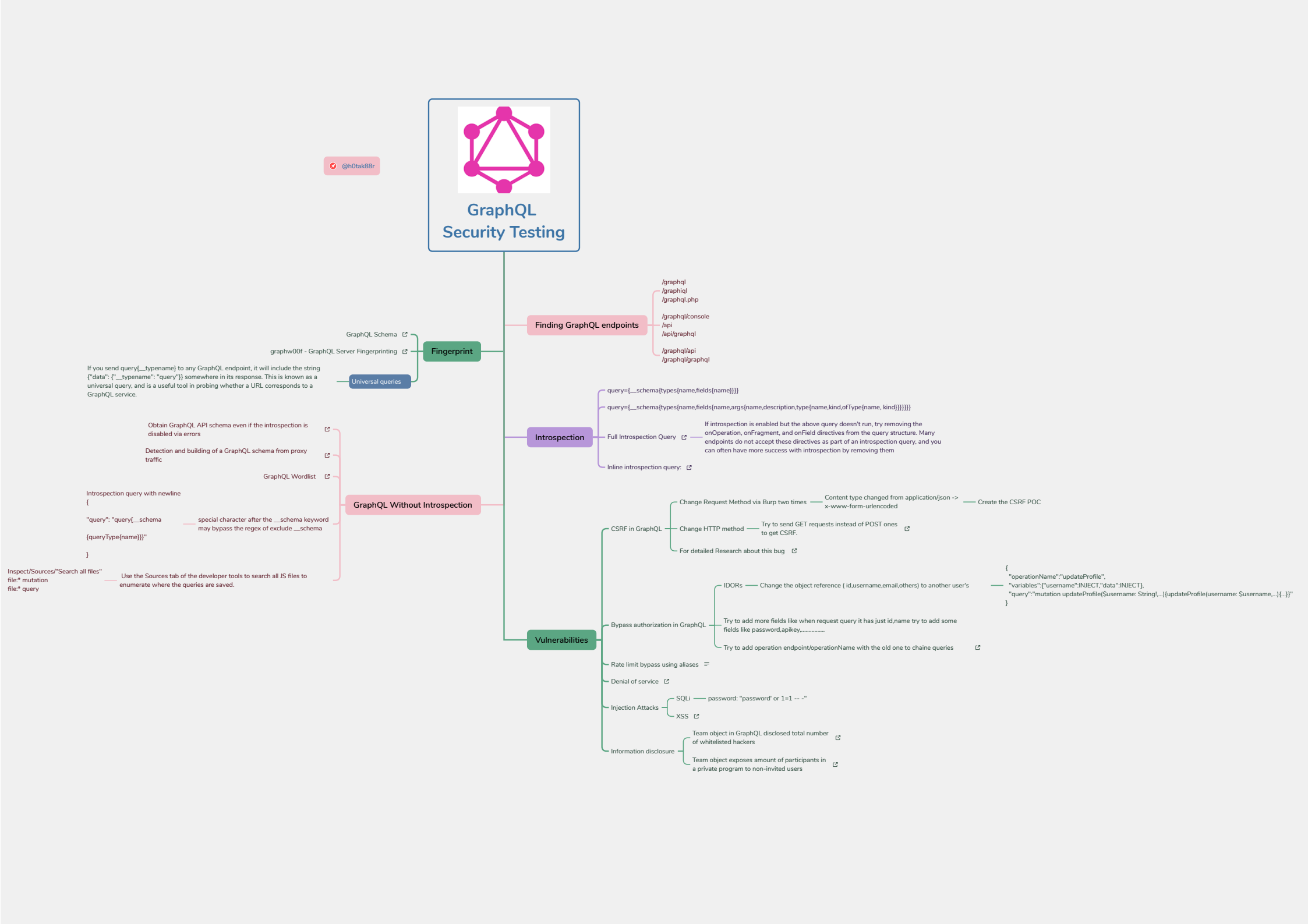
@h0tak88r
GraphQL Security Testing
Finding GraphQL endpoints
/graphql
/graphiql
/graphql.php
/graphql/console
/api
/api/graphql
/graphql/api
/graphql/graphql
Fingerprint
GraphQL Schema
graphw00f - GraphQL Server Fingerprinting
Universal queries
If you send query{__typename} to any GraphQL endpoint, it will include the string {"data": {"__typename": "query"}} somewhere in its response. This is known as a universal query, and is a useful tool in probing whether a URL corresponds to a GraphQL service.
Introspection
query={__schema{types{name,fields{name}}}}
query={__schema{types{name,fields{name,args{name,description,type{name,kind,ofType{name, kind}}}}}}}
Full Introspection Query
If introspection is enabled but the above query doesn't run, try removing the onOperation, onFragment, and onField directives from the query structure. Many endpoints do not accept these directives as part of an introspection query, and you can often have more success with introspection by removing them
Inline introspection query:
GraphQL Without Introspection
Obtain GraphQL API schema even if the introspection is disabled via errors
Detection and building of a GraphQL schema from proxy traffic
GraphQL Wordlist
Introspection query with newline
{
"query": "query{__schema
special character after the __schema keyword may bypass the regex of exclude __schema
{queryType{name}}}"
}
Inspect/Sources/"Search all files"
file:* mutation
file:* query
Use the Sources tab of the developer tools to search all JS files to enumerate where the queries are saved.
Vulnerabilities
CSRF in GraphQL
Change Request Method via Burp two times
Content type changed from application/json -> x-www-form-urlencoded
Create the CSRF POC
Change HTTP method
Try to send GET requests instead of POST ones to get CSRF.
For detailed Research about this bug
Bypass authorization in GraphQL
IDORs
Change the object reference (id,username,email,others) to another user's
{
"operationName":"updateProfile",
"variables":{"username":INJECT,"data":INJECT},
"query":"mutation updateProfile($username: String!,...){updateProfile(username: $username,...){...}}"
}
Try to add more fields like when request query it has just id,name try to add some fields like password,apikey,.....
Try to add operation endpoint/operationName with the old one to chaine queries
Rate limit bypass using aliases
Denial of service
Injection Attacks
SQLi
password: "password' or 1=1 -- -"
XSS
Information disclosure
Team object in GraphQL disclosed total number of whitelisted hackers
Team object exposes amount of participants in a private program to non-invited users