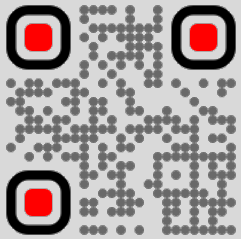
DETECT

Открытые средства анализа защищённости

Практика внедрения



Обо мне

- Омар Ганиев
- Хакер, пентестер
- Основатель DeteAct (ООО «Непрерывные технологи»)

Тема

- Философия подхода к безопасной разработке
  - С идеологией защитников (аппсекеров)
  - С идеологией атакующих (пентестеров)
  - Есть ли что почерпнуть друг у друга?

Тема

- Философия подхода к безопасной разработке
  - С идеологией защитников (аппсекеров)
  - С идеологией атакующих (пентестеров)
  - Есть ли что почерпнуть друг у друга?
- Выбор средств анализа защищённости
  - По первичным характеристикам (качество)
  - По вторичным характеристикам (удобство)
  - Открытые или подороже?

Подход

- Фокус пентестеров:
  - Технические аспекты

Подход

- Фокус пентестеров:
  - Технические аспекты
  - Разработка эксплойта

Подход

- Фокус пентестеров:
  - Технические аспекты
  - Разработка эксплойта
  - Максимизация доступа

Подход

- Фокус защитников:
  - Организационные аспекты

Подход

- Фокус защитников:
  - Организационные аспекты
  - Разработка мер защиты

Подход

- Фокус защитников:
  - Организационные аспекты
  - Разработка мер защиты
  - Минимизация кол-ва уязвимостей

Отражение подхода

- Пентестеры:
  - Посредственно пишут рекомендации и оценивают риск

Отражение подхода

- Пентестеры:
  - Посредственно пишут рекомендации и оценивают риск
  - Не требовательны к интерфейсам сканеров

Отражение подхода

- Пентестеры:
  - Посредственно пишут рекомендации и оценивают риск
  - Не требовательны к интерфейсам сканеров
  - Стремятся демонстрировать максимальный ущерб

Отражение подхода

- Защитники:
  - Понимают, как и с какими приоритетами исправлять уязвимости

Отражение подхода

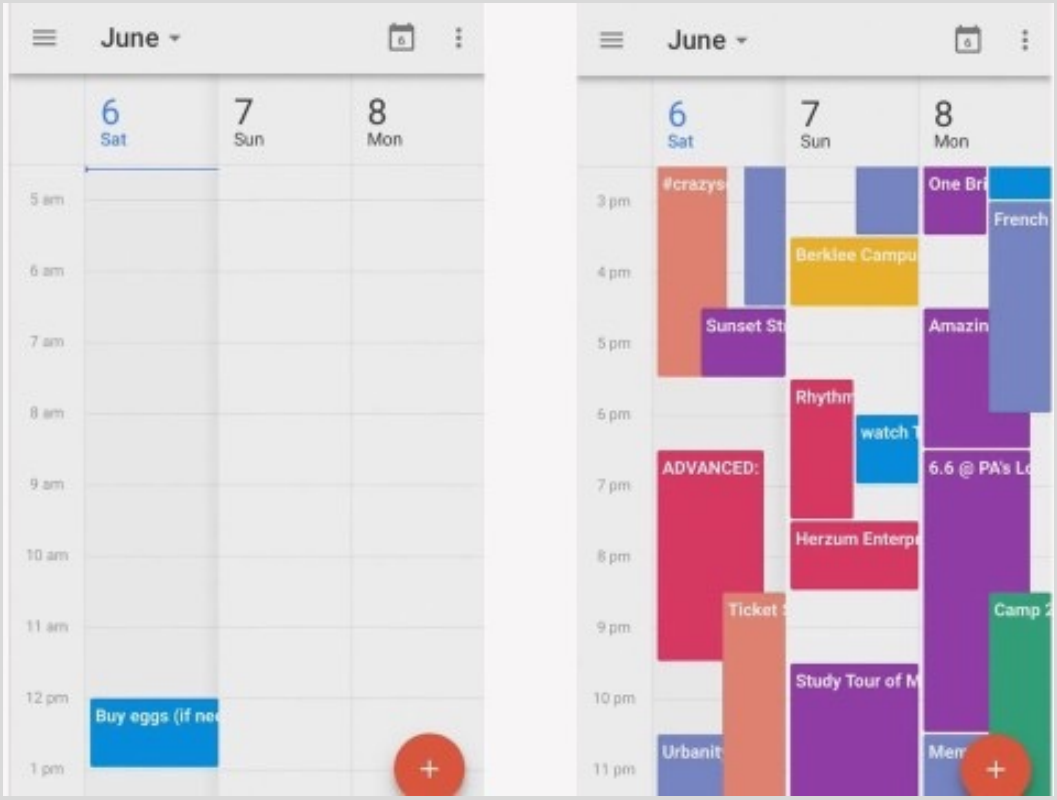
- Защитники:
  - Понимают, как и с какими приоритетами исправлять уязвимости
  - Очень требовательны к интерфейсам сканеров

Отражение подхода

- Защитники:
  - Понимают, как и с какими приоритетами исправлять уязвимости
  - Очень требовательны к интерфейсам сканеров
  - Строят процессы, а не оценивают защищённость в моменте

Различия

- Календарь пентестера vs календарь аппсека:



Различия

- Защитники:
  - Human-centric
    - Нужно убедить разработчиков исправить что-то!
  - Metrics-centric
    - Нужно измерить, стало ли лучше от внедрения процессов!
  - Solutions-centric
    - Рук нет, нужно найти решения для автоматизации!

Различия

- Защитники:
  - Human-centric
    - Нужно убедить разработчиков исправить что-то!
  - Metrics-centric
    - Нужно измерить, стало ли лучше от внедрения процессов!
  - Solutions-centric
    - Рук нет, нужно найти решения для автоматизации!
- Пентестеры:
  - Goal-centric
    - Нужно найти критическую уязвимость!
  - Impact-centric
    - Нужно показать, насколько всё плохо!
  - Technology-centric
    - Нужно придумать, как быстрее найти уязвимость!

Различия

- Конечно, взгляд пентестеров ограничен
  - Не понимают, насколько сложна безопасная разработка
  - Им лишь бы поломать

Различия

- Конечно, взгляд пентестеров ограничен
  - Не понимают, насколько сложна безопасная разработка
  - Им лишь бы поломать
- При этом взгляд аппсекеров размыт
  - Вечные переговоры с разработчиками
  - Сбор метрик и внедрение процессов

Средства анализа защищённости

- Защитники:
  - Интерфейс
    - Отображение трендов, графиков, истории уязвимостей
  - Обвязки
    - Интеграция с Jira, LDAP, ASOC, …
  - Показатели
    - Метрики для обоснования полезности

Средства анализа защищённости

- Защитники:
  - Интерфейс
    - Отображение трендов, графиков, истории уязвимостей
  - Обвязки
    - Интеграция с Jira, LDAP, ASOC, …
  - Показатели
    - Метрики для обоснования полезности
- Пентестеры:
  - Интерфейс
    - Лишь бы было понятно, где уязвимость!
  - Обвязки
    - Лишь бы запускалось!
  - Показатели
    - Лишь бы находило уязвимости!

Средства анализа защищённости

- Ловушка Парето:
  - Простой DAST/SAST сделать легко
  - Улучшить его в 2 раза – несложно
  - Улучшить ещё на 10% – гораздо сложнее

Средства анализа защищённости

- Ловушка Парето:
  - Простой DAST/SAST сделать легко
  - Улучшить его в 2 раза – несложно
  - Улучшить ещё на 10% – гораздо сложнее
- Задача в общем случае нерешаемая
  - Всегда будут уязвимости, которые не найти за нужное время
  - Ещё долго человек будет гораздо сильнее

Средства анализа защищённости

- Покупателями сканеров являются **защитники**

Средства анализа защищённости

- Покупателями сканеров являются **защитники**
- Они хотят облегчить свою работу
  - Получать в удобном виде результат анализа
  - Показывать полезность

Средства анализа защищённости

- Покупателями сканеров являются **защитники**
- Они хотят облегчить свою работу
  - Получать в удобном виде результат анализа
  - Показывать полезность
- Что это мотивирует делать вендоров?
  - Продавать дашборды и обвязки
  - + отчёты с 1000 ложных срабатываний

Средства анализа защищённости

- Полезно иногда смотреть на это глазами атакующих
- Зачем сканер уязвимостей? Чтобы искать уязвимости!
- Помимо удобства, есть и **качество**

Средства анализа защищённости

- На ранних этапах имеет смысл тестировать открытые решения
  - Или почти открытые

Средства анализа защищённости

- На ранних этапах имеет смысл тестировать открытые решения
  - Или почти открытые
- Они могут быть не хуже enterprise-решений
  - С т.з. качества обнаружения уязвимостей

Средства анализа защищённости

- На ранних этапах имеет смысл тестировать открытые решения
  - Или почти открытые
- Они могут быть не хуже enterprise-решений
  - С т.з. качества обнаружения уязвимостей
- Дополнительная мотивация – уход зарубежных вендоров

Предлагаемый стек DAST

- Основной движок:
  - Burp Suite Pro – проприетарный, но расширяемый и очень дешёвый
  - OWASP ZAP – полностью open source, слабее по качеству

Предлагаемый стек DAST

- Основной движок:
  - Burp Suite Pro – проприетарный, но расширяемый и очень дешёвый
  - OWASP ZAP – полностью open source, слабее по качеству
- Дополнения:
  - BAPPStore + расширения типа Molly Pack от Яндекса

Предлагаемый стек DAST

- Основной движок:
  - Burp Suite Pro – проприетарный, но расширяемый и очень дешёвый
  - OWASP ZAP – полностью open source, слабее по качеству
- Дополнения:
  - BAPPStore + расширения типа Molly Pack от Яндекса
- Обвязки:
  - Собственные автотесты, запущенные через прокси Burp/ZAP
  - OpenAPI + генерация запросов (schemathesis и прочие)
  - Оркестрация через API в CI/CD или на отдельном хосте

Предлагаемый стек SAST

- Основной движок:
  - Semgrep – open source анализатор (есть коммерческая версия)
  - «Продвинутый» grep, есть поддержка многих языков и taint-анализ

Предлагаемый стек SAST

- Основной движок:
  - Semgrep – open source анализатор (есть коммерческая версия)
  - «Продвинутый» grep, есть поддержка многих языков и taint-анализ
- Дополнения:
  - Разные конфиги с semgrep.dev и сторонние наборы правил

Предлагаемый стек SAST

- Основной движок:
  - Semgrep – open source анализатор (есть коммерческая версия)
  - «Продвинутый» grep, есть поддержка многих языков и taint-анализ
- Дополнения:
  - Разные конфиги с semgrep.dev и сторонние наборы правил
- Обвязки:
  - Собственные наборы YAML-правил
  - Diff-aware анализ, интеграция с Github/Gitlab

Итого

- Философия:
  - Пентестеры и аппсекеры по-разному понимают проблему безопасной разработки
- Вендоры средств анализа защищённости:
  - Ориентируются на основного потребителя – аппсек-инженеров
- Защитникам полезно:
  - Смотреть на SDLC глазами хакеров и внедрять их инструменты

DETEACT

Questions?

bechedeteact.com