Digital Security

2011 CEE-SEC(R)

Разработка ДБО: что нужно сделать, чтобы Вас не взломали

Алексей Синцов

Руководитель департамента аудита ИБ,

Digital Security

#whoami

Digital Security:

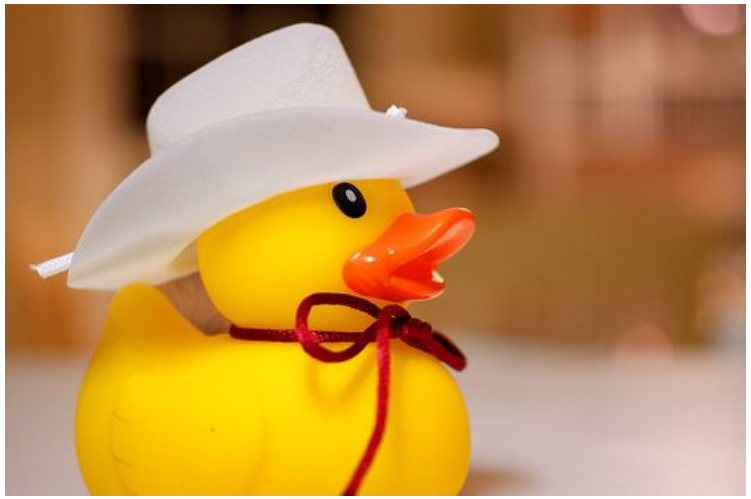
- Аудит/Тест на проникновение (ISO/PCI/PA–DSS и бла-бла-бла)
- Анализ защищенности ERP/SAP/ **ДБО**/Citrix/VMware
- Разработка «специализированного софта»
- Поиск ошибок и уязвимостей (**DSECRG**)
- Поиск путей эксплуатации

Журнал ХАКЕР:

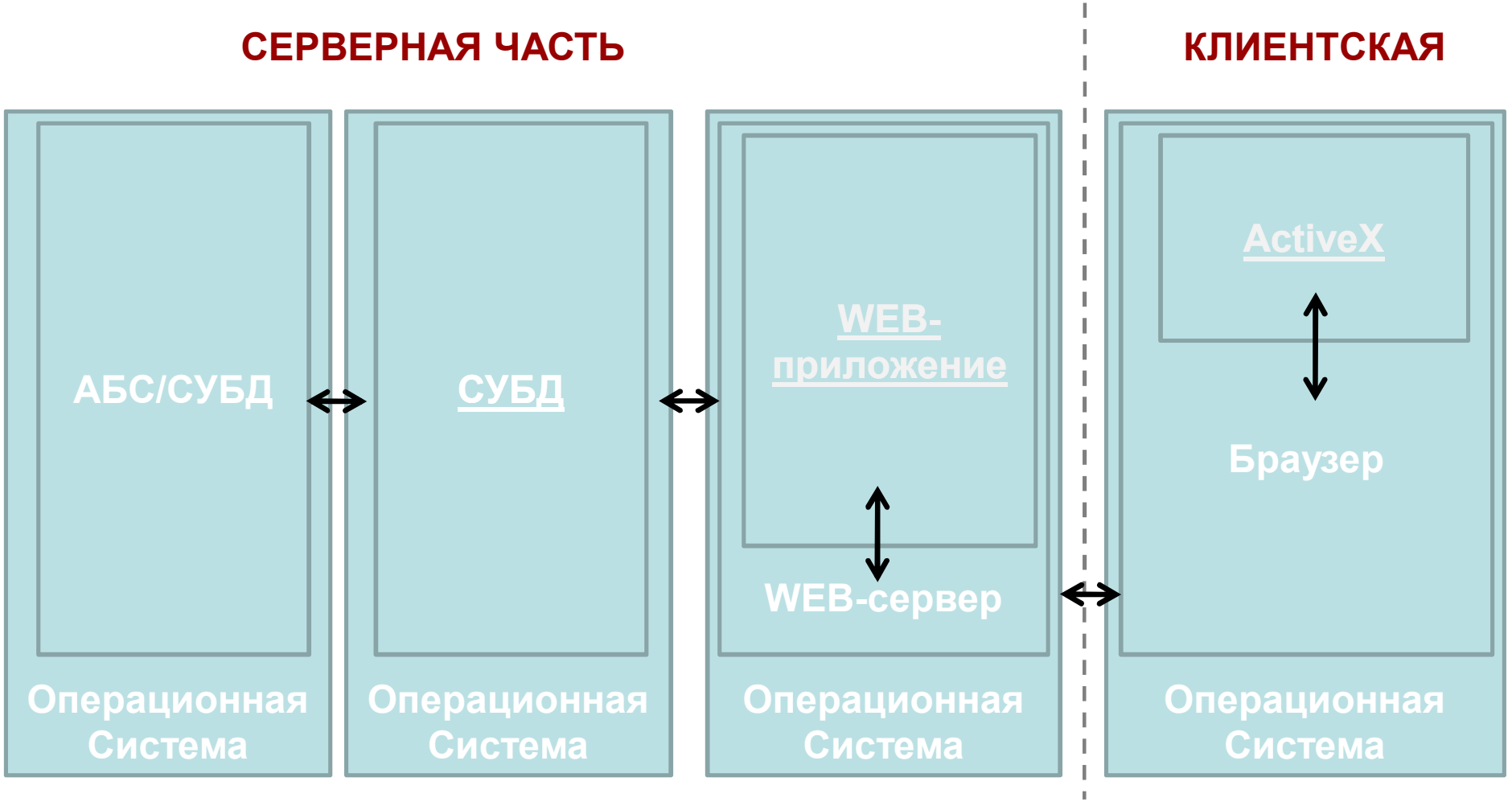
- **Когда-то:** колонка «Обзор Эксплойтов»
- Статьи на тему разработки эксплойтов и тестов на проникновение

Люблю поболтать:

- **CONFidence** 2011 Krakow
- **Hack In The Box** 2010 Amsterdam
- **Chaos Construction** 2011 СПБ



ДБО



Клиентское ПО

- Сервер приложений для «толстого» клиента
- ActiveX
- Прочее ПО

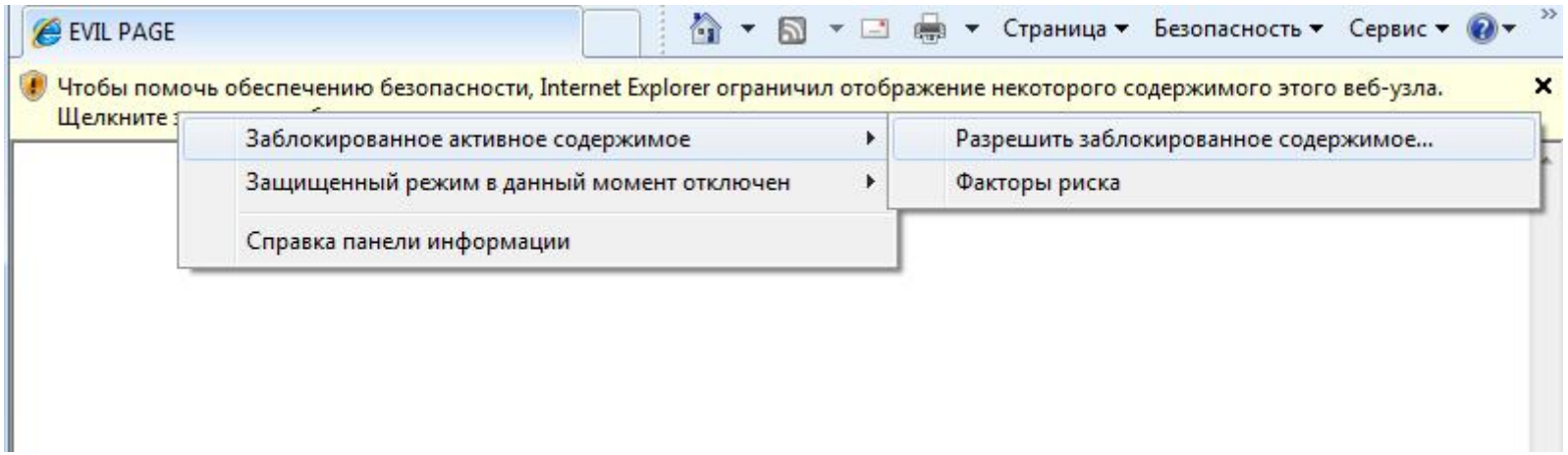
Клиентское ПО

- Установка ЭЦП
- Шифрование
- Работа с документами
- Работа с устройствами хранения ключей

Клиентское ПО

ActiveX

- SafeForScripting
- SafeForInit
- Подпись



Клиентское ПО

ActiveX

- Buffer Overflow — strcpy, memcpy, etc
- Format String — snprintf(var1,var2,…), printf(var)
- Memory Corruption — malloc, free
- Unsecure methods — obj.readfile() → fopen()

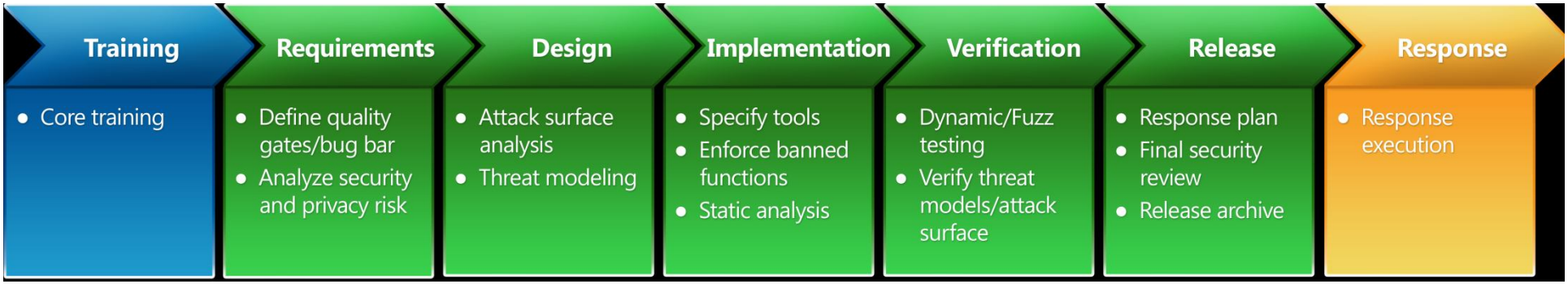
CVE-2008-1107

Summary: Multiple stack-based buffer overflows in the Danske Bank e-Sec Control Module ActiveX control (DanskeSikker.ocx) 3.1.0.48, and possibly earlier versions, allow remote attackers to execute arbitrary code via long arguments to unspecified methods, which are not properly handled by a logging function.

Published: 04/17/2009
CVSS Severity: 9.3 (HIGH)

Клиентское ПО

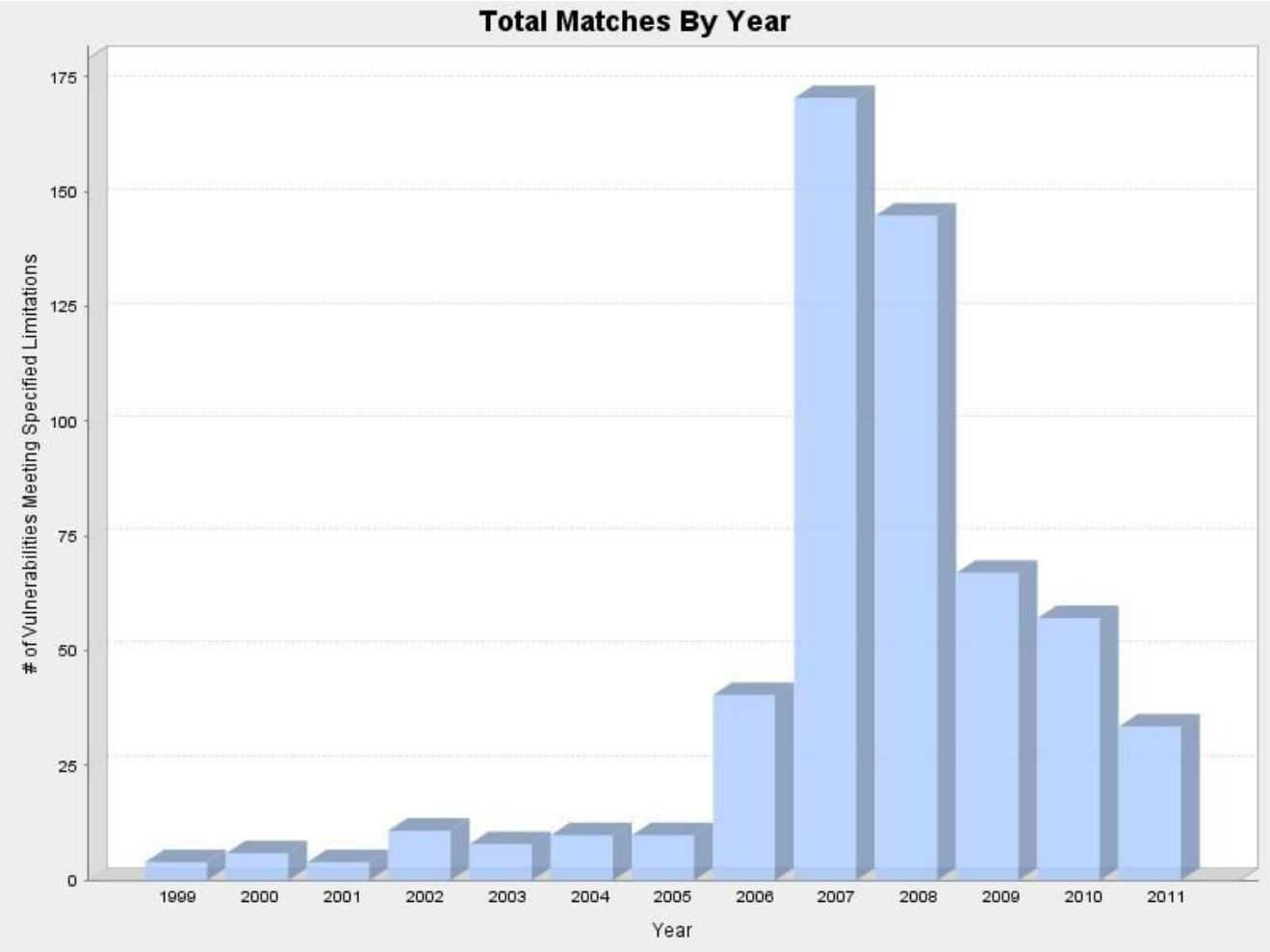
- DEP
- ASLR
- /GS
- SafeSEH
- SEHOP



http://msdn.microsoft.com/ru-ru/security/cc448177

http://msdn.microsoft.com/en-us/magazine/cc337897.aspx

Клиентское ПО



Клиентское ПО

Отечественное ПО (из пяти вендоров):

2009 - Две уязвимости

2010 - Еще две уязвимости

2011 - ?

Не только ActiveX

Inter-PRO – HTTP прокси сервер,
шифрующий трафик с помощью СКЗИ Сигнал-КОМ

В 2010 году нами были обнаружены 2 уязвимости в клиентской и серверной части ПО:

- Удаленное переполнение буфера в сервере - любой клиент может «**отключить**» сервер банка
- Локальное переполнение буфера в клиенте - возможность выполнять произвольный код в случае несоблюдения рекомендаций при работе с АРМ

Защитные механизмы ОС

Inter-PRO скомпилирован с флагом **GS** (защита от переполнения буфера в стеке)

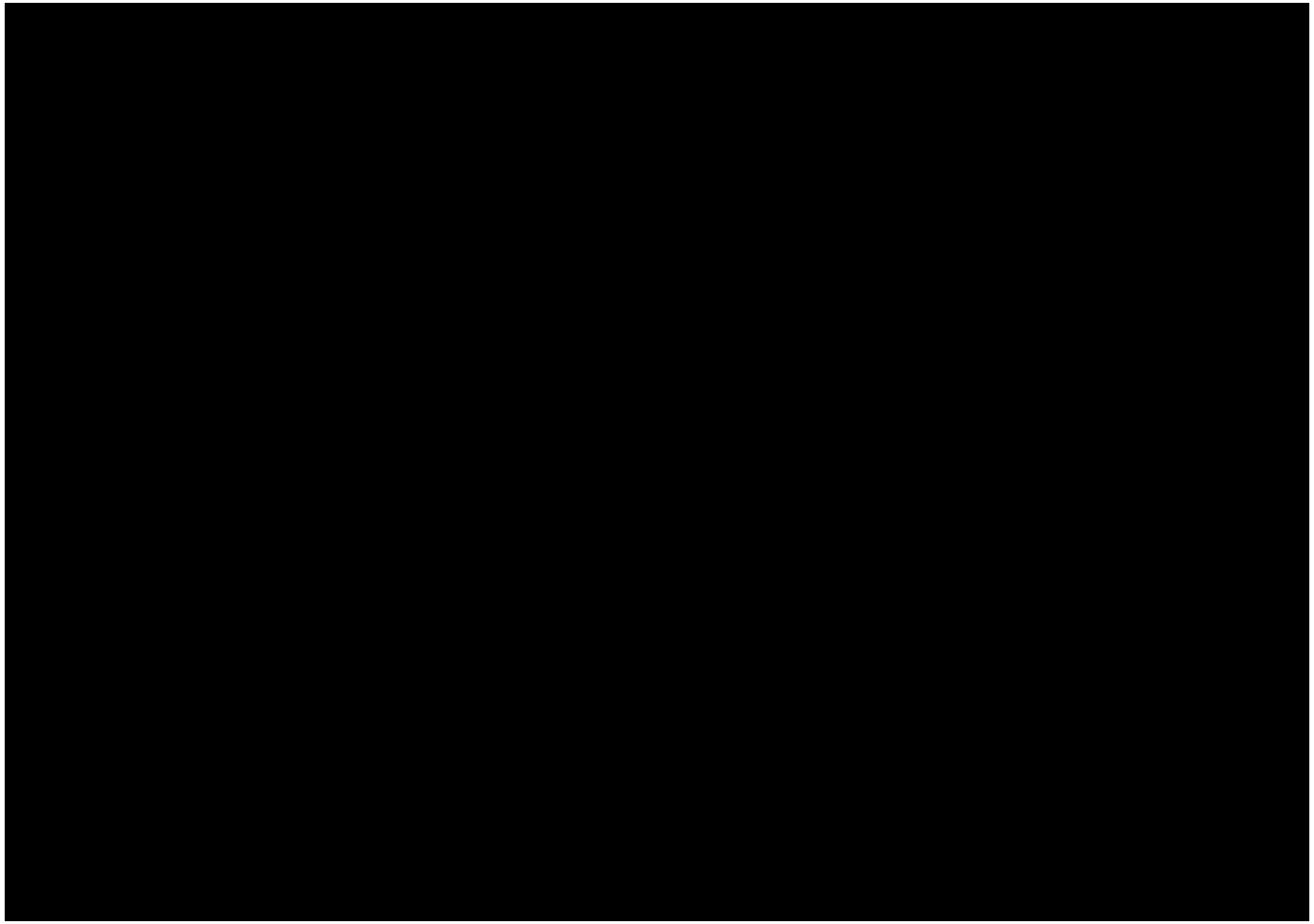
- Если бы не эта деталь, то было бы удаленное выполнение произвольного кода

А что же в версии под Linux?

- Почти никто из разработчиков не использует типовые защитные механизмы ОС: **DEP, ASLR, SafeSEH, GS**

- Это позволяет писать вредоносное ПО для Windows XP/Vista/2008/Windows 7

ActiveX от одной системы ДБО



WEB

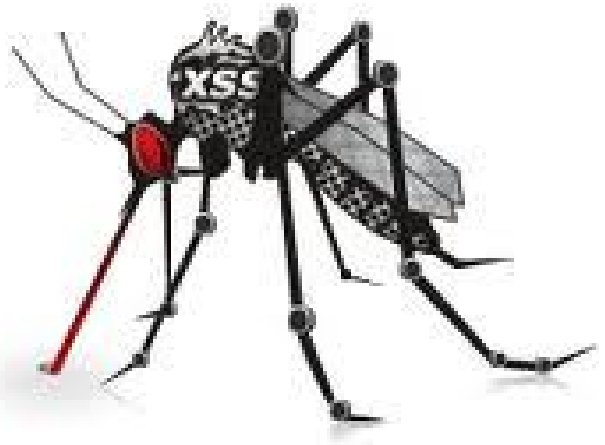
Ошибки в WEB:

- Межсайтовый скриптинг - Фишинг, перехват сессии и др.
- Межсайтовые запросы - Обход авторизации
- SQL-Инъекция - Обход аутентификации и др.
- XPath-Инъекция - Обход авторизации
- Внедрение кода - Выполнение кода
- Логические ошибки - Обход авторизации и др.

https://www.owasp.org/index.php/Top_10_2010

Меры смягчения

- 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

SSL

- Для всех форм аутентификации
- Не использовать смешанный контент
- Флаг ‘Secure’ для Cookie
- Использовать доверенный УЦ для подписи сертификата
- Использовать сильный крипто-алгоритмы
  - AES
  - 3DES
  - ГОСТ
  - SHA1
- Использовать сертификат только на домен Системы
- Использовать последний проверенные протоколы

https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
и не только…

СУБД

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

Заключение

- Анализ угроз
- Архитектура
  - SSL
  - httpOnly
  - FrameBasting
  - RDBS

- Проверка исходного кода
  - XSS
  - Injections
  - OpenRedirects
  - Buffer errors

- Пост-проверки, фаззинг
  - XSS
  - Injections
  - Buffer errors

Digital Security

www.twitter.com/asintsov
a.sintsov@dsec.ru