OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо

Напишите в чат, если есть проблемы

Проверить, идет ли запись!

Автоматизация анализа защищенности веб-приложений

Колесников Александр

Правила вебинара

Активно участвуем

Задаем вопросы в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

Методологии

Ресурсы и инструменты

Тестирование приложения

Цели

1. Познакомиться с инструментами автоматизации
2. Рассмотреть подробно несколько приложений
3. Подвести итоги


Burp Suite modules and functions

Intruder

- Модуль, который позволяет перебирать запросы
- Есть по-умолчанию в Burp
- Pro версия содержит больше опций

Уязвимости, которые можно автоматизировать

- XSS
- Broken Access Control
- CSRF
- Deserialization
- Sensitive Data Exposure
- SQL Injection
- XXE
- Insecure File Upload
- Directory Traversal
- Session Management
- Command Injection

Extensions

- **XSS** - Burp Hunter
- **Broken Access Control** - BurnPlay
- **CSRF** - CSRF Scanner
- **Deserialization** - Java Serial Killer
- **Sensitive Data Exposure** - SpyDir
- **SQL Injection** - InjectMate
- **XXE** - Content Type Converter
- **Insecure File Upload** - Upload Scanner
- **Directory Traversal** - Uploader
- **Session Management** - TokenJar
- **Command Injection** - Command Injection Attacker

OTUS
ОНЛАЙН ОБРАЗОВАНИЕ

WFUZZ

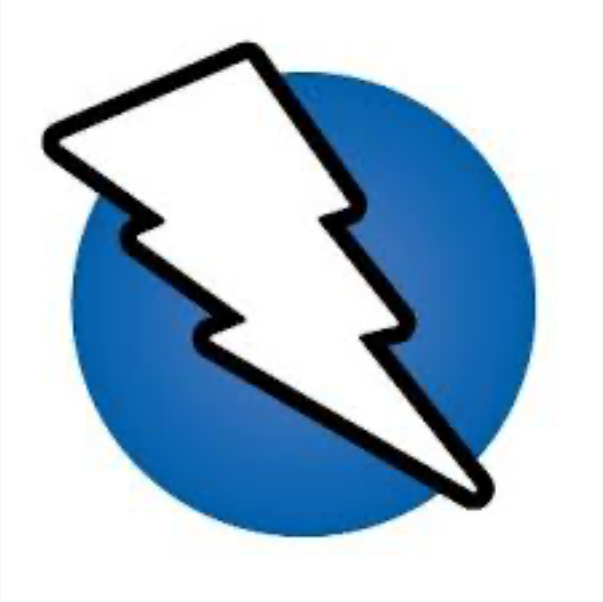
wFuzz

- Framework для автоматического тестирования:
  - Cookie
  - Path
  - HTTP Requests


OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ
OWASP ZAP

OWASP ZAP

- Автоматический сканер
- Ориентирован на web приложения
- Проводит тестирование для заданного набора входных параметров

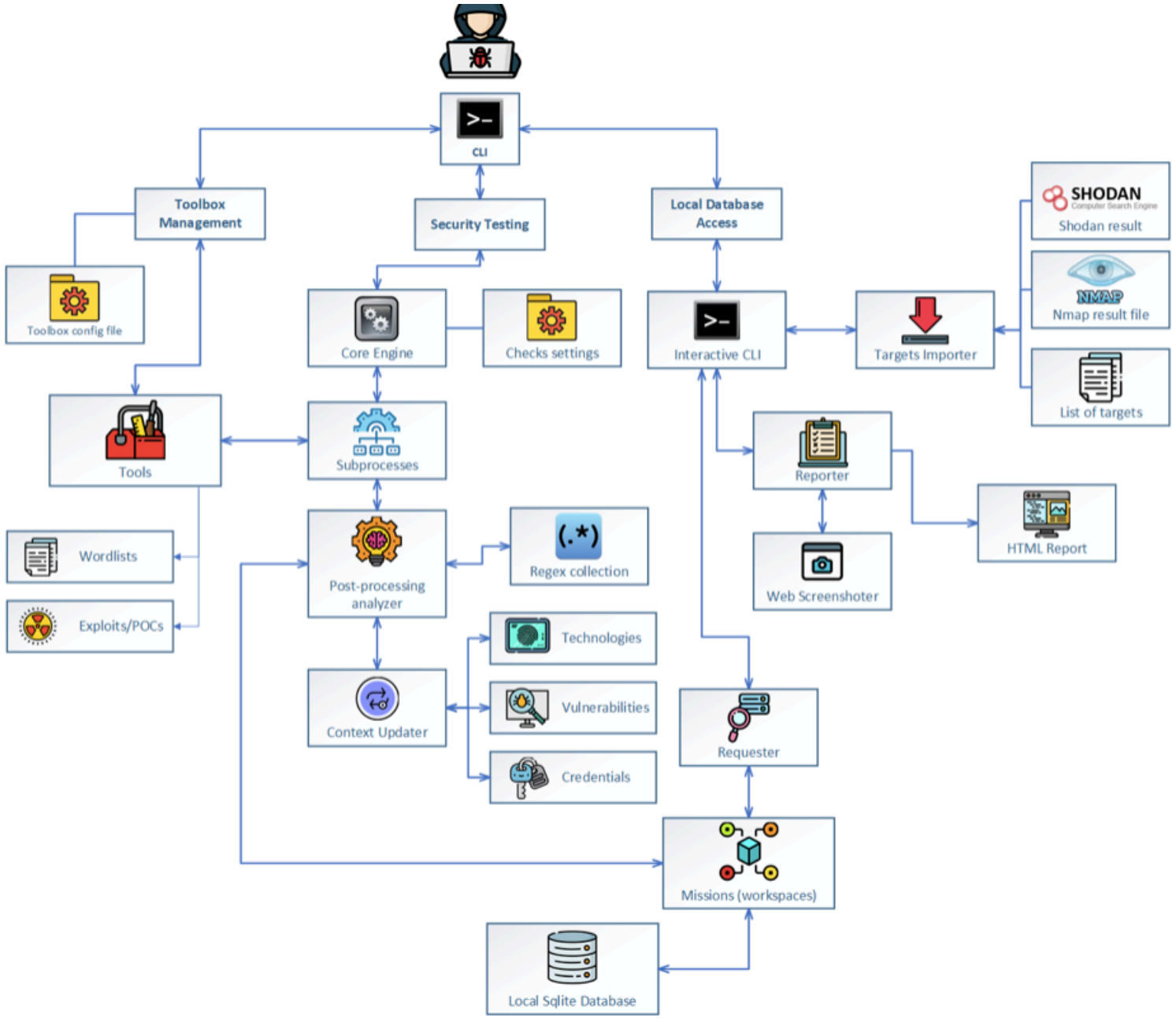


Какие уязвимости можно автоматизировать

- Application error disclosure
- Cookie not HttpOnly flag
- Missing anti-CSRF tokens and security headers
- Private IP disclosure
- Session ID in URL rewrite
- SQL injection
- XSS injection

OTUS
ОНЛАЙН ОБРАЗОВАНИЕ

Jock3r


CLI
Toolbox Management
Security Testing
Local Database Access
Toolbox config file
Core Engine
Checks settings
Interactive CLI
Targets Importer
SHODAN
Computer Search Engine
Shodan result
NMAP
Nmap result file
List of targets
Tools
Subprocesses
Reporter
HTML Report
Wordlists
Exploits/POCs
Post-processing analyzer
Regex collection
Web Screenshoter
Technologies
Vulnerabilities
Credentials
Context Updater
Requester
Missions (workspaces)
Local Sqlite Database

Jok3r

- Framework для автоматического тестирования
- Предоставляет больше опций, помимо web pentest
- Полный список: https://github.com/koutto/jok3r#id12

Wapiti

Список уязвимостей

- Command Execution detection
- CRLF injection
- Database injection
- File disclosure
- Shellshock or Bash bug
- SSRF (Server Side Request Forgery)
- Weak .htaccess configurations that can be bypassed
- XSS injection
- XXE injection

OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ

w3af

Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр