Cowbell Shop 1 - NOSQL

Explain the security problem

The auth.js makes a JSON.parse(...) by this the {"$ne": null} is parsed to valid javascript code. It would be better to parse to a string.

Explain your attack. (exploit, screenshot, hacking journal)

Add {"$ne": null} to username and password field an press login. Javascript parse this to valid javascript code and the following query is executed:

```
Account.findOne({
            username: {"$ne": null},
            password: {"$ne": null},
            isRetailer: false,
        }, {
            password: false,....
```

Explain mitigation (remedy)

Don't use JSON.parse and eval(). Input should be parsed to a string before the query takes place. The best would be to use validator.js.