NoSQL

MEANS *no* SECURITY?

Philipp Krenn

@xeraa

elastic

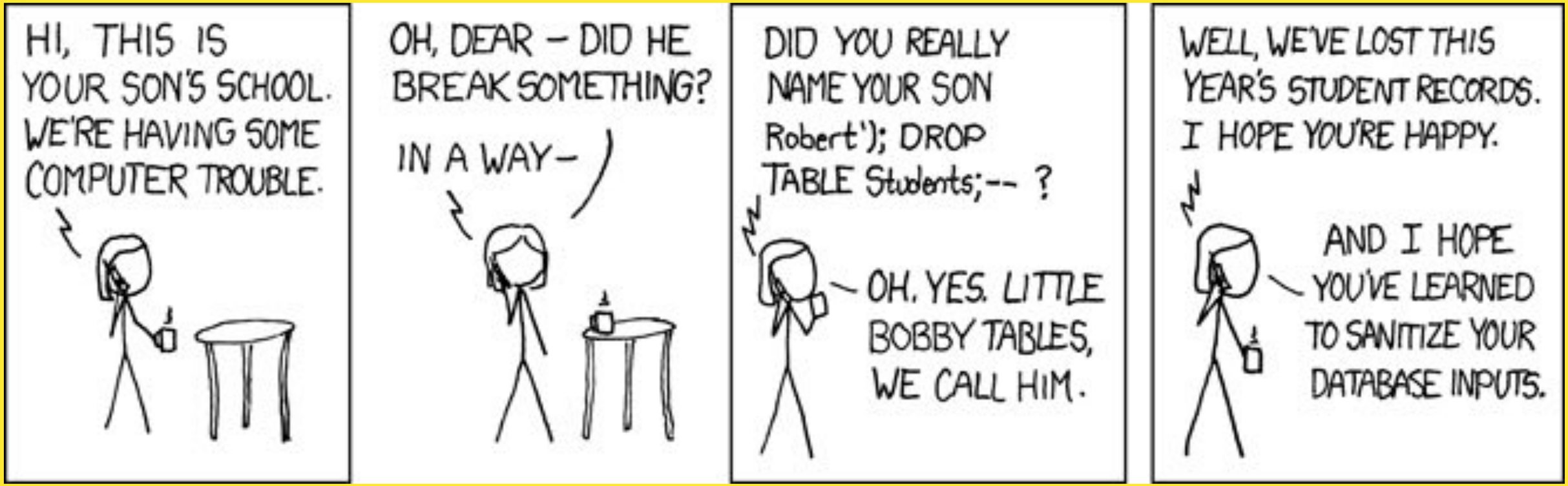
elastic

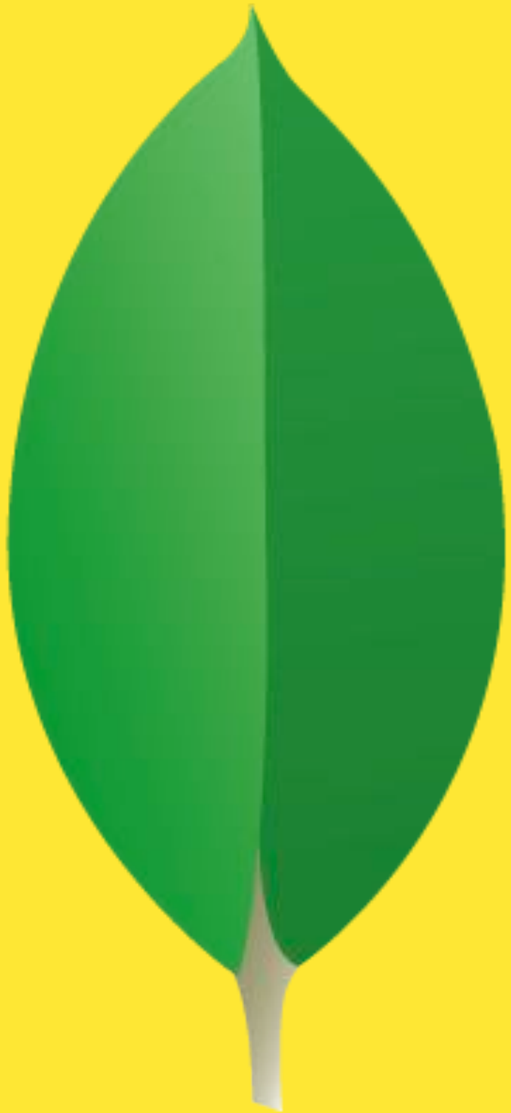
INFRASTRUCTURE | DEVELOPER ADVOCATE

ViennaDB

Papers We Love Vienna

elastic


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR - DID HE BREAK SOMETHING?
IN A WAY-
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.



elastic

Web Scale / MongoDB

elastic

SQL Injections?

JavaScript Injection

HTTP://WWW.KALZUMEUS.COM/2010/09/22/SECURITY-LESSONS-LEARNED-FROM-THE-DIASPORA-LAUNCH/

```
def self.search(query)
  Person.all('$where' => "function() {
    return this.diaspora_handle.match(/^#{query}/i) ||
           this.profile.first_name.match(/^#{query}/i) ||
           this.profile.last_name.match(/^#{query}/i);
  }")
end
```

Problem JS Evaluation

```
$where

db.eval()

db.runCommand( { mapReduce:

db.collection.group()
```

Solution JS Evaluation

DEACTIVATE: `--noscripting` **OR** `security.javascriptEnabled: false`

ESCAPE: `CodeWScope`

Saarbrücker Cybersicherheits-Studenten entdecken bis zu 40.000 ungesicherte Datenbanken im Internet

– http://www.uni-saarland.de/nc/aktuelles/artikel/nr/12173.html

Bound to all interfaces by default?

Authentication enabled by default?

Authentication & Authorization

Enable

`auth=true`

<3.0

MONGODB CHALLENGE RESPONSE

MONGODB-CR

>=3.0

IETF RFC 5802

SCRAM-SHA-1

SCRAM-SHA-1

CONFIGURABLE `iterationCount`

SALT PER USER INSTEAD OF SERVER

SHA-1 INSTEAD OF MD5

SERVER AUTHENTICATES AGAINST THE CLIENT AS WELL

Predefined Roles

`read` / `readAnyDatabase`

`readWrite` / `readWriteAnyDatabase`

`dbAdmin` / `dbAdminAnyDatabase`

`userAdmin` / `userAdminAnyDatabase`

`dbOwner`

BACKUP, RESTORE, CLUSTER MANAGEMENT,...

```
$ mongod --noauth --port 27017 --dbpath test/ --logpath testlog

$ mongo localhost/admin
> db.createUser({
  user: "philipp",
  pwd: "password",
  roles: [ {
    role: "root",
    db: "admin"
  } ]
})
> db.system.users.find()
> exit
```

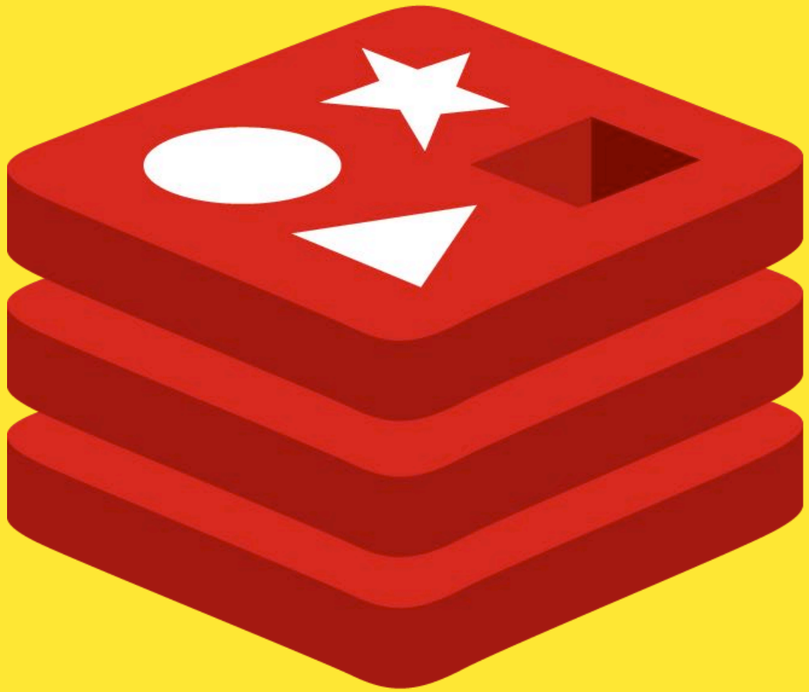
```
$ mongod --auth --port 27017 --dbpath test/ --logpath testlog

$ mongo localhost/admin
> show dbs
> exit

$ mongo localhost/admin -u philipp -p --authenticationDatabase admin
> show dbs
> db.createUser({
  user: "alice",
  pwd: "password",
  roles: [
    { role: "read", db: "testA" },
    { role: "readWrite", db: "testB" }
  ]
})
> db.system.users.find()
> exit
```

```
$ mongo localhost/testA -u alice -p --authenticationDatabase admin --norc
> db.test.insert({ foo: "bar" })
> db.test.find()
> use testB
> db.test.insert({ foo: "bar" })
> db.test.find()
> use testC
> db.test.find()
```

SSL Commercial
OR SELF-COMPILED



redis

Bound to all interfaces by default?

SINCE 3.2.0 (2016/05)

Protected Mode

ANSWER LOCAL QUERIES

RESPOND WITH AN ERROR FOR REMOTE

Authentication & ~~Authorization~~

a tiny layer of authentication

– http://redis.io/topics/security

AUTH <password> COMMAND

PLAIN-TEXT PASSWORD IN REDIS.CONF

NO (BUILT-IN) SSL OR RATE LIMITS

Hiding Commands

SET IN REDIS.CONF

RESET AFTER RESTART

```
rename-command CONFIG
mysecretconfigname
```

```
rename-command CONFIG ""
```

PS: Don't Pass in Random Lua Scripts

elasticsearch

elastic

HTTPS://WWW.ELASTIC.CO/COMMUNITY/SECURITY

CVE-2014-3120 (6.8): Dynamic scripting
CVE-2014-6439 (4.3): CORS misconfiguration
CVE-2015-1427 (6.8): Groovy sandbox escape
CVE-2015-3337 (4.3): Directory traversal
CVE-2015-4165 (3.3): File modifications
CVE-2015-5377 (5.1): RCE related to Groovy
CVE-2015-5531 (5.0): Directory traversal

HTTPS://WWW.ELASTIC.CO/COMMUNITY/SECURITY

CVE-2014-3120 (6.8): Dynamic scripting

CVE-2015-1427 (6.8): Groovy sandbox escape

CVE-2015-5377 (5.1): RCE related to Groovy

Painless

HIRED DEVELOPER

1 YEAR DEVELOPMENT

Why build a brand new language when there are already so many to choose from?

– https://www.elastic.co/blog/painless-a-new-scripting-language

Goal

SECURE & PERFORMANT

```
{"name": "Philipp", "goals": [9,27,15], "assists": [0,0,0]}

GET /hockey-stats/_search
{
  "query": {
    "function_score": {
      "script_score": {
        "script": {
          "lang": "painless",
          "inline": "int total = 0; for (int i = 0; i < input.doc.goals.size(); ++i) {
                       total += input.doc.goals[i];
                     }
                     return total;"
        }
      }
    }
  }
}
```

STATIC & DYNAMIC TYPES

LIST, MAP, AND ARRAY INITIALIZERS

SHORTCUTS RELATED TO MAPS AND LISTS

BUILT-IN REGULAR EXPRESSIONS

LAMBDA EXPRESSIONS

PERFORMANCE SIMILAR TO JAVA

METHOD AND FIELD LEVEL WHITELISTING (NO `<class>.forName`)

SCORING SCRIPTS

PAINLESS DEFAULT

GROOVY, PYTHON, JAVASCRIPT DEPRECATED

PS: Authentication, Authorization & SSL

Conclusion

Injections Are Still a Thing

Enable Security by Default

Be Creative — or not

Custom Scripting Can Make Sense

elastic

Security Takes Time

Thanks!

QUESTIONS?

Philipp Krenn @xeraa

PS: STICKERS

elastic