**Osint** – для создания карточки , Первый взгляд на компанию , сбор информаций. Имеет отношение one to many с классом Pentest для того чтобы не терять связь между классами .

***-- Имеет свой отчет –***

***-- Имеет место быть в отчете по пентесту для общей инфы –***

**Pentest –** Главный класс для отчета , в себе имеет информацию о компаний , доп документы по тесту , имеет .txt документы логов , логи берутся из консоли встроенной в интерфейс каждого документа класса. Есть проверки на базовые типы атак.

* **Pentest ( passive ) – Пасивная часть отчета “ Сбор информаций как можно больше”, имеет поля такие как :**
  1. **Название**
* **Pentest ( active ) – Активная чать теста ИС в которой проходит непосретсявенная попытка войти в систему , имеет поля такие как :**
  1. **Название**

***-- Имеет свой отчет –***

***-- Главная ось всего отчета –***

***Методолгий для пентеста.***

***OWASP***

***Open Web Application Security Project (OWASP)*** — открытое интернет-сообщество, которое предлагает самую исчерпывающую методологию для тестирования приложений, сайтов и API. Документация OWASP полезна любой ИТ-компании, которая заинтересована в создании безопасного программного обеспечения.

Одно из главных преимуществ OWASP в том, что методология описывает тестирование на каждой стадии жизненного цикла разработки приложений: определение требований, проектирование, разработка, внедрение и поддержка. При этом тестируются не только сами приложения, но и технологии, процессы, а также люди. Второе важное преимущество: OWASP могут применять как пентестеры, так и веб-разработчики.

***ISSAF***

***Information System Security Assessment Framework (ISSAF)*** разработан Open Information Systems Security Group (OISSG). Документ охватывает большое количество вопросов, связанных с информационной безопасностью. В ISSAF приведены подробные рекомендации по тестированию на проникновение. Описаны утилиты, которыми можно провести пентест, указания по их использованию, а также подробно разъяснено, какие результаты и при каких параметрах можно получить в результате тестирования.

ISSAF считается достаточно сложной и подробной методологией, которую можно адаптировать для проверки информационной безопасности любой организации. Каждый этап тестирования согласно ISSAF тщательно документируется. Также даны рекомендации по использованию конкретных инструментов на каждом из этапов.

***PTES***

***Penetration Testing Methodologies and Standards (PTES)*** предлагает рекомендации для проведения базового пентеста, а также несколько расширенных вариантов тестирования, для организаций с повышенными требованиями к информационной безопасности. Одно из преимуществ PTES в том, что он дает подробное описание целей и ожиданий от пентеста.

Основные этапы PTES:

* Обследование (Intelligence Gathering)
* Моделирование угроз
* Анализ уязвимостей
* Эксплуатация уязвимости
* Составление отчета

В PTES также содержится руководство по выполнению повторного, или постэксплуатационного, тестирования. Это помогает определить, насколько эффективно были закрыты выявленные уязвимости.