XXIII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ "КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ"

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

ОБЗОР СОВРЕМЕННЫХ МЕТОДОВ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Сидорович Владислав Олегович

Значимость корректной работы ПО

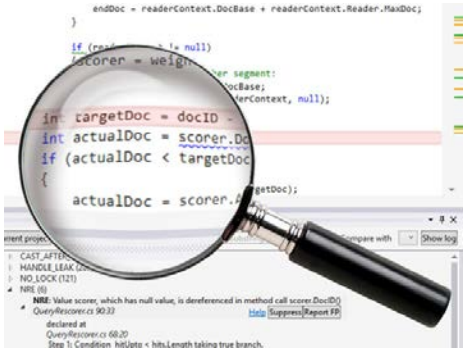
Уязвимости ПО

- Переполнение буфера
- Ошибки при работе с динамической памятью
- Ошибки обработки пользовательских данных
- Ошибки форматных строк
- Ошибки синхронизации
- Утечки памяти и других ресурсов системы
- Некорректная работа с временными файлами и другими интерфейсами ОС
- Уязвимости безопасности

Различные подходы к поиску уязвимостей ПО

Методы анализа ПО

- Статический анализ
- Динамический анализ



Статический анализ

Аргументы "за"

- Могут использоваться на ранних этапах разработки ПО
- Могут использоваться ранее протестированные базы кодов
- Средства могут быть интегрированы в среду разработки в качестве части компонента
- Низкие стоимостные затраты.

Аргументы "против"

- Могут обнаруживаться программные ошибки и уязвимости, которые не обязательно приводят к отказу программы
- Ненулевая вероятность "ложного срабатывания".

Динамический анализ

Аргументы "за"

- Редко возникают "ложные срабатывания"
- Для отслеживания причины ошибки может быть произведена полная трассировка стека и среды исполнения.
- Захватываются ошибки в контексте работающей системы, как в реальных условиях, так и в режиме имитации моделирования.

Аргументы "против"

- Происходит вмешательство в поведение системы в реальном времени. Это не всегда приводит к возникновению проблем, но об этом нужно помнить при работе с критическим ко времени кодом.
- Полнота анализа ошибок зависит от степени покрытия кода.

Фаззинг (fuzzing)

Цель - получение набора данных, выявляющих дефекты работы целевой программы.

Типы фаззеров

1. **Глупый (dumb) ничего не знает о структуре**
2. **Умный (smart) имеет некоторое представление о структуре данных**

Этапы фаззинга

1. Анализ приложения, разработка фаззера

2. Генерация данных

3. Собственно, фаззинг

4. Анализ результатов

Спасибо за внимание!