

NoSQL

MEANS *No* SECURITY?

Philipp Krenn

@xeraa



elastic

INFRASTRUCTURE | DEVELOPER ADVOCATE

341 systems in ranking, February 2018

Rank			DBMS	Database Model	Score		
Feb 2018	Jan 2018	Feb 2017			Feb 2018	Jan 2018	Feb 2017
1.	1.	1.	Oracle +	Relational DBMS	1303.28	-38.66	-100.55
2.	2.	2.	MySQL +	Relational DBMS	1252.47	-47.24	-127.83
3.	3.	3.	Microsoft SQL Server +	Relational DBMS	1122.04	-26.03	-81.42
4.	4.	4.	PostgreSQL +	Relational DBMS	388.38	+2.19	+34.70
5.	5.	5.	MongoDB +	Document store	336.42	+5.47	+0.92
6.	6.	6.	DB2 +	Relational DBMS	189.57	-0.36	+2.07
7.	7.	7.	Microsoft Access	Relational DBMS	171.07	-2.57	-3.32
8.	↑ 9.	↑ 10.	Redis +	Key-value store	127.02	+3.85	+12.98
9.	↑ 10.	↑ 11.	Elasticsearch +	Search engine	125.32	+2.76	+17.01
10.	↓ 8.	↓ 7.	Cassandra +	Wide column store	122.78	-1.10	-11.60
11.	11.	↓ 9.	SQLite +	Relational DBMS	117.27	+3.02	+1.96
12.	12.	12.	Teradata	Relational DBMS	72.99	+0.36	-2.60
13.	↑ 15.	↑ 16.	Splunk	Search engine	67.27	+3.27	+11.24
14.	14.	14.	Solr	Search engine	63.87	-0.50	-3.81
15.	↓ 13.	↓ 13.	SAP Adaptive Server +	Relational DBMS	63.49	-1.98	-8.25

<https://db-engines.com/en/ranking>

341 systems in ranking, February 2018

Rank			DBMS	Database Model	Score		
Feb 2018	Jan 2018	Feb 2017			Feb 2018	Jan 2018	Feb 2017
1.	1.	1.	Oracle	Relational DBMS	1303.28	-38.66	-100.55
2.	2.	2.	MySQL	Relational DBMS	1252.47	-47.24	-127.83
3.	3.	3.	Microsoft SQL Server	Relational DBMS	1122.04	-26.03	-81.42
4.	4.	4.	PostgreSQL	Relational DBMS	388.38	+2.19	+34.70
5.	5.	5.	MongoDB	Document store	336.42	+5.47	+0.92
6.	6.	6.	DB2	Relational DBMS	189.97	-0.30	+2.07
7.	7.	8.	Microsoft Access	Relational DBMS	130.07	+3.37	-3.32
8.	9.	10.	Redis	Key-value store	127.02	+3.88	+12.98
9.	10.	11.	Elasticsearch	Search engine	125.32	+2.76	+17.01
10.	8.	7.	Cassandra	Wide column store	122.78	-1.10	-11.60
11.	11.	9.	SQLite	Relational DBMS	117.27	+3.02	+1.96
12.	12.	12.	Teradata	Relational DBMS	72.99	+0.36	-2.60
13.	15.	16.	Splunk	Search engine	67.27	+3.27	+11.24
14.	14.	14.	Solr	Search engine	63.87	-0.50	-3.81
15.	13.	13.	SAP Adaptive Server	Relational DBMS	63.49	-1.98	-8.25

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.



Marcus Fulbright

@MarcusFulbright

Follow



Best argument for NoSQL: You can't have SQL injection attacks if you don't have SQL.

1:32 AM - 27 Oct 2017

8 Retweets 16 Likes



4

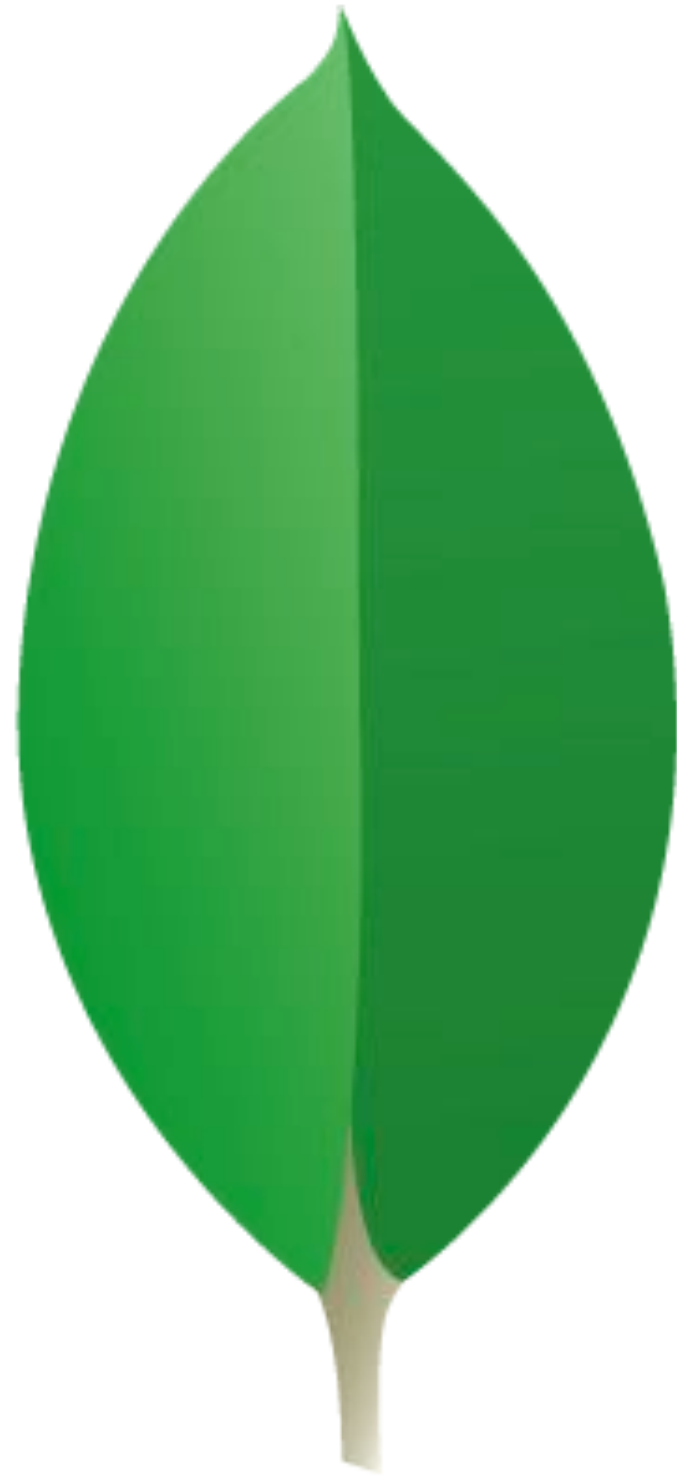


8



16





Web Scale / MongoDB

YouTube

Upload





Adam Kent

@akent

Follow



MongoDB IPO? Now you can lose your data
AND your money!

2:49 AM - 22 Sep 2017

18 Retweets 15 Likes



1



18



15



InjectiOns

JavaScript Injection

[HTTP://WWW.KALZUMEUS.COM/2010/09/22/SECURITY-LESSONS-LEARNED-FROM-THE-DIASPORA-LAUNCH/](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>**,
Feb 2015

*Massive ransomware attack takes out
27,000 MongoDB servers*

– **<http://www.techrepublic.com/article/massive-ransomware-attack-takes-out-27000-mongodb-servers/>**, Jan 2017

Bound to all interfaces by default?

MongoDB 3.6 comes hardened against database ransomware by default



by **MATTHEW HUGHES** — 28 days ago in **SECURITY**

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

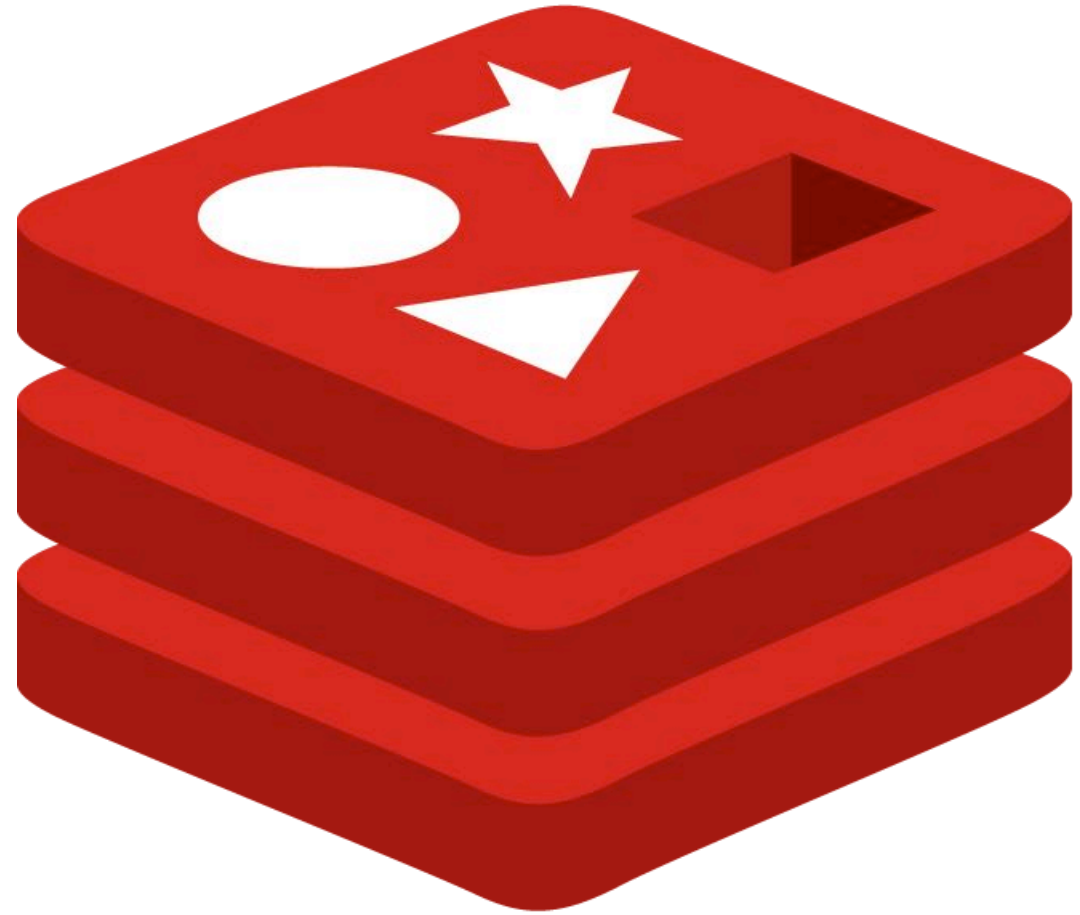
BACKUP, RESTORE, CLUSTER MANAGEMENT,...



≥ 3.0

SSL INCLUDED

(ALMOST) EVERYWHERE



redis

Bound to all interfaces by default?

Protected Mode

>=3.2.0

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



Bound to all interfaces by default?

Broadcasting on the local subnet?

Running as root?

A large group of cockroaches, likely German cockroaches, are shown crawling on a piece of light-colored wood. The cockroaches are dark brown with lighter brown stripes on their backs. The background is dark and out of focus, suggesting a natural or laboratory environment. The text is overlaid on the image.

Cockroaches

claims that disappear for a while when proved wrong, but just keep on coming back

Scripting

ELASTICSEARCH

[HTTPS://WWW.ELASTIC.CO/COMMUNITY/SECURITY](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

ELASTICSEARCH

[HTTPS://WWW.ELASTIC.CO/COMMUNITY/SECURITY](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

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

```
POST posts/doc/1/_update
```

```
{  
  "script": {  
    "lang": "painless",  
    "source": ""  
if(ctx._source.details.containsKey("plus_ones")) {  
  ctx._source.details.plus_ones++;  
} else {  
  ctx._source.details.plus_ones = 1;  
}  
""  
  }  
}
```


Painless **DEFAULT**

GROOVY, PYTHON, JAVASCRIPT DEPRECATED

Authentication & Authorization



port:"9200" 200 OK



Explore

Downloads

Reports

Enterprise Access

Contact Us

My Account

Upgrade

Exploits

Maps

Images

Share Search

Download Results

Create Report

TOTAL RESULTS

15,356

TOP COUNTRIES

United States	3,968
China	2,908
France	1,023
Germany	721
Netherlands	632

TOP ORGANIZATIONS

Amazon.com	1,669
Hangzhou Alibaba Advertisin...	1,191
Microsoft Azure	675
OVH SAS	663
Digital Ocean	568

TOP OPERATING SYSTEMS

Linux 3.x	14
Windows 7 or 8	1

TOP PRODUCTS

Elastic	9,137
Elasticsearch	118

Welcome to Badoo!

31.222.67.197

u98.badoo.com

Greysom Limited

Added on 2017-12-06 16:20:41 GMT

United Kingdom

[Details](#)

HTTP/1.1 200 OK

Server: nginx

Date: Wed, 06 Dec 2017 16:20:41 GMT

Content-Type: text/html

Content-Length: 344

Last-Modified: Wed, 28 Sep 2016 15:37:33 GMT

Connection: keep-alive

ETag: "57ebe3bd-158"

Expires: Thu, 06 Dec 2018 16:20:41 GMT

Cache-Control: max-age=31536000

Cache-Control: no...

广发证券（香港）预约开户

59.41.16.181

China Telecom Guangdong

Added on 2017-12-06 16:18:52 GMT

China, Guangzhou

[Details](#)

HTTP/1.1 200 OK

Vary: Accept-Encoding

Last-Modified: Mon, 13 Nov 2017 06:06:57 GMT

Content-Length: 775

Cache-Control: max-age=0

Content-Type: text/html; charset=utf-8

ETag: W/"307-15fb3fce7e8"

X-Response-Time: 6ms

Date: Wed, 06 Dec 2017 16:52:09 GMT

Connection: keep-alive

5.79.76.116

LeaseWeb Netherlands B.V.

Added on 2017-12-06 16:17:23 GMT

Netherlands

[Details](#)

4.0 kB

1

Nodes

HTTP/1.1 200 OK

Content-Type: application/json; charset=UTF-8

Content-Length: 341

```
$ curl -XGET 'http://67.205.153.88:9200/_cat/indices'  
yellow open goal12          5 1 9397 0    27mb    27mb  
yellow open please_read     5 1      1 0    4.9kb   4.9kb  
yellow open un-webhose      5 1 2294 1   25.4mb  25.4mb  
yellow open goal11         5 1 4828 0   13.3mb  13.3mb
```

```
$ curl -XGET 'http://67.205.153.88:9200/please_read/_search?pretty'
{
  "took" : 1,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "failed" : 0
  },
  "hits" : {
    "total" : 1,
    "max_score" : 1.0,
    "hits" : [ {
      "_index" : "please_read",
      "_type" : "info",
      "_id" : "AVm3qmXeus_FduwRD54v",
      "_score" : 1.0,
      "_source" : {
        "Info" : "Your DB is Backed up at our servers, to restore send 0.5 BTC
                  to the Bitcoin Address then send an email with your server ip",
        "Bitcoin Address" : "12JNfaS2Gzic2vqzGMvDEo38MQSX1kDQrx",
        "Email" : "elasticsearch@mail2tor.com"
      }
    } ]
  }
}
```

1 Bitcoin equals

8588.10 US Dollar

<input type="text" value="1"/>	Bitcoin
<input type="text" value="8588,10"/>	US Dollar



Disclaimer



On 03 Feb 14:12, reports@reports.cert-bund.de wrote:

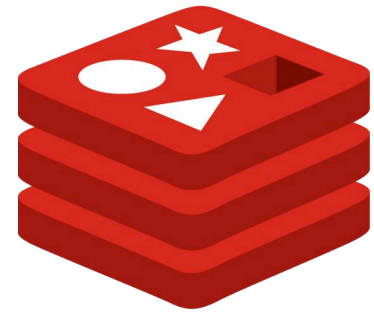
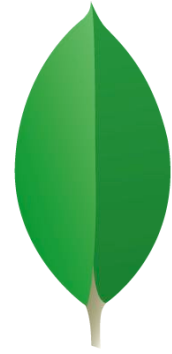
Dear Sir or Madam,

Elasticsearch is a popular search engine based on Apache Lucene, often used with web applications.

If an Elasticsearch server is openly accessible from the Internet and not protected by any forms of authentication, anyone who can connect to the server has unrestricted access to the data stored with it. This allows attackers to modify or delete any data or potentially steal sensitive information. In addition, prior to versions 1.2.x an attacker can use dynamic scripting to perform arbitrary code execution on the machine that Elasticsearch is hosted on.

Affected systems on your network:

Format: ASN | IP | Timestamp (UTC) | Elasticsearch version | Instance name
24940 | ██████████.176 | 2018-02-02 04:14:47 | 6.2.0 | docker-test-node-1



redis



elasticsearch

Conclusion

InjectiOns Are Still a Thing

Enable Security by Default

Be Creative — Or Not

Custom Scripting Can
Make Sense

Security Takes Time

Thanks!

QUESTIONS?

Philipp Krenn

@xeraa