



Под капотом Vulners

Из чего мы его собрали

Кир Ермаков
Russian Open Source Summit 2017

- Основатель vulners.com
- Технический директор группы QIWI
- Сайтики ломать умею
- В багбаунти неплохо так отметилcя (Yandex, Mail.ru, Apple...)
- Ярый активист «не_бумажной_безопасности»



База Данные Уязвимостей Vulners

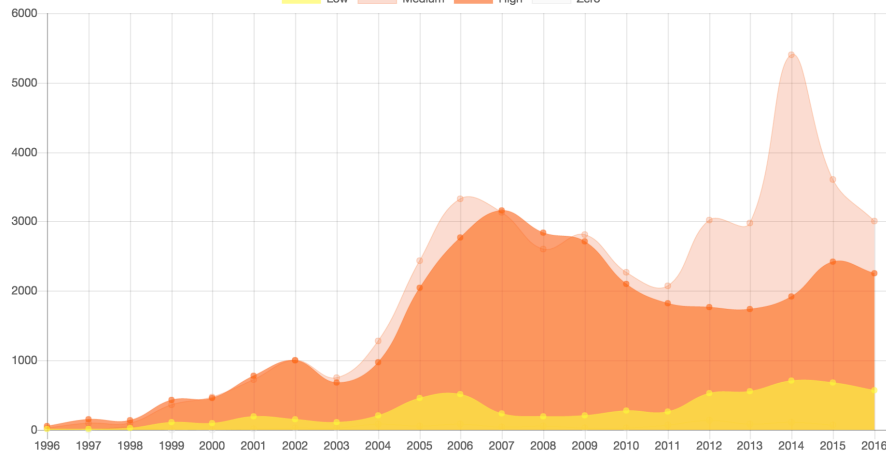
CVE progression

Visualization of security bulletins appearance in recent years divided by types and families

Bulletin Type

cve

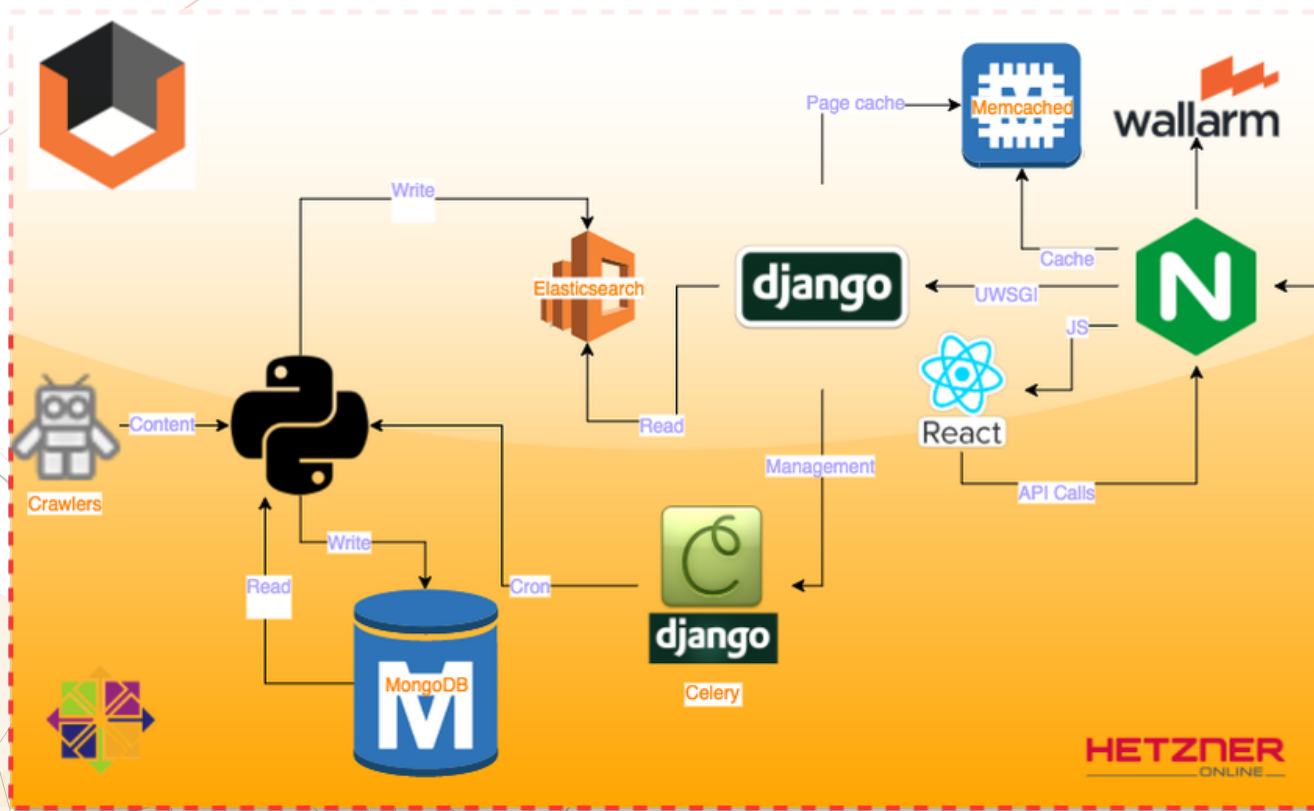
Low Medium High Zero



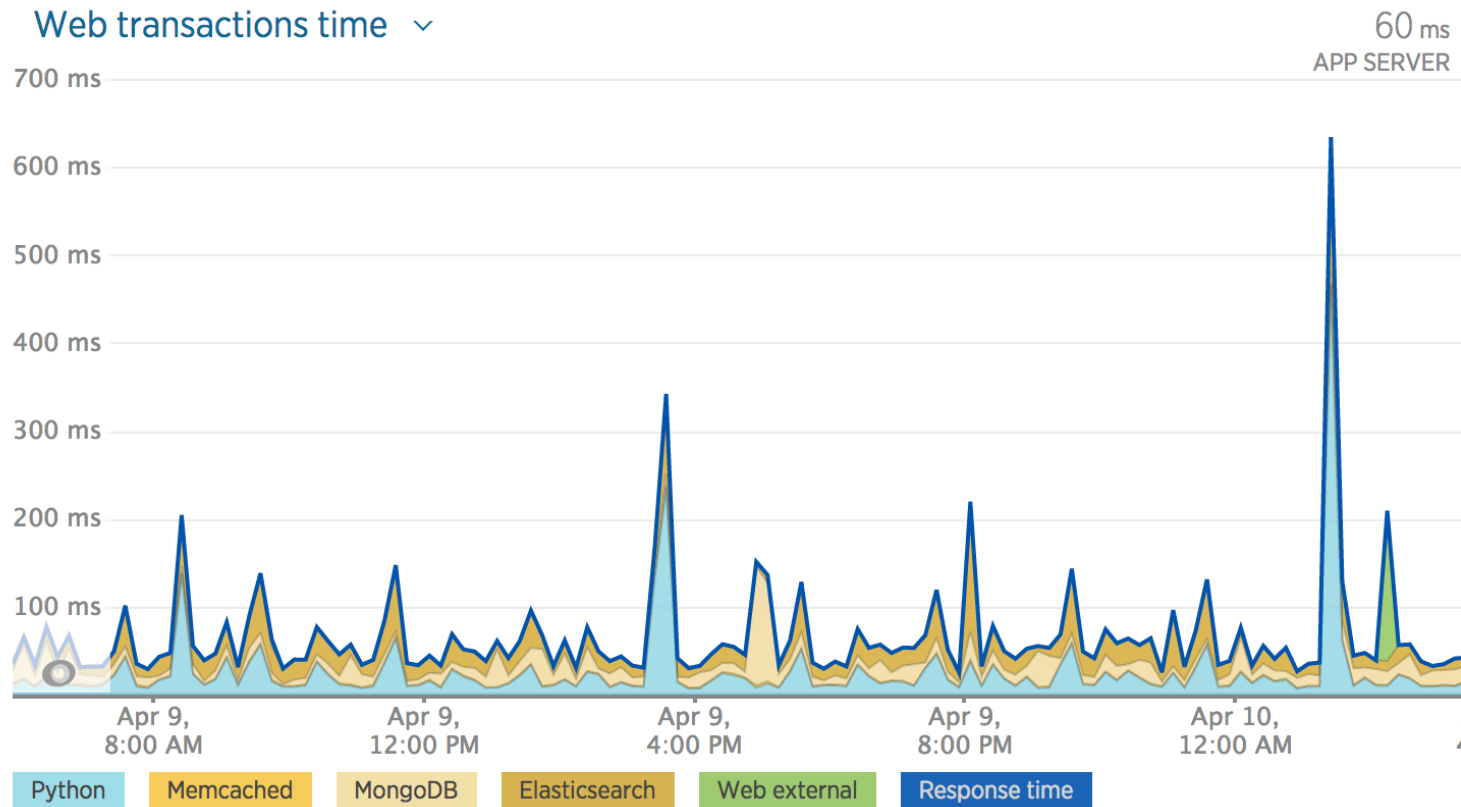
- Яндекс – подобный ПОИСКОВИК
- 600.000+ разнообразных элементов «по ИБэ»
- 71 источник данных
- Подписки и оповещения
- Умеет сканировать Линукс на уязвимости



Технологическая платформа



Шустро работает



Задняя часть

- **Питон 3.6**
 - Да, нам нравится асинхронность и юникод
- **Джанго (не освобожденный, а фреймворк)**
 - Со своими костылями и велосипедами
 - Собственная модель объектов, управление сеансами
- **Рукастена(Wallarm), ДвижокИкс(Nginx) + UWSGI (непереводимо)**
 - Интегрированная защита приложения и вполне обычный способ работы



Змеиная библиотека

- Ох и много их
- Обычный набор любителей Django
- Традиционное «а теперь разрули зависимости»



```
requirements.txt x
7  rpyc
8  tweepy
9  pymongo
10 elasticsearch_dsl
11 elasticsearch
12 django-cors-headers
13 celery>4
14 django
15 telepot
16 passwordmeter
17 lepl
18 djangoestframework
19 pyparsing
20 bs4
21 recaptcha2
22 scrypt
23 argon2
24 six
25 pyga
26 version_utils
27 yandex.translate
28 pyopenssl
29 ndg-httpsclient
30 python3-memcached
31 whois
32 python-whois
33 django-pylibmc
34 django-mongodb-cash-backend
35 xhtml2pdf
36 cfscrape
37 markdown
38 weasyprint
39 pyrabbit
40 billiard
41 aiocfscrape
42 tqdm
43 yandex.translate
44 markdown2
45 celerybeat-mongd
```

Планирование и краулинг

- Сельдерей 4.*
 - Подтягивает расписание и задачи из базы данных
- Кролик (очередь сообщений)
 - Просто очередь 😊
- Асинхронный вход/выход на Питоне
 - Что бы не расцеплять процесс краулинга на подпроцессы



Базы данных

- Гибкий поиск 2.*
 - Индекс, поиск и магия
- Монго Ди Би 3.*
 - Для внутренних объектов, долгоживущей сверхоперативной памяти и расписания планировщика
- Сверхоперативная-память-память (Memcache)
 - Веб-кеш и семафор с перекрестными процессами



Задержки

/search - lucene



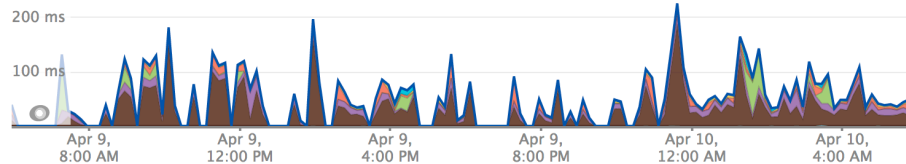
App performance

App server breakdown



1.0 72.7 ms
APDEX AVERAGE

300 ms



/search - id



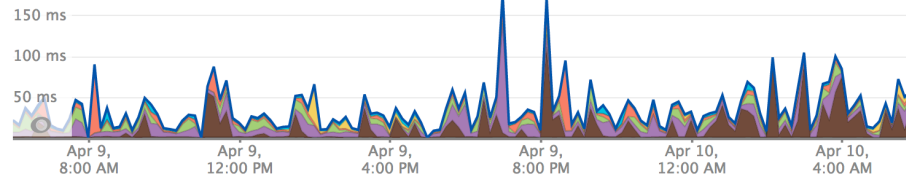
App performance

App server breakdown



0.99 39.6 ms
APDEX AVERAGE

200 ms



/audit - audit



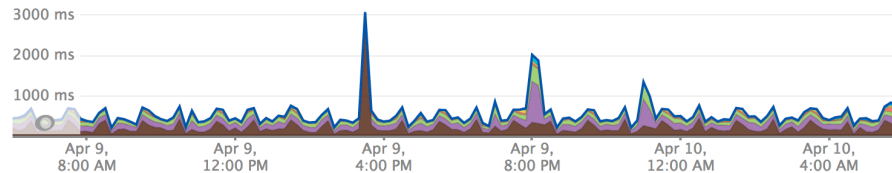
App performance

App server breakdown



0.82 618 ms
APDEX AVERAGE

4000 ms



- Обычный кэш на каждый день
 - Положим его в Мемкеш
- Плачущий вебкеш
 - Плачет из Мемкеша в Монго Ди Би
- Кеш для больших объектов
 - Файлы



Зачем столько баз?

- Исторически так сложилось
- Точный поиск гораздо менее больно делать в Монге
- Гибкий поиск что бы искать как Яндекс
- Сверхоперативная-память-память очень быстрая



Передний край

- Реактивный кофейный сценарий (ReactJS)
 - С кофе все можно делать быстрее
- Материальный интерфейс пользователя (MaterialUI)
 - Красивенько же!
- Веб-упаковщик(Webpack)
 - А теперь весь этот код надо собрать воедино
- ЙеЭс6 (ES6)
 - Нам нравится кофе с сахаром
 - Не поддерживает ослов. Ну и ладно.



Реактивный кофе скрипт == безопасность

Копируете контент с хакерских сайтов?

Нельзя просто так взять и вставить его в свой собственный сайт.

Чужой контент в нашем кофе не растворяется.

Description

WordPress Plugin Firewall 2 1.3-
Scripting (XSS), Cros...

vulners.com says:

1

form. Tags: Cross-Site

OK

```
<!--
```

Details

```
Software: WordPress Firewall 2
```

```
Version: 1.3
```

```
Homepage: https://wordpress.org/plugins/wordpress-firewall-2/
```

```
Advisory report: https://security.dxw.com/advisories/csrfstored-xss-in-wordpress-firewall-2-allows-unauth
```

```
CVE: Awaiting assignment
```

```
CVSS: 5.8 (Medium; AV:N/AC:M/Au:N/C:P/I:P/A:N)
```

Description

```
CSRF/stored XSS in WordPress Firewall 2 allows unauthenticated attackers to do almost anything an admin c
```

Vulnerability

```
HTML is not escaped and there is no CSRF prevention, meaning attackers can put arbitrary HTML content ont
```



Вот так вот!

- Легкий
 - 4 центральных процессора + 32 гигабайта памяти
- Быстрый
 - <50мс на поисковые запросы
 - <500мс на сканирование пакетов
- Гибкий
 - Любой компонент умеет плодиться горизонтально



Спасибо!

- isox@vulners.com
- Продюсер попросил меня обязательно перевести слайды на русский язык
- Оригинальную презентацию я выложу на СлайдоПоделилке
- Стараемся делать мир лучше
- **Хватит платить за то, что доступно бесплатно**

