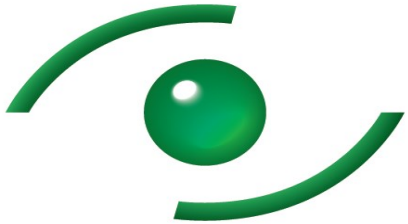
Практика исследования кода заказных финансовых приложений в российских банках

Рустэм Хайретдинов
Appercut Security

#MSSD. Москва. 5 марта 2013



INFOWATCH®

InfoWatch Holding

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

2004

KRIBRUM
Reputation management

2010

EGOSECURE

2011

APPERCUT
APPLICATION ERRORS CUTTING

2012

SDLC – НЕТ И НЕ ПРЕДВИДЕТСЯ

- **Долго / дорого / нецелесообразно**
  => Упор на функционал и нагрузку, игнорирование стандартов
- **Не вся разработка ведется внутри**
  => Требования сложно проконтролировать при приемке
- **Нет требований регулятора и KPI от бизнеса**
  => Программистам это не надо
- **Основная разработка уже закончена**
  Доделки идут непрерывно,

ИСТОЧНИКИ РИСКОВ

- Ошибки программирования
- Ошибки архитектуры
- Отладочные ветви
- Технические учетные записи
- «Закладки»

МОДЕЛЬ НАРУШИТЕЛЯ

	Случайные	Намеренные
Пользователь Интернет	Ошибки	Атаки, DoS
Клиент	Ошибки, социнженерия, атака на клиента	Мошенничество
Оператор	Ошибки	Мошенничество
Администратор	Ошибки	Саботаж

Внешние угрозы

Внутренние угрозы

СПЕЦИФИКА ВНУТРЕННИХ УГРОЗ

- Не только web-технологии
- «Толстые клиенты»
- Специфические языки
- Высокая критичность
- Большое количество связей
- Большинство угроз специфично

Нельзя просто запустить сканер, нужно выстраивать процесс

СЛЕДСТВИЯ ИЗ СПЕЦИФИКИ

- **Сканирование запрещено (высокая критичность)**
- **Динамический анализ нереален (много связей)**
- **Толстые клиенты (no XSS)**
- **DSL – Скрипты (no SQLi и др. OWASP хиты)**

Не все средства для контроля внешних угроз можно использовать

СЛЕДСТВИЯ ИЗ СПЕЦИФИКИ

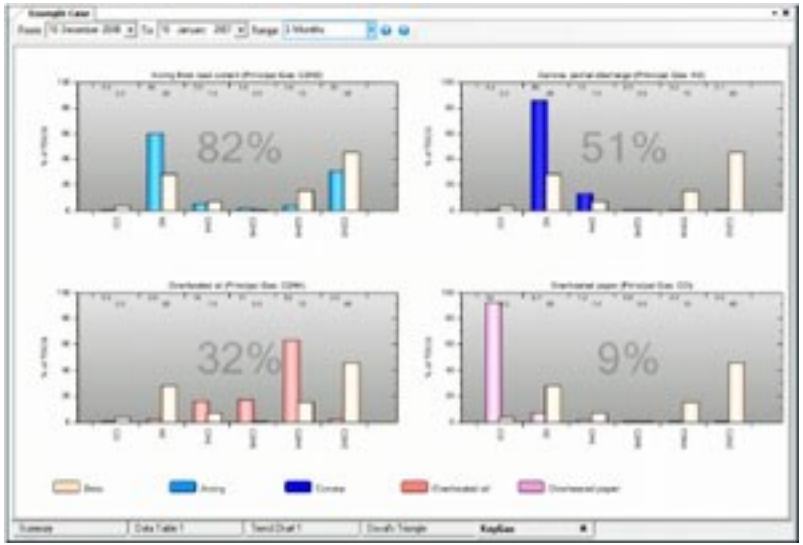
- Что ищем?
  - Application specific недостатки в логике и авторизации
  - Backdoors, закладки, логические бомбы
  - Некорректную конфигурацию платформы и приложения
- Как ищем
  - Вручную
  - Специально настроенными статическими сканерами

ШАГ ПЕРВЫЙ: АНАЛИЗ ASIS

- Будет обнаружено много некорректностей
- Не все их надо исправлять
- Результаты анализа – не менее секретны, чем данные

Не надо паники! Пока все работает!

ШАГ ВТОРОЙ: ИНТЕРПРЕТАЦИЯ РЕЗУЛЬТАТОВ



- Рекомендуем исправить только критичные ошибки
- Вычленяем специфичные для приложения угрозы
- Формируем правила и требования

ШАГ ТРЕТИЙ: ДОВОДИМ И КОНТРОЛИРУЕМ ТРЕБОВАНИЯ

- Обсуждаем требования с внешними и внутренними подрядчиками
- Вычленяем специфичные для приложения угрозы
- Формируем правила и требования

ВЫСТРАИВАЕМ ПРОЦЕСС

КОНТРОЛЬ ЗАКАЗНОГО ПРИЛОЖЕНИЯ

АУДИТ КОДА
Известные уязвимости кода

АУДИТ ПРИЛОЖЕНИЯ
Комплексные уязвимости

РУЧНОЙ АНАЛИЗ КОДА
Поиск НДВ

АУДИТ ДОПОЛНЕНИЙ
Все уязвимости

Appercut Service / Стандартная база

Наполнения базы требований

APPERCUT
APPLICATION ERRORS CUTTING

Appercut Service / База клиента

КОНТРОЛЬ ЗАКАЗНОГО ПРИЛОЖЕНИЯ

Анализ известных уязвимостей кода

Моделирование уязвимостей архитектуры

Моделирование уязвимостей бизнес-процессов

Компенсирующий контроль всех уязвимостей

Appercut Service / Стандартная база

Наполнения базы требований

APPERCUT
APPLICATION ERRORS CUTTING

Appercut Service / База клиента

APPERCUT CCS – быстро и удобно

- Не предполагается встраивание в процесс разработки
- Не предполагается участие программистов
- Аудируется любое количество приложений
- Возможность добавлять пользовательские образцы уязвимостей!
- Архитектура - веб-сервис (Public/Private Cloud)
- Сертификация ФСТЭК (ТУ, НДВ4 – в процессе)

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ

- Традиционные средства разработки: Java, JavaScript, PHP, Cobol, C/C++, T-SQL, .NET (VB, C#, ASP), Delphi, Objective C, Python, Ruby…
- Традиционные бизнес-платформы: ABAP4 (SAP), PL/SQL (Oracle), LotusScript (IBM Lotus Notes), 1C ver 7 и 8, Microsoft Dynamics (X++), …
- Проприетарные языки и скрипты приложений, в т.ч. российских (БОСС, Directum, Atlantis, …)
- Любая платформа на заказ (нормализатор + 10 TOP-уязвимостей) – 1 месяц

ВОПРОСЫ, ПОЖАЛУЙСТА!

APPERCUT

APPLICATION ERRORS CUTTING

Рустэм Хайретдинов
Appercut Security
sales@appercut-security.com
+7(903)961-7312
www.appercut.com