Взлом 

Выбираем карьеру правильно

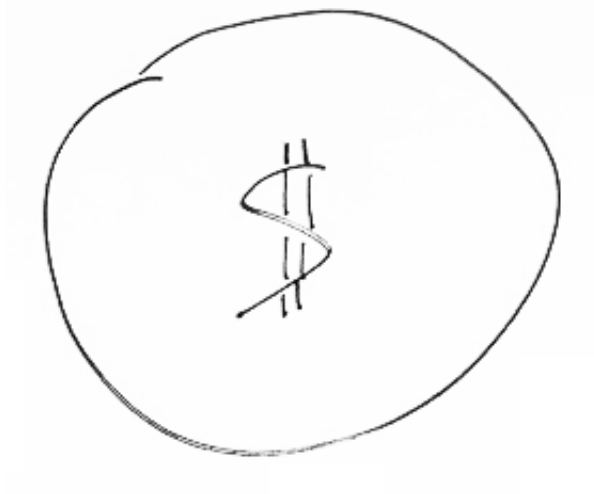
Тимур Юнусов, Positive Technologies

POSITIVE TECHNOLOGIES

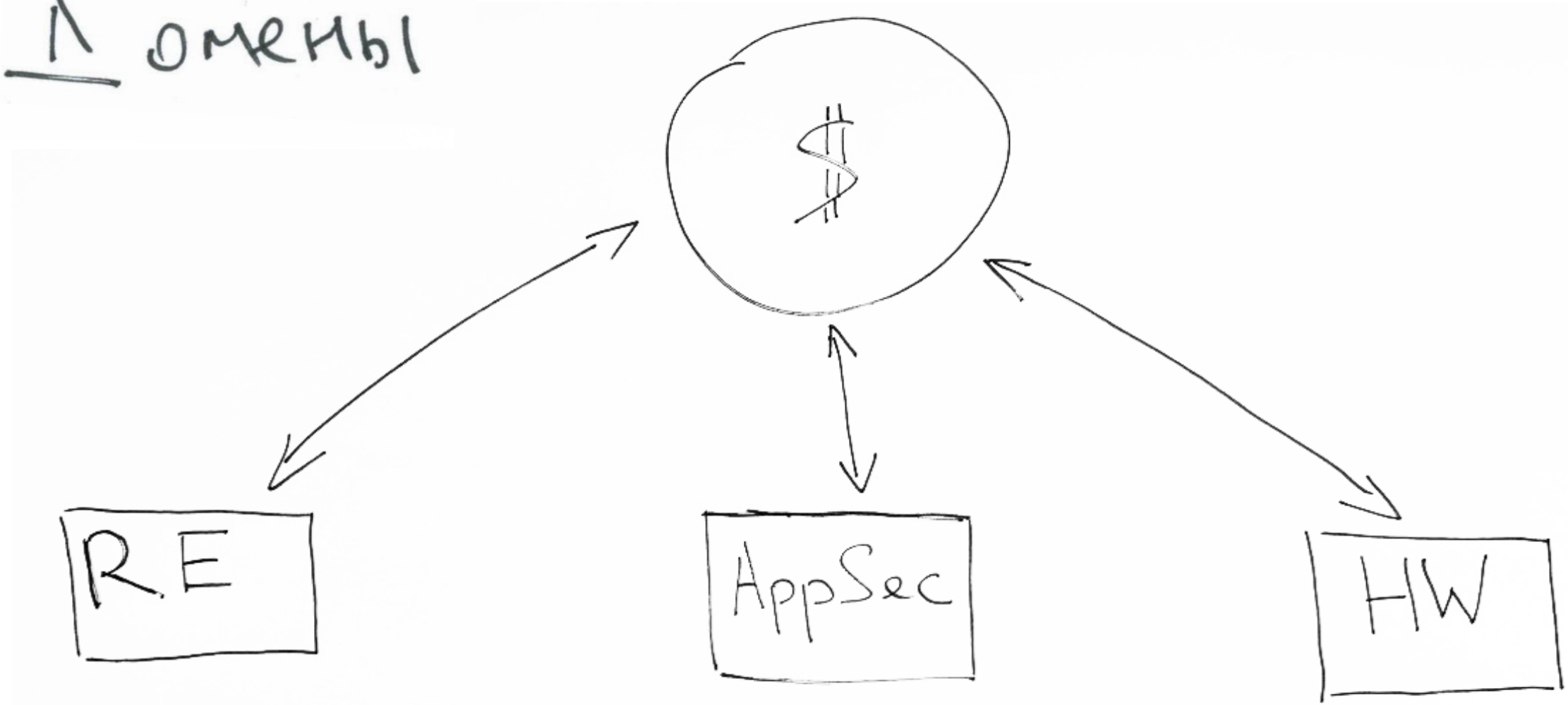
- Домены информационной безопасности в финтехе
- Карьерные возможности и идеи
- Примеры
- Вопросы и ответы

Prepared by: Arif Sidiqui

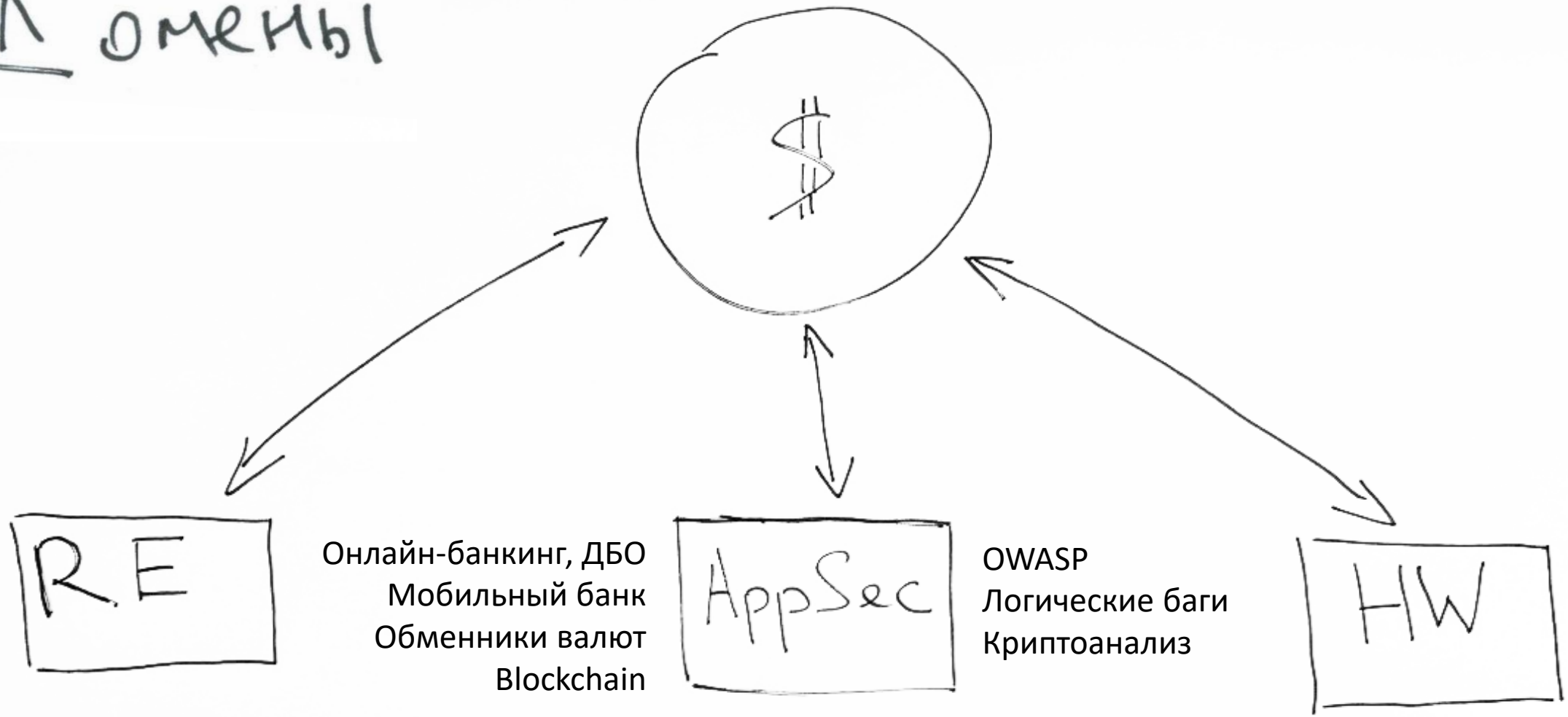
1 Деньги



Домены



Домены



Онлайн-банкинг, ДБО
Мобильный банк
Обменники валют
Blockchain

OWASP
Логические баги
Криптоанализ

Домены

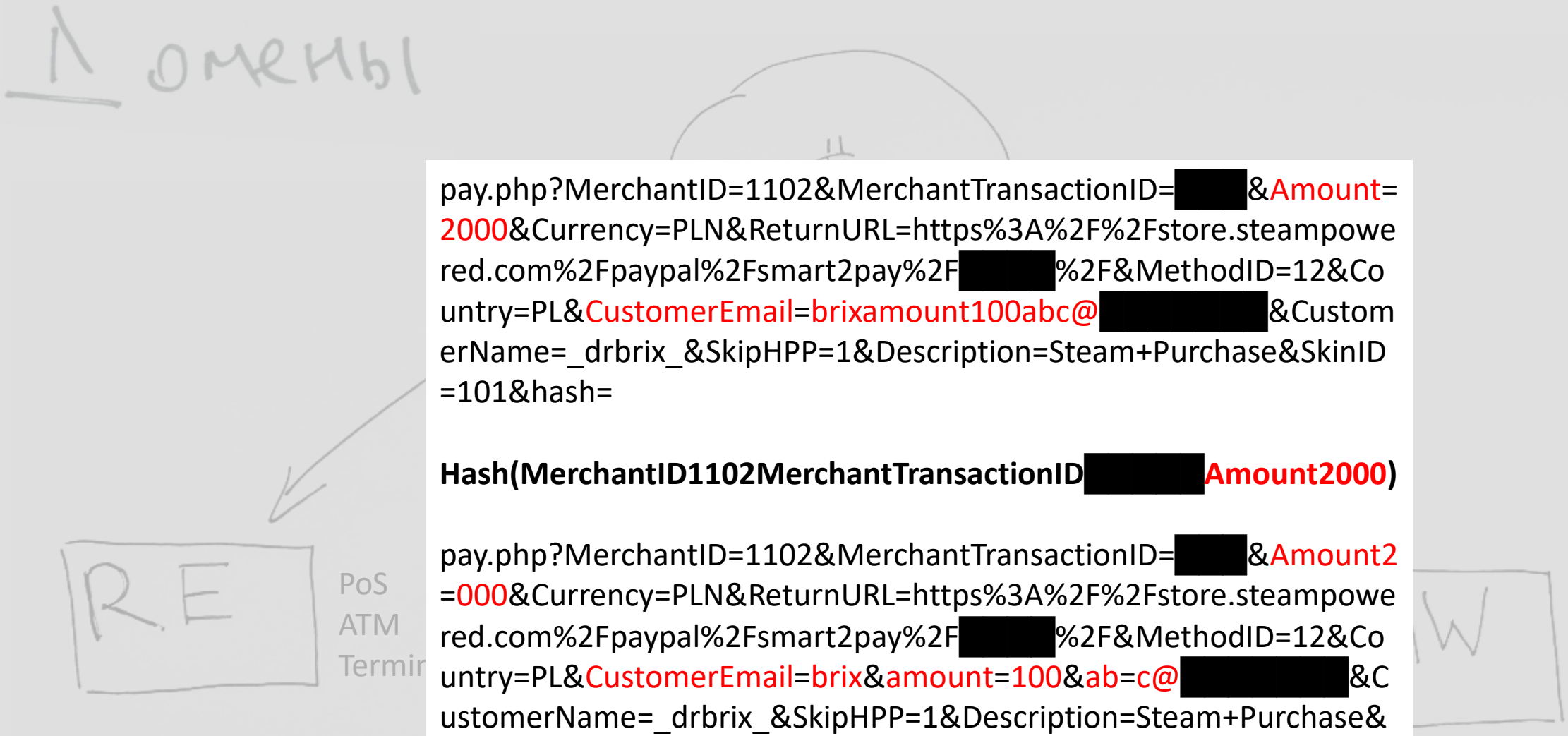
Платежные карты
POS терминалы
Банкоматы
Киоски и кассы

Платежные карты
POS терминалы
Банкоматы
Киоски и кассы

KindleDrip — From Your Kindle's Email Address to Using Your Credit Card

Yogev Bar-On Jan 21 · 9 min read

> *Or the story of how I received an 18K$ bug bounty for a critical Amazon Kindle vulnerability.*



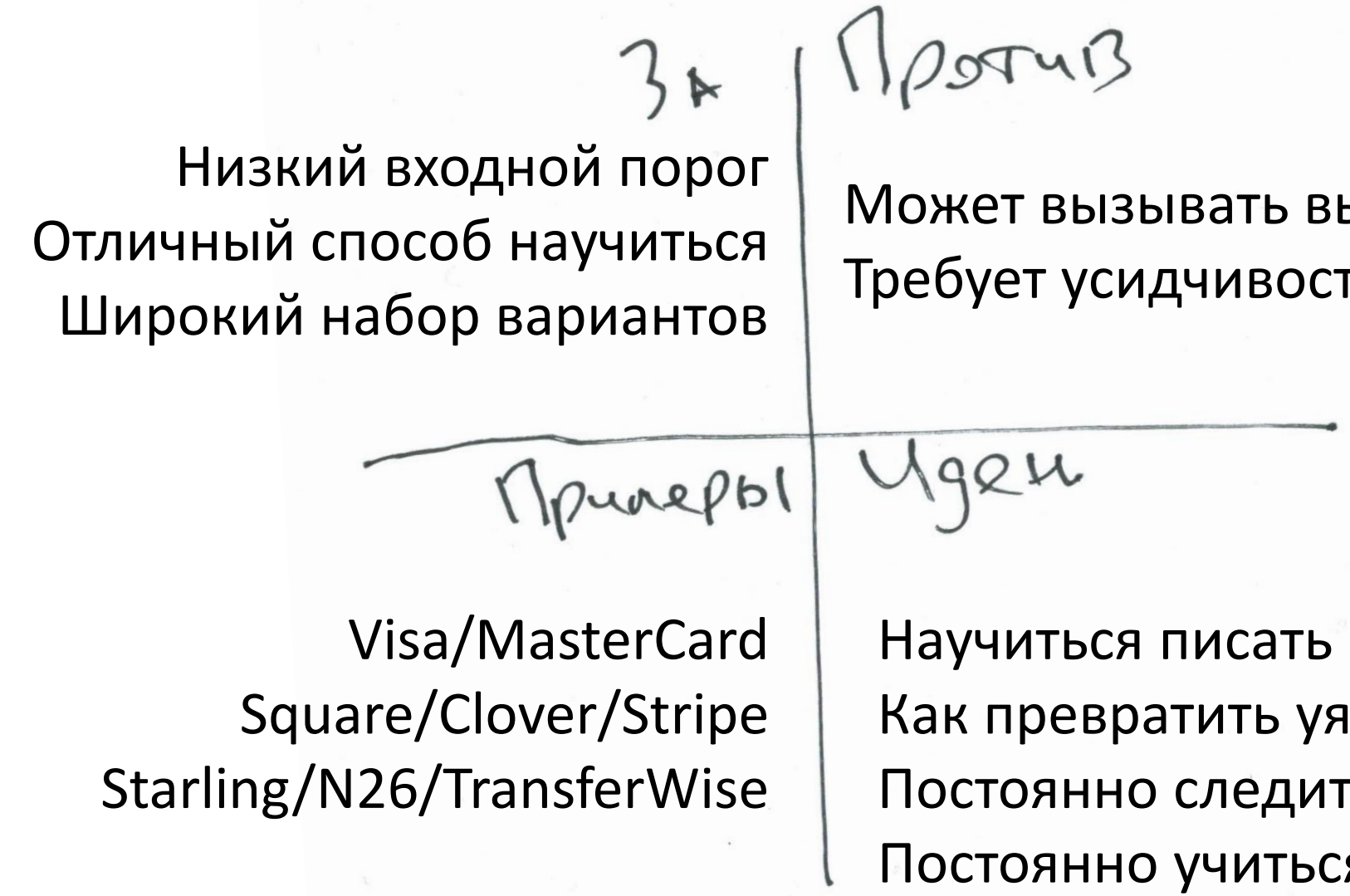
pay.php?MerchantID=1102&MerchantTransactionID=[redacted]&Amount=2000&Currency=PLN&ReturnURL=https%3A%2F%2Fstore.steampowered.com%2Fpaypal%2Fsmart2pay%2F[redacted]%2F&MethodID=12&Country=PL&CustomerEmail=brixamount100abc@[redacted]&CustomerName=_drbrix_&SkipHPP=1&Description=Steam+Purchase&SkinID=101&hash=

Hash(MerchantID1102MerchantTransactionID[redacted]Amount2000)

pay.php?MerchantID=1102&MerchantTransactionID=[redacted]&Amount2=000&Currency=PLN&ReturnURL=https%3A%2F%2Fstore.steampowered.com%2Fpaypal%2Fsmart2pay%2F[redacted]%2F&MethodID=12&Country=PL&CustomerEmail=brix&amount=100&ab=c@[redacted]&CustomerName=_drbrix_&SkipHPP=1&Description=Steam+Purchase&SkinID=101&hash=<the same>

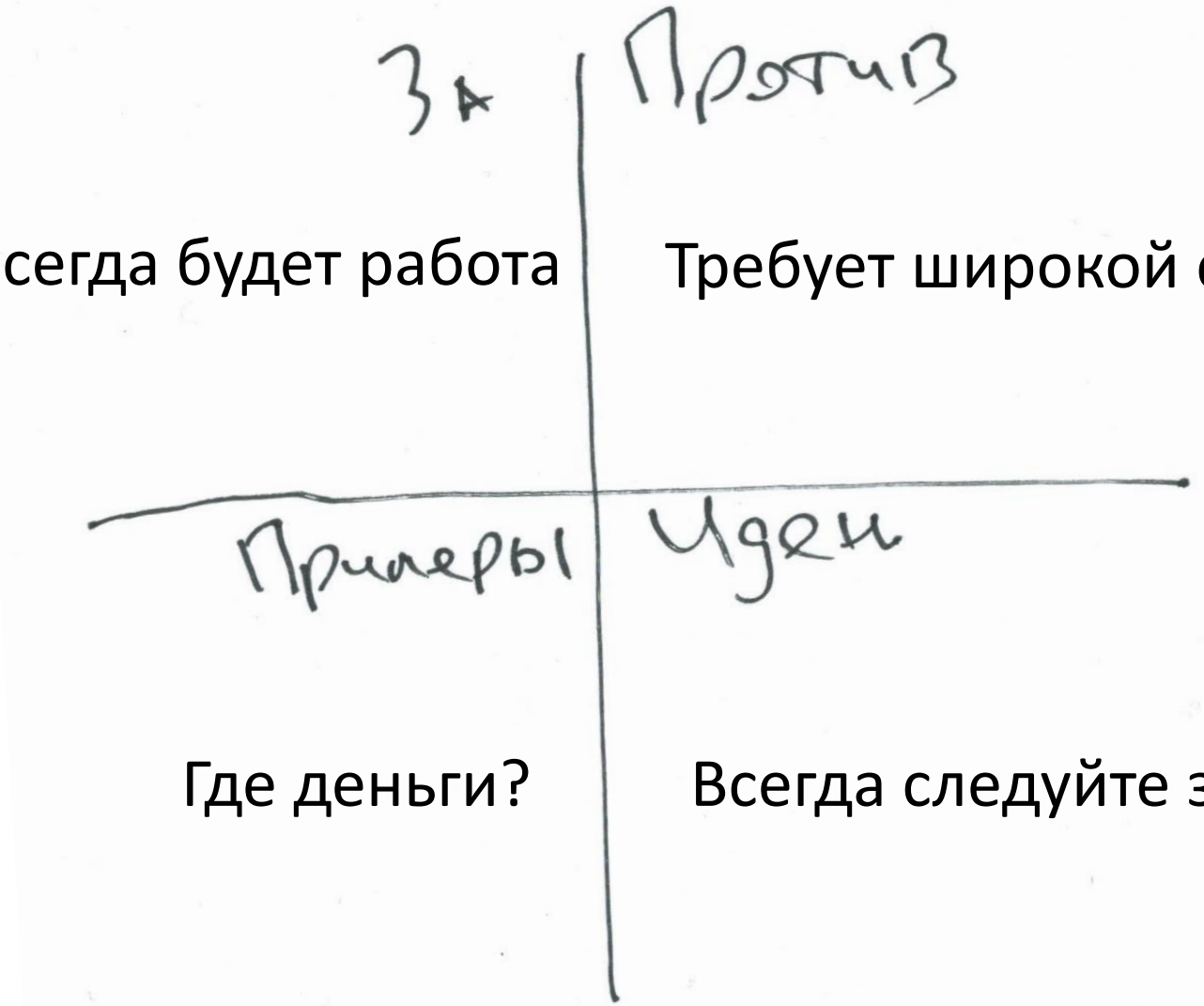
Карьера

Баг баунти


За
Против
Низкий входной порог
Отличный способ научиться
Широкий набор вариантов
Может вызывать выгорание
Требует усидчивости и выдержки
Примеры
Идеи
Visa/MasterCard
Square/Clover/Stripe
Starling/N26/TransferWise
Научиться писать и читать
Как превратить уязвимость в риск
Постоянно следить за рынком
Постоянно учиться чему-то новому

Карьера

Пентест/
Red Team



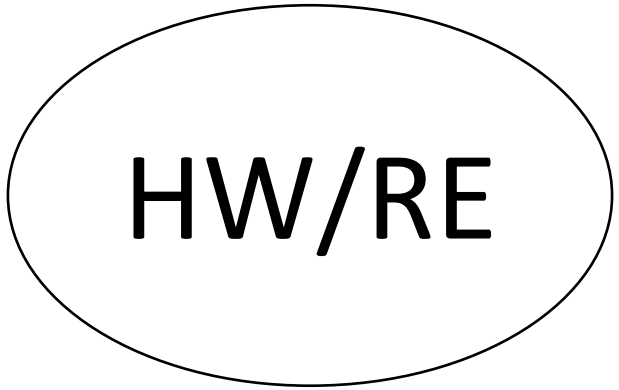
У вас всегда будет работа

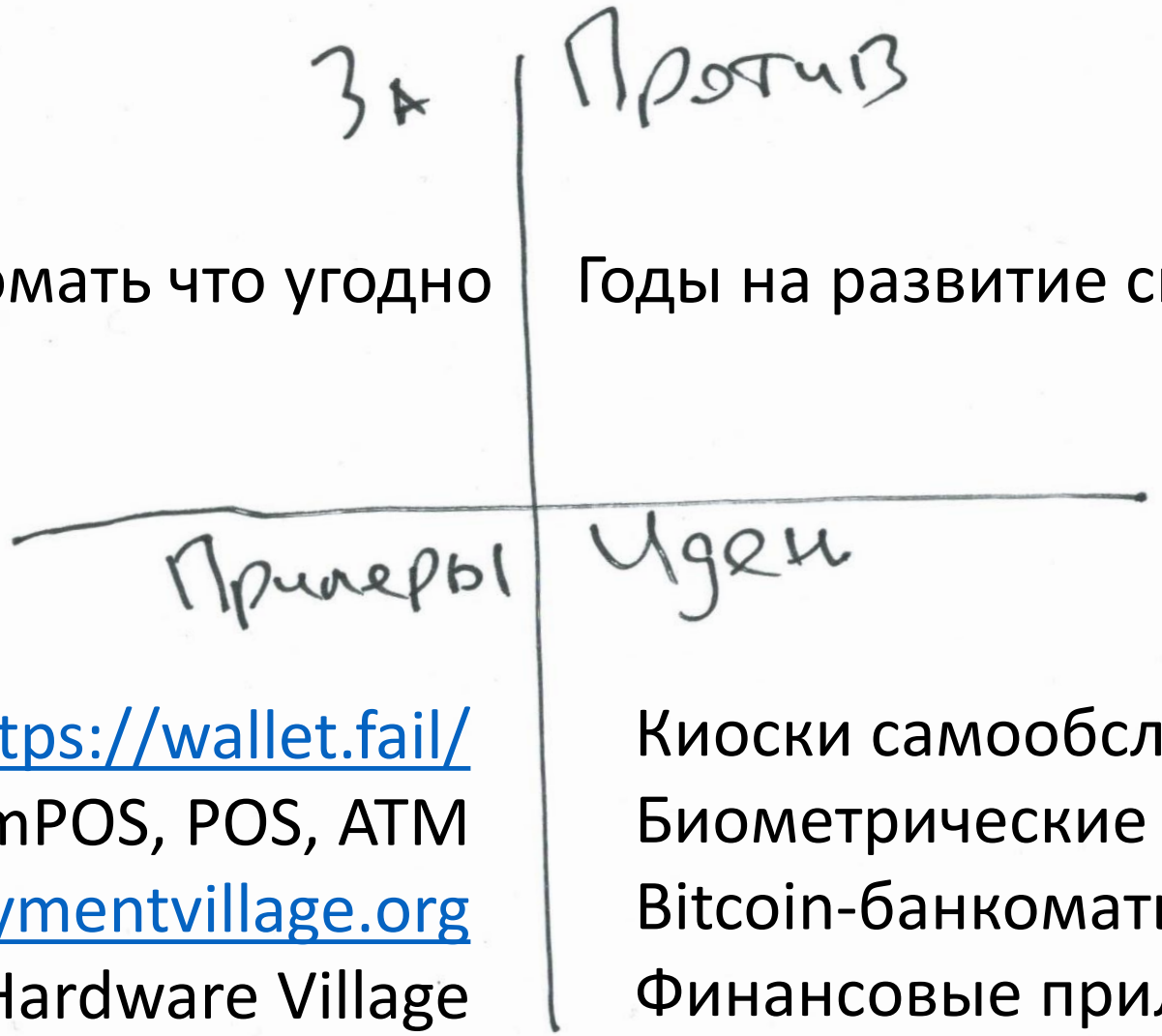
Требует широкой специализации

Где деньги?

Всегда следуйте за деньгами

Карьера





Вы сможете ломать что угодно

Годы на развитие скиллов

Ledger - https://wallet.fail/

mPOS, POS, ATM

https://paymentvillage.org

Hardware Village

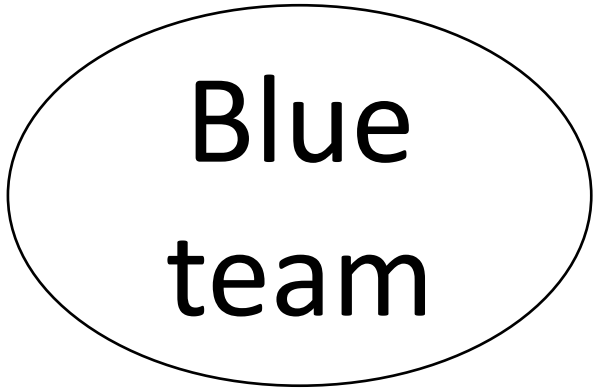
Киоски самообслуживания

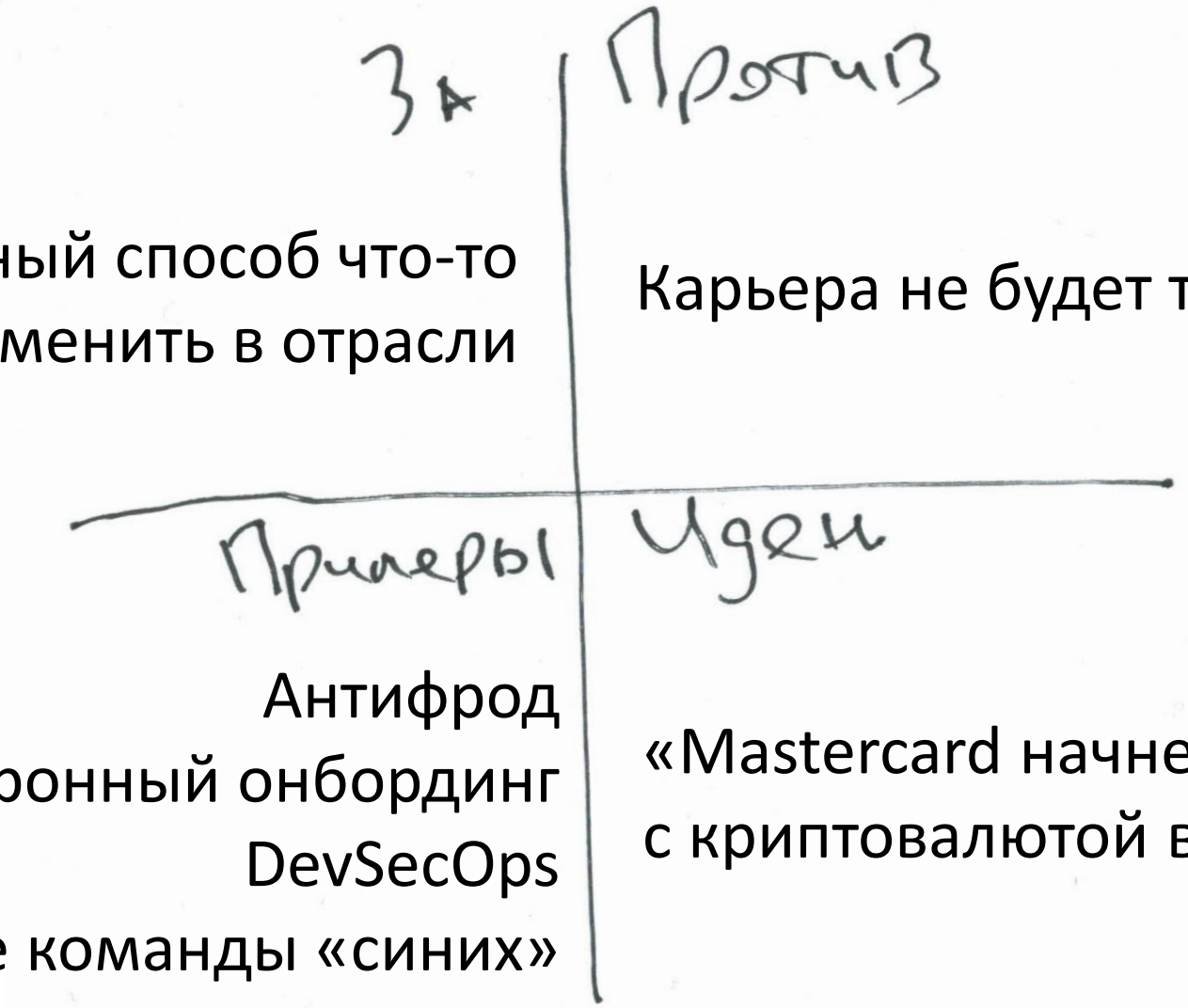
Биометрические системы, SoftPOS

Bitcoin-банкоматы

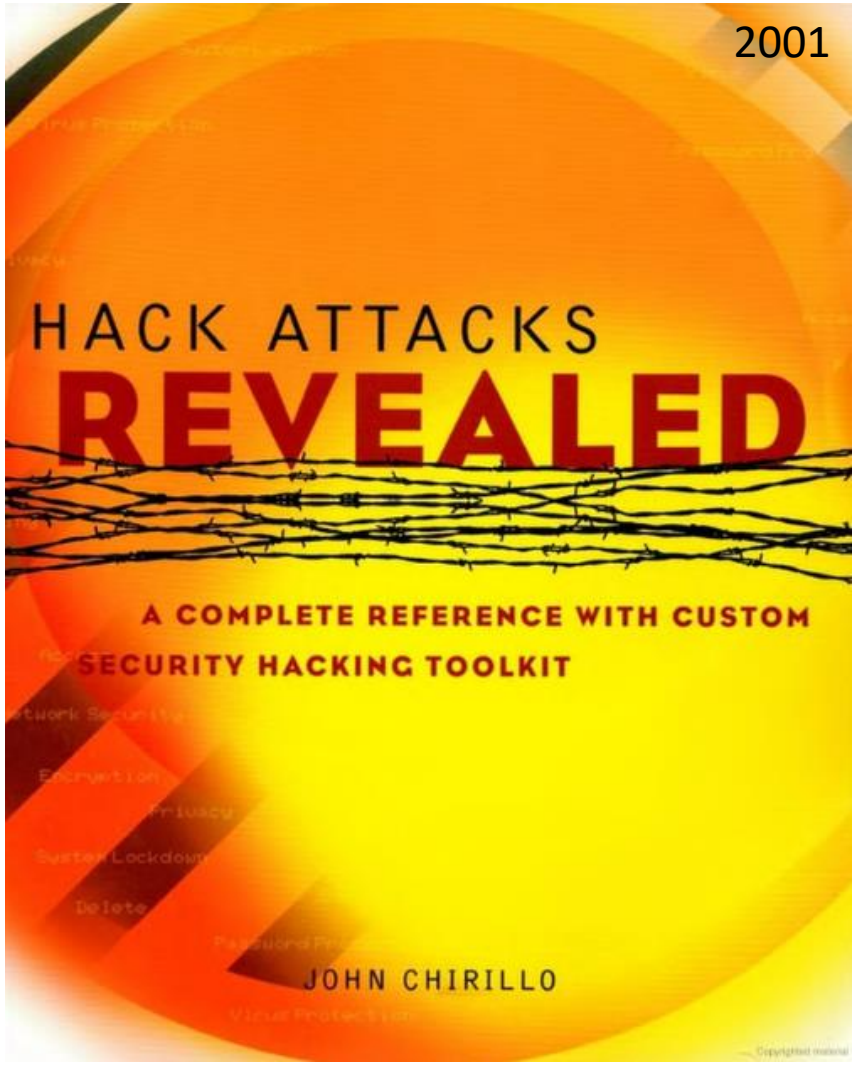
Финансовые приложения (MT4, MT5)

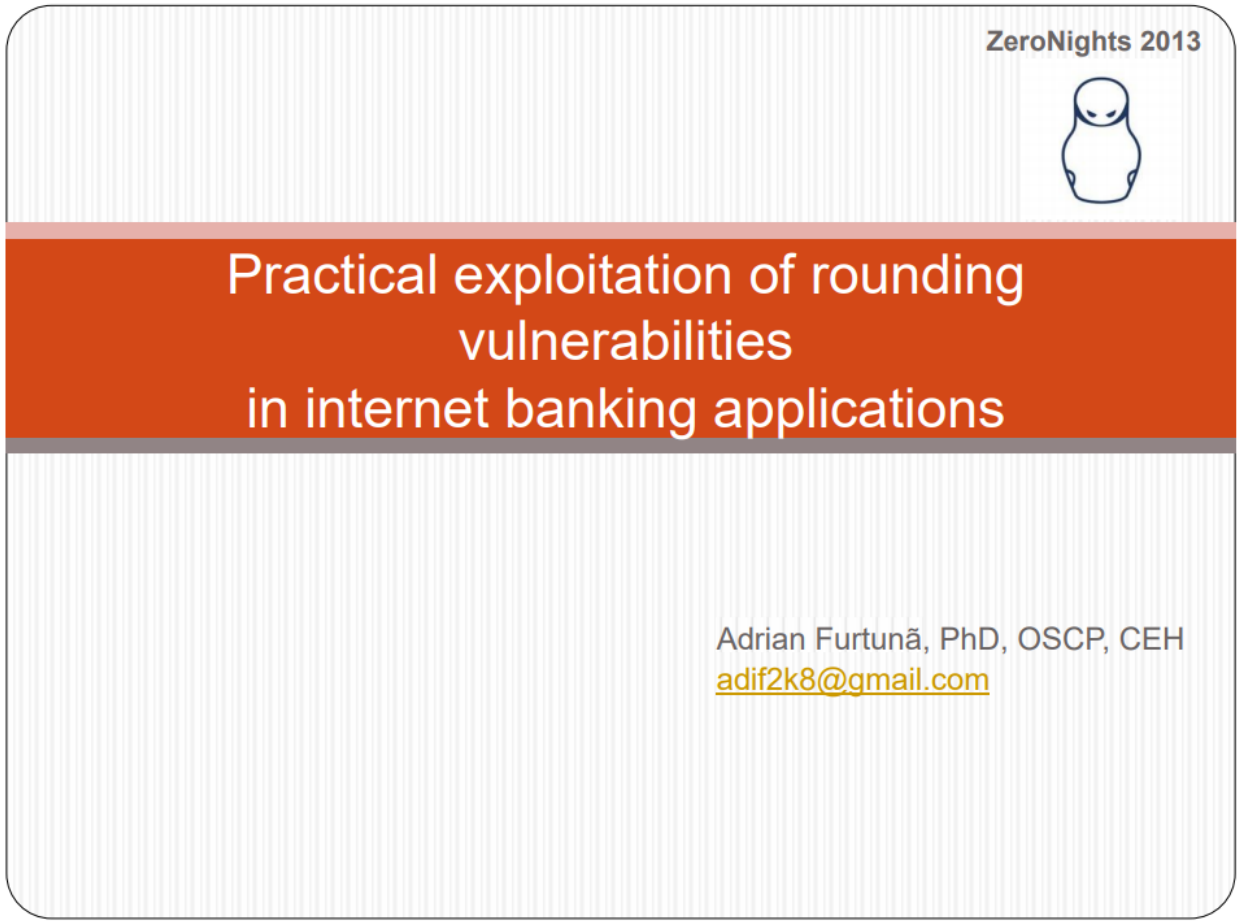
Карьера




За
Против
Единственный способ что-то изменить в отрасли
Карьера не будет такой яркой
Примеры
Идеи
Антифрод
KYC и электронный онбординг
DevSecOps
Различные команды «синих»
«Mastercard начнет работать с криптовалютой в 2021 году»

Округления


2001
HACK ATTACKS
REVEALED
A COMPLETE REFERENCE WITH CUSTOM
SECURITY HACKING TOOLKIT
JOHN CHIRILLO


ZeroNights 2013
Practical exploitation of rounding vulnerabilities in internet banking applications
Adrian Furtunã, PhD, OSCP, CEH
adif2k8@gmail.com


Hacker News new | past | comments | ask | show | jobs | submit
Round error issue – produce money for free on itBit bitcoin exchange (hackerone.com)
70 points by waffle_ss on Mar 3, 2017 hide | past | web | favorite | 60 comments

Округления

Хорошо объяснил: https://youtu.be/f7tWWyCeqNM

Если коротко:

- 1 GBP = 1,30 USD
- 0.02 USD => float(0.0153; 2) == 0.02 GBP
- Выгода = 0.0047 USD

Округления

Хорошо объяс

Если коротко:

- 1 GBP = 1,30
- 0.02 USD => f
- Выгода = 0.0

Округления

Хорошо объяснил: https://youtu.be/f7tWWyCeqNM

Если коротко:

- 1 GBP = 1,30 USD
- 0.02 USD => float(0.0153; 2) == 0.02 GBP
- Выгода = 0.0047 USD

- x500 ($2)
- x10,000 ($47)
- Обход одноразовых паролей
- Обход antifraud
- Автоматизация

Совкомбанк выявил новую схему закольцованных транзитных операций

16:04 / 7 Мая, 2021

Совкомбанк | Авангард | бонусные мили

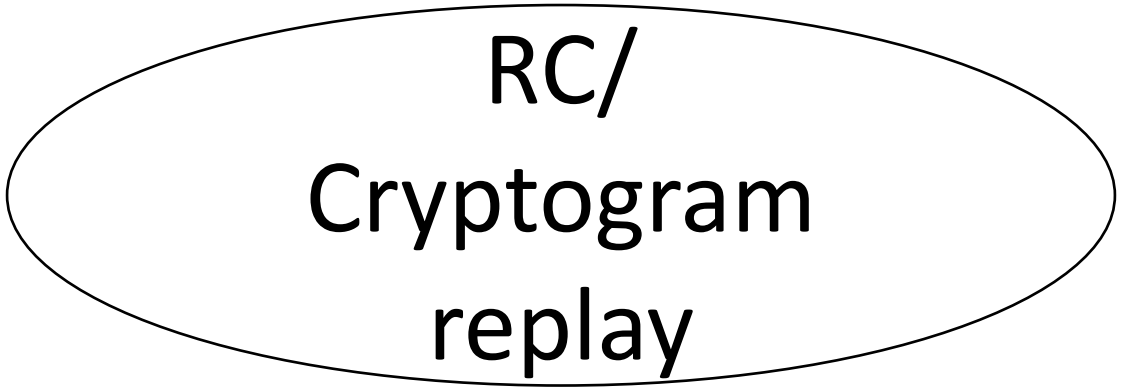
Идеи

- Обмен валют уже не работает везде
- Онлайн эквайринг в валютах – PayPal/Square ($) + карта в рублях + возвраты
- Card2card: отправить $0.02 на GBP карту (всегда получим 0.02GBP)
- 0.01[любая] (PHP, RUB) -> 0.01[любая] (USD, GBP) – эффективно
- Кэшбек, бонусы – работает почти везде

This configures fraud and is addressed on another sphere of control, normally through Law Enforcement Agencies and internally by finance departments—not bug bounty programs. Your effort is nonetheless appreciated and we wish that you'll continue to research and submit any future security issues you find.

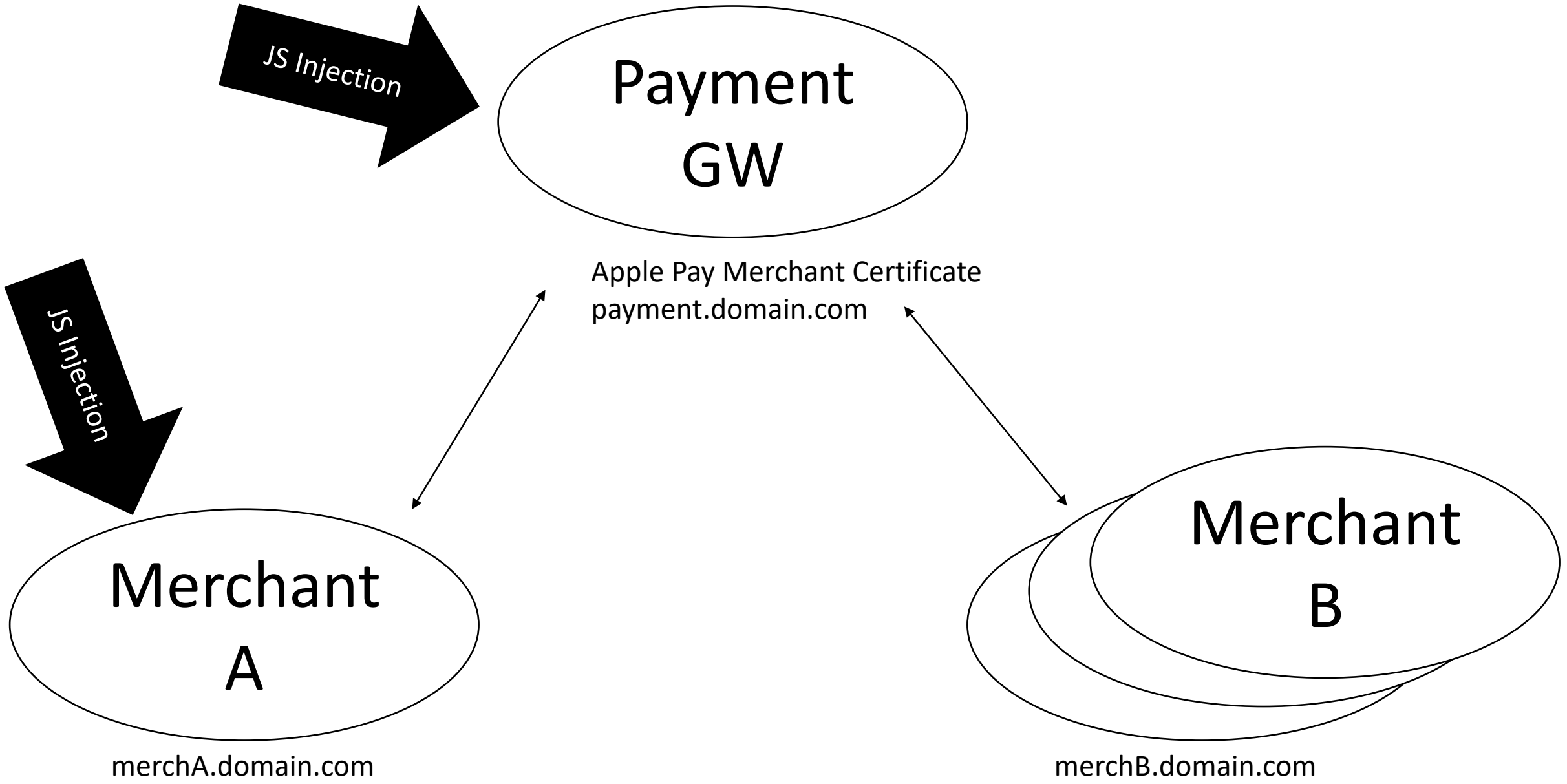
Thank you for your submission! Unfortunately, this particular issue you reported is explicitly out of scope as outlined in the [Policy Page](https://hackerone.com/paypal):

> - Attacks involving payment fraud, theft, or malicious merchant


RC/
Cryptogram
replay

Apple doesn't know what you bought

That's true ;)


JS Injection
Payment GW
Apple Pay Merchant Certificate
payment.domain.com
JS Injection
Merchant A
merchA.domain.com
Merchant B
merchB.domain.com

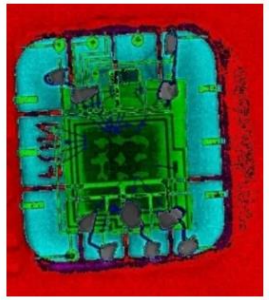
PIN OK

Детали: https://www.paymentvillage.org/wiki/pinok

Если коротко:

- Список методов верификации на карте
- Подмена первого метода на “Offline PIN”
- Вводим случайный PIN
- Карта отвечает 63C2 (еекорректный PIN, 2 attempts left)
- Replace the answer to 9000 (PIN OK)

PIN OK



“Chip and Spin”,

Ross Anderson, Mike Bond, Steven J. Murdoch

2005

2010

“Chip and PIN is broken”,

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond

2011

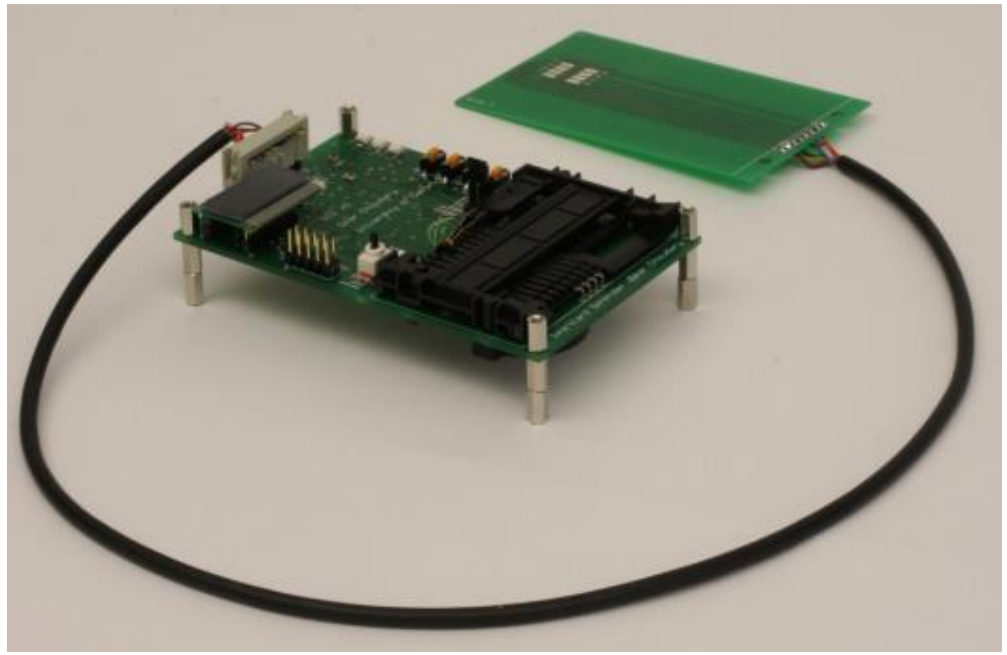
2020

Bypassing of PSD2 Cumulative limits

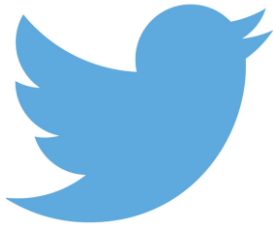
https://www.cyberdlab.com/research-blog/card-fraud-in-a-psd2-world-a-few-examples

2021…

Ожидание vs Реальность



Q&A



@a66ot

www.paymentvillage.org

tyunusov@ptsecurity.com