Digital Security

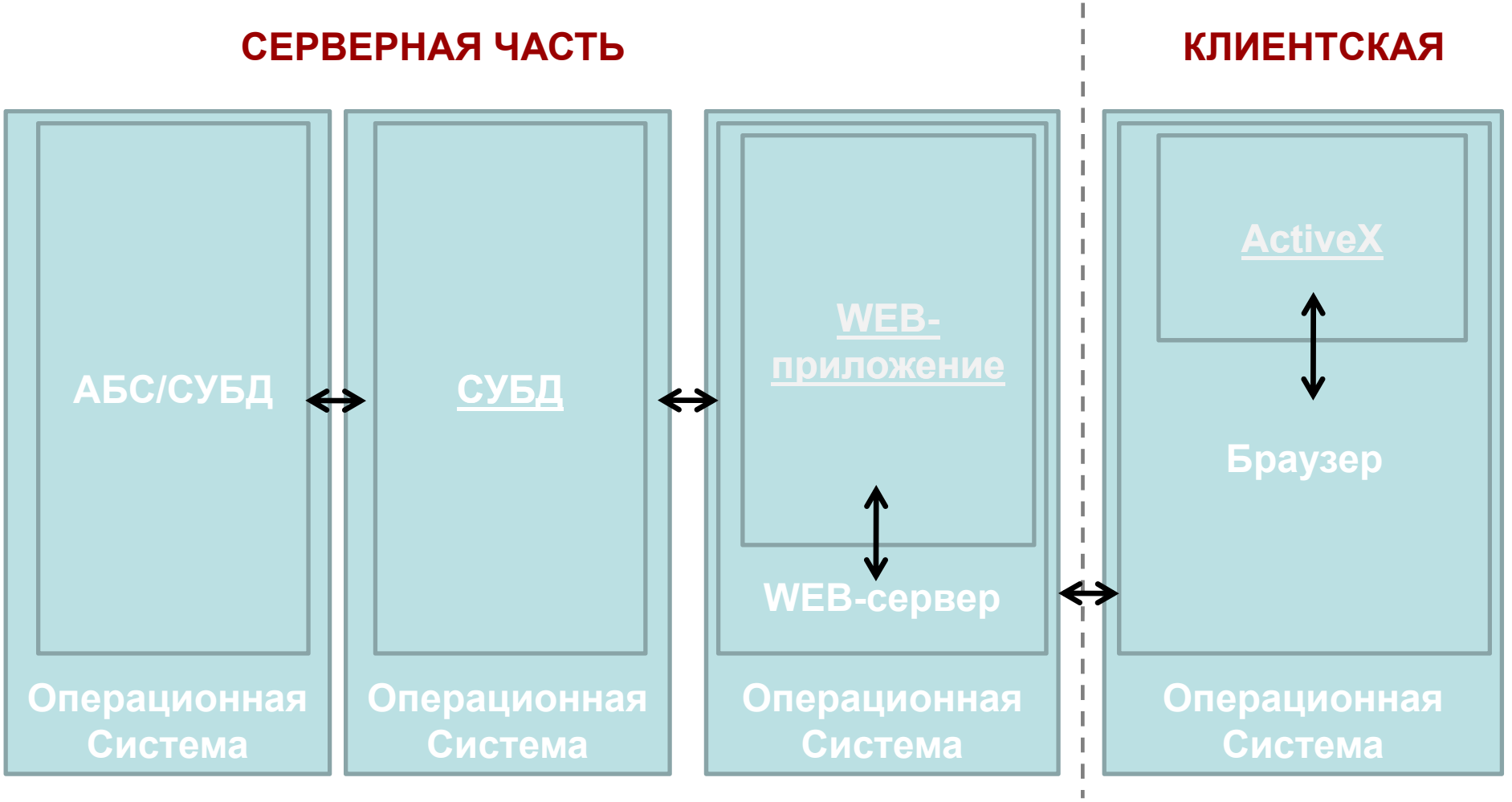
Где лежат деньги?

Дмитрий Частухин

Аудитор ИБ

Digital Security

Как это работает



Атака в лоб…. WEB

- В **90%** отечественных ДБО есть/были XSS
- SQLi - то же бывают

^^^^^^^^^^^^^^^^^^^^^^^^^^^

…это и так все знают (Правда?)

Атака в лоб…. WEB

- В **90%** отечественных ДБО есть/были XSS
- SQLi - то же бывают

^^^^^^^^^^^^^^^^^^^^^^^^^^^

…это и так все знают (Правда?)

- Ошибки авторизации
  (местами их и вовсе не бывает)
- Раскрытие данных
- Ошибки АРХИТЕКТУРЫ
- И многое другое……..

Не слишком ли много для такого критичного продукта?

Пример 1

ДБО для физ. лиц (**pre-auth)**:

> GET /online/usersPANList.jsp?uname=**OAOKlient3** HTTP/1.1
> ….
> ….

< 200 OK HTTP/1.1
< ….
< PAN[0]=4234567890123456
< PAN[1]=4234567890123457
< ….

Получаем карты без аутентификации…

Пример 2

ДБО для юр. лиц (**post-auth**):

GET /online/userinfo.jsp?uid=1478 HTTP/1.1

- Это было с CitiBank недавно….

GET /online/main_template.jsp?uid=1478 HTTP/1.1

- Доступ к ЧУЖИМ шаблонам страниц
- С возможностью ИЗМЕНЕНИЯ
- С уязвимостью типа stored XSS …

➔ Инфицирование всех профелей

EPIC FAIL

Баги-багами, а деньги-то где?

Для примера с физ. лицами :

- CSRF для получения данных виртуальных карт CVV2 …
- HolderName = Virtual Card
- EXP. Date = + 1 месяц

// Если не вируталка, то все кроме CVV2

Profit!

Для примера с юр лицами:

- ЭЦП ставит клиент на своем ПК!
- Баги на сервере НЕ могут влиять на ключ клиента.
- **Деньги не украсть?**

P.S.

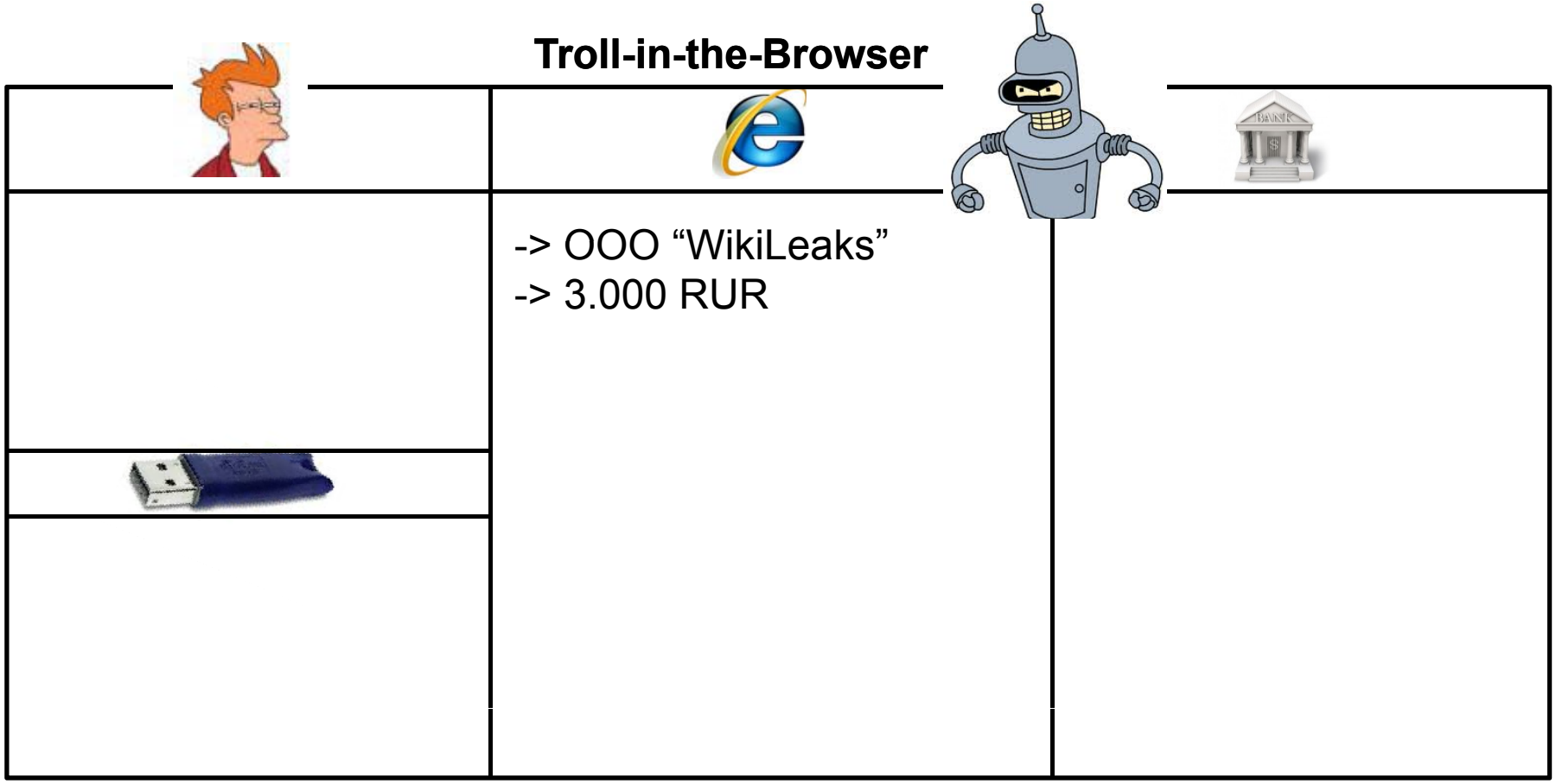
- Мы говорим о клиенте который защищен и не затроянен.
- Используем только дыры на ДБО.

XSS vs. Token

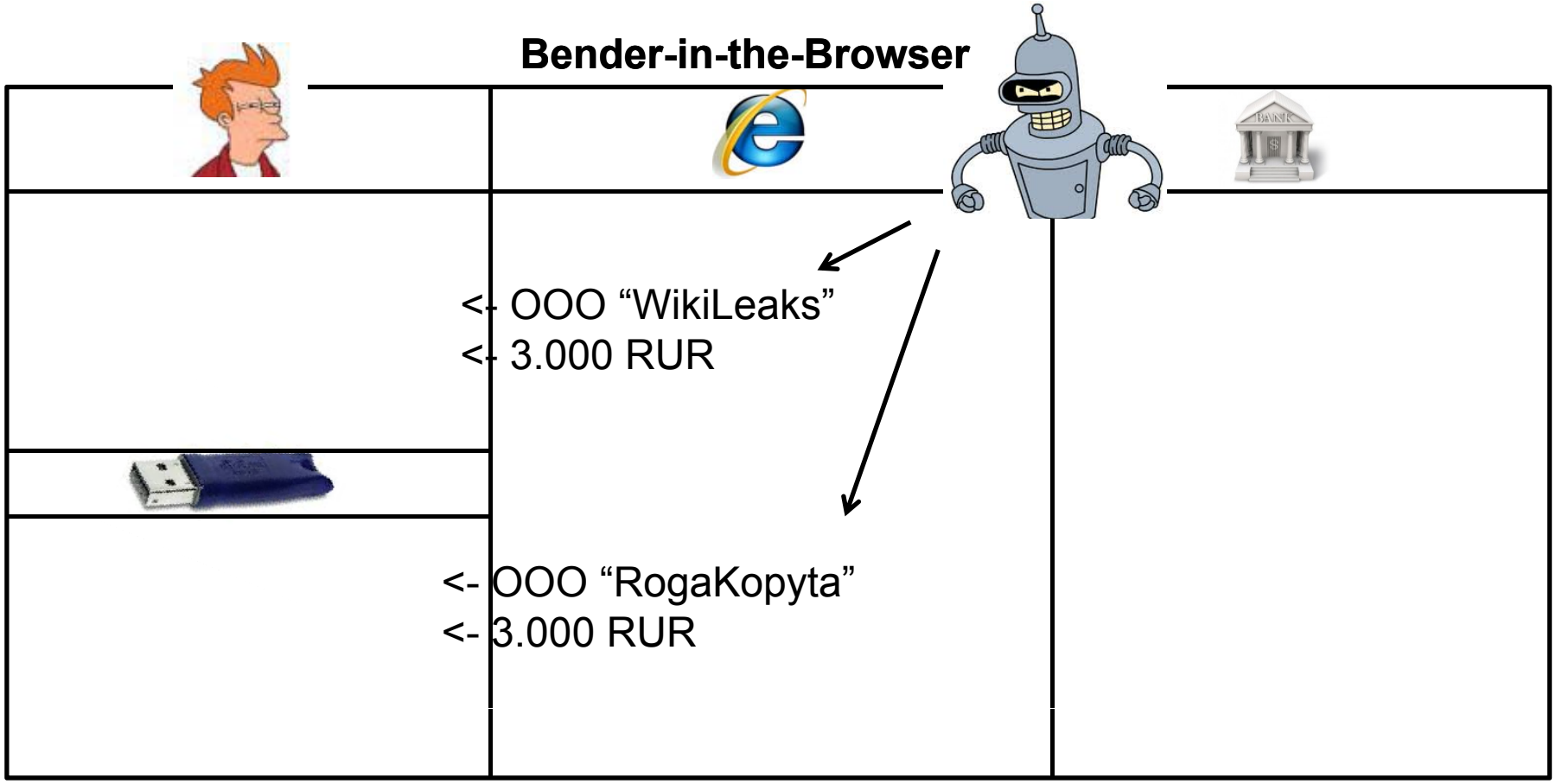
XSS

-> OOO “WikiLeaks”
-> 3.000 RUR

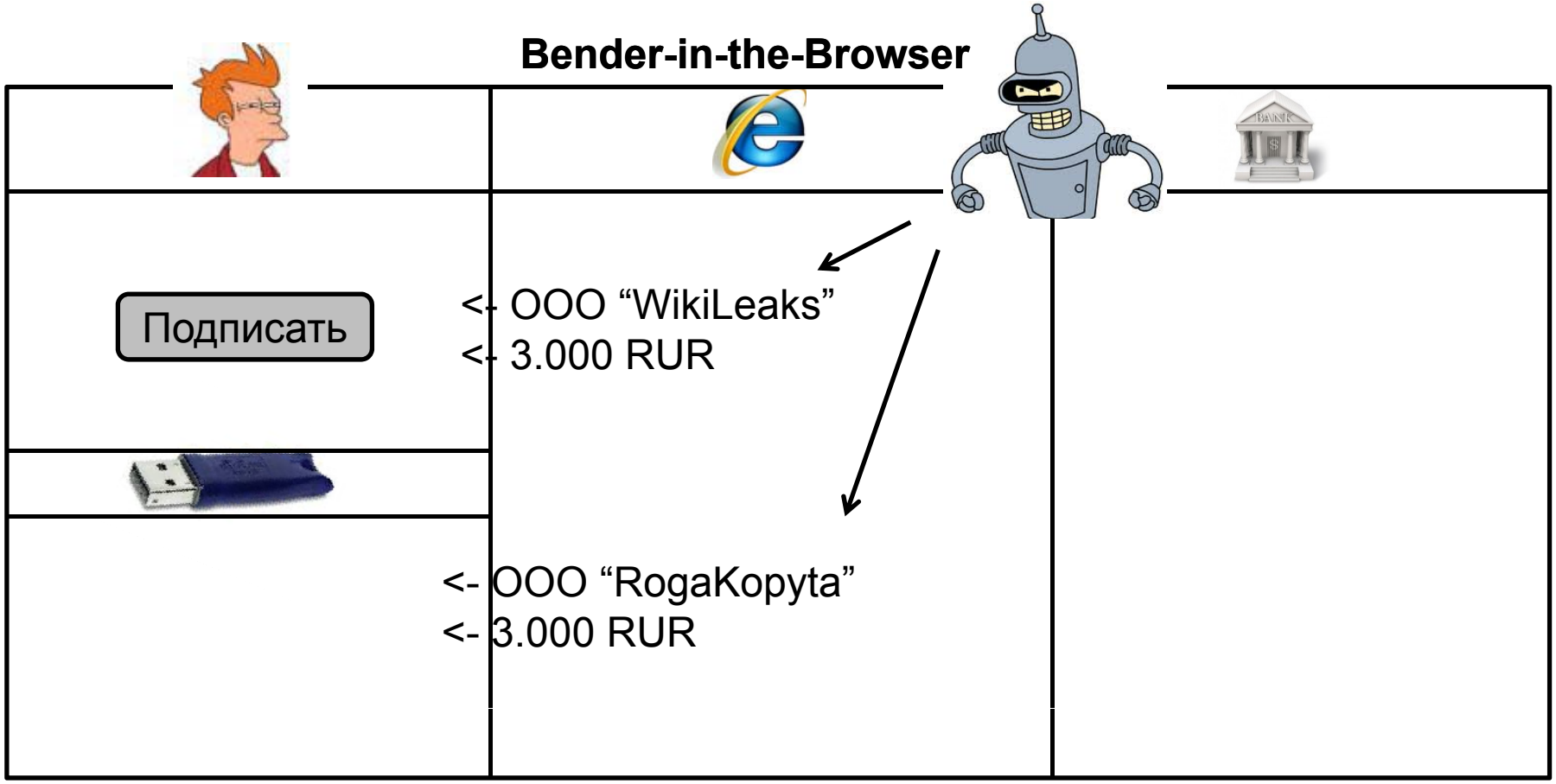
XSS vs. Token



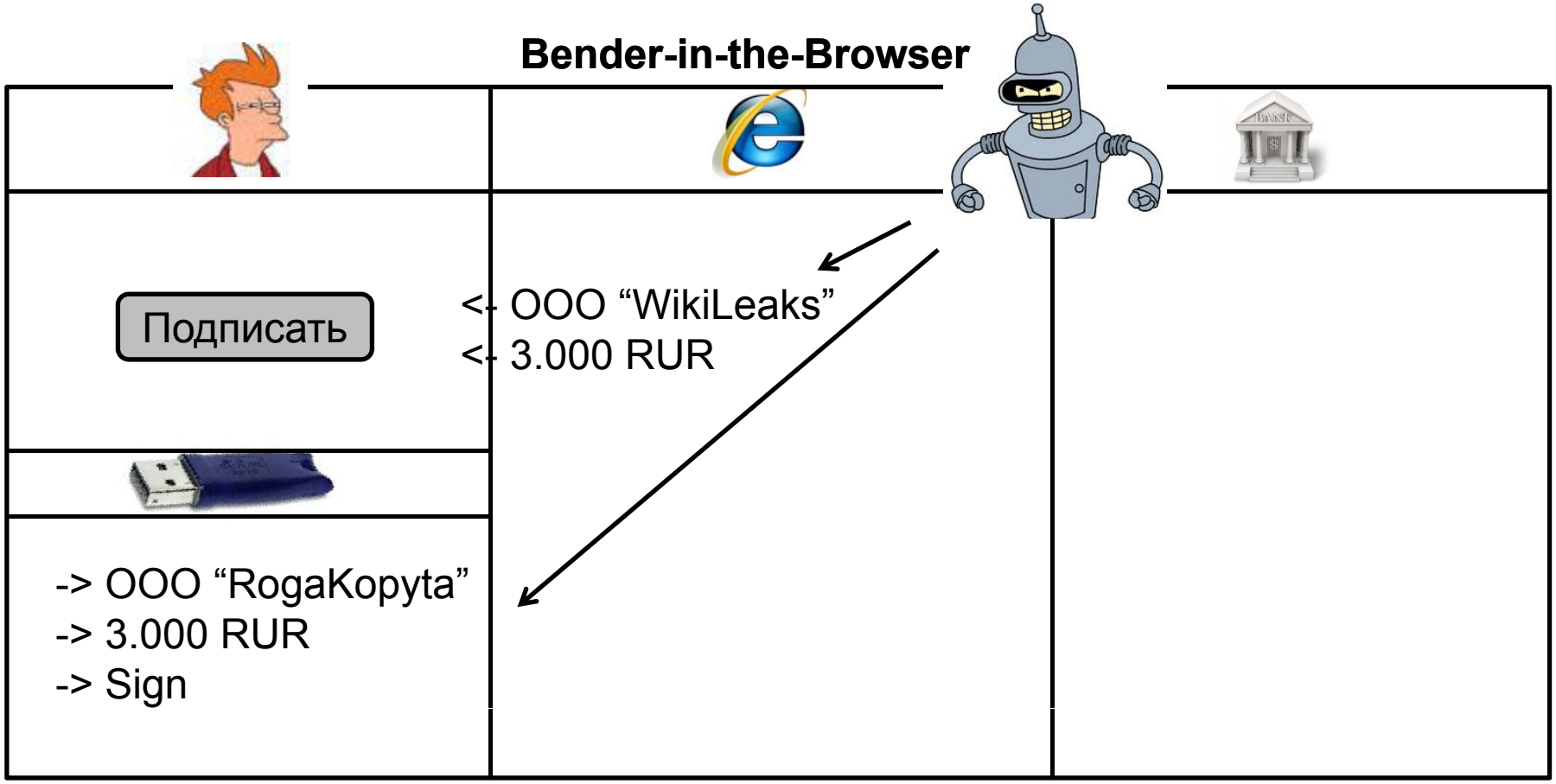
XSS vs. Token



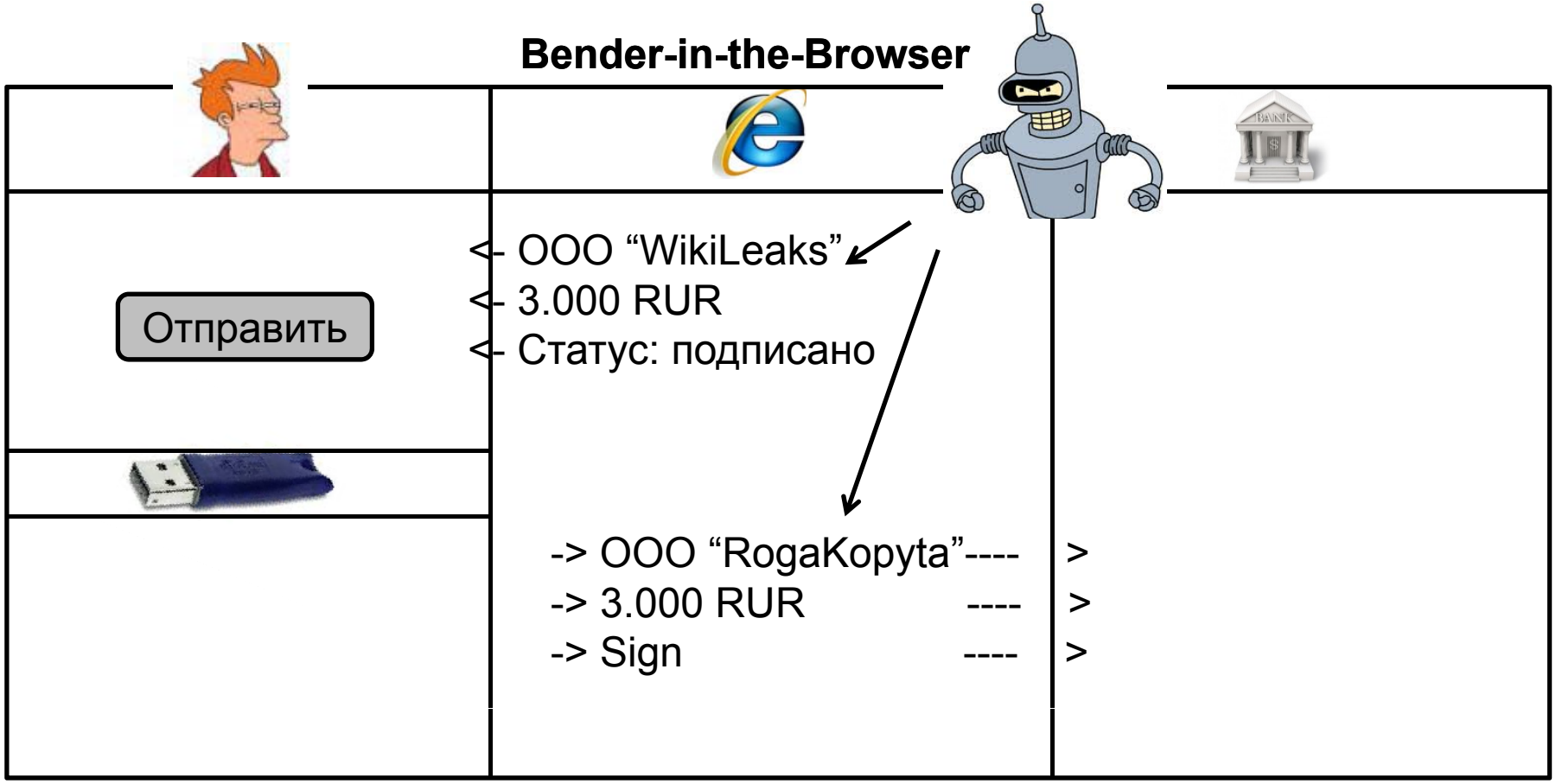
XSS vs. Token



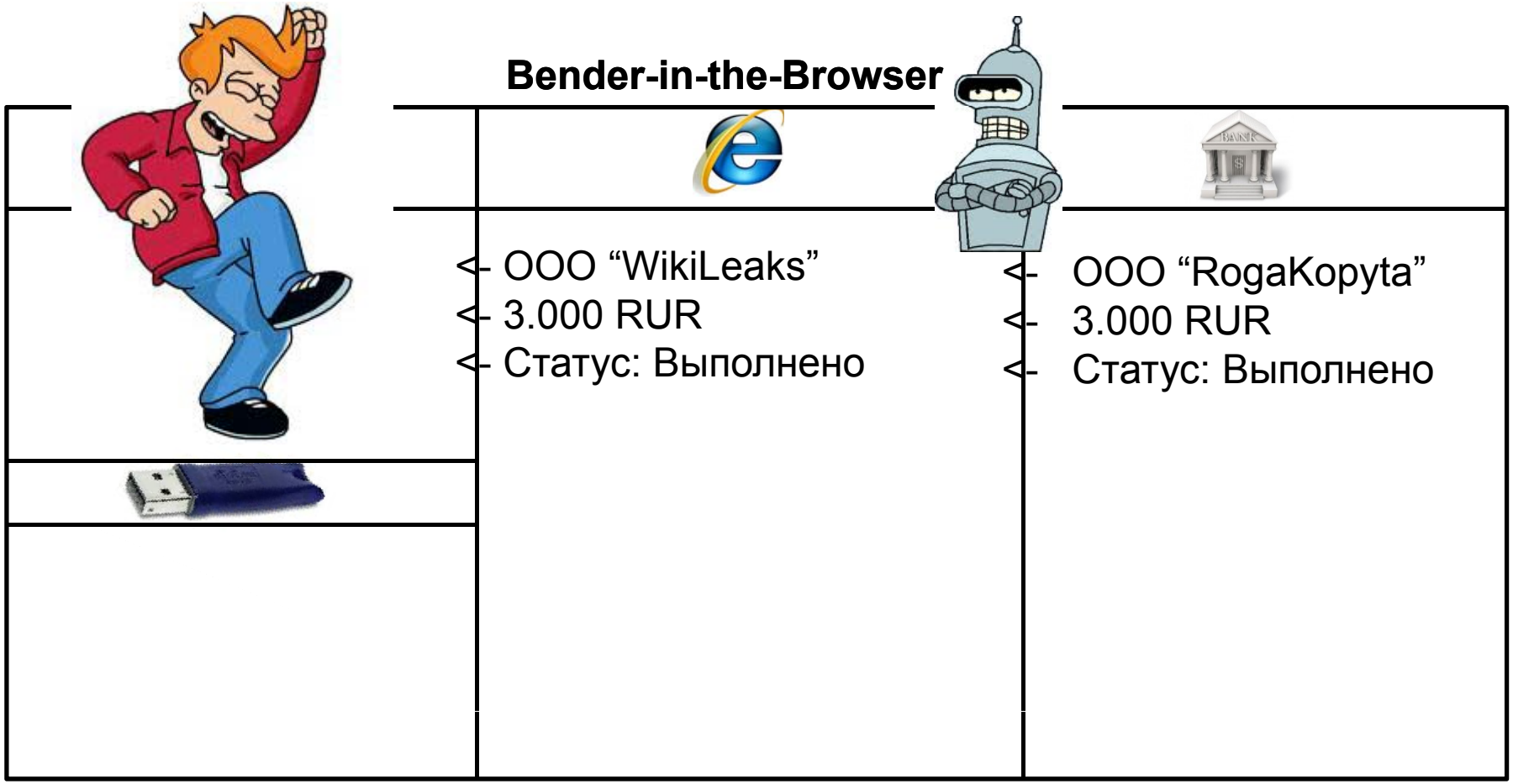
XSS vs. Token



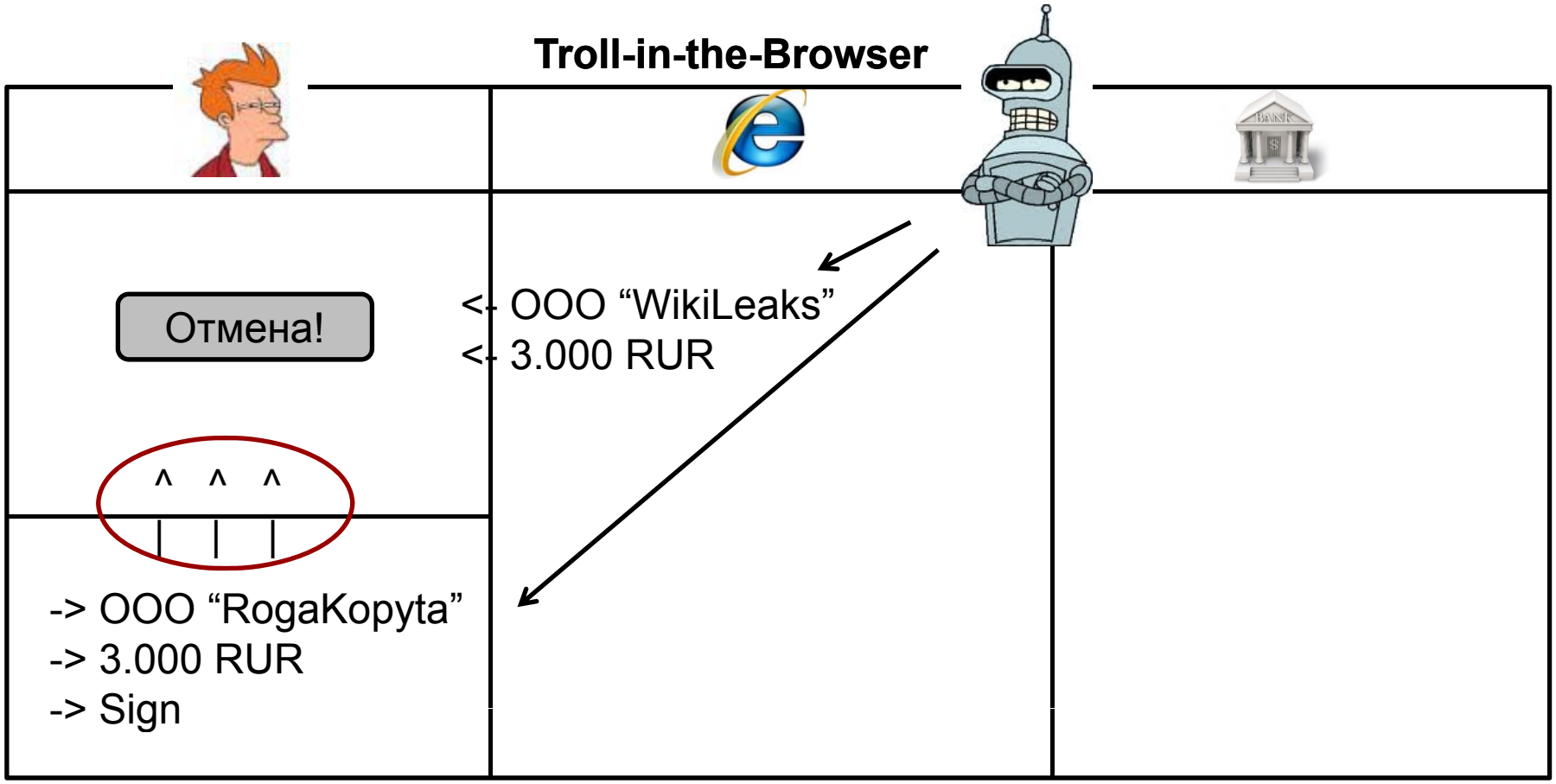
XSS vs. Token



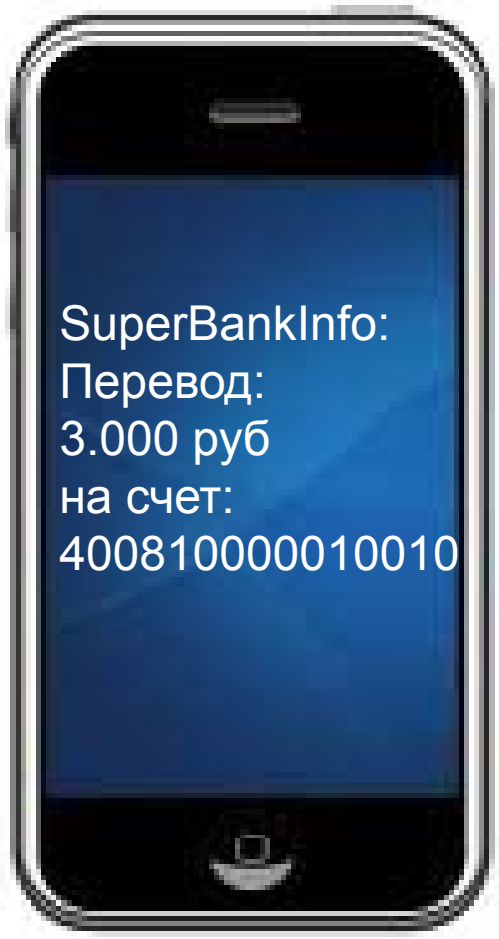
XSS vs. Token



Решение 2: Токен с дисплеем



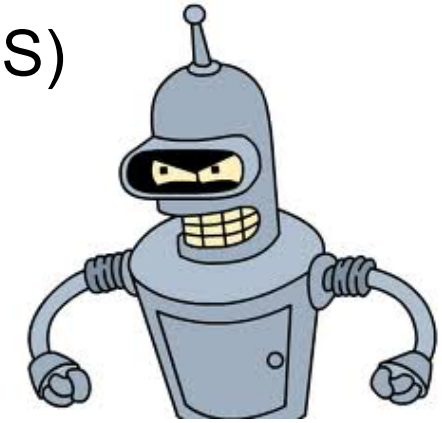
SMS - OTP



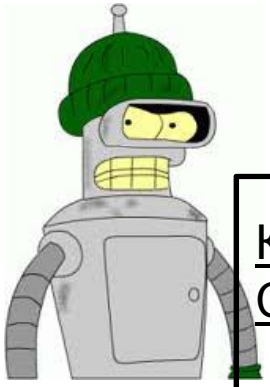
Атака с учетом архитектуры

- Обход проверки ЭЦП
- Не спасут Токены
- Не спасут Токены с дисплеем

- Уведомления - постфактум (DoS via SMS)



Атака



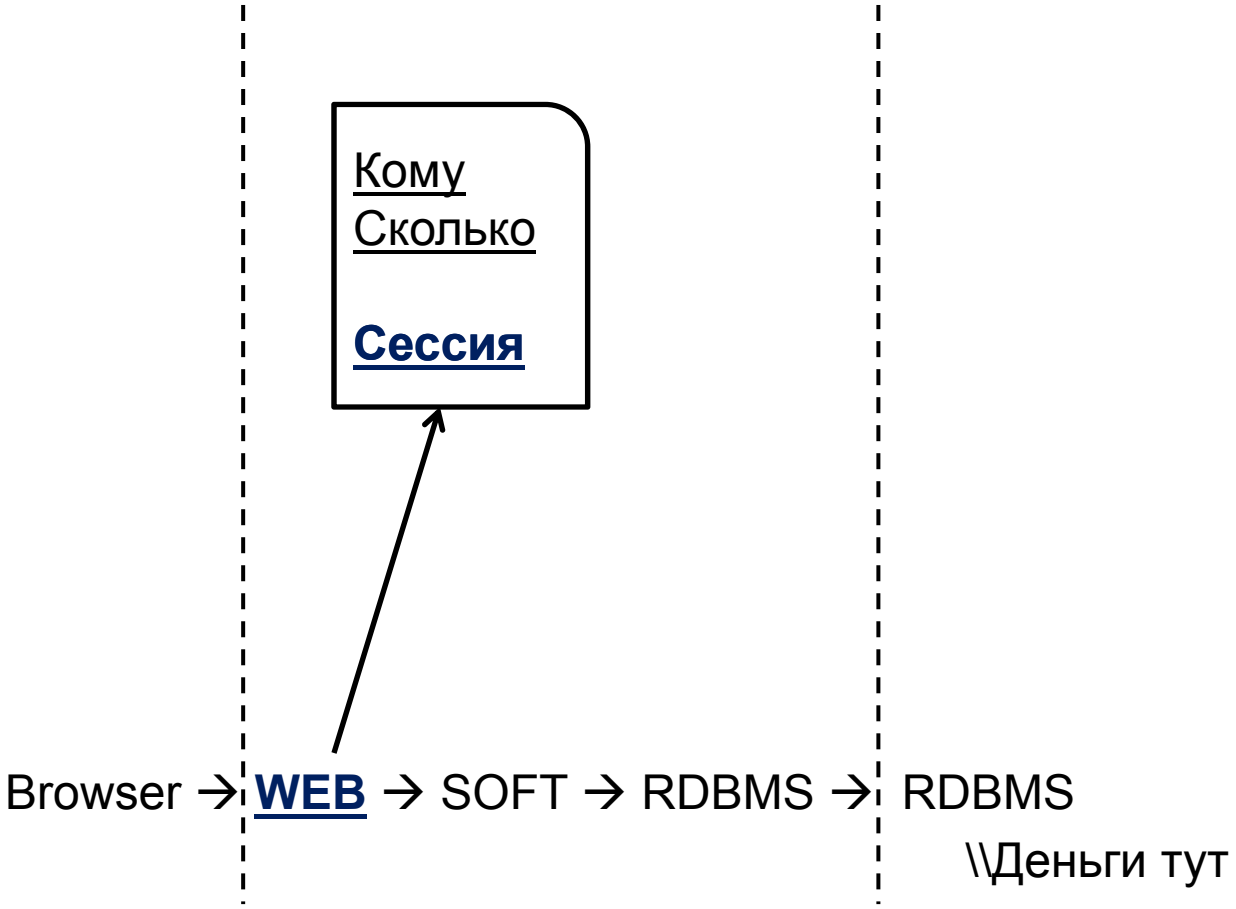
Кому
Сколько

Сессия

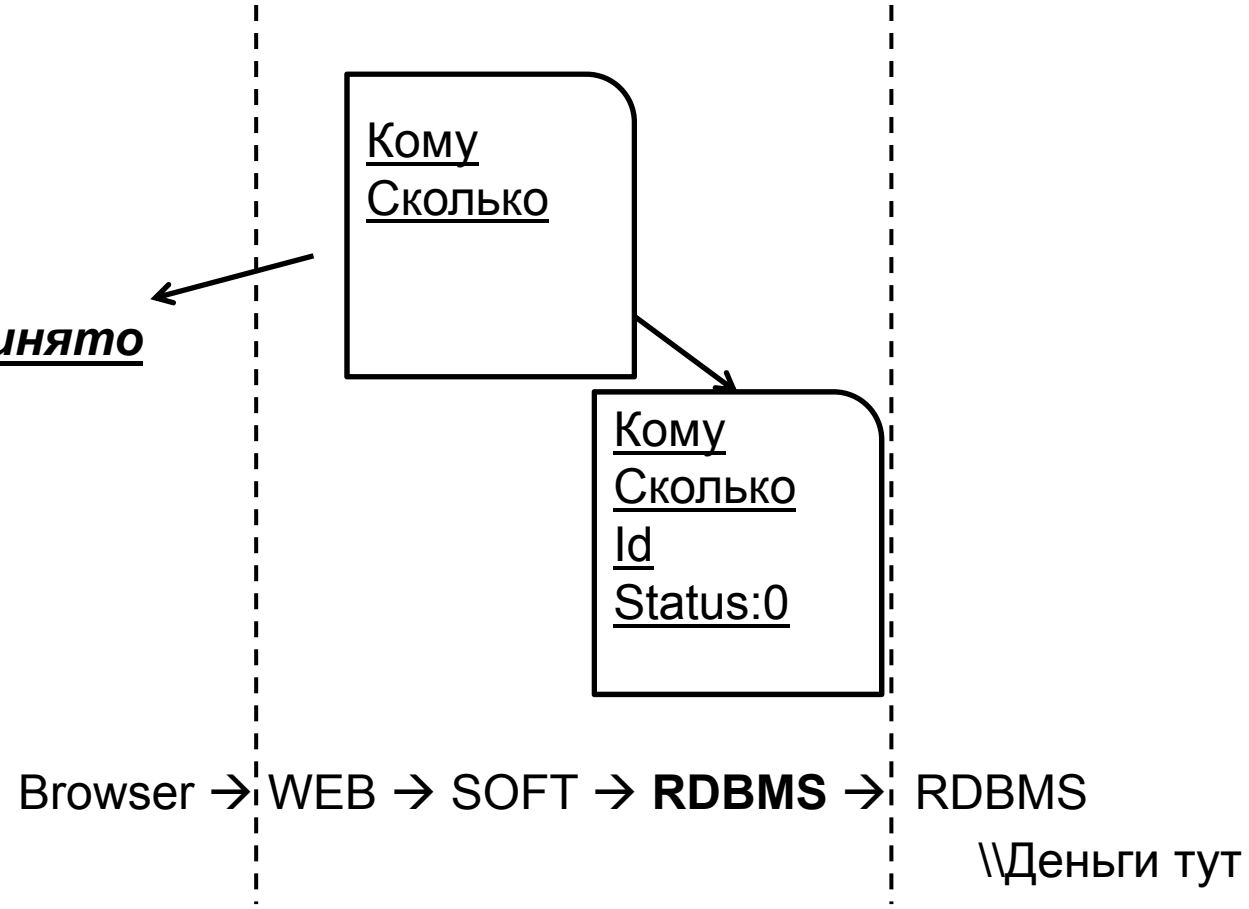
Browser → WEB → SOFT → RDBMS → RDBMS

\\Деньги тут

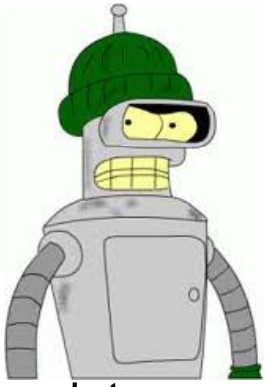
Отсылка без ЭЦП…



Жаль, что нет ключа у нас



SQLi против АБС



‘; update … set status =1

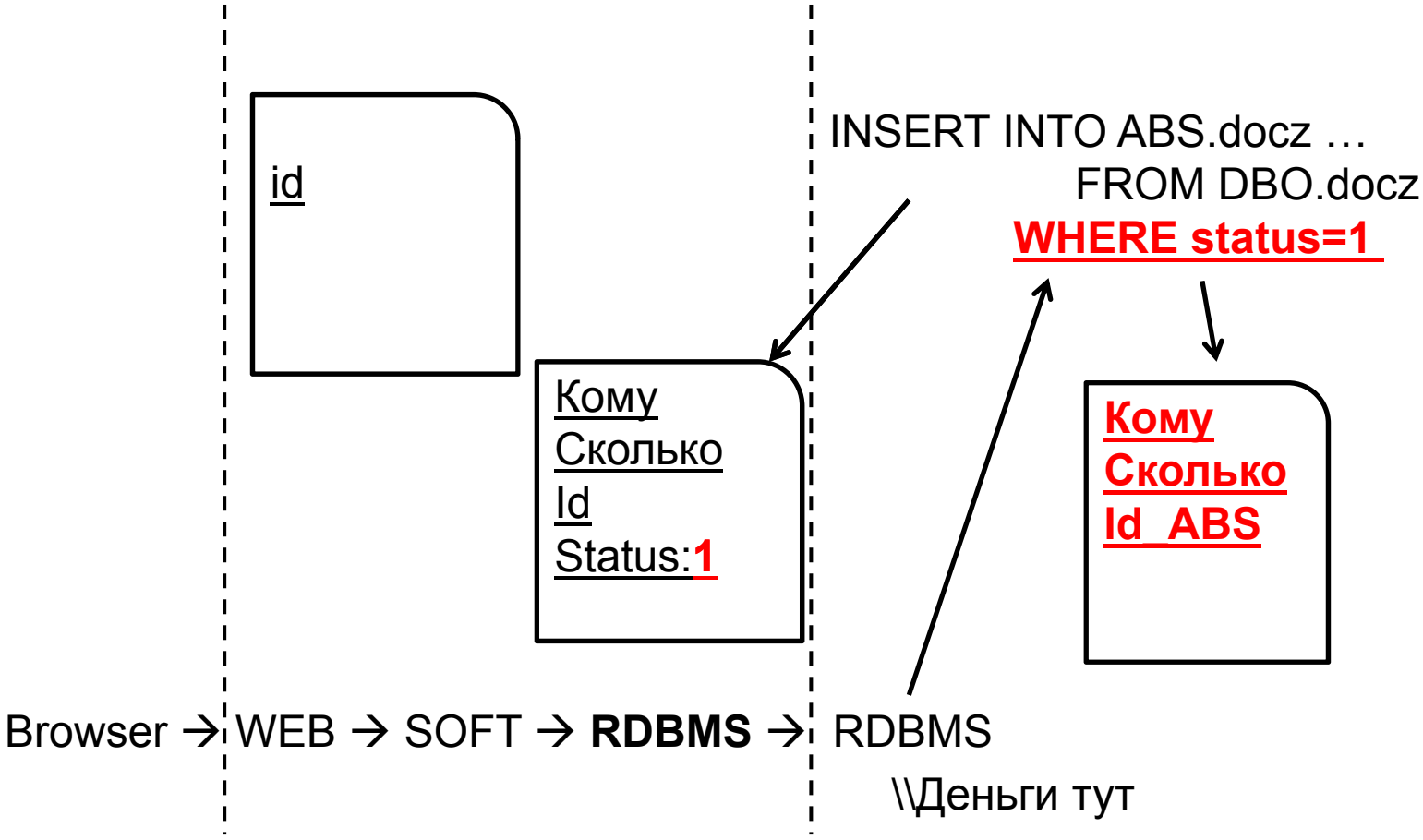
Id; update …

Кому
Сколько
Id
Status:1

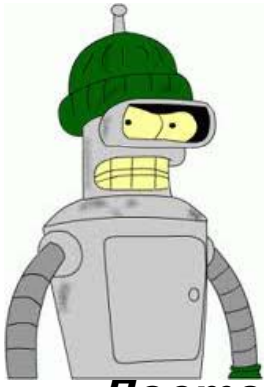
Browser → WEB → SOFT → **RDBMS** → RDBMS

\\Деньги тут

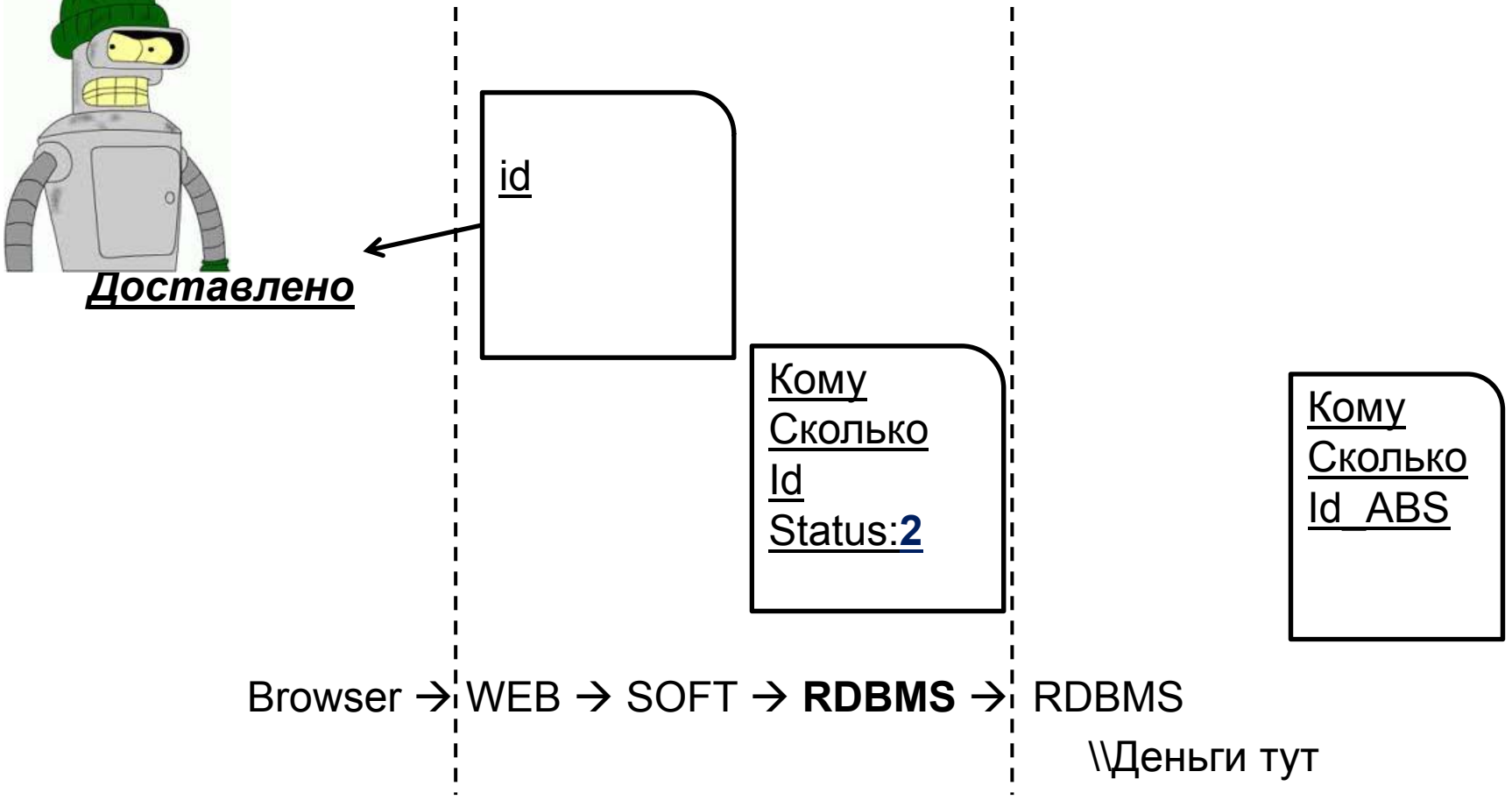
Троллим АБС



Платежка ушла

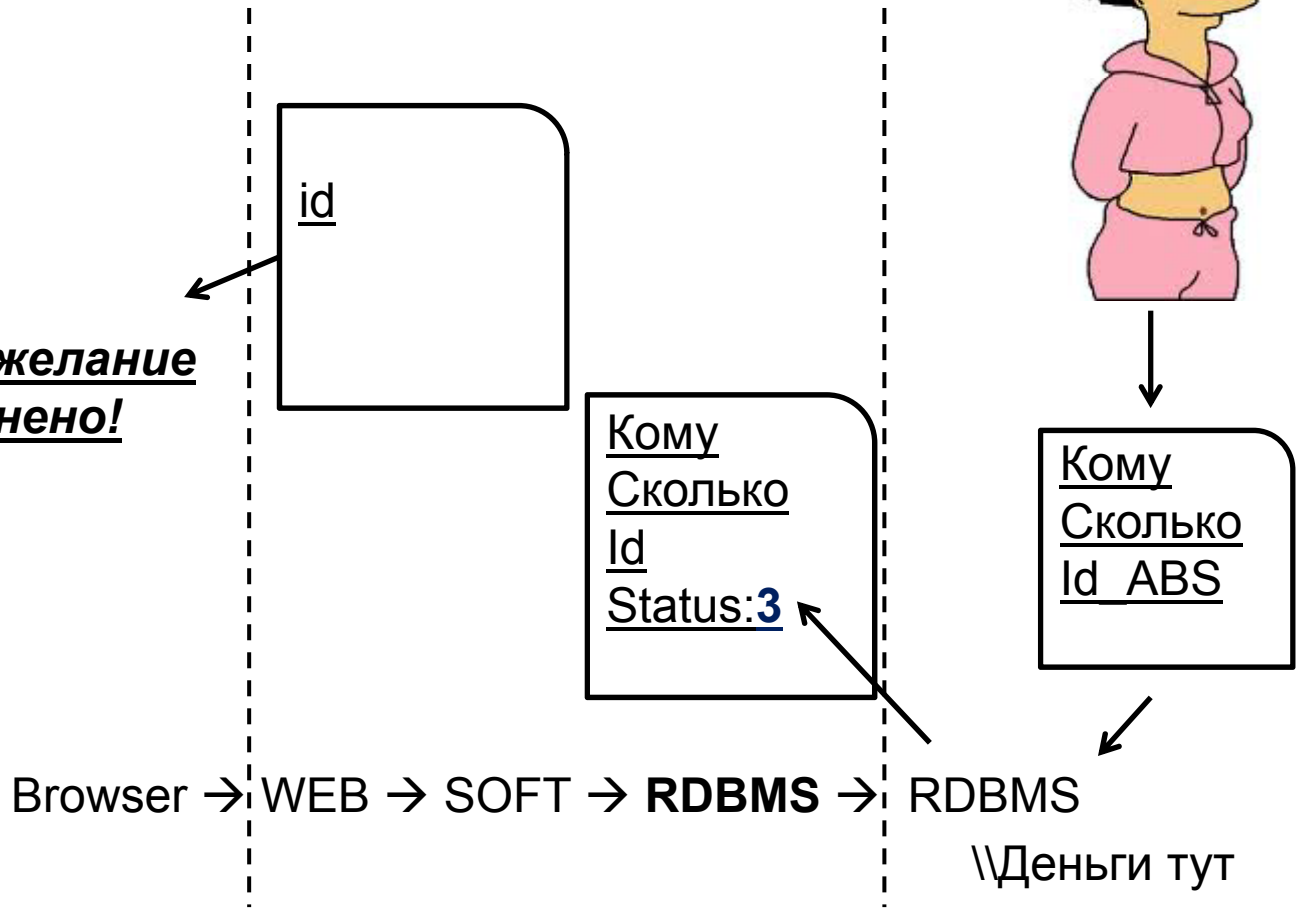


Доставлено



… yea.

Ваше желание исполнено!



Логика работы с Token'ом

- Подпись «на лету»
- Подпись с сохраненным PIN'ом
- Ввод PIN'а средствами JavaScript

```
<object … id='token'>
…
<script>
token.silent_mode=true;
var sign = token.Sing(data); //PIN из памяти…
</script>
```

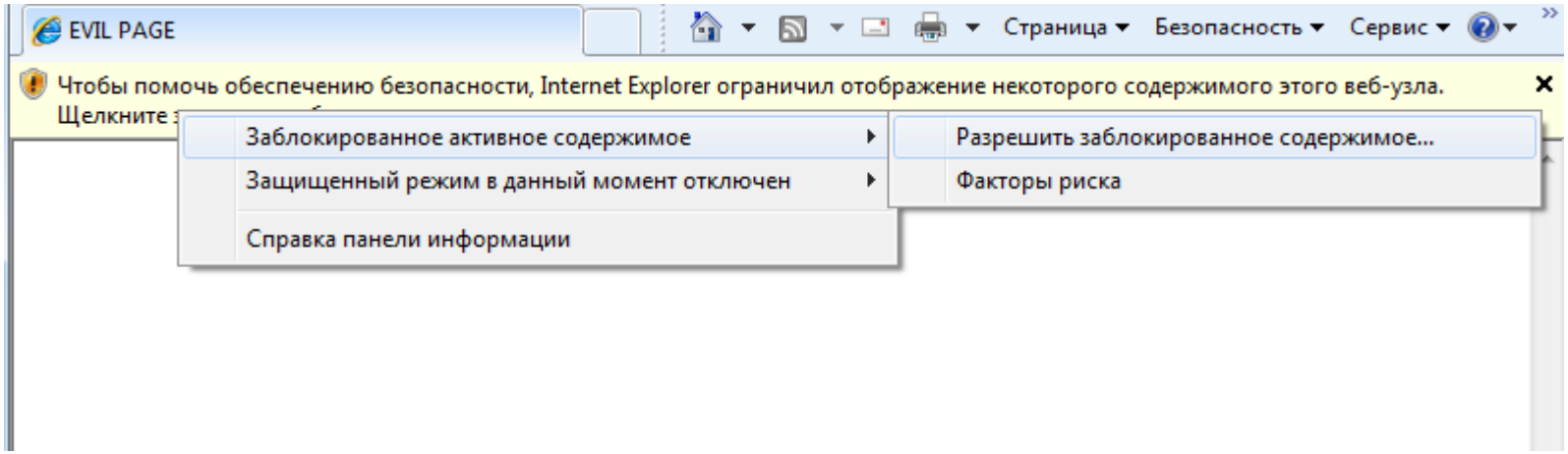
➔ **Можно выполнить подпись на ДРУГОМ сайте и отправить платежку, например, используя CSRF**

P.S. Молчу уж про XSS…

Клиентское ПО

ActiveX

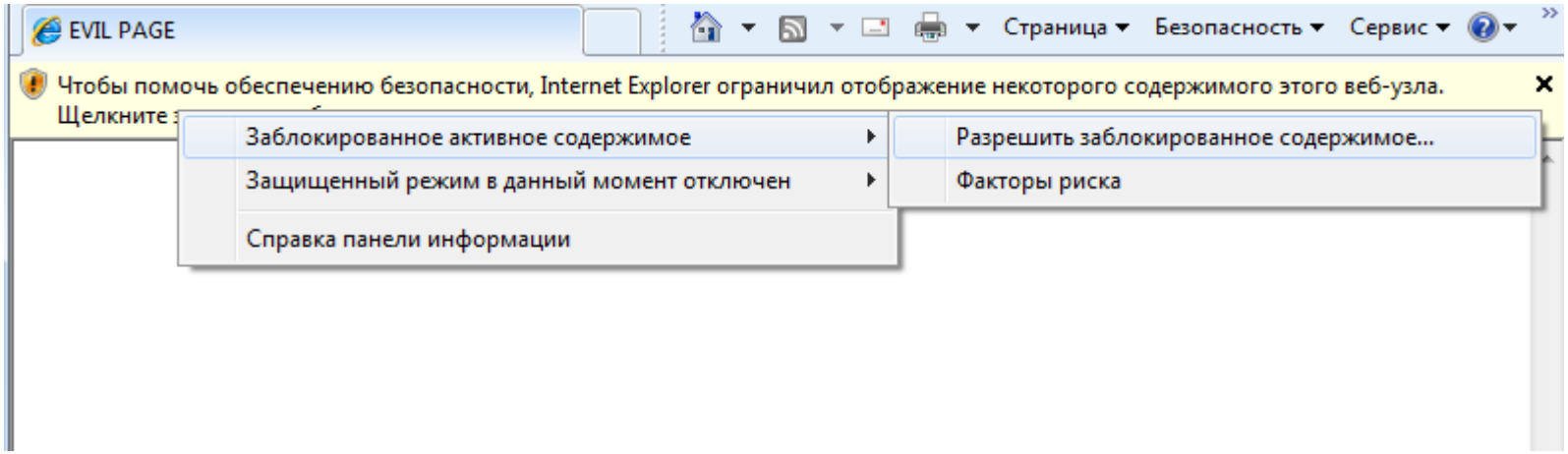
- SafeForScripting
- SafeForInit
- Домен



Клиентское ПО

ActiveX

- SafeForScripting
- SafeForInit
- Домен ----------> **bankZ.ru** <> **bankckient.bankZ.ru**



Old 1DAY - CENSORED

Мы уведомили производителя ДВА года назад

Но на одном из доменов обновления нет…

New 0DAY CENSORED

Ошибки логики…

New 0/1DAY

CENSORED

Мне нечего сказать…

p.S Не только ActiveX

Выводы

- Ошибки в коде
- Ошибки в архитектуре
- Ошибки при внедрении
- Отсутствие применения существующих мер защиты (от DEP до HTTPOnly)
- Отсутствие процедур проверки ИБ
- Отсутствие процедуры распространения КРИТЧИНЫХ патчей!
- Банки НЕ информируются о наличиях проблем с ИБ в ПО!

Классические ошибки в коде + слабая архитектура + отсутствие защит = ДБО

Меры смягчения: СУБД

- Роли приложений
- Роли операторов
- Роли администраторов
- Шифрование паролей
- Хранение ЭЦП
- Хранимые процедуры

Меры смягчения: WEB

- HttpOnly
- Secure
- Уникальный токен запроса
- SSL
- Frame Busting

XSS позволяет подменять данные и код на странице платежной системы!

CSRF позволяет выполнять действия от имени пользователя в Системе!

https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

https://www.owasp.org/index.php/Clickjacking

Меры смягчения: ПО

- ASLR
- DEP
- /GS
- SEHOP
- Анализ кода
- Анализ логики
- Фаззинг

https://www.securecoding.cert.org/confluence/display/seccode/CERT+C+Secure+Coding+Standard

https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=637

http://www.microsoft.com/security/sdl/default.aspx

Процессы…

Заключение

- Большая часть ДБО - содержит уязвимости. (По результатам пен-тестов, в 100% системах были XSS уязвимости)
- Что бы обойти защиту Token'а - достаточно XSS или CSRF
- Большую часть ошибок могут поэксплуатировать НЕ специалисты (CitiBank)
- При неправильной архитектуре - ЭЦП и вовсе 'ФИКТИВНАЯ' защита
- Уязвимое ПО выдается не только Банку, но и его клиентам.
- Вендоры НЕ информируют Банки о наличиях проблем с ИБ в ПО!

- Системы разрабатывалась без учета возможных угроз

+

- Проблемы ИБ внутри Банка (фильтрация, сегментация, патч-менеджмент)
- Ошибки при внедрении

➔ **Деньги лежат в …**

Заключение

- Большая часть ДБО - содержит уязвимости. (По результатам пен-тестов, в 100% системах были XSS уязвимости)
- Что бы обойти защиту Token'а - достаточно XSS или CSRF
- Большую часть ошибок могут поэксплуатировать НЕ специалисты (CitiBank)
- При неправильной архитектуре - ЭЦП и вовсе 'ФИКТИВНАЯ' защита
- Уязвимое ПО выдается не только Банку, но и его клиентам.
- Вендоры НЕ информируют Банки о наличиях проблем с ИБ в ПО!

- Системы разрабатывалась без учета возможных угроз

+

- Проблемы ИБ внутри Банка (фильтрация, сегментация, патч-менеджмент)
- Ошибки при внедрении

➔ **Деньги лежат в …**

Заключение

Digital Security

www.twitter.com/_chipik
d.chastuhin@dsec.ru