Digital Security

Проблемы и уязвимости в системах ДБО

Digital Security

ДБО - механизмы защиты

В отечественных системах ДБО для юридических лиц кроме аутентификации применяется только ОДНА система защиты - **СКЗИ**

Любая другая технология или система - **добровольное дело разработчика.**

- **Нет стандарта безопасности для таких систем**
- **Никто не проверяет безопасность кода системы**
- **Никто не проверяет, как была внедрена система**
- **Системы ДБО не проверяются даже QSA аудиторами в рамках работ по PCI DSS**

Хакеры

Злоумышленники могут использовать уязвимости не только клиента банка, но и самого банка, а вернее системы ДБО. Используя эти уязвимости, хакер может получить большие возможности по манипуляции данными в системе ДБО, в том числе, может управлять счетами клиентов.

Это возможно:

- Множество уязвимостей в коде
- Ошибки в архитектуре
- Отсутствие защитных технологий (разработчик просто не использует их)
- Ошибки при внедрении
- Уязвимости в банковской сетевой инфраструктуре

Уязвимости

- Межсайтовый скриптинг
- Внедрение SQL запросов
- Обход аутентификации
- Обход авторизации
- Выполнение кода
- Ошибки логики
- Уязвимости клиентских плагинов

 Эти и многие другие ошибки в WEB интерфейсе ДБО приводят к возможности фишинга на домене банка, атакам Man-In-The-Browser, атакам на клиентов с доверенного домена, что в конечном счете приводит к нарушению **банковской тайны**, утечке **персональных данных**, **выполнению поддельных платежных поручений** и **компрометации ПК** пользователей

Обход СКЗИ

Имея уязвимости в WEB или, например, доступ к СУБД, в некоторых случаях возможен **обход проверки ЭЦП** вообще, а в некоторых случаях достаточно лишь уязвимости межсайтового скриптинга, чтобы **поставить подпись для поддельного платежного поручения**, даже если клиент **использует Token** и даже если **ПК клиента не скомпрометирован**.

В большинстве случаев, СКЗИ используется в прозрачном режиме, что позволяет хакеру незаметно использовать её даже удаленно за счет механизмов управления СКЗИ методами WEB.

 Все это, в совокупности с общепроцессными проблемами ИБ ведет к существованию реального риска неавторизированной установки ЭЦП или обхода проверки ЭЦП вообще даже без компрометации ПК клиента.

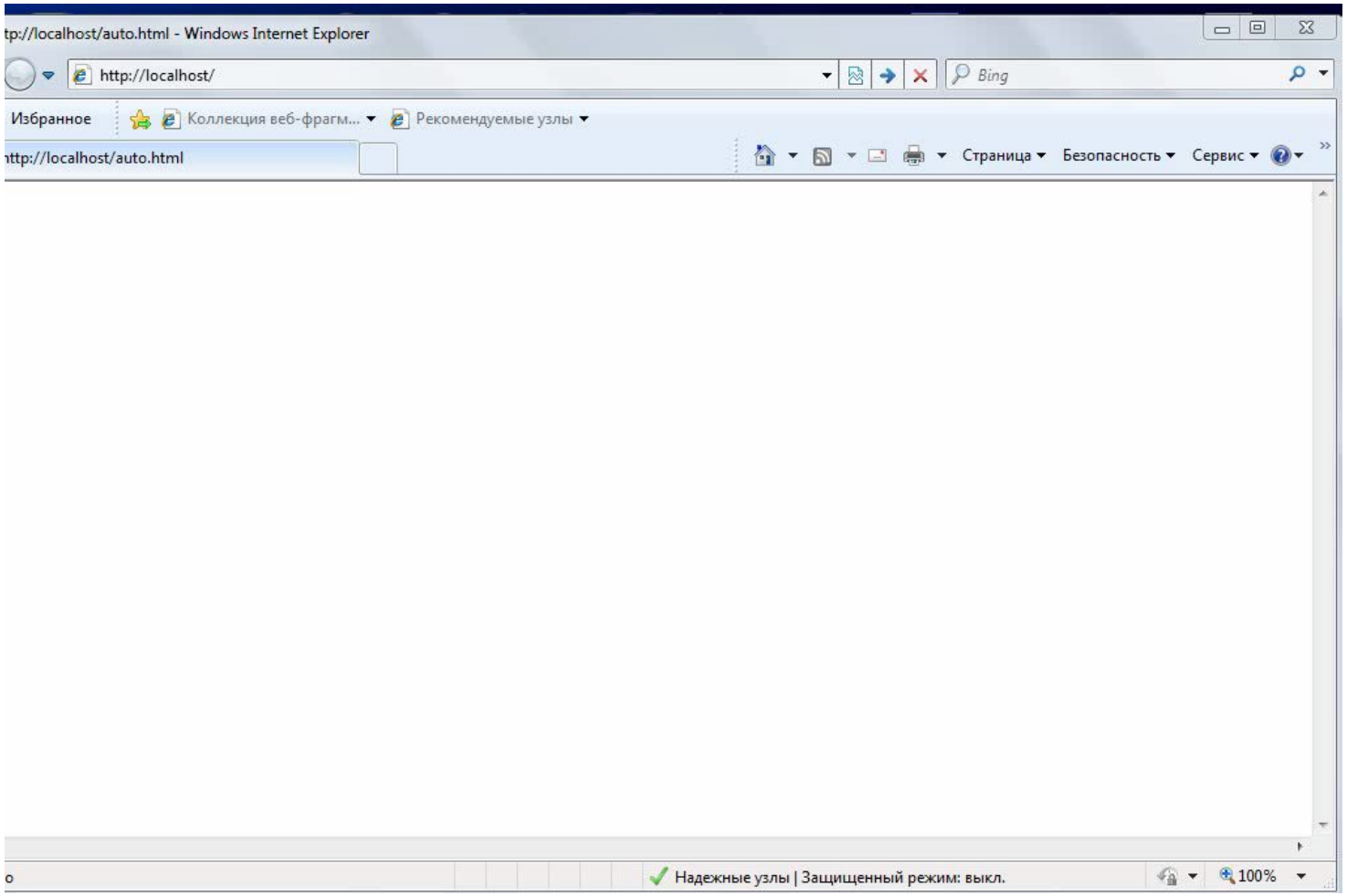
Плагины

Установка плагинов для клиентов - необходимая часть для того, чтобы клиент мог работать с системой ДБО. Однако эти плагины также содержат ошибки и уязвимости, что позволяет компрометировать ПК клиента, даже если все другие известные уязвимости в прикладном ПО и ОС устранены.

Устанавливая новый непроверенный софт, мы ухудшаем безопасность клиента.

- Используя уязвимости в плагинах, злоумышленник может выполнить целевую атаку и установить вредоносное ПО без ведома пользователя.

Видео-демонстрация



Обновления

Не все разработчики ДБО и далеко не всегда уведомляют о проблемах ИБ своих клиентов - банки. Так как у большинства банков «специализированые» инсталляции, обновление которых затруднительно в массовых масштабах (фактически, каждое обновление уникально).

Существуют банки с уязвимым ПО о дырах которого разработчики знают уже более года. Тем не менее банк об этом не знает за счет закрытости такой информации.

Отсутствие защиты

Разработчики систем ДБО не были готовы к тому, что их продукт будут ломать хакеры. У разработчиков отсутствуют процессы разработки безопасного кода. Это следует из того, какие уязвимости и в каком количестве мы находили, а также с тем, что менялось со временем, например, по использованию защитных технологий и методов. В системах ДБО они не применяются в 90% случаев. Например:

- FrameBusting
- HTTPonly
- Secure cookie
- DEP
- ASLR

Всех этих известных и популярных средств защиты нет в Ваших ДБО

Итого

Мы знаем о чем говорим, за 3 года нам удавалось находить уязвимости в продуктах от следующих производителей:

- BSS
- Inist
- R-Style Softlab
- Сигнал-КОМ
- CompassPLUS
- StepUP
- ЦФТ