

Single quote injection to find them all

Александр Трифанов
инженер по информационной
безопасности' drop database students; -- -

whoami

- Замкадыш из Новосибирска
- Занимаюсь тестированием на проникновение и разработкой решений по поиску уязвимостей
- Неравнодушен к реверс-инжинирингу и эксплуатации бинарных уязвимостей

~~Во славу Сатаны, конечно~~

Москва, 2020



SQL-injections, способы обнаружения

Способы обнаружения:

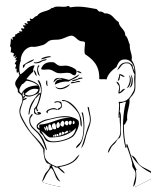
- DAST
- SAST
- WAF
- QA
- Pentest
- Bug Bounty (кстати это реклама)
- Вашу базу выложили в darknet

Не спрашивайте что это за слова, сам в первый раз вижу

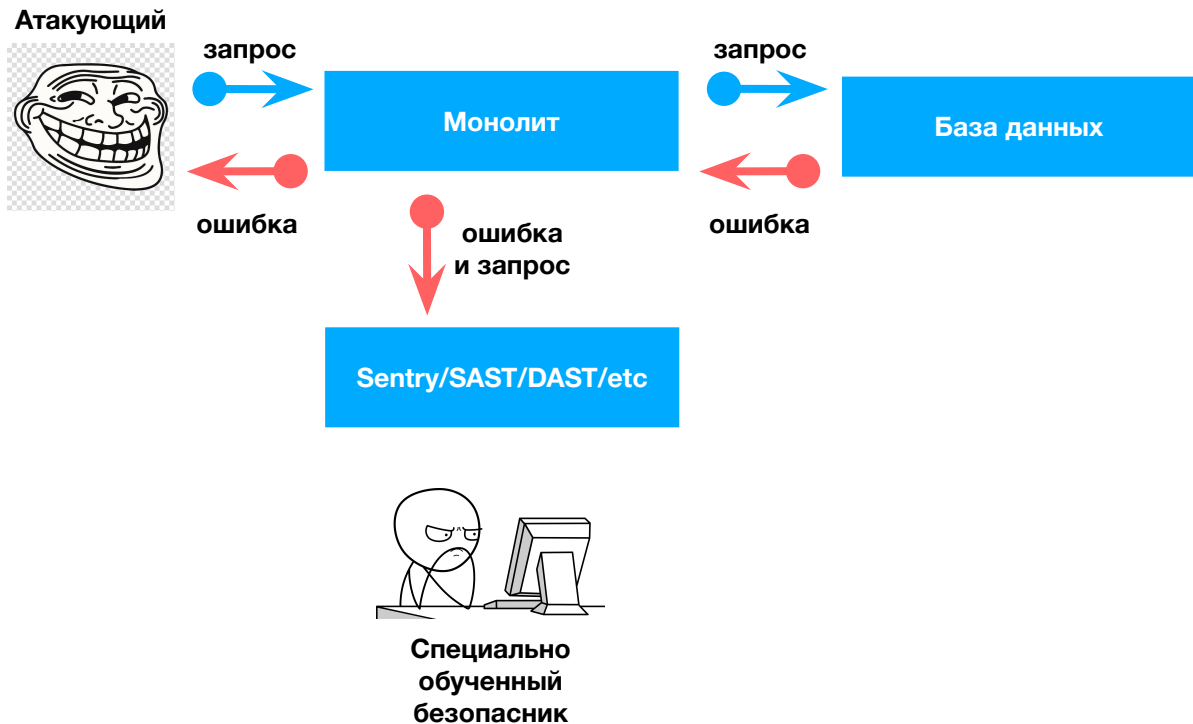
Москва, 2020

Почему может не сработать:

- Не было оригинального запроса к API
- Сложная предобработка данных до запроса в БД
- Большая кодобаза
- Один пентестер на весь продукт (привет, это я)

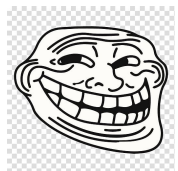


Проблема обнаружения уязвимостей: тогда



Проблема обнаружения уязвимостей: сейчас

Атакующий



запрос



ошибка

Gateway
и прочая магия

запрос



ошибка

Микросервис 1

запрос



ошибка

Микросервис 100

запрос



ошибка

База данных 1

запрос



ошибка

База данных 100

Sentry/SAST/DAST/etc



Специально
обученный
безопасник

Как выглядит атака на БД?

- Первоначально это веб-запрос
- Есть какое-то API с параметрами
- Кто-то пытается найти там SQL-инъекцию
- ' - ошибка
- ' UNION select null - ошибка
- ' UNION select null, null - ошибка
- ' UNION select null, null, null - успешный запрос (всё, БД утекла, game over)

- Если эксплуатация порождает столько ошибок - где это можно заметить?



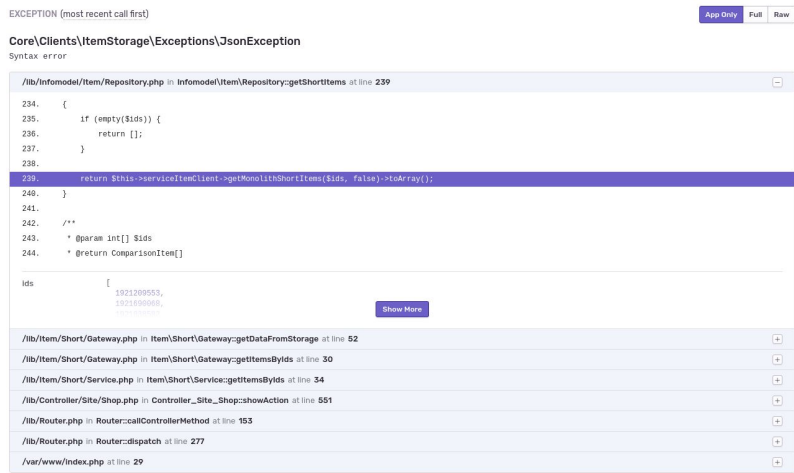
Заглянуть в логи базы данных

- Все ошибки будут в базе данных
- Одно и то же место в коде может вызвать сотни и тысячи ошибок
- Нет возможности быстро понять какой код вызвал ошибку
- Нет возможности быстро восстановить веб-запрос, вызвавший ошибку



Error Tracking Software (на примере Sentry)

Ошибка в приложении порождает issue в sentry.
Отличный способ для детекта (подумали мы).



The screenshot displays the Sentry web interface for an exception. At the top, it says 'EXCEPTION (most recent call first)' and shows the exception type 'Core\Exceptions\JsonException' with a 'Syntax error' message. Below this, the stack trace is visible, with the current frame highlighted: `/lib/Infomodel/Item/Repository.php in Infomodel\Item\Repository::getShortItems at line 239`. The code snippet shows a function that returns an array of item IDs. Below the code, the 'ids' variable is shown as an array containing a single integer: `[1021209953]`. At the bottom, a list of other frames in the stack trace is visible, including `/lib/Item/Short/Gateway.php`, `/lib/Item/Short/Service.php`, `/lib/Controller/Site/Shop.php`, `/lib/Router.php`, and `/var/www/index.php`.

Читая логи с умным видом,
Восстановив их из dev null
Мы говорим своим Тим лидам
"Один лишь раз мы дали слабину,
Все точно будет распрекрасно,
Вы беспокоитесь напрасно."
Везде используем защиту,
Случайно на ошибку эту,
Наткнулся хакер, чтоб его,
Да это легаси подход
Писался, чтобы быстро в прод
Продукт наш выкатить давно
Исправить времени нехватка,
Вот и работает заплатка



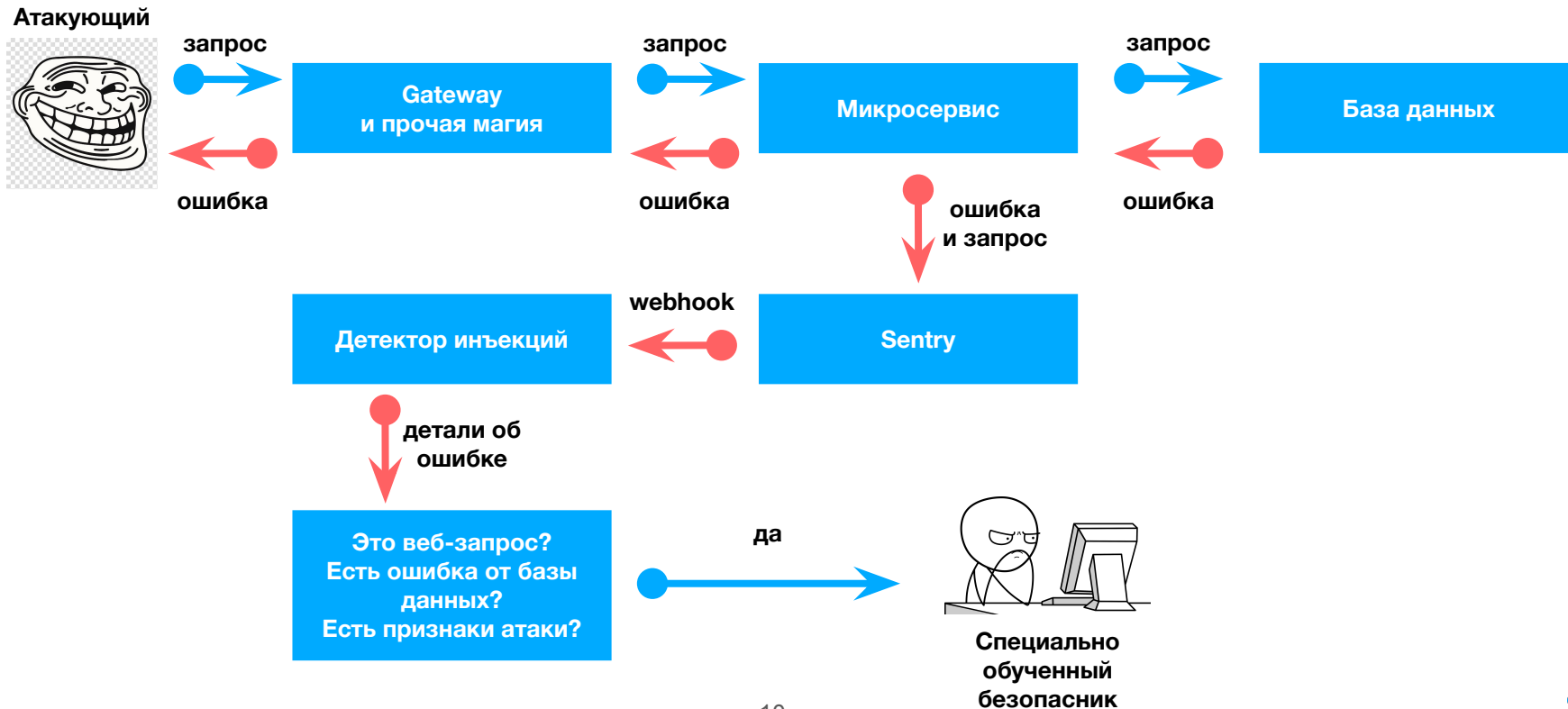
Наш велосипед

1. Sentry в сервисах уже работает из коробки
2. Разработчику не нужно ничего настраивать
3. Автоматическая интеграция в sentry через api
4. Вебхук на каждый новый issue в sentry
5. Ищем признаки атаки на БД в каждом issue
6. Уведомляем Security, если что-то нашлось

Суть рекурсии сурово
Донести до новичка
Можно ошибаясь немного
В обработке веб-хука



Схема работы велосипеда



Вечная борьба с ложными срабатываниями

- Исходные признаки атаки:
 - список возможных ошибок от базы данных
 - спецсимволы/ключевые слова
 - алерт при нахождении любого подозрительного запроса
- Статистика срабатываний:
 - 10-20 срабатываний в час - это печально
- Весьма... неожиданные ложные срабатывания



Кавычка, там кавычка!!!
Вы что не понимаете?
Там КА-ВЫ-ЧКА!!!!

Примеры ложных срабатываний при поиске





бензопила echo 360



air-flex drop table

L'Or (2017)




shimano ax match 450 spc



Улучшаем признаки атаки на базу данных

- Собираем разные критерии:
 - спецсимволы (', ", %, --, (,), 0x, etc)
 - ключевые слова (select, union, or, and, like, match, ...)
 - Текст ошибки (syntax error, ambiguous column, permission denied for relation, ...)
 - список типичных атак на базу данных, взяли от него url encode, base64 encode, html encode (' or 1=1 -- -, ' union select * from users -- -)
- Вводим “степень похожести” запроса на атаку
 - сумма найденных критериев
- Сообщаем только в случае превышения заданного порога похожести
- В итоге получаем от 1 до 5 сообщений в день (ужасно много, хотим придумать что-нибудь ещё)



A wide-angle photograph of a gravel or dirt road in a rural setting. In the foreground, a large, round hay bale sits on the left side of the road. The road stretches into the distance, curving slightly to the right. The background features a flat, golden-brown field under a clear blue sky with a few wispy clouds. A utility pole is visible on the left side of the road.

И замираем в ожидании

На пару месяцев, пока однажды...

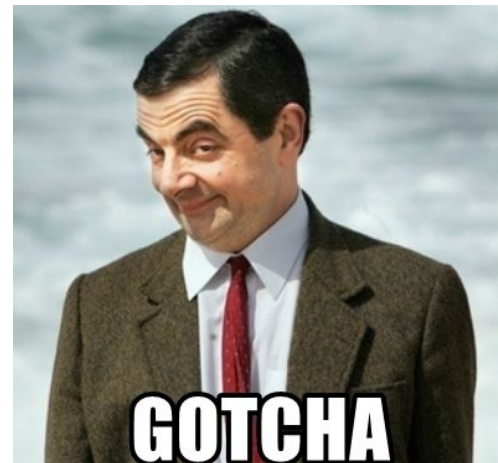
Пример алерта

avito **Syntax error** - <http://sentry.msk.avito.ru/avito/avito/issues/33984757/>

func: **Infomodel\Item\Repository::getShortItems** type: **Core\Clients\ItemStorage\Exceptions\JsonException**

```
Url: http://www.avito.ru/velo-pro_shop, params: [{"gdlkerfdnwq", "102"}, {"shopId", "120960"}, {"page_from", "from_items_list"}, {"iid", "1557717182"}, {"161930154 or 6824=68240-- ", "1"}]
```

- Сразу видно наличие атаки в имени последнего параметра
161930154 or 6824=68240--



Core\Clients\ItemStorage\Exceptions\JsonException

Syntax error

/lib/Infomodel/Item/Repository.php in **Infomodel\Item\Repository::getShortItems** at line **239**

```
234.     {
235.         if (empty($ids)) {
236.             return [];
237.         }
238.
239.         return $this->serviceItemClient->getMonolithShortItems($ids, false)->toArray();
240.     }
241.
242.     /**
243.      * @param int[] $ids
244.      * @return ComparisonItem[]
```

```
ids
    [
        1921209553,
        1921690068,
        1921690583
```

[Show More](#)**/lib/Item/Short/Gateway.php** in **Item\Short\Gateway::getDataFromStorage** at line **52****/lib/Item/Short/Gateway.php** in **Item\Short\Gateway::getItemsByIds** at line **30****/lib/Item/Short/Service.php** in **Item\Short\Service::getItemsByIds** at line **34****/lib/Controller/Site/Shop.php** in **Controller_Site_Shop::showAction** at line **551****/lib/Router.php** in **Router::callControllerMethod** at line **153****/lib/Router.php** in **Router::dispatch** at line **277****/var/www/index.php** at line **29**

Исходный запрос

```
curl \
--compressed \
-H "Accept: */*" \
*censored*
"http://www.avito.ru/velo-pro_shop?gdlkerfdnwq=102&shopId=12
0960&page_from=from_items_list&iid=1557717182&161930154 or
6824=68240--%20=1"
```



161930154 or 6824=68240--

- Атака != Уязвимость
- Приходится проверять руками
- Сужается область поиска
- Можно быстро проверить код
- Позволяет приоритизировать исправление именно этого бага

Мораль сей басни такова:
~~Купите нашего слона~~
Смотрите в логи иногда

Удалить перед
выступлением!



Вопросы

Directed by
ROBERT B. WEIDE