

Поиск уязвимостей ПО при эксплуатации — **БАЗОВЫЙ МИНИМУМ ИЛИ РОСКОШНЫЙ МАКСИМУМ**

24 процесс ГОСТ Р 56939-2024

AKTIV.
CONSULTING



Артём Храмых

Руководитель отдела
по анализу защищённости
AKTIV CONSULTING



Три кита РБПО



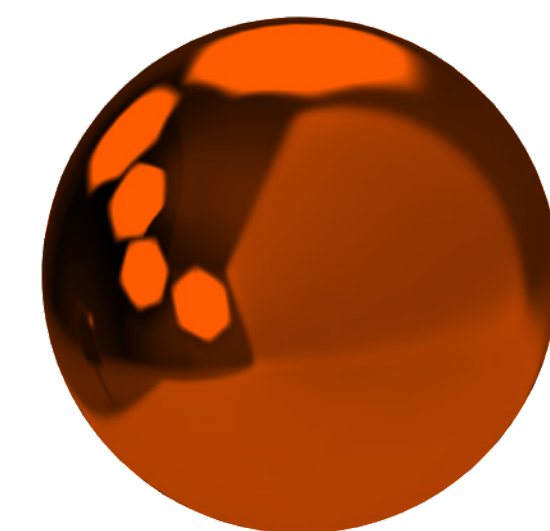
Статистический
анализ



Динамический
анализ



Композиционный
анализ



Автоматизированный поиск уязвимостей

В современных реалиях — **базовый минимум**

Сканеры и инструменты▶



Важность точной настройки инструментов

К чему стремиться (**Pentest Continius, SOC**)

Ручной поиск уязвимостей

В современных реалиях — **роскошный максимум**

Если исследование не для галочки

Отчёт покажет много неожиданного

Ценность опыта и критического мышления

Этапы тестирования на уязвимости

1

Разведка

2

Поиск уязвимостей

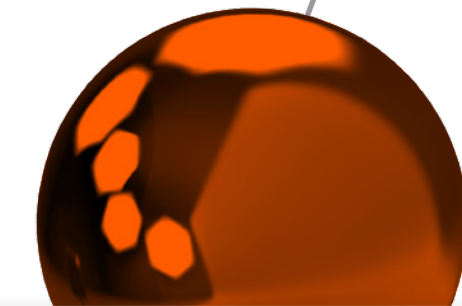
3

Эксплуатация уязвимостей и проведение атак

4

Отчёт

OWASP TOP-10



- A01: 2025 – Нарушение контроля доступа
- A02: 2025 – Неправильная конфигурация системы безопасности
- A03: 2025 – Сбои в цепочке поставок программного обеспечения
- A04: 2025 – Криптографические сбои
- A05: 2025 – Внедрение вредоносного программного обеспечения
- A06: 2025 – небезопасный дизайн
- A07: 2025 – Сбои аутентификации
- A08: 2025 – Сбои целостности программного обеспечения или данных
- A09: 2025 – Сбои ведения журнала безопасности и в оповещениях
- A10: 2025 – Неправильная обработка исключительных условий



Внедрение процесса **поиска** **уязвимостей ПО** при эксплуатации

Нетривиальная задача

Кому доверять?

Трудности

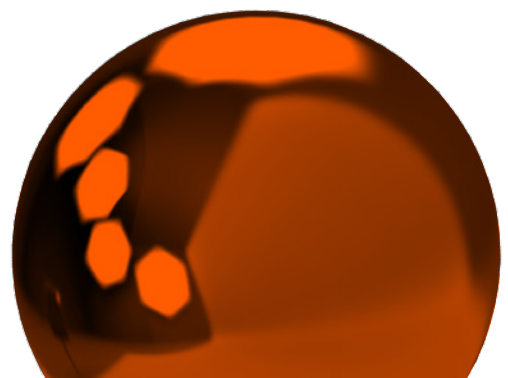


Security Champion или пентестер

Разное мышление

Ключевая роль пентестера – поиск уязвимостей

Ключевая роль Security Champion – минимизировать уязвимости в ПО



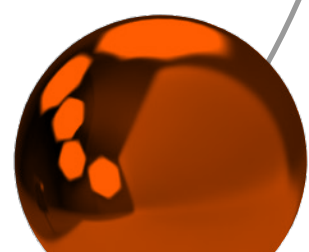
Кейсы



Внедрение РБПО у крупного вендора СЗУ

Инцидент у крупного вендора

Пентест торговой системы



БЛАГОДАРЮ ЗА ВНИМАНИЕ!

AKTIV.
CONSULTING



Артём Храмых

Руководитель отдела
по анализу защищённости

khramykh@aktiv.consulting



