Функциональные характеристики программы

Управление пользователями и ролями:

- Возможность регистрации и авторизации пользователей.
- Настройка ролей и уровней доступа для пользователей, таких как Администратор, Менеджер компании и Клиент.
- Управление учетными записями на основе ролей пользователей (создание, изменение, удаление учетных записей, управление правами доступа).
- Доступен функционал личного кабинета пользователя с возможностью изменить пароль, сбросить двухфакторную аутентификацию, а также редактировать данные собственного профиля.
- Ведение журнала действий пользователей для аудита и безопасности.

Управление объектами сканирования:

- Добавление и удаление объектов (целей) сканирования, просмотр подробной информации об объектах (целях) сканирований.
- Создание и управление списком доменов, IP-адресов и других ресурсов для сканирования.
- Поддержка нескольких типов объектов сканирования, включая веб-приложения, серверы, сетевые устройства.
- Визуализация состояния объектов сканирования, включая историю проведенных сканирований, детали адресов, профили сканирования, статус и сводку угроз, а также детали сканирования по каждому объекту.
- Возможность задания приоритетов и категорий для объектов сканирования.
- Управление (создание, изменение, удаление) коллекциями ресурсов сканирования.

Выполнение сканирований:

- Запуск сканирования для обнаружения уязвимостей в сетевой инфраструктуре, веб-приложениях и других ресурсах.
- Поддержка различных типов сканирования, включая сканирование портов, проверку безопасности веб-приложений и поиск уязвимостей.
- Формирование отчета о каждом просканированном объекте, возможность просмотра детального отчета.
- Обработка и анализ результатов сканирования с выделением критичных уязвимостей.
- Управление (создание, изменение, удаление) профилями сканирования.

Типы сканирования:

1) **Полное сканирование:** Комплексный анализ веб-ресурсов для выявления всех возможных уязвимостей.
2) **Критичные уязвимости высокой опасности:** Обнаружение уязвимостей с высоким уровнем риска, таких как несанкционированный доступ и утечка данных.
3) **Критичные уязвимости средней опасности:** Обнаружение уязвимостей со средним уровнем риска, таких как возможные сценарии атак с ограниченным воздействием.
4) **Межсайтовые скрипты (XSS):** Проверка на наличие уязвимостей, связанных с межсайтовыми скриптами, которые могут привести к краже данных или компрометации пользователя.
5) **SQL-инъекции:** Проверка на наличие уязвимостей, связанных с SQL-инъекциями, которые могут привести к утечке или изменению данных в базе данных.
6) **Слабые пароли:** Проверка на наличие уязвимостей, связанных с использованием слабых паролей, что может привести к несанкционированному доступу.
7) **Кросс-сканирование:** Обнаружение уязвимостей, связанных с кросс-сканированием и анализом связей между различными ресурсами.
8) **OWASP Top 10:** Проверка на соответствие уязвимостей списку OWASP Top 10, который включает наиболее критичные угрозы безопасности веб-приложений.
9) **Проверки PCI:** Проверка на соответствие стандартам PCI DSS для защиты данных платежных карт.
10) **SANS Top 25:** Проверка на уязвимости из списка SANS Top 25, представляющие наибольшую опасность для программного обеспечения.
11) **Вредоносное ПО:** Выявление и анализ вредоносного ПО, которое может скомпрометировать системы и данные.
12) **Сканирование TCP портов:** Выполнение проверки состояния TCP портов на целевых хостах, включая определение открытых, закрытых и фильтруемых портов, а также выявление угроз, связанных с уязвимыми сервисами и неправильно настроенными портами.
13) **Сканирование UDP портов:** Выполнение проверки состояния UDP портов, включая определение доступных сервисов и их состояния, а также выявление угроз, связанных с открытыми или неправильно настроенными портами.

Отчеты и аналитика:

- Генерация детализированных отчетов по результатам сканирования, включая описание выявленных уязвимостей, их серьезность и рекомендации по устранению.
- Экспорт отчетов в различные форматы (Excel, PDF, CSV) для последующего анализа и предоставления внешним заинтересованным сторонам.
- Анализ тенденций уязвимостей и оценка рисков для конкретных ресурсов или групп ресурсов.
- Визуализация данных через графики и диаграммы для удобного восприятия информации.

- Возможность создания специальных запросов, используемых для поиска уязвимостей и информации в системах поиска.

Уведомления и оповещения:

- Настраиваемая система уведомлений о результатах сканирования, появлении новых уязвимостей или важных изменениях в состоянии системы.
- Поддержка отправки уведомлений по электронной почте, SMS или через другие интегрированные каналы связи.
- Настройка триггеров и условий для отправки уведомлений (например, при обнаружении критической уязвимости).
- История отправленных уведомлений и событий.

Планирование и автоматизация:

- Возможность создания расписаний для регулярного выполнения сканирований.
- Автоматическое обновление базы данных уязвимостей с новыми сведениями о угрозах и методах их устранения.
- Скрипты для автоматического развертывания и настройки сканеров на различных платформах и окружениях.
- Автоматическое назначение задач сканирования на доступные ресурсы.
- Возможность ручного или автоматического запуска сканирования по расписанию.
- Управление (создание, изменение, удаление) сканированием по расписанию (периодическое и единоразовое отложенное сканирование).

Управление пользовательским интерфейсом:

- Возможность выбора языка интерфейса (русский, английский).
- Разные темы оформления графического интерфейса («светлая», «темная»).
- Настройка отображения результатов в виде таблиц (выбор видимых столбцов).