ГАРДА

Автоматизация фаззинг-тестирования в CI

Кирилл Стуженов

Руководитель направления
Центр компетенций информационной безопасности

ГАРДА

Производитель решений в сфере безопасности данных и сетевой инфраструктуры

- Более 1000 B2B-клиентов
- Более 120 глобальных проектов
- Решения внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ

Наши системы защищают 50% всего российского Интернета от DDoS-атак

Наши продукты стали отраслевым стандартом в области мониторинга и защиты баз данных

Наши решения обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба*

Полностью российские решения

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий
- Решения сертифицированы ФСТЭК
- Включены в реестр отечественного программного обеспечения

* Электронные выборы, Госуслуги, защита от подмены А-номера абонента

Системы безопасности

Защита данных

- Защита баз данных
- Обезличивание копий баз данных
- Защита неструктурированных данных
- Защита корпоративных коммуникаций
- Защита от утечек конфиденциальных данных
- Защита сетевых хранилищ данных

Сетевая безопасность

- Системы для выявления внутрисетевых атак
- Расследование сетевых инцидентов
- Threat Intelligence
- Защита от DDoS-атак
- Сетевые ловушки
- NGFW
- WAF

Управление трафиком

- Глубокий анализ пакетного трафика
- Система применения правил передачи данных мобильных абонентов
- Антифрод
- Пакетные брокеры
- Коммутаторы
- NMS

Аналитика и сервис

- Сервисы по сопровождению систем безопасности
- Экспертиза по защите от кибератак
- Платформа аналитики информационной и экономической безопасности

Что такое фаззинг для Гарды?

- Много автоматизации
- Надёжность и безопасность приложений
- Выявление широкого спектра багов
- Взаимодействие команд AppSec и RnD
- Ускорение процессов сертификации

Наша фаззинг-ферма:

104 ядра x 4.0 ГГц

208 потоков

512 гигабайт ОЗУ

Фаззер находит разные ошибки

- Переполнение переменных
- Выход за границы массива
- Пропущенные исключения
- Ошибки сегментации
- Зависание в бесконечном цикле
- Состояние гонки
- И многие другие!

Обнаружить ошибки недостаточно

Чем больше багов, тем важнее оценивать их критичность и приоритет исправления

Преимущества автоматизации фаззинга

Ускорение обнаружения ошибок

Надёжное заведение задач без траты времени на False Positive

Снижение кадрового голода

Снижение числа ручных ошибок оператора

Эффективное управление ресурсами

Масштабируемость

Сложности в автоматизации фаззинга

Долгое время тестирования

Много неприоритетных багов

Сложность интеграции инструментов

Как боролись с этими проблемами

Долгое время тестирования	отдельный пайплайн для фаззинга, приоритизация фаззинг-целей
Много неприоритетных багов	автоматическое отсеивание ложных сработок, приоритизация оставшихся
Сложность интеграции инструментов	создание собственных инструментов, обучение разработчиков, совместная разработка фаззинг-целей

Набор инструментов BugBane

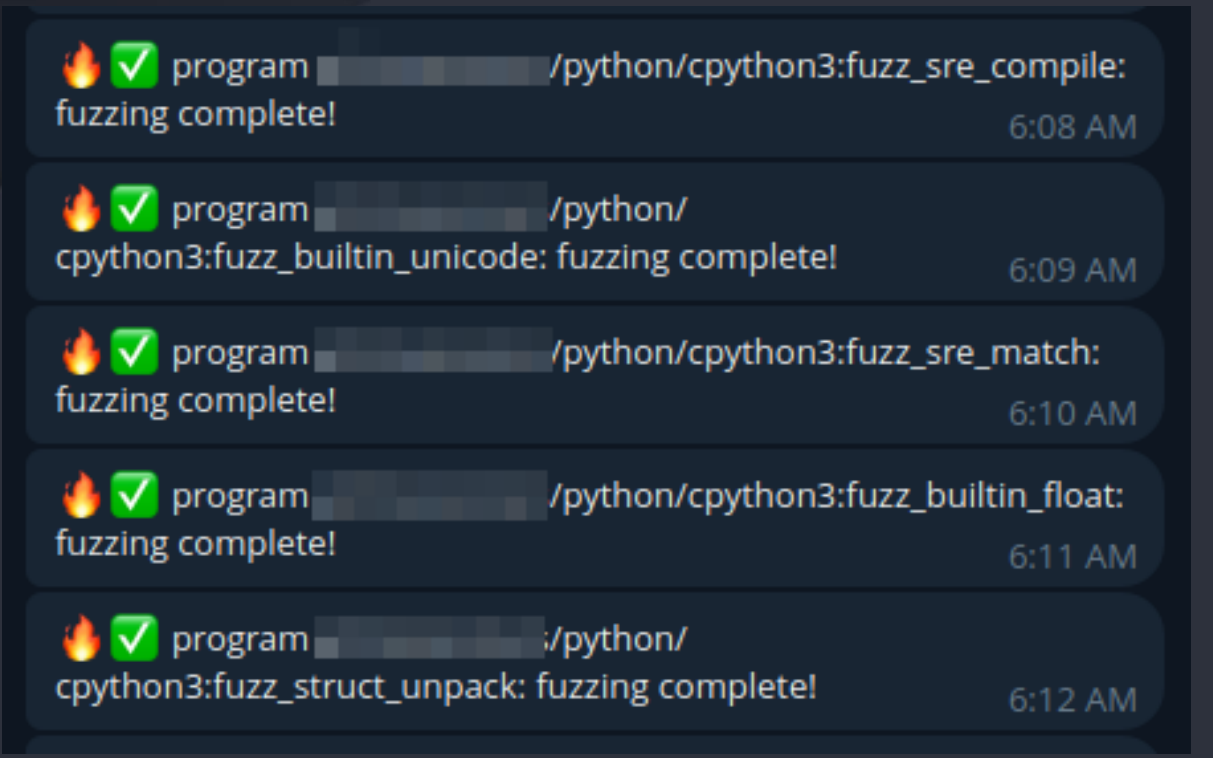
ГАРДА

- [x] Делает сборки под фаззинг
- [x] Выполняет фаззинг
- [x] Отправляет воспроизводимые баги в Defect Dojo
- [x] Собирает покрытие
- [x] Минимизирует тестовые примеры
- [x] Создаёт отчёты по шаблону Jinja2

Оркестратор OmniFuzz

ГАРДА

- Управляет контейнерами с BugBane
- Максимизирует использование доступных ресурсов
- Обеспечивает регулярный фаззинг актуальных версий ПО
- Создан под нужды Гарды



Участие в сообществе РБПО

- 500+ разметок Svace в .NET
- 120+ разметок в Python
- 50+ разметок в Nginx
- Новые фаззинг-цели Nginx с высоким покрытием
- Настройка фаззинга среды .NET

* Данные за январь 2023 – январь 2024

@kirill21h

k.stuzhenov@gardatech.ru

Спасибо за внимание!