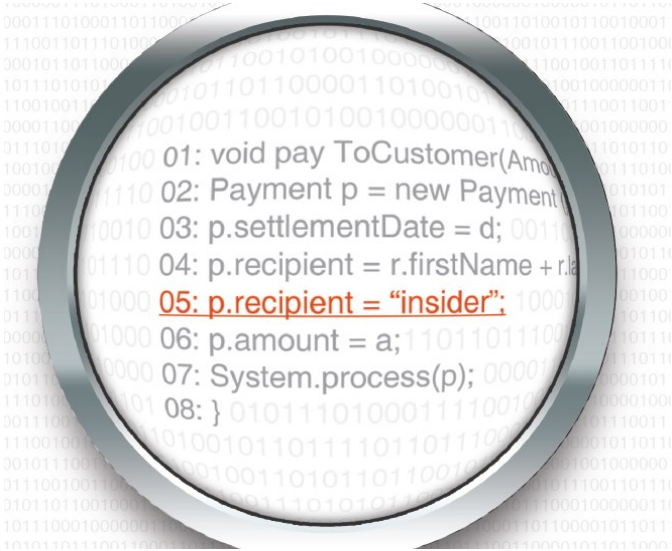


ОРГАНИЗАЦИЯ ПРОЦЕДУРЫ СТАТИЧЕСКОГО АНАЛИЗА КОДА ФИНАНСОВЫХ ПРИЛОЖЕНИЙ:

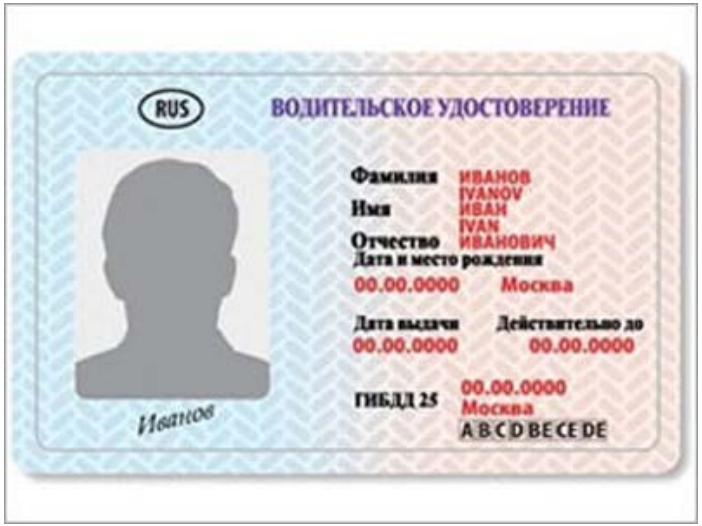
ОТ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ - К БЕЗОПАСНОЙ РАЗРАБОТКЕ

Рустэм Хайретдинов
CEO Appercut Security

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

Единый ГосЭкзамен

Водительское удостоверение

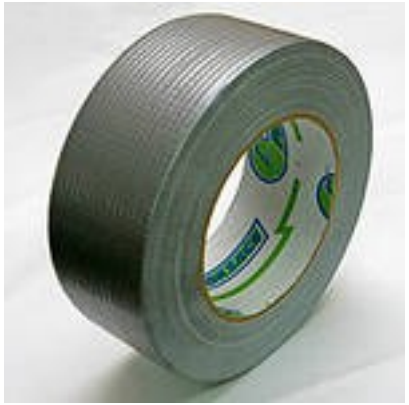


Требования 6.5 и 6.6

6.5 Предотвращать распространенные уязвимости программного кода в процессе разработки ПО следующим образом:
• обучение разработчиков методикам безопасного программирования, включая информацию о том, как избежать распространенных программных уязвимостей и как определить способ хранения критичных данных в памяти;
• разработка приложений в соответствии с основными принципами безопасного программирования.

6.6 Следует обеспечить защиту общедоступных веб-приложений от известных атак (а также регулярно учитывать новые угрозы и уязвимости) одним из следующих методов:
проверять приложение на наличие уязвимостей с использованием методов ручного или автоматического анализа защищенности приложений не реже одного раза в год, а также после внесения изменений.

Малой кровью

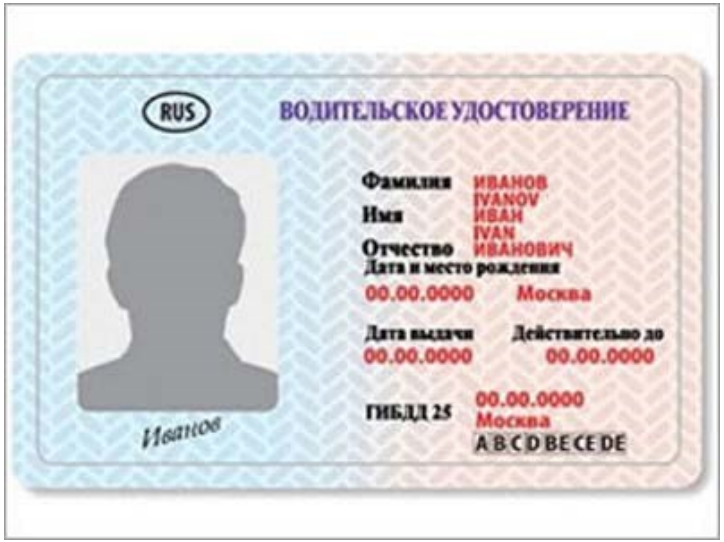


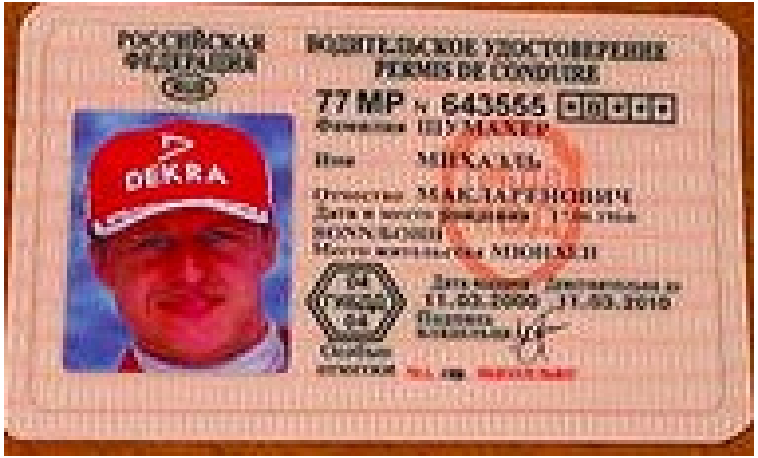
- Обучить персонал на курсах, которые дают сертификат
- Заключить «рамочный» договор с тестовой лабораторией
- Получить доступ на бесплатный сервер сканирования

ПО ВЗРОСЛОМУ?

- Рассматривать PCI DSS compliance, как первый шаг
- Проанализировать текущие финансовые приложения
- Используя различные инструменты, организовать правильную приемку
- Затем – тестирование и разработку
- Научиться формировать требования по безопасной разработки
- Соответствовать рекомендациям Банка России по безопасной разработке финансовых систем

СРАВНИТЕ РЕЗУЛЬТАТ





СПАСИБО ЗА ВНИМАНИЕ!
ЗАДАВАЙТЕ ВОПРОСЫ

rustem@khairetdinov.com