Digital Security

Атакуем ДБО и мобильный банкинг

Глеб Чербов
ведущий аудитор
Digital Security

Системы ДБО

Модели:

- Банк-клиент
- Мобильный сервис ДБО

Типовые источники проблем?

- WEB уязвимости
- Уязвимости клиентских хост-компонентов
- Уязвимости на стороне сервера
- Ошибки логики

WEB

XSS

Межсайтовый скриптинг

WEB. XSS

Разновидности атаки:

- Кража идентификатора сессии
- Выполнение действий от имени пользователя
- Проксирование через подконтрольный хост
- Фишинг

WEB. XSS

хакер

клиент

браузер

ДБО

WEB. XSS

хакер

Хранимая XSS

клиент

браузер

ДБО

WEB. XSS

Отраженная XSS

хакер

клиент

браузер

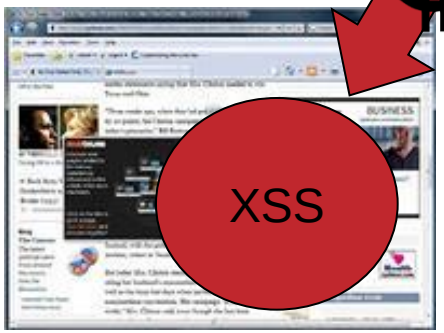
ДБО

WEB. XSS

Удаленное управление,
подмена отображаемых данных
- **Кража денег**

хакер

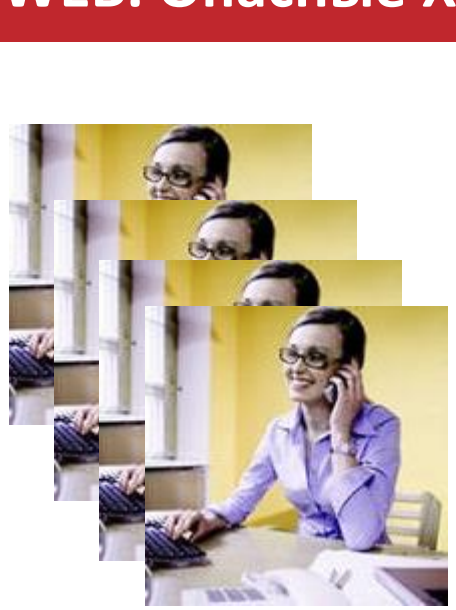
клиент



браузер

ДБО

WEB. Опасные XSS



клиенты

браузеры

XSS

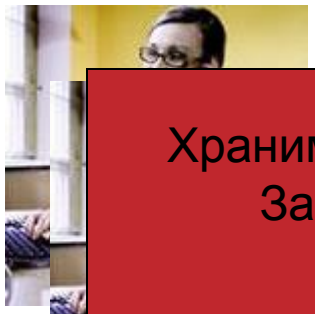
ДБО

Свяжем вместе две уязвимости:

1) Хранимая XSS

2) Некорректное разграничение доступа между клиентами

WEB. XSS



Хранимая XSS + Некорректное разграничение доступа =
Заражение всех клиентов банка JavaScript-кодом

КРАЖА ДЕНЕГ У ВСЕХ/ЛЮБОГО КЛИЕНТА БАНКА

SS

клиенты

браузеры

ДБО

Свяжем вместе две уязвимости:

1) Хранимая XSS
2) Некорректное разграничение доступа между клиентами

WEB. XSS

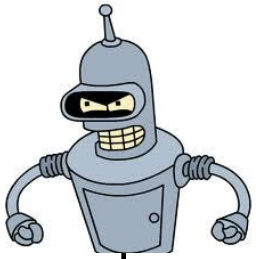
XSS + misconfig = MiTM

WEB. XSS

XSS

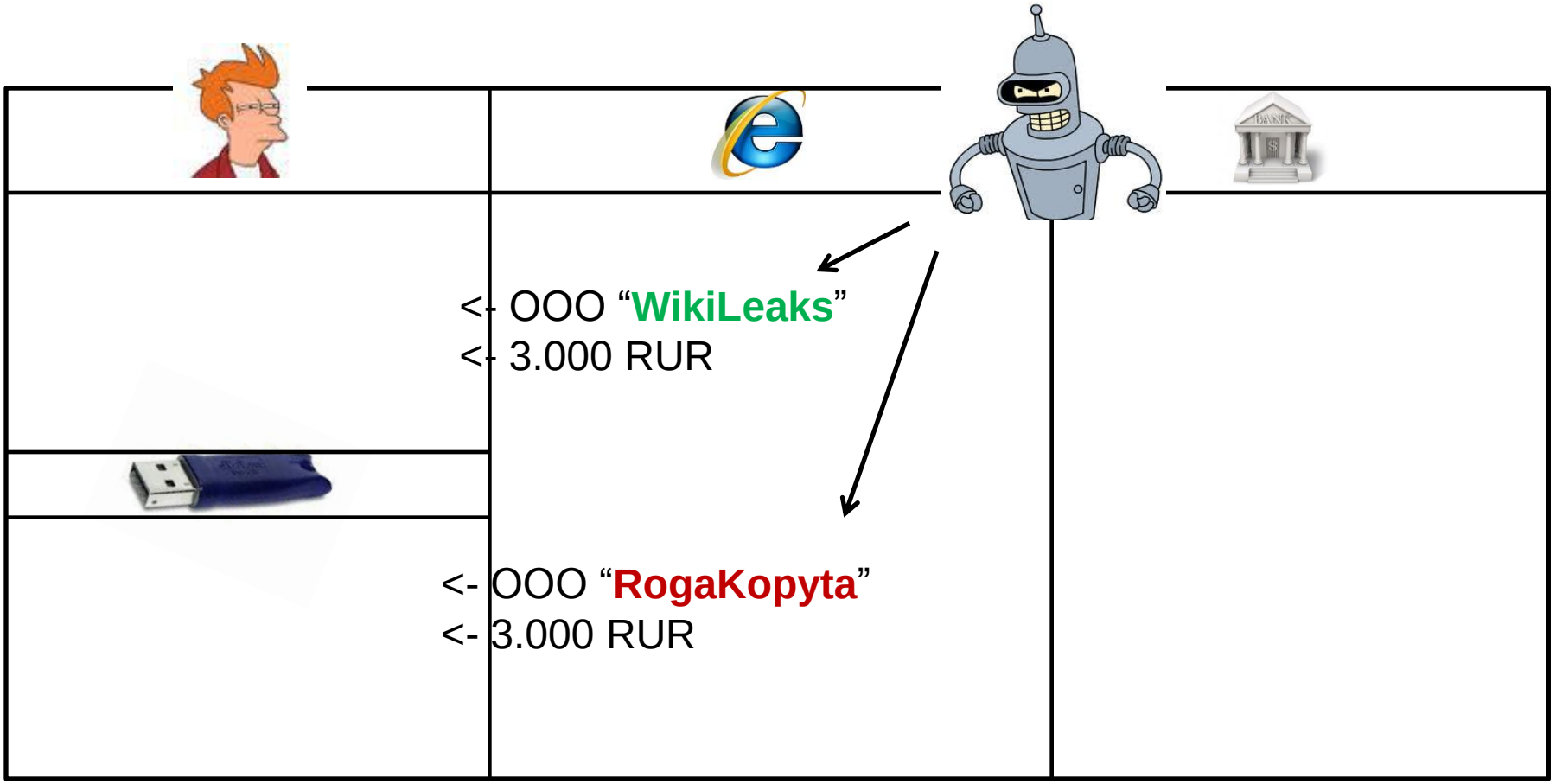
-> OOO “**WikiLeaks**”
-> 3.000 RUR

WEB. XSS

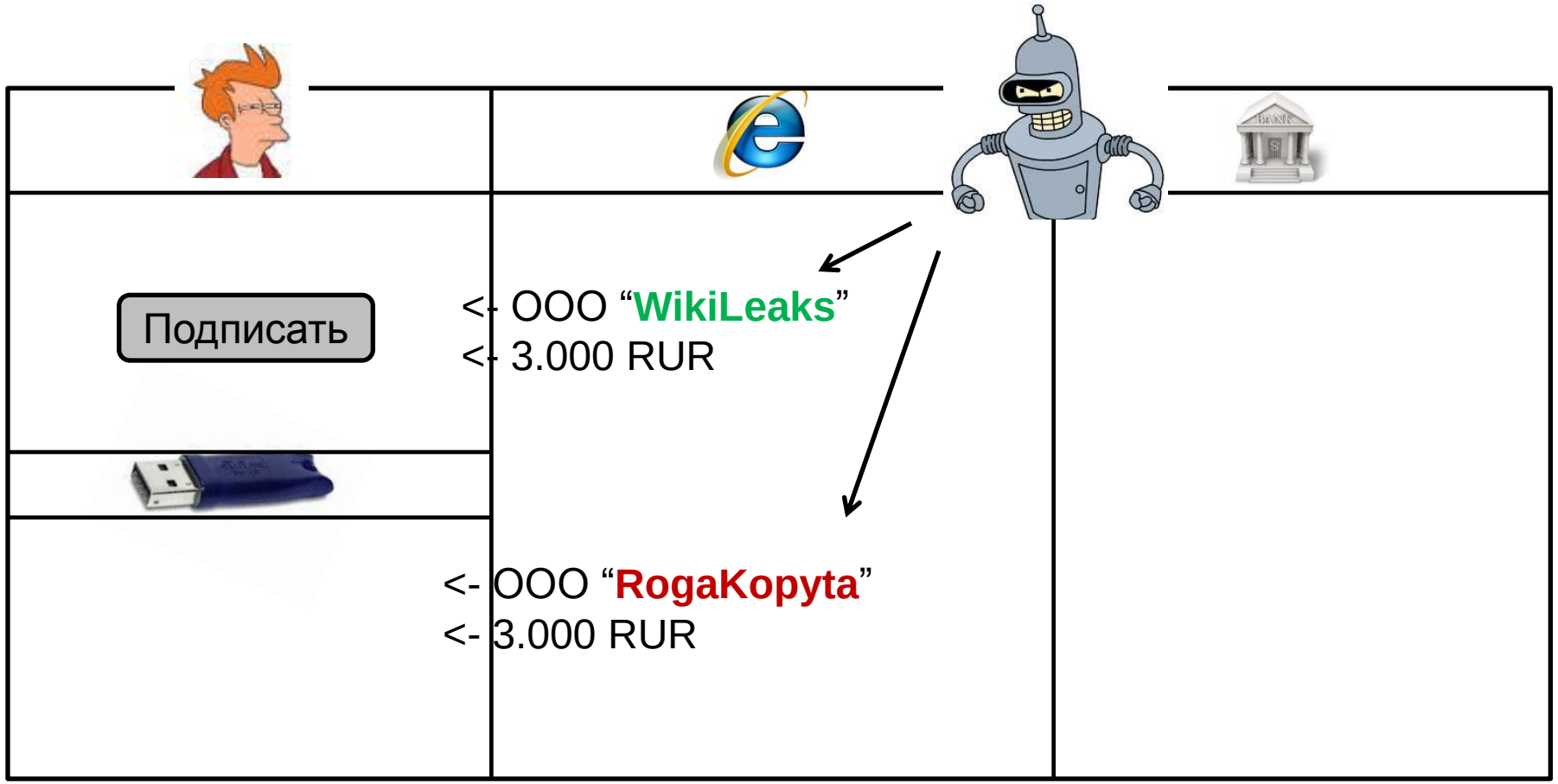


-> OOO “**WikiLeaks**”
-> 3.000 RUR

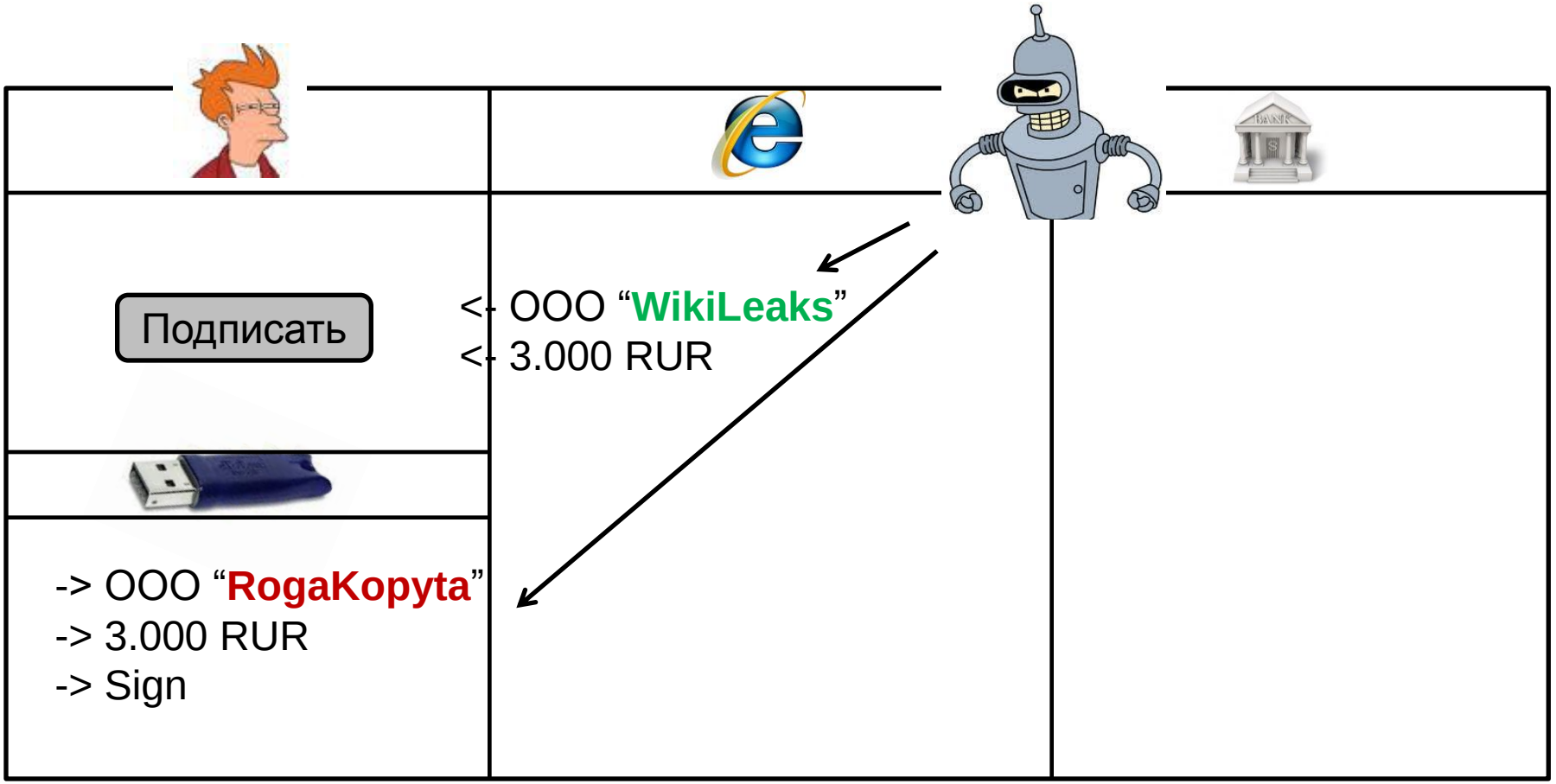
WEB. XSS



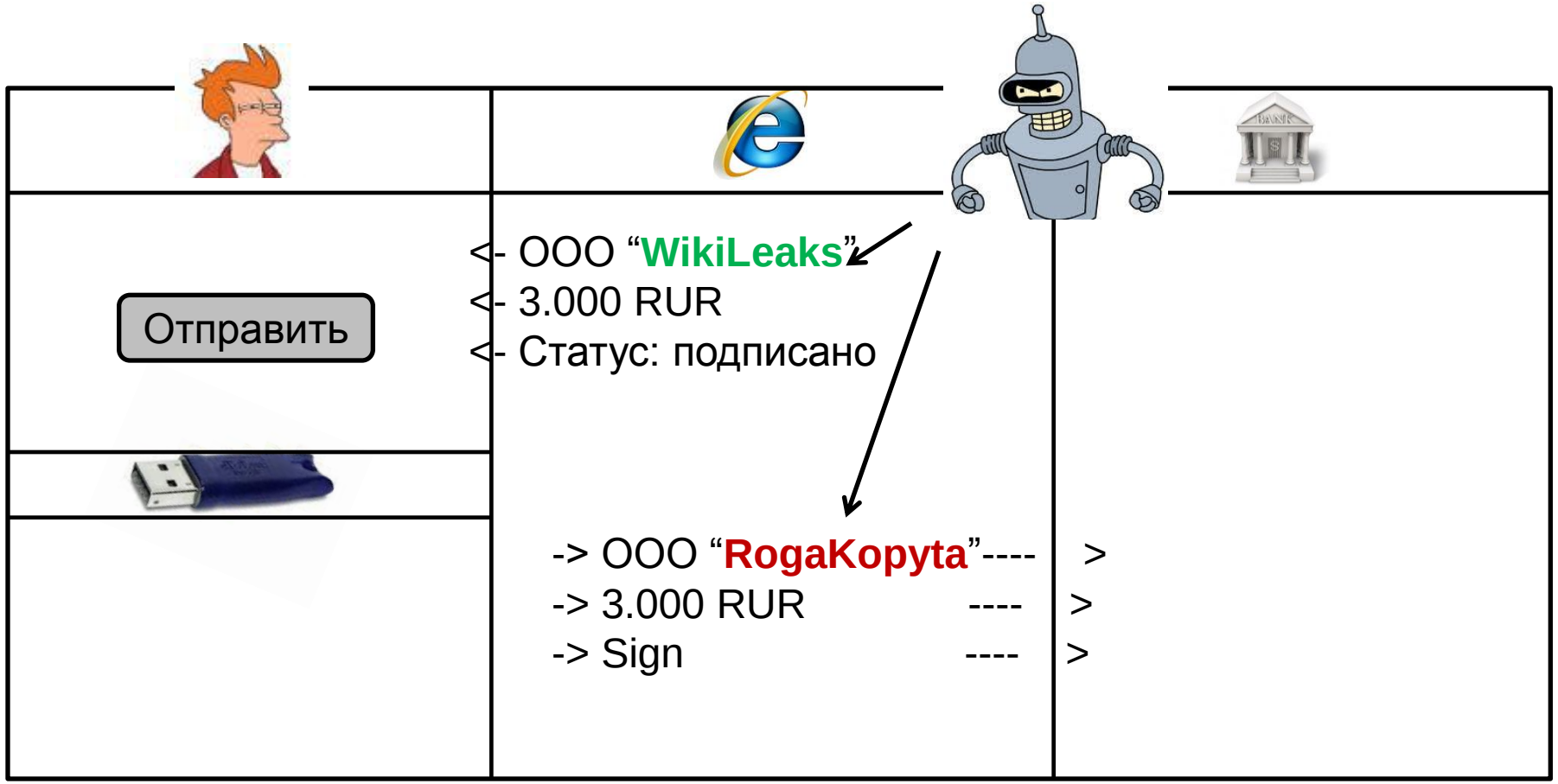
WEB. XSS



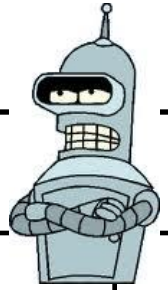
WEB. XSS



WEB. XSS



WEB. XSS



<- ООО “**WikiLeaks**”
<- 3.000 RUR
<- Статус: Выполнено

<- ООО “**RogaKopyta**”
<- 3.000 RUR
<- Статус: Выполнено

WEB. XSS

Противодействие:

- Флаги защиты Cookie (HTTPOnly, Secure)
- Встроенные средства защиты браузеров
- Заголовки (X-FRAME-OPTIONS)
- Content Security Policy (CSP)

WEB

CSRF

Межсайтовые запросы

WEB. Межсайтовые запросы

Злоумышленник имеет возможность выполнять действия в ДБО от имени клиента. Это в совокупности с другими уязвимостями приводило к краже денег клиентов.

WEB. Межсайтовые запросы

клиент

ДБО

хакер

WEB. Межсайтовые запросы

клиент

ДБО

хакер

WEB. Межсайтовые запросы

клиент

ДБО

хакер

WEB. Межсайтовые запросы

клиент

ДБО

Отсутствие защиты от CSRF

Можно выполнить запросы от любого пользователя Системы

хакер

WEB. CSRF

Выполнение действия от имени пользователя:

- Управление настройками оповещения
- Смена пароля
- Модификация данных

WEB. CSRF

Противодействие:

Использование CSRF-токенов

WEB. CSRF

Противодействие:

Корректное использование CSRF-токенов

ActiveX / Java

ActiveX / Java

Клиентские хост-компоненты

Хост-компоненты

Разновидности атаки:

- Контроль над хостом клиента
- Кража ключевой информации
- Скрытое использование средств ЭЦП
- Кража личной информации клиента

Хост-компоненты

Проблемы:

- ActiveX: Переполнение буфера
- ActiveX / Java: Небезопасный функционал

Почему?

1) Не поставлен процесс тестирования и анализа безопасности у разработчиков систем ДБО

2) Кодовая база берет начало в далеком прошлом

Хост-компоненты

Небезопасный функционал:

- Функции работы с ФС
- Функции конфигурации компонента
- Системные функции

Хост-компоненты

Хост-компоненты

Противодействие:

- Конфигурация безопасности ActiveX
- Механизмы защиты памяти для нативного кода (DEP, ASLR)
- Исключить из компонент избыточный функционал
- Качество кода

Хост-компоненты

Противодействие:

- Конфигурация безопасности ActiveX
- Механизмы защиты памяти для нативного кода (DEP, ASLR)
- Исключить из компонент избыточный функционал
- Качество кода

Серверная часть

Уязвимости на стороне сервера

Серверная часть

Типовые уязвимости:

- Инъекции кода (SQL-inj, XXE, Xpath-inj, etc.)
- Доступность сервисных интерфейсов
  - Административные панели
  - Отладочные инструменты
  - Избыточный функционал фреймворков

Серверная часть

Последствия:

От раскрытия информации пользователей

До получения контроля над сервером приложений

Серверная часть

Противодействие:

- Конфигурация сервера
- Web Application Firewall
- Качество кода

Логика

Ошибки логики

Логика – разграничение привилегий

ДБО для юр. лиц (**post-auth**):

Смотрим данные пользователей:

GET /online/userinfo.jsp?uid=**1234** HTTP/1.1
GET /online/userinfo.jsp?uid=**1235** HTTP/1.1
GET /online/userinfo.jsp?uid=**1236** HTTP/1.1
…

GET /online/main_template.jsp?uid=1235 HTTP/1.1

- Доступ к ЧУЖИМ шаблонам платежей
- С возможностью ИЗМЕНЕНИЯ
- Возможность эксплуатации хранимой XSS

➔ Инфицирование всех профилей

Логика

Противодействие:

- Качество кода
- Функциональное тестирование

Mobile

Мобильный банкинг

Mobile

Проблемы:

- Контроль среды исполнения
- Защита канала связи
- Уязвимости используемых сторонних средств

Mobile

Проблемы:

- Контроль среды исполнения
- **Защита канала связи**
- Уязвимости используемых сторонних средств

Mobile

Mobile

Противодействие:

- Детектирование ROOT / Jailbreak
- Правильное использование средств защиты канала (SSL Pinning)
- Использование доверенной кодовой базы

Digital Security

Digital Security в Москве: (495) 223-07-86
Digital Security в Санкт-Петербурге: (812) 703-15-47