SuperSliv.Biz - Курсы, Тренинги, С<mark>еминары, К</mark>аждый дены

```
все сплоиты по определенной баге :))
05. Задача: узнать, сколько денег и на каких bug bounty заработал определенный хакер
06. Задача: найти баги по плагинам Nessus
07. Работа с АРІ
08. Бот для Telegram с подписками на результаты запроса
09. Выводы
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
```

04. Задача: обосновать ІТ-департаменту, зачем нужен патч-менеджмент (или просто найти

03. Задача: найти критичные баги CentOS со ссылками на сплоиты

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

rdot.org

Bulletins 221

Bulletins 1347

02. Пробуем искать

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

• Вендорские бюллетени безопасности. Это баг-репорты, которые пишут сами вендоры

Lab, XSSed, CERT, ICS, Zero Day Initiative, Positive Technologies, ERPScan.

- 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.

Nginx

Bulletins 22

Cent OS

Bulletins 2267

Bulletins 3175

Hackapp

Bulletins 21872

Bulletins 144

Arch Linux

Bulletins 387

Bulletins 1359

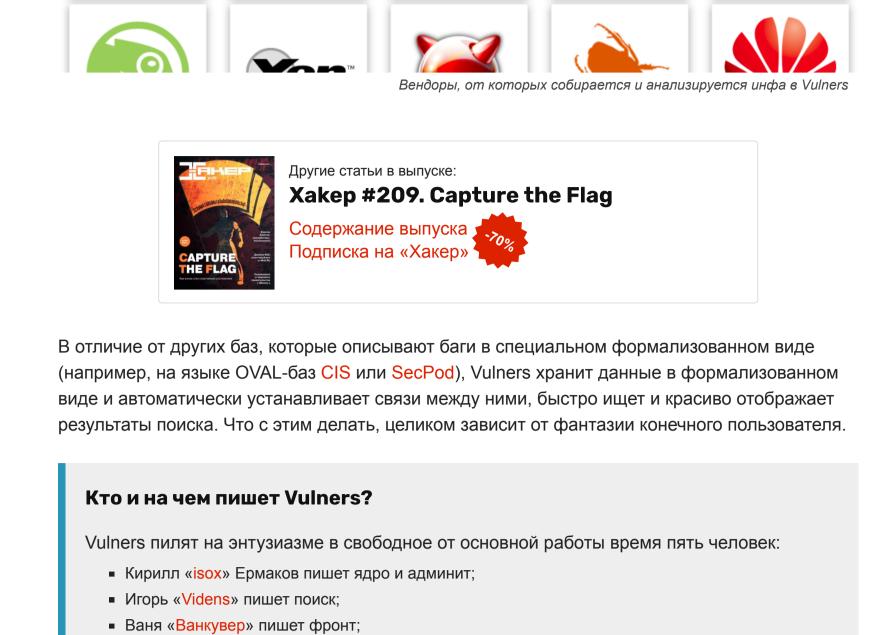
Саша «Plex» пишет роботов-сборщиков;

очень быстро :).

Александр Леонов пишет статьи и аналитику.

allalla ORACLE CISCO. ThreatPost Cisco Oracle Linux Metasploit Opera

Bulletins 2350



Первую версию Vulners выкатили уже через пару месяцев с начала разработки к

Весь движок Vulners написан на Python + Django, в качестве базы взята MongoDB +

сборщиками информации, Elasticsearch только для фронтенда. Деплой производится с

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

На текущий момент в базе Vulners 319 557 бюллетеней и 144 684 эксплоита. А занимает

Elasticsearch. MongoDB используется только для закладки данных роботами —

Bitbucket'a скриптом. Масштабирование заложено прямо в ядре: MongoDB и

конференции Black Hat USA 2015 в Лас-Вегасе. Сейчас проекту уже год.

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. wallarm django React HETZNER 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. 9 wordpress HOME SEARCH DORKS STATS HELP Wordpress Levo Slideshow 2.3 Shell Upload Vulnerability 2016-06-07T00:00:00 Exploit for php platform in category web applications Source WordPress Karma 4.7 - Responsive Theme Exploit 2016-06-07T00:00:00

Source

Source

Запрос: type:centos order:published Vulners позволяет фильтровать результаты поиска и/или сортировать их по любому полю баги:

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

данные, на странице CVE ты увидишь доступные патчи и эксплоиты.

Ha https://vulners.com/api/v3/search/lucene/?

придет отформатированный машиночитаемый JSON.

детекта, эксплоиты и прочее). Например, такой запрос:

references=True&query=type:centos%20cvss.score:

Получаем больше двадцати записей от Vulners

результаты при помощи параметра skip.

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

OpenSSL TLS Heartbeat Extension - Memory Disclosure

return x.replace(' ', '').replace('\n', '').decode('hex')

2014-04-08T00:00:00

optparse import OptionParser

ID EDB-ID:32745 Type exploitdb

Description

ort sys struct socket time select

hello = h2bin('''

определенный хакер

Запрос: isox order:bounty

HOME

http://fitter1.i.mail.ru/browser/

У нее RCE через PICLE.

type:hackerone Vimeo

Vimeo: XSS on Vimeo

Если верить: http://fitter1.i.mail.ru/version/

ID H1:60573 Type hackerone Reporter isox Description

Ответ (в долларах):

2640

SEARCH

Mail.Ru: http://fitter1.i.mail.ru/browser/ торчит Graphite в мир

http://www.rapid7.com/db/modules/exploit/unix/webapp/graphite_pickle_exec

конкретном сервисе, например на Vimeo: type: hackerone Vimeo.

Vimeo: Vimeo + & Vimeo PRO Unautorised Tax bypass

Reporter Jared Stafford

https://vulners.com/api/v3/search/lucene/?

Exploit for php platform in category web applications

Exploit for php platform in category web applications

Exploit for php platform in category web applications

2016-06-07T00:00:00

• по типу бюллетеня;

• по имени ресерчера.

по номеру плагина детекта;

по CVSS Score;

по дате;

из базы.

Date published

Date

баге:))

WordPress Uncode Theme 1.3.1 - Arbitrary File Upload Exploit

WordPress Simple Backup Plugin 2.7.11 - Multiple Vulnerabilities

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

Естественно, простые запросы вроде «wordpress» или «хакер.ru» рассматривать скучно, с

Задача: найти критичные баги CentOS со ссылками на сплоиты

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

пригодится тебе в автоматизированных сканерах. Для этого достаточно сделать GET-запрос

query=type:centos%20cvss.score:[8%20T0%2010]%20order:published. B otbet

Еще один полезный параметр API-запросов — references=true, который позволяет

получить в результатах запроса не только объекты безопасности, но и все их связи (плагины

[8%20T0%2010]%20order:published — выведет еще и все references, связные элементы

Также результаты выполнения этого запроса можно получать при помощи АРІ — это

этим ты и сам разберешься. Давай посмотрим, что интересного умеет Vulners.

Uber Pays Researcher \$10K for Login Bypass Exploit

② type:centos cvss.score:8 order:published **Bulletin Type**

centos CVSS score 8 Order by

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

Задача: обосновать ІТ-департаменту, зачем нужен патч-

менеджмент (или просто найти все сплоиты по определенной

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

Графическое задание запроса

⇔②♦ 5

Эксплоит можно просмотреть в удобной превьюшке

которым также можно искать. CVE-2014-0160 type:exploitdb DORKS HOME **SEARCH** OpenSSL TLS Heartbeat Extension - Memory Disclosure **↔②○** 5 2014-04-08T00:00:00 OpenSSL TLS Heartbeat Extension - Memory Disclosure. CVE-2014-0160, CVE-2014-0346. Remote exploits for multiple platform OpenSSL 1.0.1f TLS Heartbeat Extension - Memory Disclosure Mult... <-> ② ♦ OpenSSL 1.0.1f TLS Heartbeat Extension - Memory Disclosure (Multiple SSL/TLS versions). CVE-2014-0160,CVE-2014-0346. Remote exploits for multiple platform Heartbleed OpenSSL - Information Leak Exploit 1 **⟨→⟩ ② ⟨** 2014-04-10T00:00:00 Heartbleed OpenSSL - Information Leak Exploit (1). CVE-2014-0160, CVE-2014-0346. Remote exploits for multiple platform Source Heartbleed OpenSSL - Information Leak Exploit 2 - DTLS Support ↔⊙⊙ 2014-04-24T00:00:00 Ищем сплоиты по CVE-2014-0160 Как видим, на странице эксплоита приводится его полный текст. По этому тексту также можно искать.

OpenSSL TLS Heartbeat Extension - Memory Disclosure. CVE-2014-0160, CVE-2014-0346. Remote exploits for multiple platform

options = OptionParser(usage='%prog server [options]', description='Test for SSL heartbeat vulnerability (CVE-2014-

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

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.

options.add_option('-p', '--port', type='int', default=443, help='TCP port to test (default: 443)')

Например, ищем по нику, сортируем по размеру вознаграждения за баг-баунти: isox order:bounty Mail.Ru: http://fitter1.i.mail.ru/browser/ торчит Graphite в мир \$400 http://fitter1.i.mail.ru/browser/ Он тут. Если верить: http://fitter1.i.mail.ru/version/ Версия: 0.9.10 У нее RCE через PICLE. http://www.rapid7.com/db/modules/exploit/unix/webapp/graphite_pickle_exec Source Mail.Ru: store-agent.mail.ru: stacked blind injection 2015-05-10T08:46:45 \$400 Vulnerability description not provided Source Mail.Ru: RCE через JDWP 2015-02-27T09:13:28 \$300 Привет! На айпи 195.211.20.198 открыт JDWP без auth-a. Результат - удаленный шелл:) MacBook-Pro-Kirill:Pentest isox\$ python2.7 jdwp-shellifier.py -t 195.211.20.198 -p 7605 --break-on 'java.lang.String.indexOf' [+] Targeting '195.211.20.198:7605' [... Mail.Ru: Possible xWork classLoader RCE: shared.mail.ru \$200 Пример поиска по bounty Find out your vulners. **非** →

400 \$

\$250

\$100

Найденная уязвимость с GNU C Library

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.

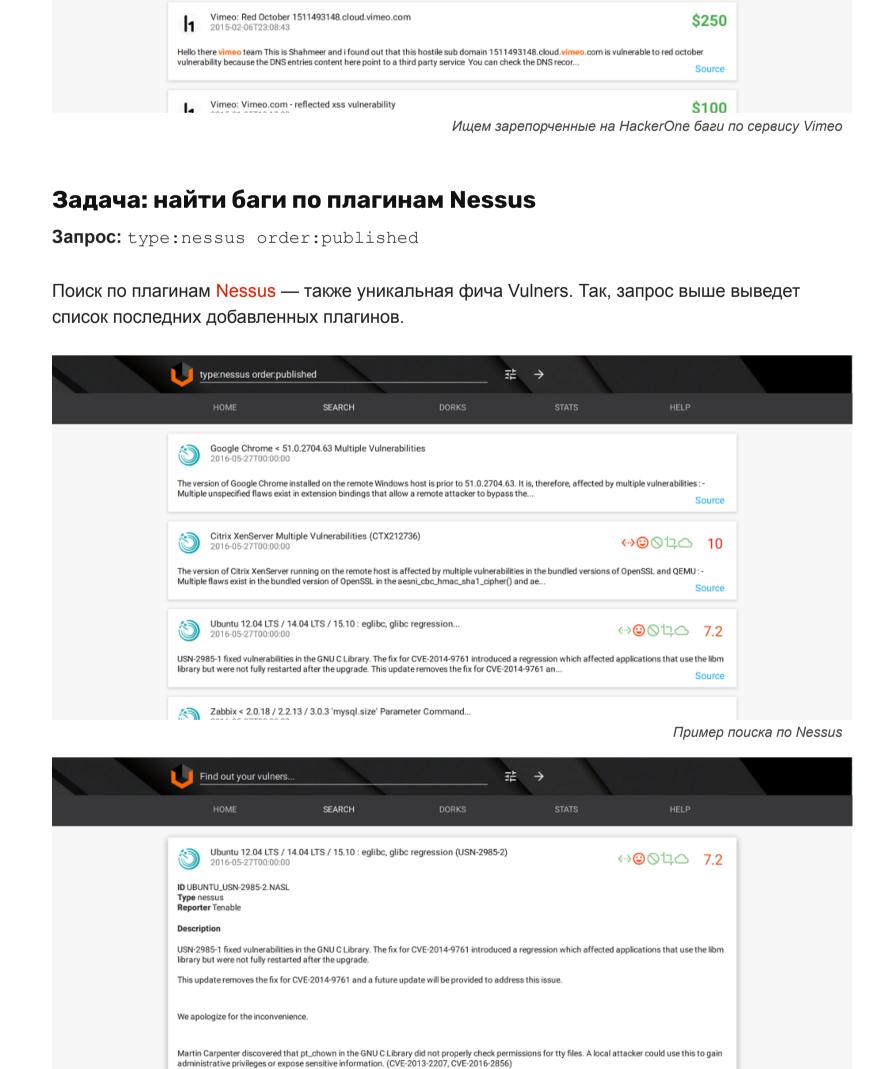
\$ curl "https://vulners.com/api/v3/search/lucene/?query=type%3Ahackerone+order%3Alastsee

Также можно искать примеры реальных SQL-инъекций или уязвимостей, которые находили на

Hello! I've found a Vuln' which allows to override the taxification applied when buying Vimeo + or Vimeo PRO (tested by selecting France as country) Comparing data sent when attempting to purchase on demand movie, I noticed a field named 'vin_Trans...

Poc video: XSS on Vimeo: http://youtu.be/w5QgEEcMARY 1. Go to https://vimeo.com/settings/profile 2. Add a link with the payload on URL:

javascript:alert(document.domain+'http://") 3. Click the link and payload will execute. Thanks @niyaax



Robin Hack discovered that the Name Service Switch (NSS) implementation in the GNU C Library did not properly manage its file descriptors. An

Еще одна крутая особенность Vulners — возможность искать по уязвимостям более чем 13 000 топовых Android-приложений из Google Play! Store US через базу НаскАрр. Для поиска

нужно указать тип type: hackapp. Подробнее об этой фиче читай в рубрике Easy Hack в этом

На момент написания статьи публично доступен только поисковый API. В JSON передается

Поскольку Vulners использует Elasticsearch, любой запрос обрабатывается Apache Lucene. A

можно узнать в помощнике API. Любой ключ «схемы» для каждого типа коллектора можно

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

это значит, что запросы к Vulners строятся точно так же, как к Lucene. Имена полей для поиска

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

attacker could use this to cause a denial of service (infinite loop). (CVE-2014-8121)

использовать в качестве «ключа» в запросе Lucene, например:

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

же номере][.

Работа с АРІ

параметра skip.

title

description

■ sourceData

Ответы также в JSON:

"exactMatch": null,

},

},

"result": "OK"

уязвимостей на практике.

/subscribe type:cve

/subscribe type:debian

Выводы

Хочешь видеть апдейты по эксплоитам?

/subscribe bulletinFamily:exploit

Хочешь просмотреть свежие публикации CVE? Нет проблем:

Твои серверы работают под Debian? Следи за их безопасностью!

"id": "CVE-2014-0160",

"bulletinFamily": "NVD"

" id": "CVE-2014-0160",

" type": "bulletin"

"scanner": [],

"data": {

cvelist

affectedPackage

"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

В апреле Vulners запустили бота для мессенджера Telegram: 🖲 🗇 Telegram 🛑 📵 Telegram Settings Contacts About Settings Contacts About vulners **Alexander Leonov** What can this bot do? leonov_av, you successfully subscribed to the news for query vulners.com assistant bot /start 18:40 **//** %username%, here are your news for 'type:cve': CVE: IBM Security AppScan Standard 8.7.x, 8.8.x, and 9.... **Alexander Leonov** Hello, leonov_av! I'm VulnersBot and I'm ready to help you! %username%, here are your news for 'type:cve': There are several command that I know. Here they are: /start - Start page command. CVE: The vmsvga_fifo_run function in hw/display/vmware_.. /search - Search vulnerability information with query. /subscribe - Subscribe to the news feed query. Like "subscribe CVE: The AMQP 0-8, 0-9, 0-91, and 0-10 connection handl... type:cve order:lastseen" /show - Show CVE description CVE: libcontainer/user/user.go in runC before 0.1.0, as... /last - List your last search queries /help - Display help page CVE: The Fileserver web application in Apache ActiveMQ ... /unsubscribe - Unsubscribe from newsfeed 7 · U **/** : Write a message... Write a message... Бот позволяет делать запросы, так же как на сайте. Ho 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

Бот для Telegram с подписками на результаты запроса

А y 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.

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 Скачанорования для выплаты вознаграждений нет. непирование разработчики скачанорую в сай для сыязи support person, иро не контактные данные оделиняйся!

Vulners — уникальный и незаменимый помощник любому хакеру и безопаснику. Он очень

сильно экономит время при исследовании и эксплуатации сложных векторов атак. Конечно,