МЕТОДИКА ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

JET SECURITY TEAM

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Общая организационная информация	
1.	Автоматическое обновление базы уязвимостей по сети	1.Доступными в решении средствами убедиться в актуальности базы уязвимостей	Решение позволяет обновлять базу уязвимостей по сети в автоматическом режиме
2.	Офлайн обновления базы уязвимостей сканера	1. На выделенном (изолированном) сканере обновить базу уязвимостей без подключения к Интернету 2. Убедиться что база уязвимостей актуальна	Решение позволяет проводить офлайн обновления базы уязвимостей
3.	Открытый доступ к базе уязвимостей в продукте	1.Доступными в решении средствами убедиться в возможности просмотра всех имеющихся в базе уязвимостей	Решение позволяет просматривать все уязвимости в базе
4.	Централизованное управление через веб-интерфейс	1. Убедиться в доступности веб-интерфейса для управления решением 2. Проверить возможность управления всеми компонентами системы через веб-интерфейс	Решение предоставляет возможность управления всеми компонентами системы через веб-интерфейс
5.	Возможность установки агентов на хосты	1. Произвести установку агента на хосты (Linux, Windows)	Решение позволяет устанавливать агенты на хосты
6.	Возможность обновления агентов встроенным механизмом продукта	1. В интерфейсе решения запустить обновления агентов 2. Убедиться, что на хостах агент обновлен	Решение позволяет обновлять агенты встроенным механизмом продукта
7.	Возможность работы в частично или полностью изолированных сегментах сети	1. Убедиться, что сканер не имеет доступа в Интернет 2. Произвести сканирование изолированного сегмента с конфигурацией для изолированного сегмента	Решение позволяет производить сканирование изолированного сегмента с обновленной базой уязвимостей
8.	Поддержка мультиязычности	1.Убедиться, что в решении есть возможность выбора языка интерфейса во время установки или в интерфейсе управления	Решение предоставляет возможность выбора языка, при этом, в перечне поддерживаемых языков присутствует русский язык
9.	Наличие сертификата ФСТЭК и присутствие решения в реестре отечественного ПО	1. На сайте ФСТЭК найти сертификат решения 2. Найти решение в реестре отечественного ПО	1. Решение имеет действующий сертификат ФСТЭК 2. Решение присутствует в реестре отечественного ПО
10.	Возможность поставки от производителя в виде программно-аппаратного комплекса	1. Убедиться в наличии поставки в виде программно-аппаратного комплекса	Решение поставляется в виде программно-аппаратного комплекса
		Управление активами	
11.	Построение интерактивной карты сети	1. По результатам сканирований построить интерактивную карту сети	Решение позволяет строить интерактивную карту сети
12.	Создание динамических групп активов	1. Создать динамическую группу с любым критерием (например, версия ОС) 2. Изменить критерий, убедиться, что состав группы изменился	Решение позволяет создавать динамические группы активов
13.	Поиск по группам активов	1. Произвести поиск по имени группы 2. Произвести поиск актива в определенной группе	Решение позволяет производить поиск по группам активов
14.	Кастомизация карточки актива	1. Добавить кастомное поле в карточку актива	Решение позволяет добавлять кастомные поля в карточки актива

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
15.	Скоринг активов: расчет уровня критичности	1. Задать уровень критичности актива	Решение выполняет скоринг активов в части расчета уровня критичности
16.	Дедупликация данных об активах	1. Убедиться что в результатах сканирования нет дубликатов активов	Решение не создает и не хранит дубликаты активов
17.	Создание пользовательских отметок (тегов)	1. Для актива установить тег	Решение поддерживает установку пользовательских отметок (тегов) для активов
18.	Хранение истории изменения актива	1.Открыть журнал изменений/карточку актива 2.Проверить наличие записей о добавлении, изменении или удалении информации об активе (например, конфигурация актива, уязвимость актива, пользовательские отметки)	Решение хранит полную историю изменения активов
19.	Запуск административных действий/команд, выполняемых на активах	1.Проверить возможность выполнения/получения результатов по командам/действиям средствами решения(например, выключить/перезагрузить хост, запустить/остановить/перезапустить службу, остановить процесс, получить информацию по утилизации CPU, RAM и т.д.)	Решение позволяет выполнять преднастроенные или произвольные автоматизированные действий по администрированию активов и получению дополнительной информации
	Настройка общих правил и логики системы		
20.	Импорт и экспорт политики и результатов сканирования между инсталляциями в рамках одного решения	1. Произвести импорт и экспорт политик сканирования и результатов сканирования в доступном формате 2. Убедиться, что эти данные доступны для обмена между инсталляциями	Решение позволяет импортировать и экспортировать данные между инсталляциями в рамках одного решения
21.	Создание и управление задачами на устранение уязвимостей	1.Выбрать найденную уязвимость в карточке актива/отчете и инициировать создание задачи на устранение 2.Убедиться в наличии статусов задач (например: "Новая", "В работе", "Закрыта") 3.Подтвердить возможность массового создания и редактирования задач	Решение позволяет формировать и управлять задачами на устранение уязвимостей
22.	Назначение ответственных для задачи на устранение уязвимостей	1. Выбрать уязвимость и создать задачу на устранение 2. Проверить наличие поля для выбора ответственного лица или группы	Решение позволяет назначать ответственных для задачи на устранение уязвимостей
23.	Настройка правил отправки оповещений о сканированиях	1. Для ранее созданного расписания, настроить отправку уведомлений о завершении сканирования	Решение позволяет отправлять уведомление о завершении сканирования
24.	Поддержка сквозного поиска, фильтрации, сортировки по активам и уязвимостям	1. Произвести поиск по названию уязвимости 2. В результатах поиска произвести фильтрацию и сортировку по доступным параметрам	Решение имеет функционал сквозного поиска, фильтрации и сортировки по активам и уязвимостям
25.	Функционал патч-менеджмента	1. Открыть карточку объекта и выбрать уязвимость, для которой возможно устранение посредством установки патча 2. Запустить установку патча безопасности из интерфейса решения 3. По результатам установки патча, провести повторное сканирование и убедиться в устранении уязвимости	Решение имеет функционал патч-менеджмента
26.	Автоматизация управления параметрами уязвимости (например, перерасчет критичности, срока, способа устранения)	1. Создать правило для автоматического изменения параметров уязвимости 2. Убедиться в применении правила	Решение позволяет настроить правила автоматической смены параметры уязвимости
27.	Визуализация данных в виде настраиваемых виджетов и дашбордов	1. В интерфейсе решения создать дашборд/виджет	Решение имеет функционал построения виджетов и организации дашбордов

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
28.	Возможность создания и экспорта пользовательских отчетов	1.Перейти в настройки формирования отчетов 2.Проверить возможность настройки состава данных (уязвимости, активы, статусы) 3.Подтвердить поддержку экспорта в нужные форматы (например, PDF, DOCX, XLSX и др.)	Решение имеет возможность создания пользовательских отчетов
29.	Выпуск отчетов по расписанию	1.Перейти в настройки формирования отчётов 2.Установить расписание выпуска отчета 3.Проверить выпуск отчёта в заданное время	Решение позволяет выпускать отчеты по расписанию
		Поддерживаемые типы активов для сканирования	
30.	Поддержка сканирования ОС: Windows Server, Windows ARM, Astra Linux, Alma Linux, Ubuntu, РедОС, Debian	1.Создать задачи на сканирование данных типов активов в режиме пентест (сканирование без аутентификации) и аудит (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита и пентеста для данных типов активов	Решение поддерживает сканирование обозначенных типов активов
31.	Поддержка сканирования сетевого оборудования	1.Создать задачи на сканирование данных типов активов в режиме пентест (сканирование без аутентификации) и аудит (сканирование с аутентификацией). 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита и пентеста для данных типов активов	Решение поддерживает сканирование обозначенных типов активов
32.	Поддержка идентификации периферийных устройств (например, камеры, IP-телефония, принтеры)	1.Создать задачи на сканирование сети, в которой присутствуют данные типы активов 2. Запустить задачу и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы	Решение поддерживает сканирование обозначенных типов активов
33.	Поддержка сканирования СУБД (например, Oracle, PostgreSQL, MSSQL)	1.Создать задачи на сканирование данных типов активов в режиме аудит (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита для данных типов активов	Решение поддерживает сканирование обозначенных типов активов
34.	Поддержка сканирования серверного ПО (например, веб-серверы, службы каталогов, почтовые сервера, системы виртуализации)	1.Создать задачи на сканирование данных типов активов в режиме аудит (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита для данных типов активов	Решение поддерживает сканирование обозначенных типов активов

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
35.	Сканирование промышленных систем управления (ICS/SCADA)	1.Создать задачи на сканирование данных типов активов в режиме аудит (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита для данных типов активов	Решение поддерживает сканирование обозначенных типов активов
36.	Инвентаризация и поиск уязвимостей в контейнерах	1. Настроить задачу для сканирования контейнеров 2. Получить результаты сканирования с найденными уязвимостями в контейнерах	Решение позволяет получить информацию о контейнерах и найденных в них уязвимостей
		Возможности интеграции	
37.	Наличие документированного API	1. В документации производителя найти информацию об использовании API 2. Получить список активов средствами API	В документации есть подробное описание API(Endpoint, авторизация, примеры использования) API позволяет создавать и запускать задачи, получать результаты сканирований
38.	Разграничение доступа для API-ключей	1. При создании API ключа, убедиться в возможности разграничения доступа	Решение позволяет разграничивать доступ для API ключей
39.	Возможность интеграции с системами мониторинга работоспособности	1. Проверить наличие возможности интеграции с системами мониторинга работоспособности	Решение позволяет настраивать интеграцию с системами мониторинга работоспособности
40.	Поддержка доменной авторизации	1. Настроить подключение к службе каталогов 2. Проверить возможность авторизации под доменной УЗ	Решение позволяет выполнять сканирование ресурсов, авторизацию в решении с использованием доменных УЗ, взятых из службы каталогов
41.	Интеграция с Service Desk/ITSM системами	1. Проверить наличие возможности интеграции с Service Desk/ITSM системами в интерфейсе решения	Решение позволяет настраивать интеграцию с Service Desk/ITSM системами
42.	Интеграция с SIEM в части отправки событий	1. Проверить наличие возможности отправки событий журналов аудита Системы в SIEM	Решение позволяет настраивать интеграцию с SIEM
43.	Функционал получения данных об активах из смежных систем (например, из службы каталогов, среды виртуализации, SIEM-системы, смежных сканеров)	1. Выполнить импорт активов из смежной системы 2. Убедиться в корректном отображении и актуальности полученных данных	Решение имеет функционал получения данных об активах из смежных систем
		Управление сканированием и уязвимостями	
44.	Кастомизация карточки уязвимости	1.Перейти в настройки интерфейса или карточки уязвимости 2.Проверить возможность добавления/удаления полей	Решение позволяет кастомизировать карточку уязвимости
45.	Расписание сканирований	1. Настроить запуск задания по расписанию 2. Убедиться в запуске задачи в указанное время	Решение позволяет проводить сканирования по расписанию
46.	Поиск уязвимостей без повторного сканирования хостов (ретро-скан)	1. Убедиться, что решение выявляет новые уязвимости без необходимости проведения повторного сканирования	Решение позволяет находить уязвимости без необходимости проведения повторного сканирования
47.	Настройка "технологических окон" для активов	1.Установить "технологическое окно" для актива 2. Убедиться, что актив сканируется согласно технологическому окну	Решение позволяет настраивать "технологические окна" для активов
48.	Сканирование в режиме brute force для возможности перебора паролей в целевых системах	1. Создать задачу для подбора пароля к RDP и SSH по словарю 2. Убедиться, что пароль подобран	Решение позволяет производить подбор паролей

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
49.	Настройка правил и логики профилей сканирования	1. Создать новый профиль сканирования 2. Изменить настройки правил и логики нового профиля	Решение позволяет производить настройку правил и логики профилей сканирования
50.	Настройка сканирования (выбор диапазонов подсетей/IP-адресов/портов)	Создать задачу сканирования с указанием подсетей/IP-адресов/портов	Решение позволяет сканировать указанные подсети/IP-адреса/порты
51.	Добавление исключений при сканировании (например, уязвимость, порт, ПО)	1. Провести сканирование актива 2. Добавить в исключение одну из найденных уязвимостей 3. Провести повторное сканирование и убедиться в отсутствии исключенной уязвимости	Решение позволяет добавлять исключения при сканировании
52.	Описание последствий эксплуатации уязвимости в карточке	В результатах ранее проведенного сканирования найти соответствующую информацию о последствиях эксплуатации уязвимости	Решение предоставляет информацию о последствиях эксплуатации уязвимостей в карточке уязвимости
53.	Ведение и отображение идентификаторов уязвимостей (CVE, NVD, БДУ, CPE, CWE).	Убедиться, что в результатах присутствует информация о CVE, CPE, CWE и БДУ для уязвимостей	Решение предоставляет информацию о CVE, CPE, CWE и БДУ для уязвимостей
54.	Поддержка CVSS версий 2/3/4 и возможности задания кастомных метрик CVSS	1. Убедиться, что в данных об обнаруженных уязвимостях есть оценка критичности по CVSS разных версий 2. Убедиться, что есть возможность задания кастомных метрик для CVSS (Например, критичность актива в инфраструктуре, влияние на бизнес-процессы и т.п.)	Решение предоставляет информацию об обнаруженных уязвимостях с указанием оценки критичности по CVSS разных версий
55.	Добавление собственной проверки уязвимостей	1. Создать собственную проверку 2. Запустить сканирование с данной проверкой и убедиться в корректности работы	Решение позволяет добавлять собственные проверки
56.	Настраиваемый скоринг уязвимостей	В результатах сканирования изменить критичность уязвимости	Решение позволяет настраивать критичность уязвимости
57.	Проверка эксплуатируемости уязвимости	Убедиться, что уязвимость отмечается в ПО, как имеющая эксплойт	Решение позволяет проверить эксплуатируемость уязвимости
58.	Дедупликация данных об уязвимостях	1. Найти в результатах сканирования актива уязвимости с дублями (например дубликаты уязвимостей для разных сервисов) 2. Убедиться, что для дубликатов, в карточках уязвимостей есть уникальные поля, позволяющие однозначно идентифицировать ее - что уязвимости не являются полной копией друг друга	Решение позволяет дедуплицировать данные об уязвимостях
59.	Ссылки на внешние сервисы в карточке уязвимости (NVD, Vulners.com, Exploit-DB, БДУ ФСТЭК)	Проверить наличие информации или ссылки на внешние источники в карточке уязвимости	Решение предоставляет детальную информацию в карточке уязвимости
60.	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК	В результатах сканирования найти рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК или ссылки на источник	Решение предоставляет рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК
61.	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ	1. В результатах сканирования найти рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ или ссылки на источник	Решение предоставляет рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ
62.	Расчет критичности уязвимости по методике ФСТЭК	1. Убедиться в наличии расчета критичности уровня уязвимости по методике ФСТЭК	Решение позволяет рассчитывать критичность уязвимости по методике ФСТЭК
63.	Проверка обновлений Windows (KB) по БДУ ФСТЭК	1. Убедиться, что в интерфейсе решения, предлагаемое к установке обновление Windows протестировано ФСТЭК	Решение позволяет проверять обновления Windows (KB) по БДУ ФСТЭК

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
64.	Оповещения о событиях в Системе (например, появления нового актива, важной уязвимости на активе, обновление базы уязвимостей)	1. Настроить уведомление для события (например, новый актив, критическая уязвимость, обновление базы) 2. Указать каналы уведомлений (например, email, webhook, интеграция с SIEM/сервис-деском) 3. Имитировать событие 4. Проверить получение уведомления	Решение позволяет настраивать оповещения о событиям в Системе
		Оценка соответствия	
65.	Проверка активов на соответствие предустановленным стандартам защищённой конфигурации	1. Провести сканирование и проверить активы на соответствие стандартам. 2. Проанализировать результаты. По выходным данным можно однозначно оценить: - Критичность проверки; - Результат проверки (соответствие/несоответствие)	1. Решение позволяет проводить проверку соответствия требованиям 2. В предустановленных стандартах присутствуют CIS, ГОСТ, ISO 27001, PCI DSS, внутренние стандарты от вендора
66.	Формирование пользовательских проверок для актива	1. Создать пользовательскую проверку соответствия. 2. Выполнить задачу с использованием пользовательской проверки.	Решение позволяет создавать пользовательские проверки
67.	Точечная переоценка по активу	1. Для ранее просканированного актива произвести переоценку	Решение имеет функционал точечной переоценки по активу
68.	Ведение истории оценки соответствия	1. Для актива из существующей проверки на соответствие отобразить историю оценки	В решении имеется возможность отслеживать историю оценки соответствия
		Безопасность и надежность	
69.	Разграничение прав доступа к объектам решения	1. Создать роль имеющую доступ к информации об уязвимостях одной группы активов	Решение позволяет ограничивать права доступа к объектам решения
70.	Возможность настройки парольной политики - настраиваемая сложность пароля (буквы, цифры, заглавные, спецсимволы) - история ранее заданных паролей - минимальная длина паролей - время жизни пароля	1.Настроить требования (буквы, цифры, заглавные, спецсимволы) и проверить принятие/отклонение тестовых паролей 2.Сменить пароль несколько раз и убедиться, что старые пароли блокируются 3. Установить минимальную длину пароля (например, 8 символов) и проверить отклонение коротких паролей 4. Настроить срок действия пароля и убедиться, что система требует смены пароля вовремя	Настройки парольной политики работают корректно
71.	Шифрование критичных данных (в т.ч. с использованием пользовательских ключей шифрования)	1. Получить доступ к БД 2. Убедиться, что настройки УЗ для сканирований находятся в зашифрованном виде 3. Убедиться, что можно задать пользовательский ключ шифрования	Решение хранит настройки в зашифрованном виде или доступ к ним невозможен
72.	Создание и восстановления из резервной копии системы	1. Произвести резервное копирование посредством внутреннего функционала решения 2. Провести восстановление из резервной копии	Решение позволяет создавать и восстанавливать из резервной копии системы
73.	Принудительная смена паролей	1. Назначить принудительную смену пароля для ранее созданного пользователя 2. Авторизоваться от имени этого пользователя	В решении реализована принудительная смена пароля
74.	Механизмы блокировки учетных записей после нескольких неудачных попыток входа	1. Настроить блокировку пользователей после 5 неудавшихся авторизаций 2. Попробовать авторизоваться 5 раз с неверным паролем 3. Проверить статус этого пользователя в интерфейсе решения	В решении реализована блокировка пользователей при неудачной авторизации
75.	Интеграция с системами хранения секретов в части хранения учетных записей для сканирования (например, HashiCorp Vault)	1. Проверить возможность интеграции с системами внешнего хранения секретов в части хранения учетных записей для сканирования	Решение позволяет хранить учетные записи во внешнем хранилище

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Производительность и эффективность	
76.	Скорость обнаружения новых уязвимостей: Время между появлением новой уязвимости в публичных базах (например, NVD, БДУ ФСТЭК) и её добавлением в сканер	1. Зафиксировать новые опубликованные уязвимости в публичных базах. 2. Зафиксировать время появления уязвимостей в базе решения.	Время обнаружения новых уязвимостей зафиксировано и оно менее 24 часов
77.	Настройка интенсивности сканирования	1. Для задачи из ранее настроенной проверки настроить меньшую интенсивность сканирования 2. Произвести повторное сканирование 3. Сравнить время сканирования и полноту информации с результатами предыдущей итерации	Решение имеет функционал настройки интенсивности сканирования
78.	Поддержка сканирования геораспределенных филиалов, мультитенантность	1.Проверить наличие функции распределённых или удалённых сканеров 2.Настроить удалённые сканеры в разных филиалах или сетях 3.Убедиться в возможности централизованного управления сканированием 4.Проверить поддержку мультитенантности: создать отдельные среды / клиентов 5.Выполнить тестовое сканирование в разных сегментах и убедиться в изоляции данных	Решение поддерживает сканирование геораспределенных филиалов и мультитенантность
		Сканирование веб-ресурсов	
79.	Проверка OWASP Top 10	1. Настроить сканирование веб-приложения на уязвимости. В качестве целей указать сервера с уязвимыми приложениями 2. Произвести сканирование 3. Провести проверку результатов на наличие присутствующих уязвимостей	Решение позволяет выполнять проверку OWASP top 10
80.	Обнаружение WAF	1. В результатах сканирования веб-ресурса защищаемого WAF, проверить, удалось ли решению обнаружить использование WAF	Решение может обнаруживать и тестировать WAF - решения
81.	Возможность аутентификации для глубокого изучения веб-приложений (cookie, логин-пароль, заголовки и их значения)	1. Настроить УЗ для сканирования веб-ресурса 2. Провести сканирование и убедиться, что сканирование с аутентификацией прошло успешно	Решение может аутентифицироваться на сайтах при сканировании
82.	Сканирование в режиме поиска поддоменов	1. Запустить задачу на сканирование в режиме поиска поддоменов	Решение имеет функционал сканирования в режиме поиска поддоменов
83.	Поиск скрытых файлов и папок (dirsearch)	1. Запустить веб-сканирование сайта или приложения 2. В настройках активировать функцию поиска скрытых ресурсов (dirsearch/brute-force директорий) 3. Проверить результаты: наличие найденных скрытых файлов/папок	Решение имеет функционал поиска скрытых файлов и папок
84.	Обнаружение уязвимостей типа «Cross-Site Request Forgery»	1. В результатах сканирования найти уязвимостей типа «CSRF»	Решение обнаруживает уязвимости типа «CSRF»
85.	Сканирование в режиме атаки	1. Произвести сканирование веб-ресурса в режиме атаки 2. Получить результаты эксплуатации уязвимостей. 3. Убедиться, что в результатах доступна информация о полученных данных в ходе эксплуатации уязвимостей (например, ответ веб-сервера).	Решение имеет функционал сканирования ресурсов в режиме атаки

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
86.	Обнаружение уязвимостей типа «Code & Command Injection»	1. В результатах сканирования найти уязвимости типа «Code & Command Injection» Например, Server Side Code Injection, Remote OS Command Injection, SQL Injection, LDAP Injection, Command Injection, XPath Injection, Server Side Include, Insecure Deserialization	Решение обнаруживает уязвимости типа «Code & Command Injection»
87.	Обнаружение уязвимостей, связанных с загрузкой файлов и доступом к файловой системе	1. В результатах сканирования найти уязвимости, связанные с загрузкой файлов и доступом к файловой системе Например, Remote File Inclusion, Path Traversal, File Upload Vulnerabilities	Решение обнаруживает уязвимости, связанные с загрузкой файлов и доступом к файловой системе
88.	Обнаружение уязвимостей типа «Client-Side Attacks»	1. В результатах сканирования найти уязвимостей типа «Client-Side Attacks» Например, XSS (Cross-Site Scripting), Script ActiveX Object	Решение обнаруживает уязвимости типа «Client-Side Attacks»
89.	Обнаружение уязвимостей типа «Redirection & Resource Access»	1. В результатах сканирования найти уязвимости типа «Redirection & Resource Access» Например, Open Redirect (External Redirect), Server Side Request Forgery (SSRF), XML External Entity (XXE), Cross-Domain Misconfiguration (CORS))	Решение обнаруживает уязвимости типа «Redirection & Resource Access»
90.	Обнаружение уязвимостей типа «Cryptographic Weaknesses»	1. В результатах сканирования уязвимости типа «Cryptographic Weaknesses» Например, Weak Cipher Suite, Heartbleed (OpenSSL))	Решение обнаруживает уязвимости типа «Cryptographic Weaknesses»
91.	Обнаружение уязвимостей типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)»	1. В результатах сканирования найти уязвимости типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)» Например, Insecure Referrer Policy Header, Content Security Policy (CSP) Missing, X-Content-Type-Options Header Missing, X-Frame-Options Header Missing, X-Permitted-Cross-Domain-Policies Header Missing, X-XSS-Protection Header Missing, Strict-Transport-Security Header Missing, Incomplete or No Cache-control and Pragma HTTP Header Set	Решение обнаруживает уязвимости типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)»
92.	Обнаружение уязвимостей типа «Information Disclosure»	1. В результатах сканирования найти уязвимости типа «Information Disclosure» Например, PII Disclosure, Information Disclosure, Private IP Disclosure, Sensitive Information in HTTP Headers, Insecure Content	Решение обнаруживает уязвимости типа «Information Disclosure»
93.	Обнаружение уязвимостей типа «Cookie Security Issues»	1. В результатах сканирования найти уязвимости типа «Cookie Security Issues» Например, Cookie No HttpOnly Flag, Cookie No Secure Flag	Решение обнаруживает уязвимости типа «Cookie Security Issues»
94.	Обнаружение уязвимостей типа «Memory Corruption»	1. В результатах сканирования найти уязвимости типа «Memory Corruption» Например, Buffer Overflow, Format String, Integer Overflow	Решение обнаруживает уязвимости типа «Memory Corruption»