Страх и ненависть в платежных системах

Годюк Арвид (Arvīds Godjuks) a.k.a. @psihius

14 июня 2014 года

Обо мне

- 10 лет в web – PHP, MySQL
- Только средние и большие проекты
- Активен в internals mailing list
- Огранизатор WebConf Riga 2010 и 2012
  - 2015 в планах ☺
- Демоны на PHP ☺

Что в этом докладе?

- Опыт
- Ещё раз опыт
- И значительная сумма про*****ых денег ☹

Чего не будет

- Советов, как сделать пи**то
  - У каждого проекта свои заморочки
- Ответа на вопрос «Где, чёрт возьми, ты работаешь, псих ненормальный?!»

И так, платёжные системы

- Классика
  - WebMoney, PayPal, Moneybookers, etc.
- Ваучеры
  - Ukash, CashU, PaySafeCard, etc.
- Криптовалюты
  - Bitcoin, Litecoin, etc.

Реальность

- Платёжки умирают
  - R.I.P Liberty Reserve
- API платёжек координально отличаются
- Деньги можно потерять

Имейте альтернативу

Не складывайте все яйца в одну корзину – может получится гигансткий омлет

А теперь к весёлью

Приколы с API

- Отсутствие SSL
- Отсутствие status url
  - Подтверждение происходит в виде перенаправления браузера клиента
  - Это секюрно, инфа 146%!

Приколы с API

- Подтверждение транзакции методом парсинга HTML ответа от сервера платёжки
  - Пламенный привет Perfect Money

Приколы с API

- Когда докуметация ..., ну вы поняли
  - Потратил пол дня в попытках понять, почему не принимает валидный запрос на платёж.
  - Как оказалось – в поле комментария принимало буквы, цифры, пробел, @ и запятую. В документации ни слова.

Приколы с API

- Когда с сервером платёжки происходит неведома х....
  - Привет Liberty Reserve, R.I.P.
- Когда сервер платёжки начинает присылать двойные подтверждения.
  - Привет Perfect Money

Оработка нотификаций

- Унифицированное API
- Offload обработки в background
  - Демоны ☺

Защита платёжек

- У многих платёжек кроме md5 хеша нет никакой дополнительной защиты
  - Привет видеокартам, перебирающим 150 млн. хешей в секунд
  - Бывает что даже нет и этого – пропускаем ☺
- Есть платёжки, которые не имеют кастомных полей для мерчантов

Защита платёжек – о хорошем

- SHA1/SHA256
- Валидация нотификации через запрос на сервер платёжки
- Дополнительные secret keys
- Работа с SSL подписанными запросами
- OAuth – привет Yandex.Money

Защита платёжек - отсебятина

Кроме стандартных проверок на сумму платежа и валюту

Защита платёжек - отсебятина

- Испольуем custom fields
  - Генерируем свою подпись с данными, которые есть только внутри системы и валидируем
- Проверяем платёж на соответсвие платёжной системе
- Whitelisting серверов платёжек по IP

Защита платёжек - отсебятина

- Отложенная доставка купленного клиентом
  - Защищает так же от фрауда
- Ведение собственного баланса, если вы делаете выплаты
  - Но нужно это делать правильно – столкнулся с race condition и вышел double spend

Тайные знания ☺

- Только для аудитории :trollface:

Вопросы по архитектуре?

- Не тематическая секция ☺
- Yii 1.1
- MySQL

Вопросы?

@psihius
https://www.facebook.com/psihius
arvids.godjuks@gmail.com