APPSEC FROM SCRATCH

ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ С НУЛЯ

ТЕРНИСТЫЙ ПУТЬ

Юрий Колесов
Appsec в «1С-Битрикс»

ПРОБЛЕМА

Релизы часто

Тестирование безопасности редко и долго

ЦИКЛ РЕЛИЗА

- Разработчик (пилит код)
- Lead/Senior (code review)
- Тестировщик (функциональное тестирование)
- Безопасник (тестирование безопасности)

ЦИКЛ РЕЛИЗА

- Разработчик (пилит код)
- Lead/Senior (code review)
- + Админ/DevOps (выкладка)
- Тестировщик (функциональное тестирование)
- Безопасник (тестирование безопасности)

ИДЕАЛЬНЫЙ МИР

- Опытный Разработчик Lead/Senior (пилит код и не ошибается)

ИДЕАЛЬНЫЙ МИР

- Разработчик (пилит код)
- Опытный Разработчик Lead/Senior (code review)

РЕАЛЬНЫЙ? МИР

- Разработчик (пилит код)
- Опытный Разработчик Lead/Senior (code review)
- Безопасник (тестирование безопасности и функциональное тестирование)

РЕАЛЬНЫЙ МИР

- Разработчик (пилит код)
- Lead/Senior (code review)
- Безопасник (тестирование безопасности)
- Тестировщик (функциональное тестирование)

ЧАСТЫЕ РЕЛИЗЫ

- Раз в неделю?
- Раз в день?

ЦИКЛ РЕЛИЗА

- Разработчик (пилит код)
- Lead/Senior (code review)
- Админ/DevOps (выкладка на тест/stage)
- Тестировщик (функциональное тестирование)
- Безопасник (тестирование безопасности)

- Админ/SysOps (выкладка)
- Тестировщик (функциональное тестирование)
- Безопасник (тестирование безопасности публикации)

СРЕДСТВА АВТОМАТИЗАЦИИ

- Сканер безопасности
- Статический анализатор
- Динамический анализатор

Долго (

УСКОРЯЕМ

- Интеграция статического анализатора в процесс разработки
- Тестирование векторов атак в процессе функционального тестирования (см. доклад Сергея Белова из mail.ru https://youtu.be/JbtIoA3k5zA)

Регуляторы довольны)

ЭФФЕКТИВНОСТЬ

- Автоматизированные сканеры
- Тестирование на проникновение разовое
- Пентест в цикле разработки (специализированные сканеры)
- Статический анализатор

BugBounty

ВЫВОДЫ

Частые релизы – боль

Тестировать безопасность все равно надо

Тестируем каждый релиз насколько сможем

Измеряем время каждого шага релиза

Автоматизация необходима

Полный цикл тестирования с возможной периодичностью

Обучение разработчиков

BugBounty

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

ЮРИЙ КОЛЕСОВ

AppSec в «1С-Битрикс»
https://www.facebook.com/yuri.v.kolesov
+7-926-55-99-82
kolesov@bitrix.ru