Smart, Fast, Flexible

Vulnerability intelligence with Vulners DB

Kirill Ermakov,
Infosecurity Russia, 2016

#:whoami

- vulners.com founder
- QIWI Group CTO
- Web penetration tester
- Member of “hall-of-fames” (Yandex, Mail.ru, Apple and so on)
- JBFC community participant

Vulnerable

- Vulnerability - weakness which allows an attacker to reduce a system's information assurance (Wiki)
- Some kind of information that represents security issues
- Format-free description of function f(object, conditions) returning True/False

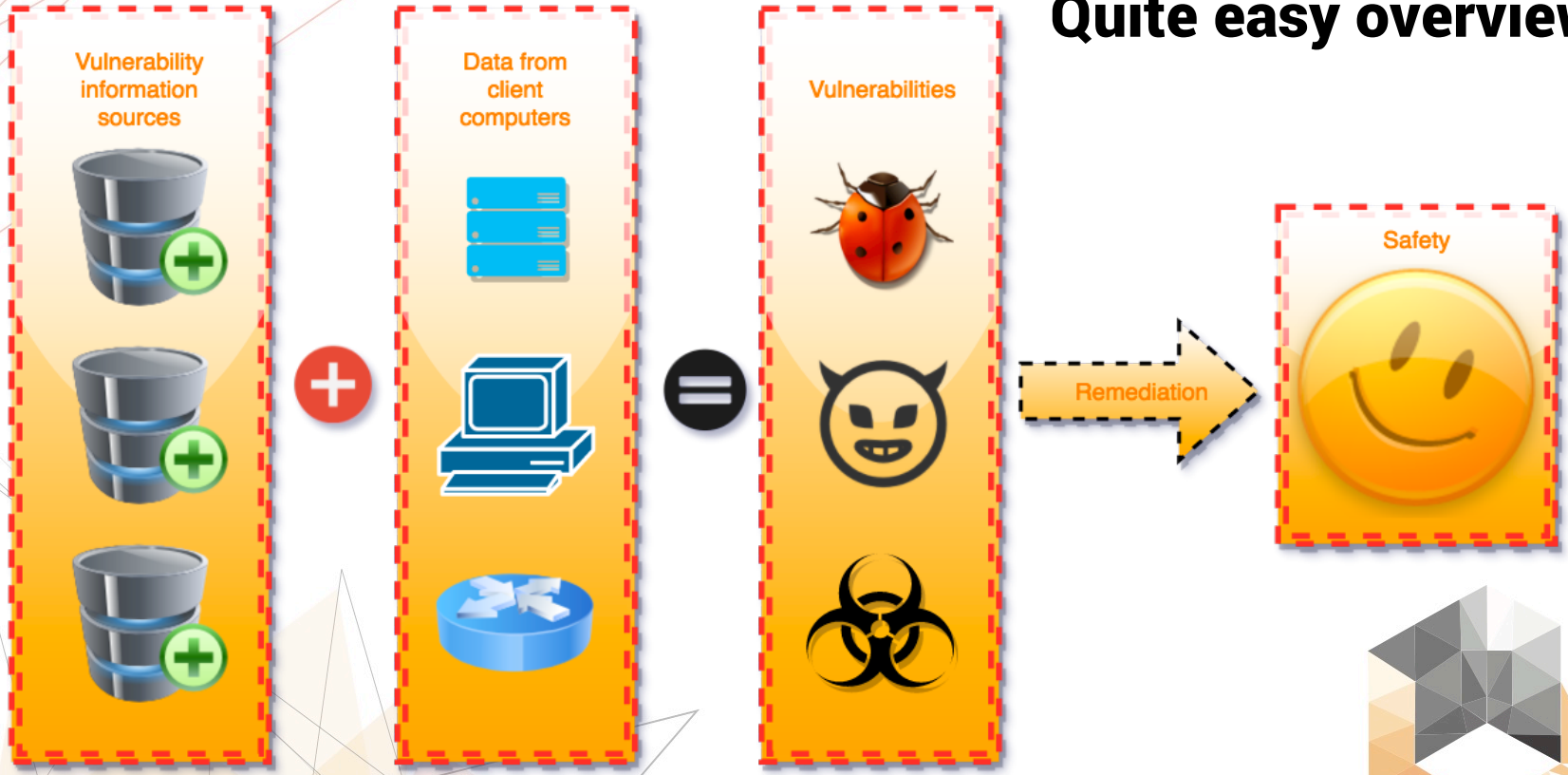
Captain Obvious: Risks

- Information systems takeover
- Revocation of the licenses
- Business continuity
- Money loss
- …and a lot of other bad things

Vulnerability management process

- Mandatory component of information security
- Need2be for a security-aware companies
- Necessary to perform in accordance with the PCIDSS and others
- Best practice for survival in the Internet

Quite easy overview



Content sources fail

- Born in 90’s
- Every product has it’s own source of vulnerability data
- Most information is not acceptable for automatic vulnerability scanners
- MITRE, NVD, SCAP, OVAL and others failed to standardize it
- Everyone is working on their own
- “Search”? Forget about it. Use Google instead.

vulners.com: Information security “Google”

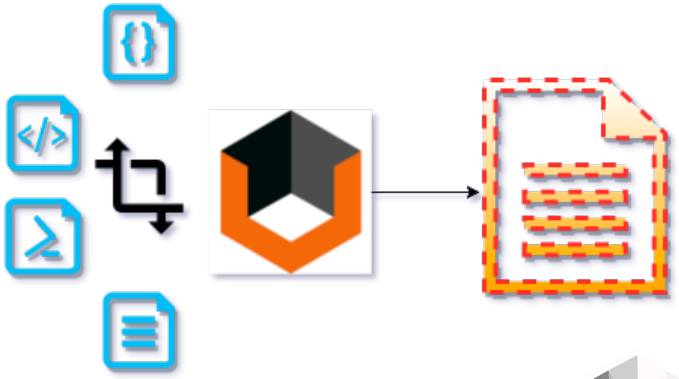
- Vulnerability source data aggregator
- Created by security specialists for security specialists
- Incredibly fast search engine
- Normalized, machine-readable content
- Audit features out-of-the-box
- API-driven development
- Absolutely free

Content

- Vendor security advisories
- Exploit databases
- Security scanners plugins and modules
- Bug bounty programs
- Informational resources
- 0 days from security scanners
- … 50+ different sources and growing

Normalization. We did it!

- All data has unified model
- Perfect for integration
- Security scanners ready
- Automatic updateable content
- Analytics welcome



Coverage? One of the largest security DB's

535928

BULLETINS

Security advisories and bulletins

SEE MORE >

51

VENDORS

Software vendors, bug bounty programs and other security sources

SEE MORE >

249212

EXPLOITS

Exploits for popular software

SEE MORE >

6.69

CVSS SCORE

Average CVSS score from beginning of time

SEE MORE >

Search

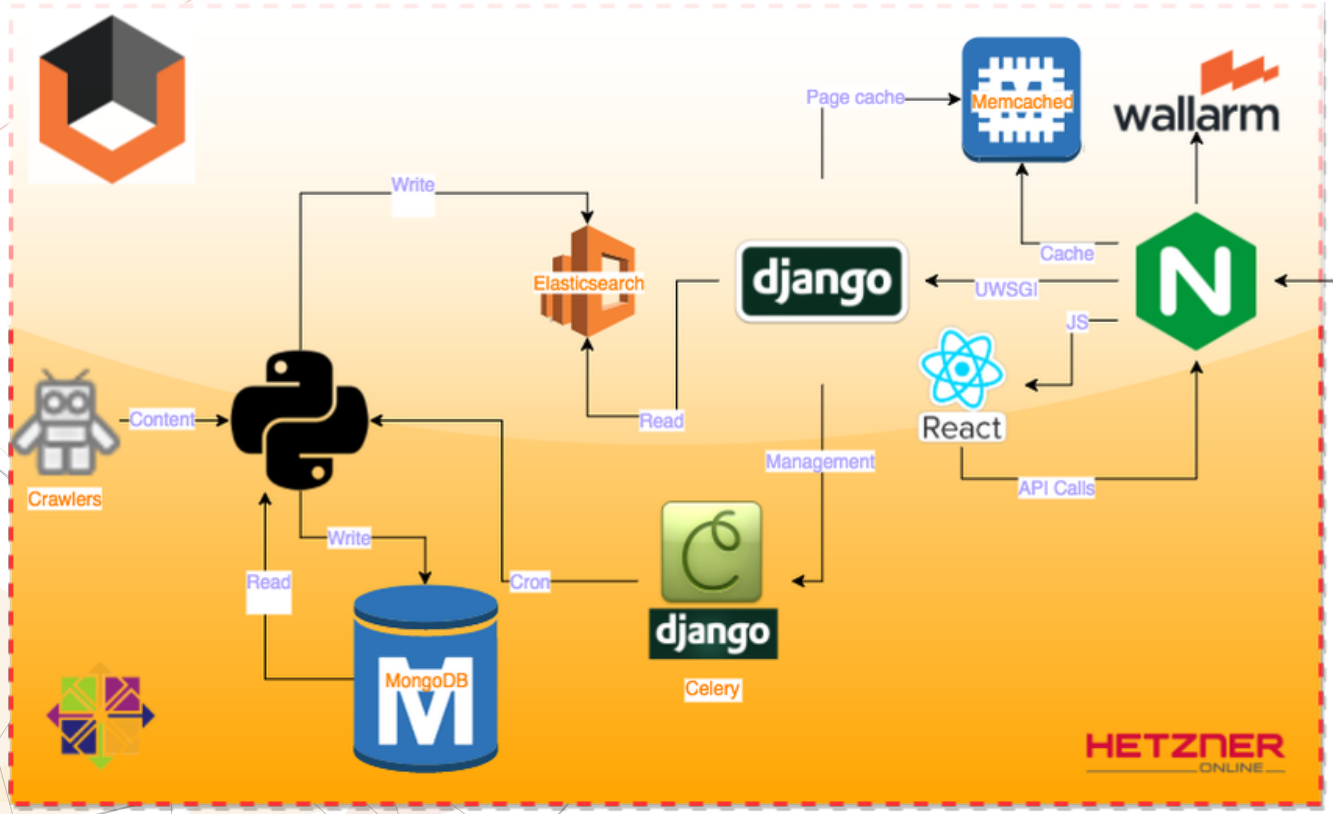
- Google-style search string
- Dorks, advanced queries and many more
- UX-driven
- Human-oriented
- References and data linkage
- Extremely fast

API


```
"documents": {
  "CESA-2016:1237": {
    "published": "2016-06-16T00:00:00",
    "modified": "2016-06-16T00:00:00",
    "id": "CESA-2016:1237",
    "type": "centos",
    "references": [
      "http://lists.centos.org/pipermail/centos-announce/2016-June/021910.html",
      "http://lists.centos.org/pipermail/centos-announce/2016-June/021909.html"
    ],
    "cvelist": [
      "CVE-2015-8895",
      "CVE-2015-8897",
      "CVE-2015-8896",
      "CVE-2016-5239",
      "CVE-2016-5240",
      "CVE-2015-8898",
      "CVE-2016-5118"
    ],
    "bulletinFamily": "unix",
    "cvss": {
      "score": 10.0,
      "vector": "AV:NETWORK/AC:LOW/Au:NONE/C:COMPLETE/I:COMPLETE/A:COMPLETE/"
    },
```


- REST/JSON
- Integration focused scan features
- Audit calls for self-made security scanners
- Easy expandable
- Content sharing features

Under the hood



Example: advanced queries

- Any complex query
  - *title:**httpd** type:**centos** order:**published** last 15 days*

- Sortable by any field of the model (type, CVSS, dates, reporter, etc)

- Apache Lucene syntax (AND, OR and so on)

- Exploit search by sources and CVE's
  - *cvelist:CVE-2014-0160 type:exploitdb*
  - *sourceData:.**bash_profile***
  - *sourceData:"magic bytes"*

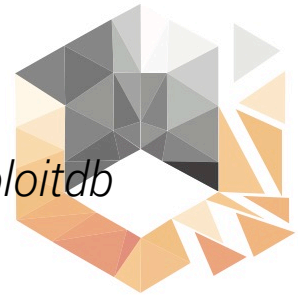
Example: API

- GET/POST REST API with JSON output

- Search
  - *https://vulners.com/api/v3/search/lucene/?query=type:centos%20cvss.score:[8%20TO%2010]%20order:published*

- Information
  - *https://vulners.com/api/v3/search/id?id=CESA-2016:1237&references=true*

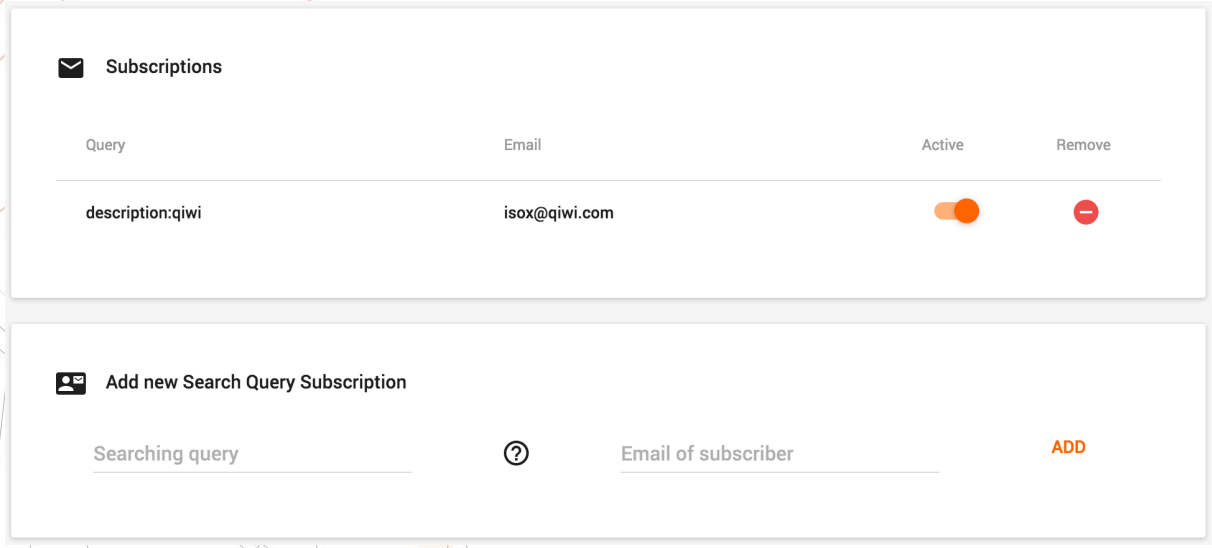
- Export
  - *https://vulners.com/api/v3/archive/collection?type=exploitdb*



Example: RSS

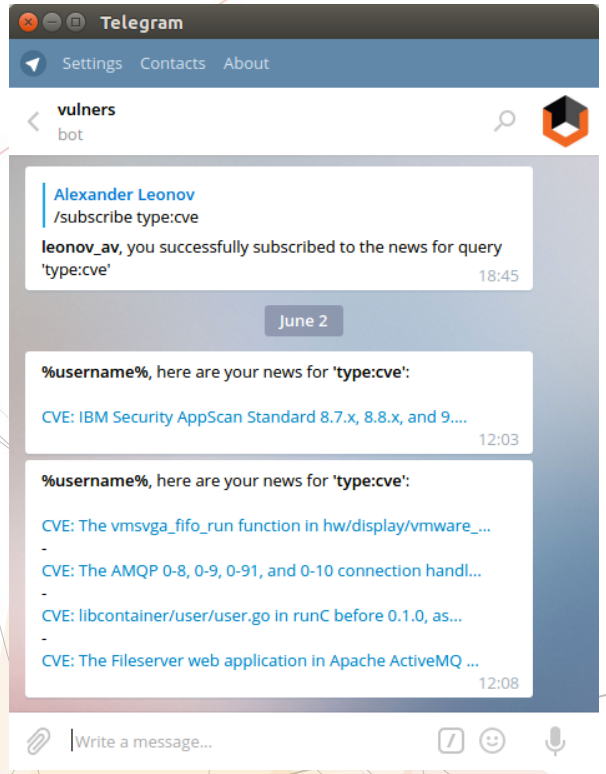
- Fully customizable news feed in RSS format
- Powered by Apache Lucene query
  - *https://vulners.com/rss.xml?query=type:debian*
- Updates-on-demand. No cache, it builds right when you ask it to.
- Atom, Webfeeds, mrss compatible

Example: Email subscriptions



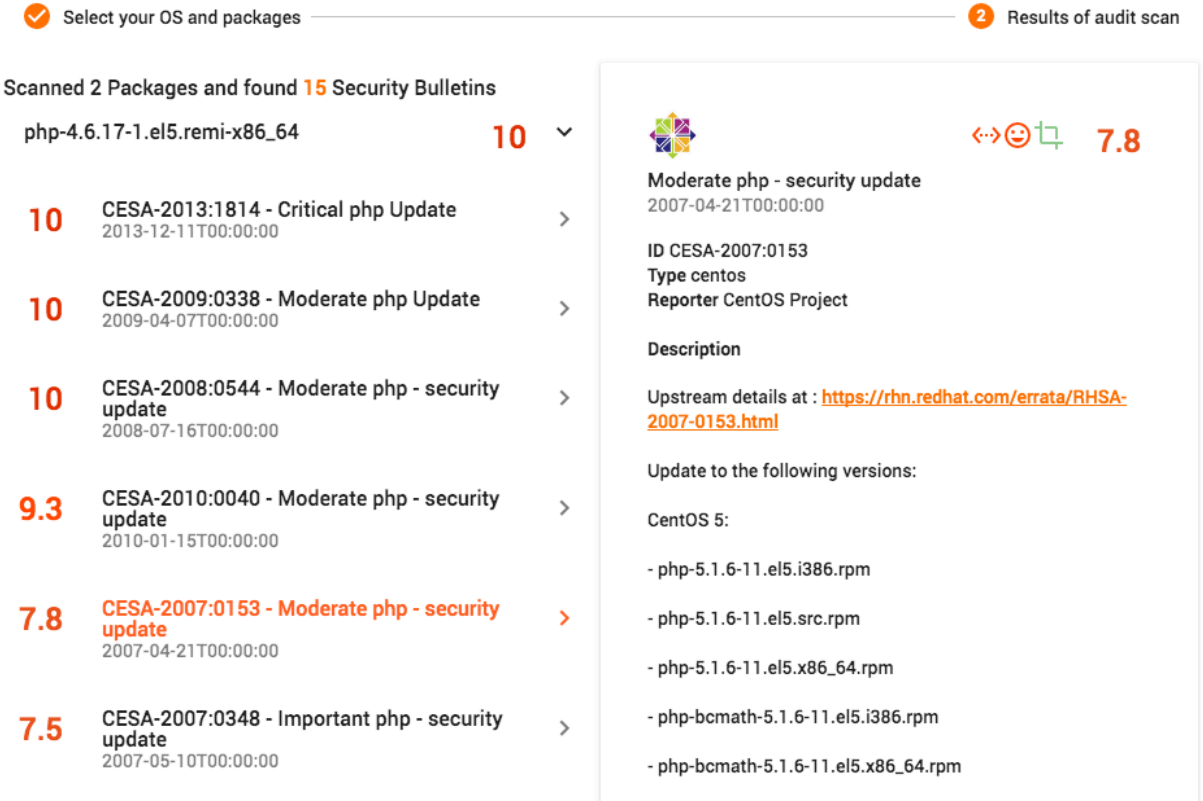
- Up to 5 subscriptions
- Awareness service
- Absolutely customizable

Example: Telegram news bot



- Up to 3 subscriptions for user
- In-app search
- Broadcast for emergency news

Example: Security audit



- Linux OS vulnerability scan
- Immediate results
- Dramatically simple

Example: Security audit API

- Easy to use: Just give us output of package manager
  - *https://vulners.com/api/v3/audit/rpm/?os=centos&version=5&package=php-4.6.17-1.el5.remi-x86_64*

- JSON result
  - Vulnerabilities list
  - Reason of the decision
  - References list (exploits, and so on)

- Ready to go for **Red Hat** and **Debian** family

- Typical call time for 500+ packages list = 160ms
  - It's fast. Really fast.

Example: Security audit API


```
"vulnerabilities": [
  "CESA-2014:0311",
  "CESA-2012:1045",
  "CESA-2013:1814",
  "CESA-2007:0348",
  "CESA-2007:0890",
  "CESA-2013:1049",
  "CESA-2012:0093",
  "CESA-2009:0338",
  "CESA-2008:0544",
  "CESA-2012:0033",
  "CESA-2007:0153",
  "CESA-2010:0040",
  "CESA-2010:0919",
  "CESA-2014:1824",
  "CESA-2012:0546"
]
```

```
"CESA-2012:0546": [
  {
    "result": true,
    "OSVersion": "5",
    "bulletinPackage": "php-5.1.6-34.el5_8.x86_64",
    "providedPackage": "php-5.1.5-1.el5.remi-x86_64",
    "operator": "lt"
  }
]

"php-5.1.5-1.el5.remi-x86_64": {
  "CESA-2014:0311": [
    {
      "result": true,
      "OSVersion": "5",
      "bulletinPackage": "php-5.1.6-44.el5_10.x86_64",
      "providedPackage": "php-5.1.5-1.el5.remi-x86_64",
      "operator": "lt"
    }
  ],
```


Example: Home made scanner

```
# git clone https://github.com/videns/vulners-scanner
# cd vulners-scanner
# ./linuxScanner.py


            _
__   ___   _| |_ __   ___ _ __ ___
\ \ / / | | | '_ \ / _ \ '__/ __|
 \ V /| |_| | | | |  __/ |  \__ \
  \_/  \__,_|_|_| |_|\___|_|  |___/

=========================================
Host info - Host machine
OS Name - Darwin, OS Version - 15.6.0
Total found packages: 0
=========================================
Host info - docker container "java:8-jre"
OS Name - debian, OS Version - 8
Total found packages: 166
Vulnerable packages:
    libgcrypt20 1.6.3-2+deb8u1 amd64
        DSA-3650 - 'libgcrypt20 -- security update', cvss.score - 0.0
    libexpat1 2.1.0-6+deb8u2 amd64
        DSA-3597 - 'expat -- security update', cvss.score - 7.8
    perl-base 5.20.2-3+deb8u4 amd64
        DSA-3628 - 'perl -- security update', cvss.score - 0.0
    gnupg 1.4.18-7+deb8u1 amd64
        DSA-3649 - 'gnupg -- security update', cvss.score - 0.0
    gpgv 1.4.18-7+deb8u1 amd64
        DSA-3649 - 'gnupg -- security update', cvss.score - 0.0
```

- Available at GitHub
- Example of integration
- Free to fork

It is absolutely free

- Free for commercial and enterprise use DB and API

- Make your own solutions using our powers:
  - Security scanners
  - Threat intelligence
  - Subscriptions
  - Security automation

- Just please, post references if you can ☺

Thanks

- isox@vulners.com
- https://github.com/videns/vulners-scanner/
- We are really trying to make this world better
- Stop paying for features, that are available for free