ВЗЛОМ

Vulners — Гугл для хакера. Как устроен лучший поисковик по уязвимостям и как им пользоваться

Александр Леонов, 08.07.2016 1 комментарий 98,476 Добавить в закладки

Содержание статьи

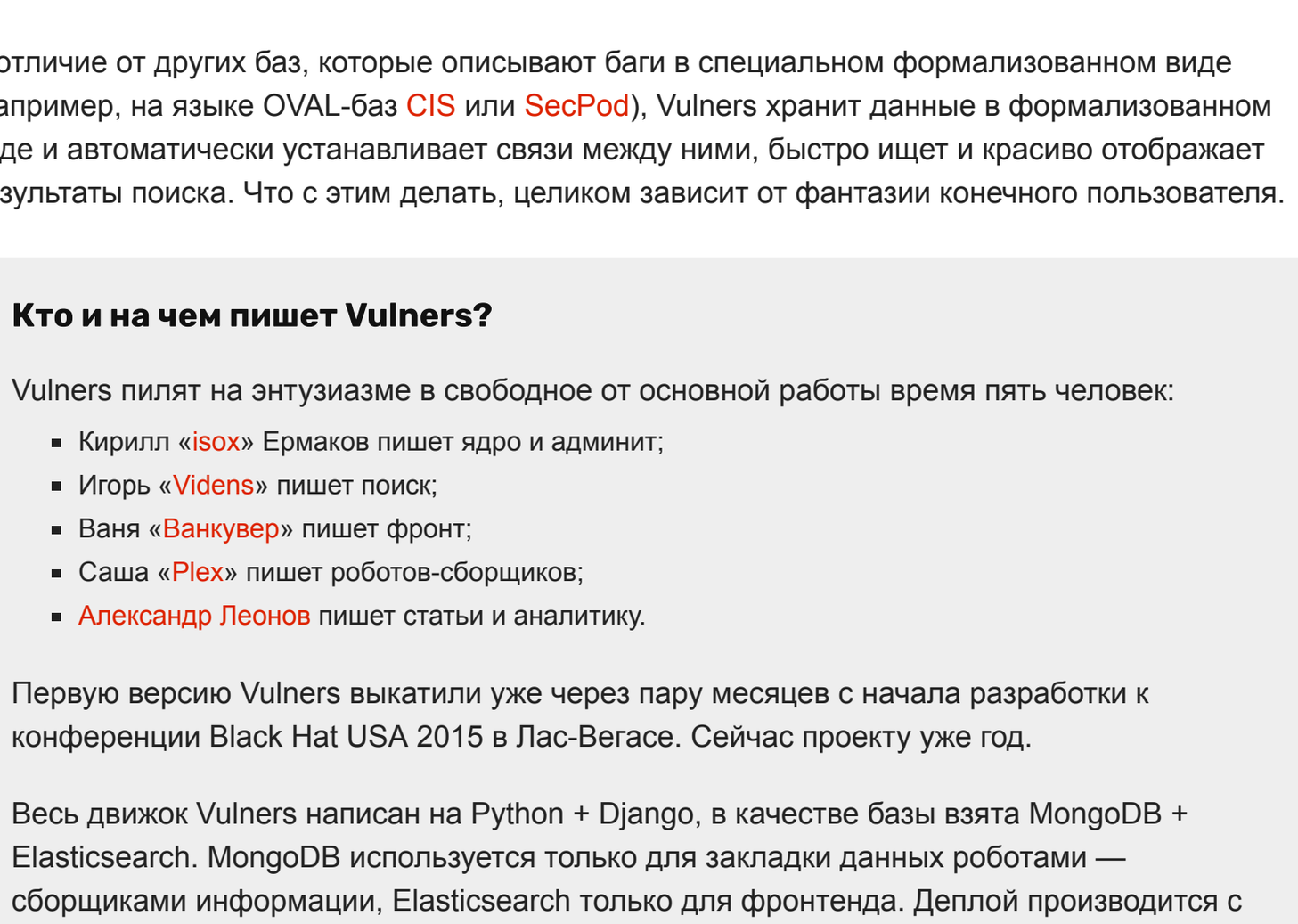
Часто нужно узнать всю информацию о какой-нибудь уязвимости: насколько найденный баг критичен, есть ли готовые сплоиты, какие вендоры уже выпустили патчи, каким сканером проверить наличие бага в системе. Раньше приходилось искать вручную по десятку источников (CVEDetails, SecurityFocus, Rapid7 DB, Exploit-DB, базы уязвимостей CVE от MITRE/NIST, вендорские бюллетени) и анализировать собранные данные. Сегодня эту рутину можно (и нужно!) автоматизировать с помощью специализированных сервисов. Один из таких — Vulners, крутейший поисковик по багам. А главное — бесплатный и с открытым API. Посмотрим, чем он может быть нам полезен.

Что это такое

Vulners — это очень большая и непрерывно обновляемая база данных ИБ-контента. Сайт позволяет искать уязвимости, эксплоиты, патчи, результаты bug bounty так же, как обычный поисковик ищет сайты. Vulners агрегирует и представляет в удобном виде шесть основных типов данных:

- **Популярные базы уязвимостей.** Они содержат общие описания уязвимостей и ссылки на источники. Например, известная CVE американского агентства MITRE и института NIST. Но, помимо информации из нее, в Vulners добавляются общие описания уязвимости и других исследовательских центров и центров реагирования: Vulnerability Lab, XSSed, CERT, ICS, Zero Day Initiative, Positive Technologies, ERPScan.
- **Вендорские бюллетени безопасности.** Это баг-репорты, которые пишут сами вендоры об уязвимостях в своих продуктах. Сейчас это разнообразные дистрибутивы Linux (Red Hat CentOS, Oracle Linux, Arch Linux, Debian, Ubuntu, SUSE), FreeBSD, сетевые устройства (F5 Networks, Cisco, Huawei, Palo Alto Networks) и популярные и критичные программы (OpenSSL, Samba, nginx, Mozilla, Opera), в том числе и CMS (WordPress, Drupal).
- **Эксплоиты из Exploit-DB и Metasploit.** Они парсятся и сохраняются полностью, с исходниками (их можно сразу смотреть в удобном редакторе).
- **Nessus-плагины для детекта уязвимостей.** Легко посмотреть, можно ли найти ту или иную уязвимость при сканировании сети этим популярным сканером.
- **Дисклозы багов с сайтов bug bounty программ.** В Vulners поддерживаются записи с HackerOne.
- **Публикации на тематических ресурсах.** Собираются данные с Threatpost и rdot.org, где часто освещают темы, связанные с уязвимостями.

Все это обрабатывается, каталогизируется, структурируется и доступно для поиска в любой момент.



Вендоры, от которых собирается и анализируется инфа в Vulners

В отличие от других баз, которые описывают баги в специальном формализованном виде (например, на языке OVAL-баз CIS или SecPod), Vulners хранит данные в формализованном виде и автоматически устанавливает связи между ними, быстро ищет и красиво отображает результаты поиска. Что с этим делать, целиком зависит от фантазии конечного пользователя.

Кто и на чем пишет Vulners?

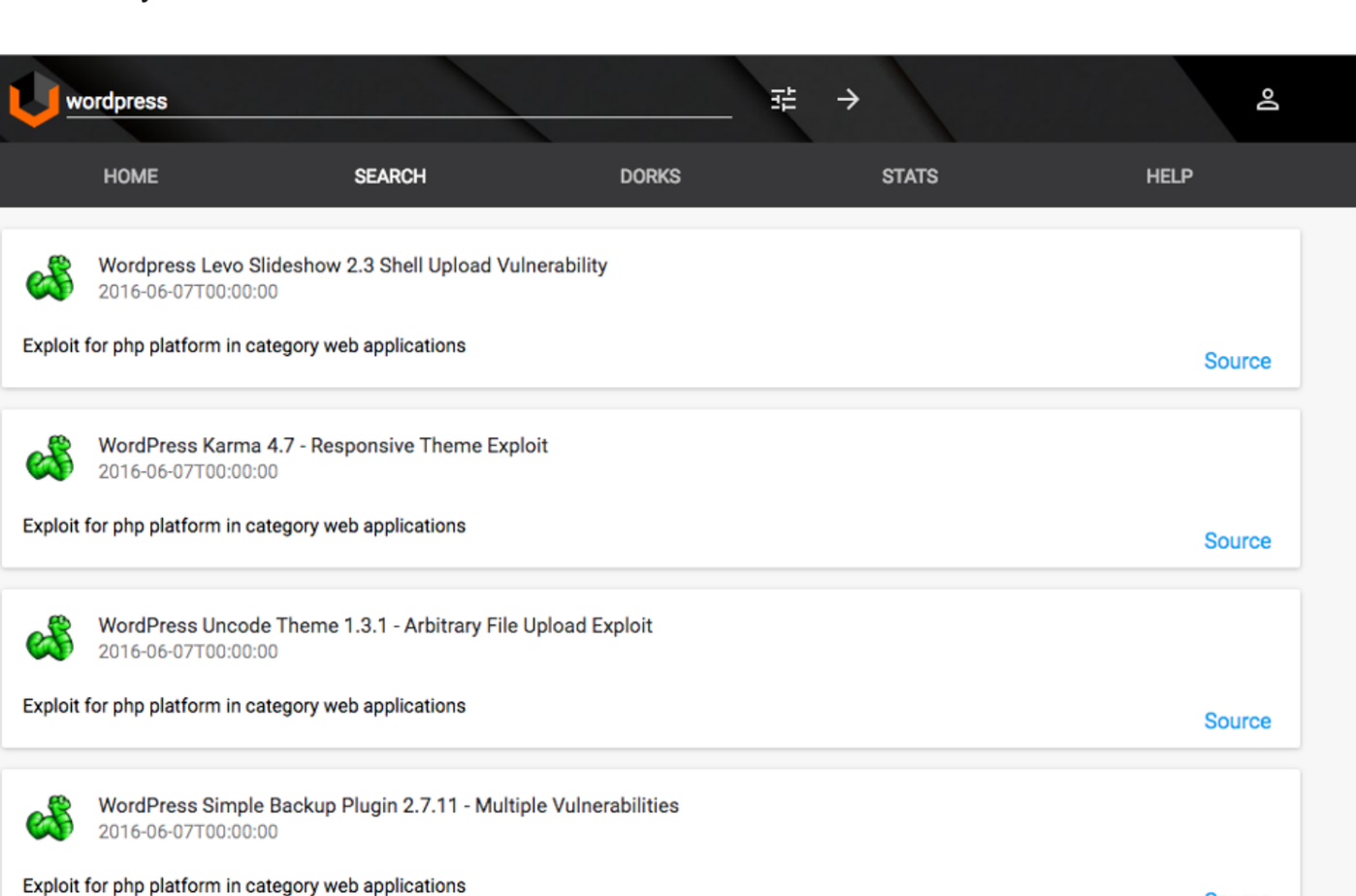
Vulners пилят на энтузиазме в свободное от основной работы время пять человек:

- Кирилл «isox» Ермаков пишет ядро и админит;
- Игорь «Videns» пишет поиск;
- Ваня «Ванкувер» пишет фронт;
- Саша «Plex» пишет роботов-сборщиков;
- Александр Леонов пишет статьи и аналитику.

Первую версию Vulners выкатили уже через пару месяцев с начала разработки к конференции Black Hat USA 2015 в Лас-Вегасе. Сейчас проекту уже год.

Весь движок Vulners написан на Python + Django, в качестве базы взята MongoDB + Elasticsearch. MongoDB используется только для закладки данных роботами — сборщиками информации, Elasticsearch только для фронтенда. Деплой производится с Bitbucket'а скриптом. Масштабирование заложено прямо в ядре: MongoDB и Elasticsearch шардятся. Фабрика роботов написана хостонезависимой и может гоняться отдельно от всего проекта. Одна из крутых фишек — ребята уже полностью перешли на Python 3.5+ и asyncio в своем проекте. Так что поиск не всегда работает точно, но всегда очень быстро :).

На текущий момент в базе Vulners 319 557 бюллетеней и 144 684 эксплоита. А занимает все это в базе меньше 2 Гбайт. Такая компактность достигается за счет дедупликации и упаковывания. Все лежит в оперативной памяти, поэтому скорость поиска значительно увеличивается. Стоит упомянуть и то, что Vulners защищается WAF Wallarm, работающим в блокирующем режиме.

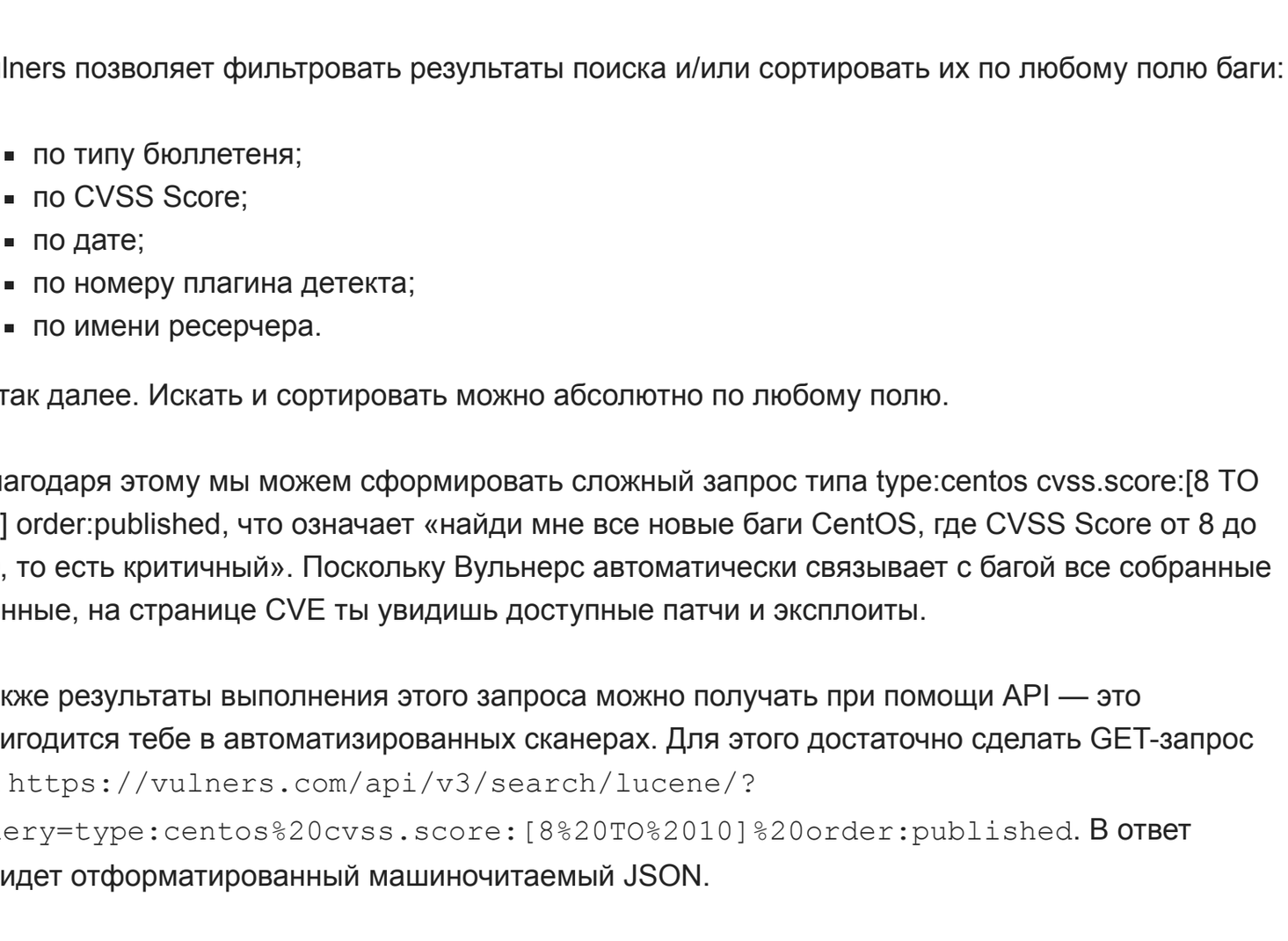


Архитектура Vulners

Но довольно слов, давай попробуем что-нибудь поискать.

Пробуем искать

Первое, что видишь, когда заходишь на Vulners, — это, конечно же, строка поиска. Просто введи название приложения, сайта или CVE-код уязвимости, и Вульнерс выдаст тебе все последние публичные баги по этому продукту со ссылками на эксплоиты, плагины для детекта и различные публикации.



Типовая выдача Vulners по багам WordPress. Обрати внимание: данные обновляются постоянно и в автоматическом режиме

Естественно, простые запросы вроде «wordpress» или «xakep.ru» рассматривать скучно, с этим ты и сам разберешься. Давай посмотрим, что интересного умеет Vulners.

Задача: найти критичные баги CentOS со ссылками на сплоиты

Запрос: `type:centos order:published`

Vulners позволяет фильтровать результаты поиска и/или сортировать их по любому полю баги:

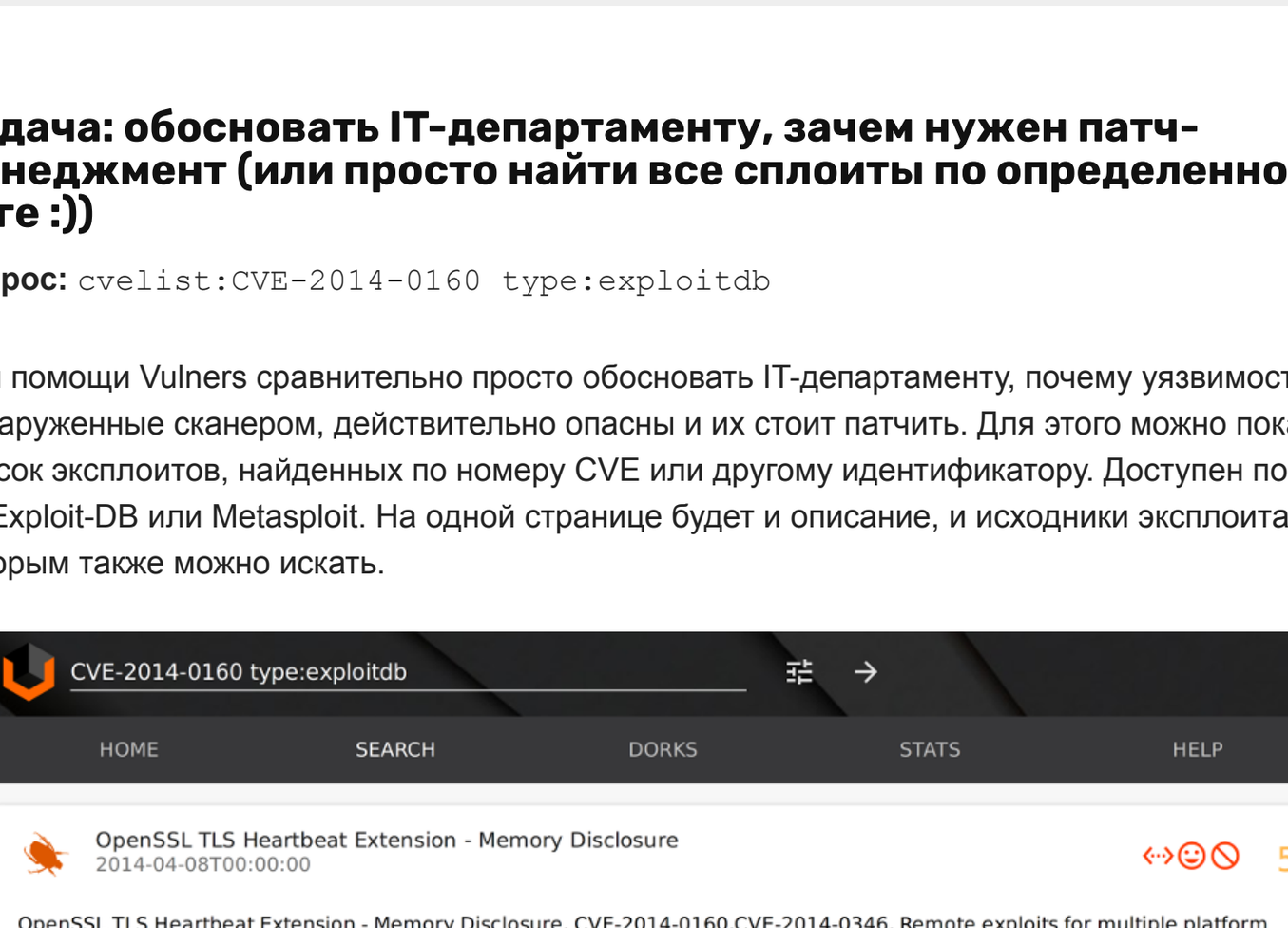
- по типу бюллетеня;
- по CVSS Score;
- по дате;
- по номеру плагина детекта;
- по имени ресерчера.

И так далее. Искать и сортировать можно абсолютно по любому полю.

Благодаря этому мы можем сформировать сложный запрос типа type:centos cvss.score:[8 TO 10] order:published, что означает «найди мне все новые баги CentOS, где CVSS Score от 8 до 10, то есть критичный». Поскольку Вульнерс автоматически связывает с багой все собранные данные, на странице CVE ты увидишь доступные патчи и эксплоиты.

Также результаты выполнения этого запроса можно получать при помощи API — это пригодится тебе в автоматизированных сканерах. Для этого достаточно сделать GET-запрос на `https://vulners.com/api/v3/search/lucene/?query=type:centos%20cvss.score:[8%20TO%2010]%20order:published`. В ответ придет отформатированный машиночитаемый JSON.

Еще один полезный параметр API-запросов — `references=true`, который позволяет получить в результатах запроса не только объекты безопасности, но и все их связи (плагины детекта, эксплоиты и прочее). Например, такой запрос: `https://vulners.com/api/v3/search/lucene/?references=True&query=type:centos%20cvss.score:[8%20TO%2010]%20order:published` — выведет еще и все references, связные элементы из базы.



Графическое задание запроса

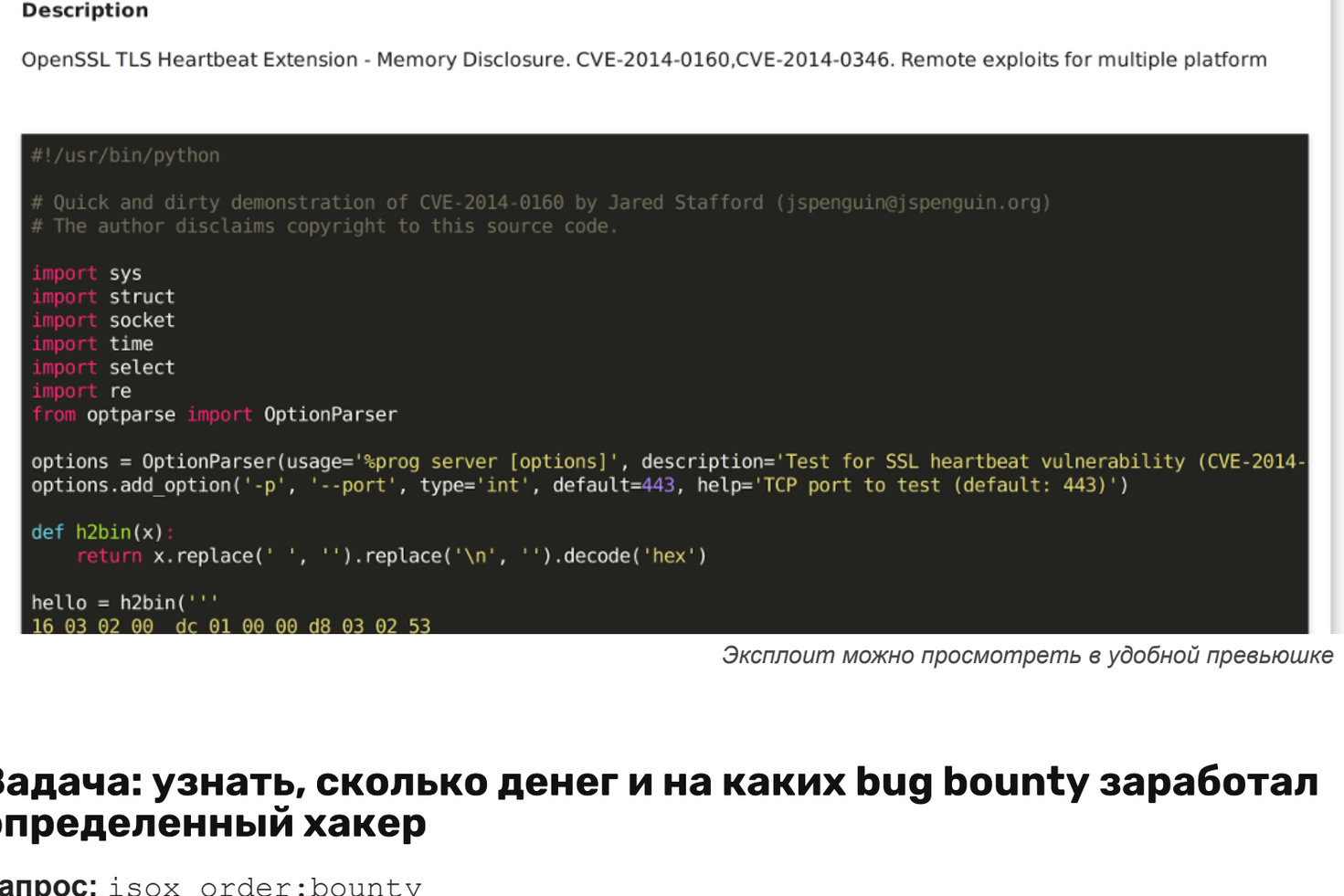
Получаем больше двадцати записей от Vulners

По умолчанию Vulners отдает только первые двадцать записей запроса. Если хочется больше, нужно задать параметр `size`. Так можно получить до 10 000. А если и этого мало, то можно запрашивать несколько раз по 10 000, пропуская уже полученные результаты при помощи параметра `skip`.

Задача: обосновать IT-департаменту, зачем нужен патч-менеджмент (или просто найти все сплоиты по определенной баге :))

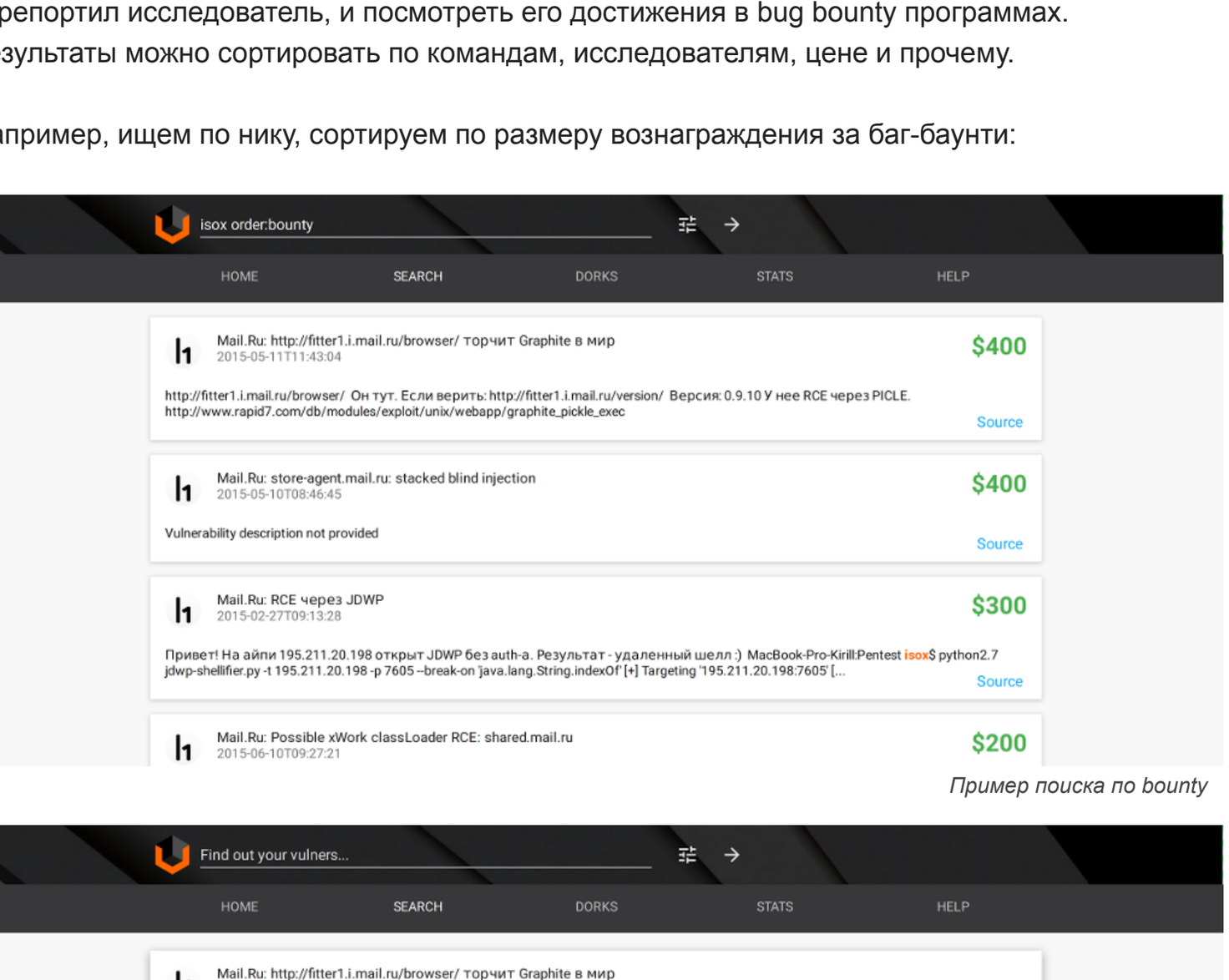
Запрос: `cvelist:CVE-2014-0160 type:exploitdb`

При помощи Vulners сравнительно просто обосновать IT-департаменту, почему уязвимости, обнаруженные сканером, действительно опасны и их стоит патчить. Для этого можно показать список эксплоитов, найденных по номеру CVE или другому идентификатору. Доступен поиск по Exploit-DB или Metasploit. На одной странице будет и описание, и исходники эксплоита, по которым также можно искать.



Ищем сплоиты по CVE-2014-0160

Как видим, на странице эксплоита приводится его полный текст. По этому тексту также можно искать.



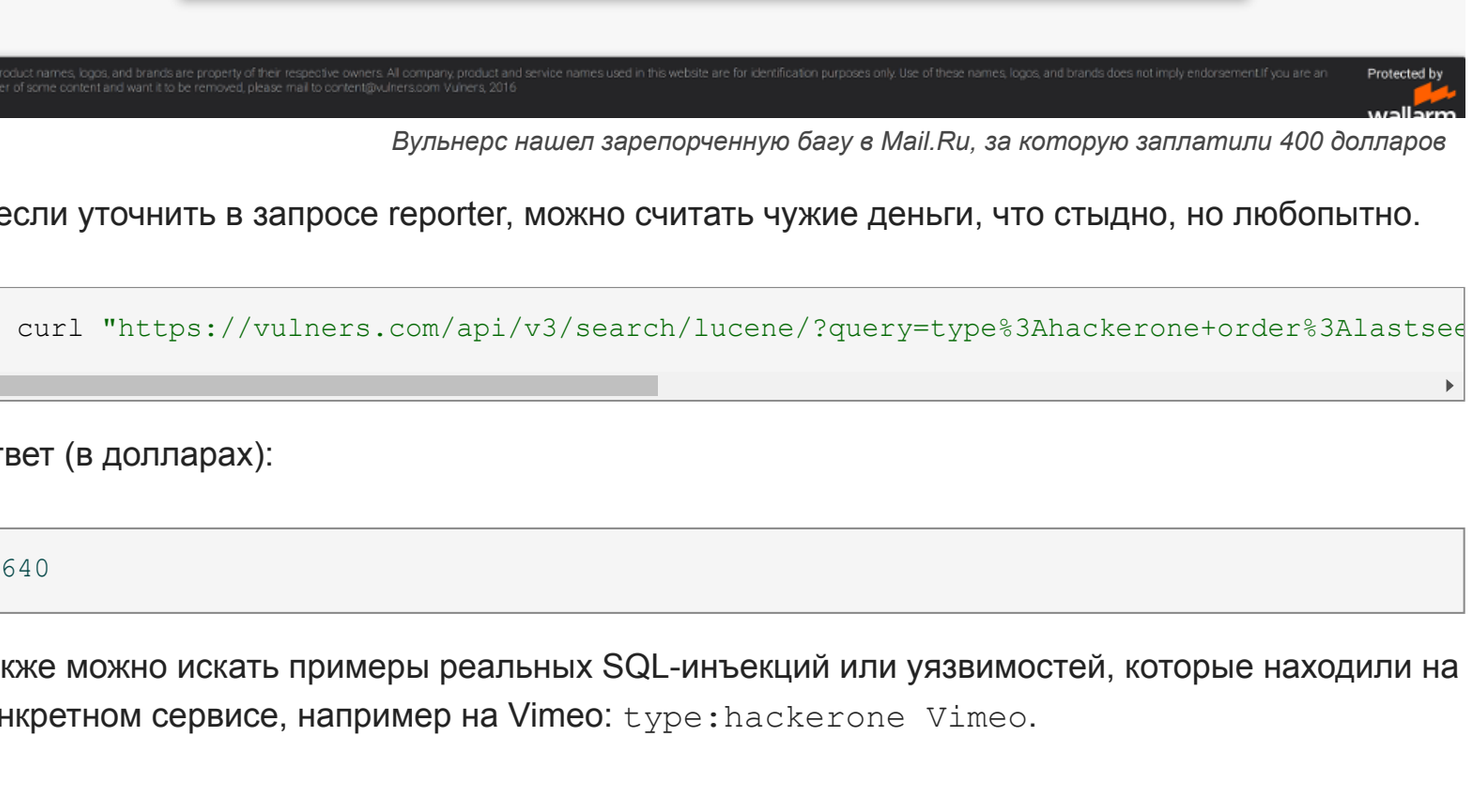
Эксплоит можно просмотреть в удобной превьюшке

Задача: узнать, сколько денег и на каких bug bounty заработал определенный хакер

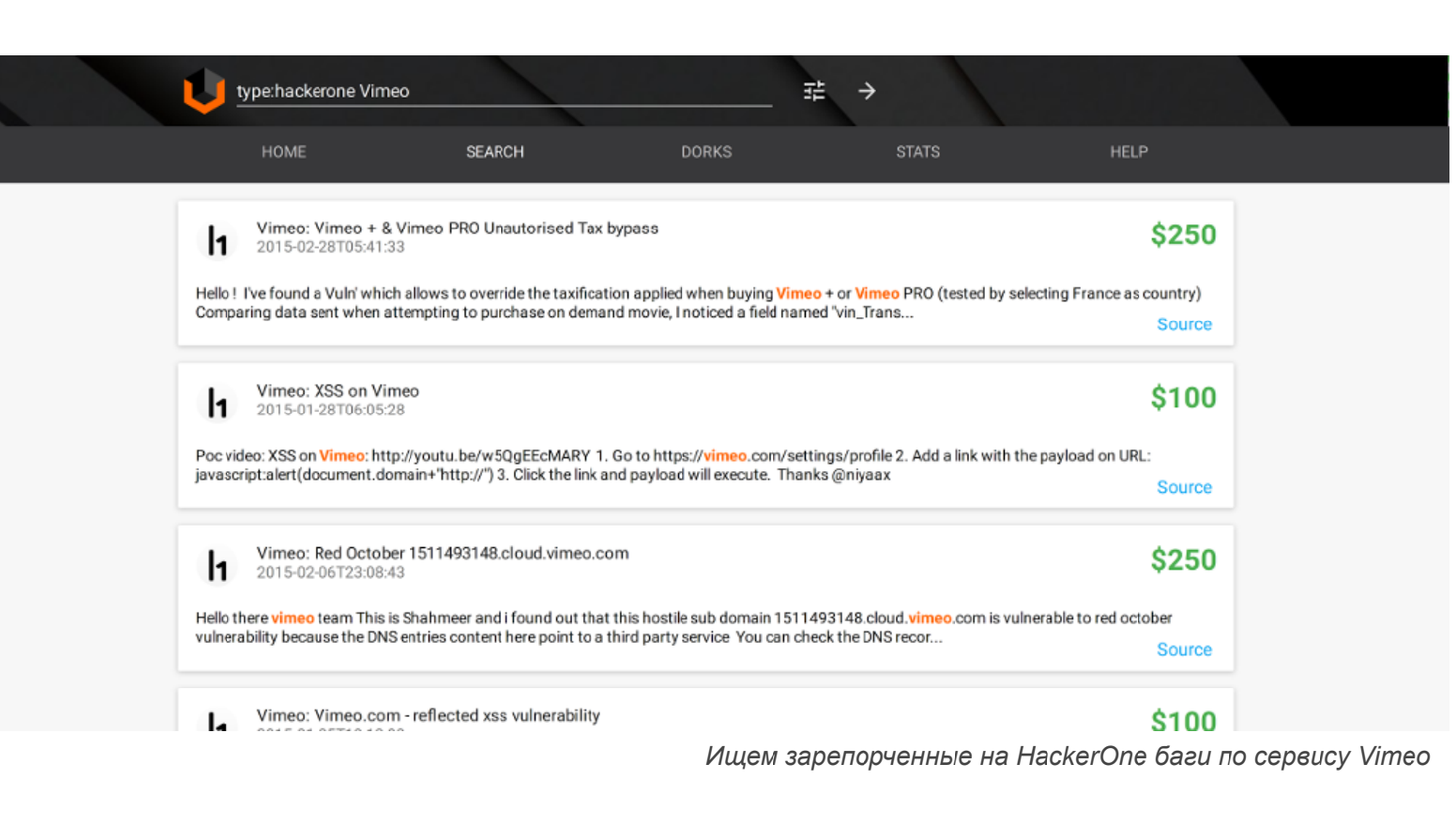
Запрос: `isox order:bounty`

Уникальная фича Vulners — поиск по баг-баунти. Можно найти, какие уязвимости софта зарепортил исследователь, и посмотреть его достижения в bug bounty программах. Результаты можно сортировать по командам, исследователям, цене и прочему.

Например, ищем по нику, сортируем по размеру вознаграждения за баг-баунти:



Пример поиска по bounty



Вульнерс нашел зарепорченную багу в Mail.Ru, за которую заплатили 400 долларов

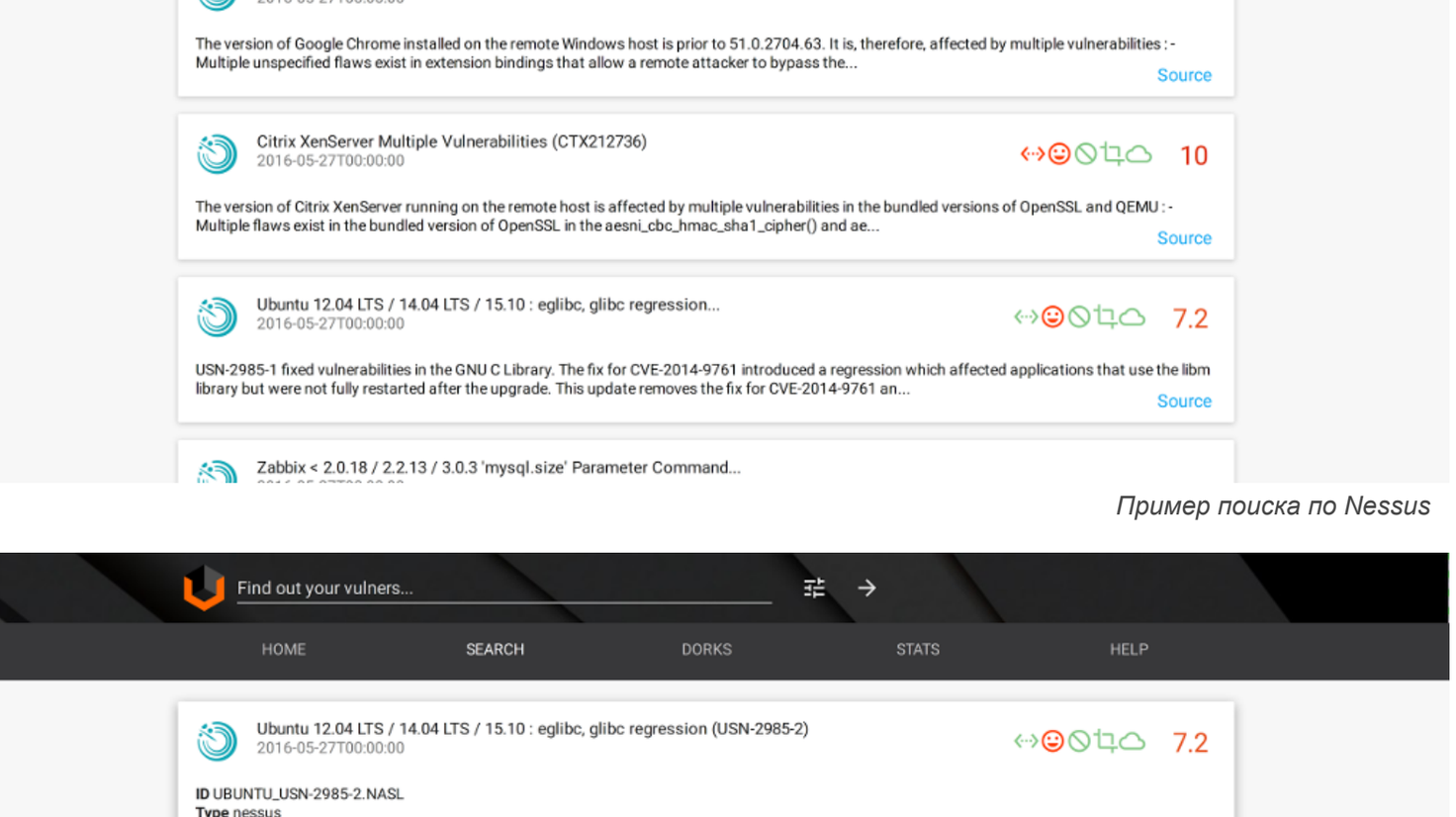
А если уточнить в запросе reporter, можно считать чужие деньги, что стыдно, но любопытно.

```
$ curl "https://vulners.com/api/v3/search/lucene/?query=type%3Ahackerone+order%3Alastsee
```

Ответ (в долларах):

```
2640
```

Также можно искать примеры реальных SQL-инъекций или уязвимостей, которые находили на конкретном сервисе, например на Vimeo: `type:hackerone Vimeo`.

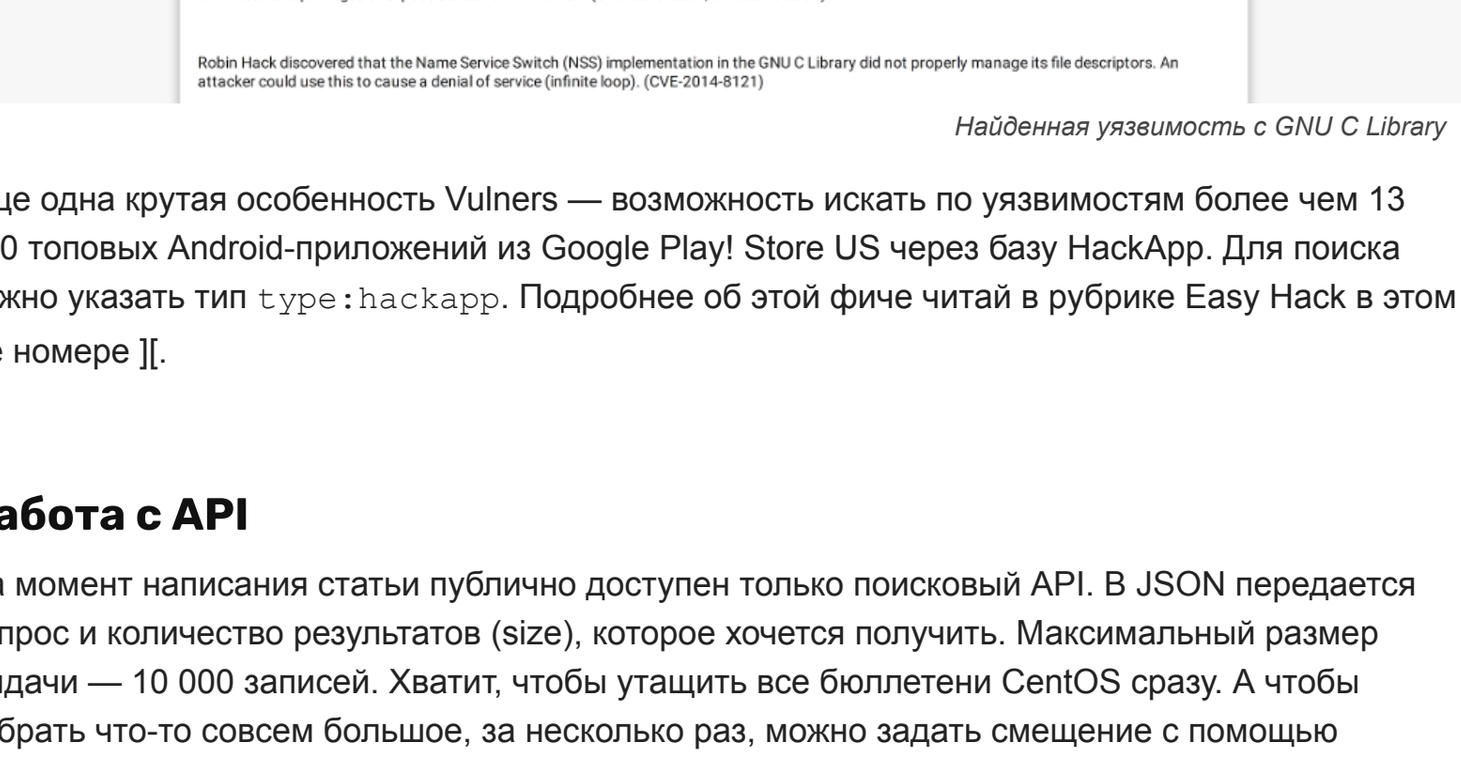


Ищем зарепорченные на HackerOne баги по сервису Vimeo

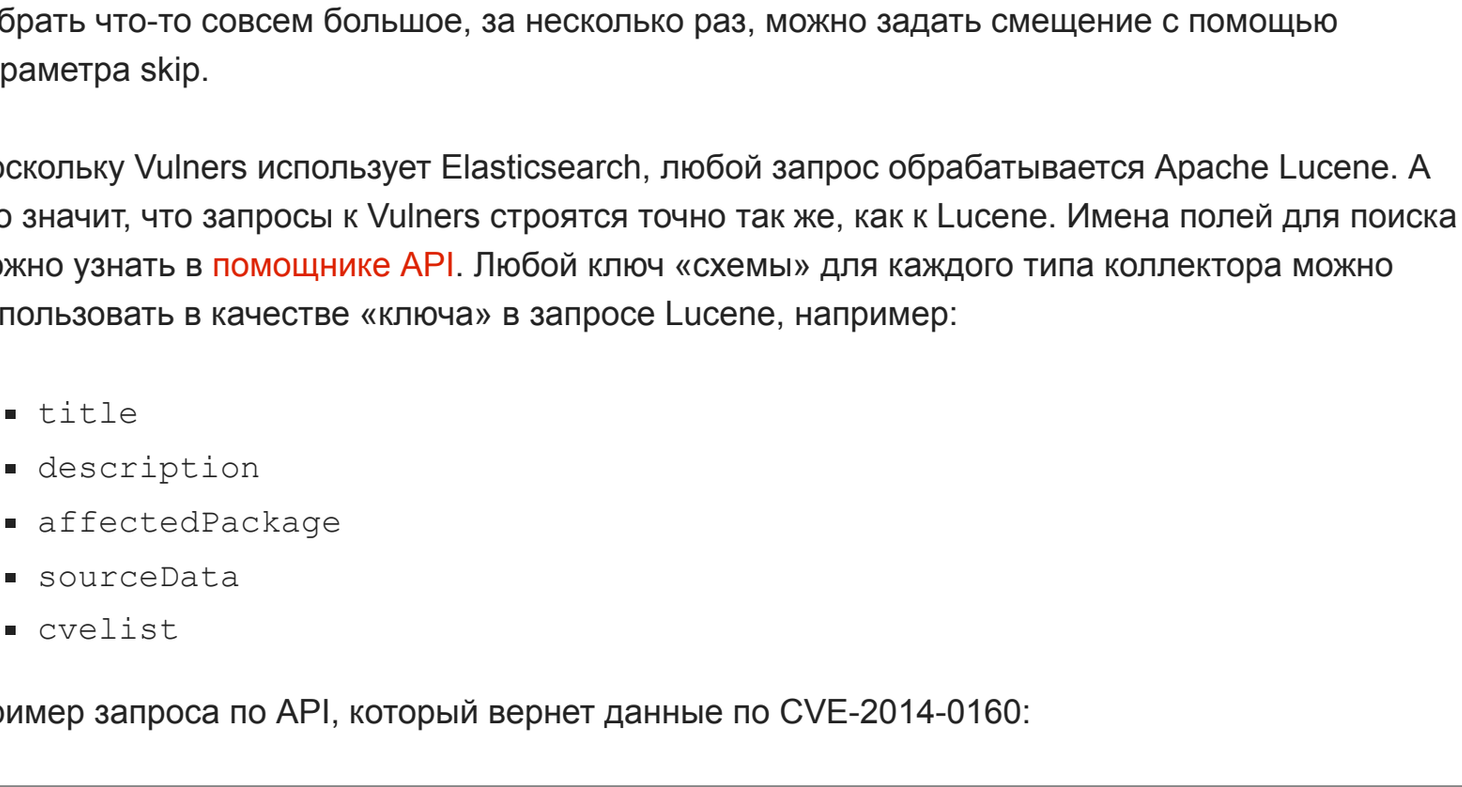
Задача: найти баги по плагинам Nessus

Запрос: `type:nessus order:published`

Поиск по плагинам Nessus — также уникальная фича Vulners. Так, запрос выше выведет список последних добавленных плагинов.



Пример поиска по Nessus



Найденная уязвимость с GNU C Library

Еще одна крутая особенность Vulners — возможность искать по уязвимостям более чем 13 000 топовых Android-приложений из Google Play! Store US через базу HackApp. Для поиска нужно указать тип `type:hackapp`. Подробнее об этой фиче читай в рубрике Easy Hack в этом же номере][.

Работа с API

На момент написания статьи публично доступен только поисковый API. В JSON передается запрос и количество результатов (size), которое хочется получить. Максимальный размер выдачи — 10 000 записей. Хватит, чтобы утащить все бюллетени CentOS сразу. А чтобы забрать что-то совсем большое, за несколько раз, можно задать смещение с помощью параметра skip.

Поскольку Vulners использует Elasticsearch, любой запрос обрабатывается Apache Lucene. А это значит, что запросы к Vulners строятся точно так же, как к Lucene. Имена полей для поиска можно узнать в помощнике API. Любой ключ «схемы» для каждого типа коллектора можно использовать в качестве «ключа» в запросе Lucene, например:

- `title`
- `description`
- `affectedPackage`
- `sourceData`
- `cvelist`

Пример запроса по API, который вернет данные по CVE-2014-0160:

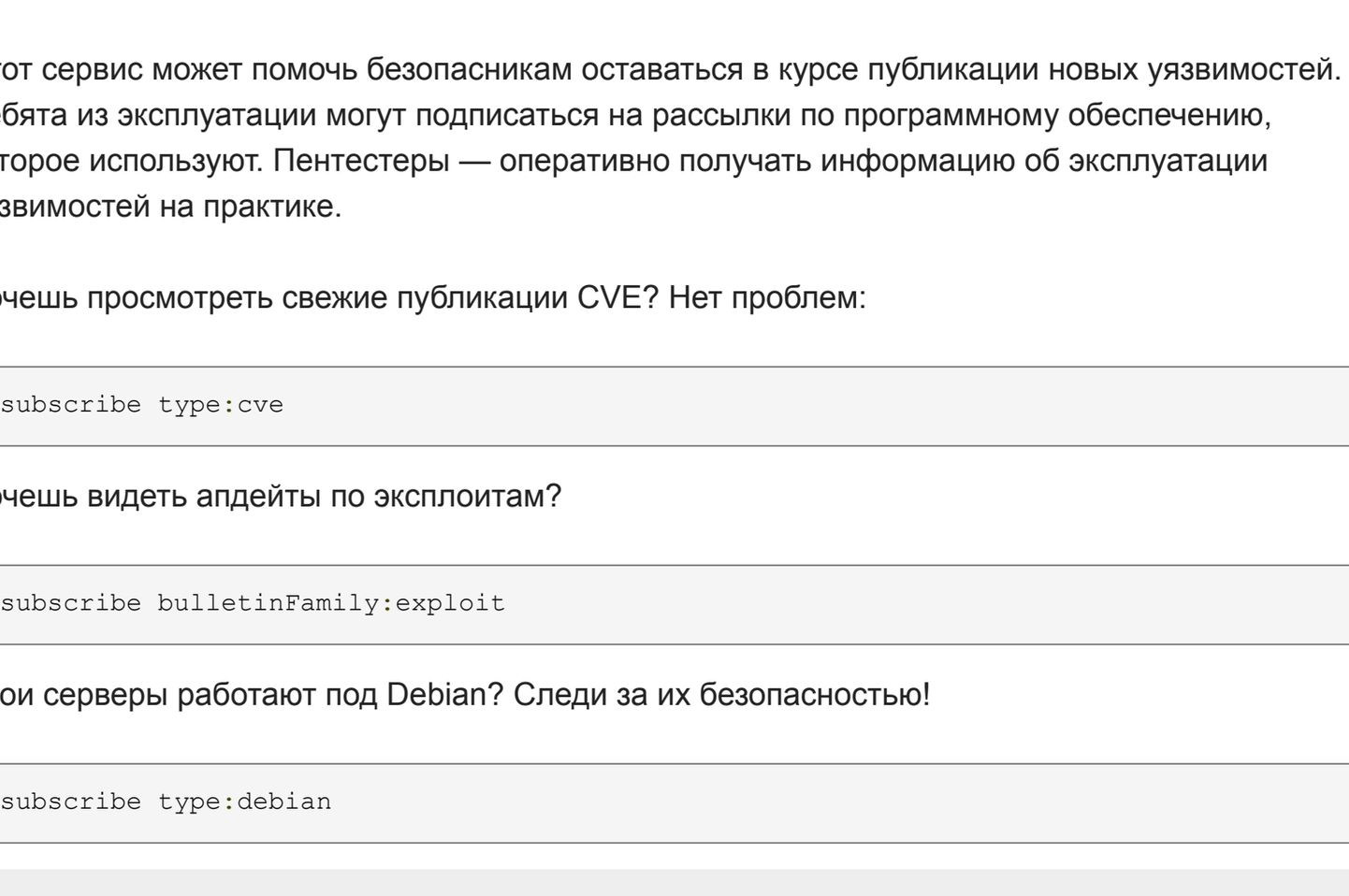
```
curl https://vulners.com/api/v3/search/lucene/?query=type:cve%20id:CVE-2014-0160
```

Ответы также в JSON:

```
{
  "data": {
    "exactMatch": null,
    "search": [
      {
        "_index": "bulletins",
        "_score": 9.942732,
        "_source": {
          "type": "cve",
          "title": "CVE-2014-0160: OpenSSL heartbeat information disclosure",
          "published": "2014-04-07T18:55:03",
          "objectVersion": "1.0",
          "href": "https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160",
          "reporter": "NVD",
          "modified": "2015-10-22T10:19:38",
          "references": [
            "http://www.securitytracker.com/id/1030081",
            "http://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt
            "http://advisories.mageia.org/MGASA-2014-0165.html",
          ],
          "description": "OpenSSL could allow a remote attacker to obtain sensitive info
          "lastseen": "2016-03-19T07:17:51",
          "cvss": {
            "vector": "AV:NETWORK/AC:LOW/Au:NONE/C:PARTIAL/I:NONE/A:NONE/",
            "score": 5.0
          },
          "id": "CVE-2014-0160",
          "scanner": [],
          "bulletinFamily": "NVD"
        },
        "_id": "CVE-2014-0160",
        "_type": "bulletin"
      }
    ]
  },
  "result": "OK"
}
```

Бот для Telegram с подписками на результаты запроса

В апреле Vulners запустили бота для мессенджера Telegram:



Бот позволяет делать запросы, так же как на сайте.

Но главное — с его помощью можно создавать настраиваемые подписки на security content.

Пользоваться просто. Отправь боту сообщение /subscribe и свой поисковый запрос и получай новые результаты поиска, как только они будут появляться на Vulners.

Этот сервис может помочь безопасникам оставаться в курсе публикации новых уязвимостей. Ребята из эксплуатации могут подписаться на рассылки по программному обеспечению, которое используют. Пентестеры — оперативно получать информацию об эксплуатации уязвимостей на практике.

Хочешь просмотреть свежие публикации CVE? Нет проблем:

```
/subscribe type:cve
```

Хочешь видеть апдейты по эксплоитам?

```
/subscribe bulletinFamily:exploit
```

Твои серверы работают под Debian? Следи за их безопасностью!

```
/subscribe type:debian
```

А у Vulners есть альтернативы?

Vulners — не единственный агрегатор уязвимостей. Есть, к примеру, базы Secunia и OSVDB, но одна закрылась 5 апреля, а другая платная.

Еще существует отечественный БнД УБИ ФСТЭК, но они хранят только описания самих уязвимостей и больше ничего (нет данных об эксплоитах), да и те, честно говоря, формализованы не очень. К тому же «Банк данных угроз безопасности информации» не предоставляет открытого API, то есть использовать его в автоматизированных сканерах не получится.

Выводы

Vulners — уникальный и незаменимый помощник любому хакеру и безопаснику. Он очень сильно экономит время при исследовании и эксплуатации сложных векторов атак. Конечно, инструмент только развивается, но уже сейчас он вполне юзабелен. А что еще более важно, Vulners открытый и бесплатный для конечного пользователя и всегда будет таким.

Кстати, уязвимости, найденные на vulners.com, можно сабмитить на https://hackerone.com/vulnerscom. Искать можно все что угодно. Так как проект бесплатный, то и финансирования для выплаты вознаграждений нет, но public disclosure разработчики гарантируют. Email для связи support@vulners.com, прочие контактные данные здесь.