Версия документа: 002-2024

Инструкция по эксплуатации системы «ASPM Platform»

Москва, 2024

Содержание

1. Общие сведения

1.1 Назначение и краткая характеристика системы

ASPM Platform (далее – платформа, система) позволяет проводить комплексный анализ приложений для обеспечения безопасности и централизованного управления процессами обнаружения и устранения уязвимостей. Платформа обеспечивает взаимодействие между командами разработки и специалистами по безопасности, способствуя совместному выявлению и устранению уязвимостей на всех этапах жизненного цикла продукта.

Платформа поддерживает работу со следующими классами решений:

- SAST;
- IAC;
- OSA;
- SCA;
- DAST;
- API fuzzing;
- BCA.

Сканирование продукта включает в себя 4 ключевых этапа:

a) Настройка и запуск анализа. На этом этапе производится конфигурация инструментов и автоматический запуск анализа приложения.

b) Агрегация и корреляция данных. По результатам проведенного анализа данные централизованно собираются в едином репозитории для последующей обработки. Далее платформа осуществляет корреляцию уязвимостей, выявленных на разных уровнях анализа, что помогает

определить взаимосвязи между ними и их совокупное влияние на безопасность приложения.

c) Оценка рисков и генерация рекомендаций. Платформа предоставляет интерфейс для обработки найденных уязвимостей, осуществляет замену исходных данных значениями, соответствующими заданным правилам из внутренней базы, обеспечивая единый механизм оценки и управления уязвимостями.

d) Создание отчетов и интеграция с другими системами. Платформа автоматически формирует отчеты о результатах проведенного анализа, выявленных уязвимостях и предложенных мерах по их устранению.

В результате система позволяет не допустить включения в состав разрабатываемых приложений уязвимых компонентов, исключить использование уязвимого функционала, определить ошибочную и вредоносную программную логику.

2. Авторизация на Платформе

Первичная авторизация начинается с получения письма о создании аккаунта[1]. Кнопка **«Перейти на платформу»** в письме служит для быстрого перехода к странице дальнейшей регистрации.

После перехода по ссылке в письме укажите код регистрации, также представленный в письме. Также задайте пароль учетной записи, соблюдая требования политики безопасности, указанные на экране.

После выполнения вышеуказанных действий при каждой последующей авторизации на Платформе будут требоваться соответствующие учетные данные – E-mail и созданный пароль.

[1] Для получения учетной записи обратитесь к администратору системы

3. Общая структура Платформы

Веб-интерфейс разделен на следующий набор вкладок, представленных на панели в левой части экрана. Полные наименования каждой вкладки отображаются при наведении курсора мыши.

Краткое описание каждого раздела (вкладки) представлено ниже.

3.1 Статистика

Состоит из следующих функциональных компонентов:

- Графики количества дефектов в разрезе характеристики «Критичность»;
- Общий список всех дефектов на Платформе, поле поиска дефекта по наименованию, а также кнопки вызова контекстного меню фильтра и экспорта содержимого списка;
- Поле фильтрации репозиториев, информация о которых отображается на странице данного раздела.

3.2 Группы

Данный раздел включает в себя группы репозиториев, подлежащих анализу, а также такую сопутствующую информацию, как количество репозиториев и другое.

Каждое из представленных в списке наименований групп является интерактивным и может служить для перехода непосредственно на страницу выбранной группы репозиториев.

На странице группы репозиториев представлена дополнительная информация относительно каждого из репозиториев в группе.

Наименования репозиториев на странице группы также являются интерактивными и может служить для перехода к выбранному репозиторию в разделе «Репозитории» Платформы.

3.3 Репозитории

Раздел включает в себя список всех репозиториев на Платформе, безотносительно проекта (группы). Помимо этого, содержит дополнительную информацию о каждом из репозиториев, такую как количество дефектов (общее, количество проверенных и количество активных дефектов), группу, к которой относится тот или иной репозиторий и другое.

Наименования репозиториев в списке данного раздела являются интерактивными и может служить для перехода на страницу выбранного репозитория.

Поле выбора ветки как один из элементов управления в разделе служит для ограничения содержимого страницы по критерию ветки-источника.

Помимо этого, данная страница дополнительно разделена на следующие вкладки:

- Статистика: Вкладка повторяет функционал раздела «Статистика» Платформы. Отличием является отсутствие фильтра по репозиторию.

- Сканирование: вкладка отображает список произведенных сканирований репозитория, а также дополнительную информацию, такую как дата сканирования, ответственный за сканирование, количество обнаруженных дефектов и другое. Вкладка повторяет функционал раздела «Сканирования» Платформы. Номера сканирований на данной вкладке также

являются интерактивными и может служить для перехода к выбранному сканированию в разделе «Сканирования» Платформы.

- Компоненты: вкладка отображает список компонентов, подверженных уязвимостям. Вкладка повторяет функционал раздела «Компоненты» Платформы.

- Дефекты: вкладка отображает список дефектов всех категорий, за исключением относящихся к категории уязвимостей компонентов программного обеспечения и к категории уязвимостей, связанной с жестким кодированием конфиденциальной информации. Вкладка повторяет функционал раздела «Дефекты» Платформы. Отличается отсутствием переключателя категорий сканеров-источников.

- Секреты: вкладка отображает список дефектов, относящихся к категории уязвимостей, связанной с жестким кодированием конфиденциальной информации. Вкладка повторяет функционал раздела «Секреты» Платформы.

- Опубликованные ресурсы: вкладка отображает список эндпоинтов, доступных по http/https запросам. Список включает в себя эндпоинты, использующие порты 80, 443 и другие. Вкладка повторяет функционал раздела «Опубликованные ресурсы» Платформы.

3.4 Сканирования

Раздел включает в себя список всех сканирований на Платформе, безотносительно репозитория. Помимо этого, содержит дополнительную информацию о каждом из сканирований, такую как дата сканирования, ответственный за сканирование, количество обнаруженных дефектов и другое.

Основная страница раздела также включает в себя такие возможности управления:

- Кнопка **«Создать отчет»** служит для быстрого создания отчета по выбранному сканированию.
- Кнопка **«Фильтр»** служит для вызова контекстного меню фильтра.

Номера сканирований в списке данного раздела являются интерактивными и служат для перехода на страницу выбранного сканирования.

3.5 Дефекты

Раздел включает в себя список дефектов всех категорий, за исключением относящихся к категории уязвимостей компонентов программного обеспечения и к категории уязвимостей, связанной с жестким кодированием конфиденциальной информации безотносительно репозитория. Помимо этого, содержит дополнительную информацию о каждом из дефектов в списке, такую как дата определения дефекта, статус, источник (информация о группе репозиториев, репозитории и ветке, в которых был обнаружен дефект) и другое.

Основная страница раздела также включает в себя такие возможности управления:

- **Поле поиска по наименованию** служит для ограничения содержимого списка по наименованию;
- **Переключатель категории инструментов-источников дефектов** предназначен для ограничения содержимого списка по категории инструментов-источников дефектов;
- Кнопка **«Фильтр»** служит для вызова контекстного меню фильтра.

3.6 Секреты

Раздел включает в себя список дефектов, относящихся к категории уязвимостей, связанной с жестким кодированием конфиденциальной информации. Помимо этого, содержит дополнительную информацию о каждом из дефектов в списке, такую как дата определения дефекта, статус, источник (информация о группе репозиториев, репозитории и ветке, в которых был обнаружен дефект) и другое.

Основная страница раздела также включает в себя такие возможности управления:

- **Поле поиска по наименованию** служит для ограничения содержимого списка по наименованию;
- Кнопка **«Фильтр»** служит для вызова контекстного меню фильтра.

3.7 Компоненты

Раздел включает в себя список компонентов, подверженных уязвимостям. Помимо этого, содержит дополнительную информацию о каждом из компонентов в списке, такую как версия компонента, дата определения дефектного компонента, статус, источник (информация о группе репозиториев, репозитории и ветке, в которых был обнаружен дефект) и другое.

Основная страница раздела также включает в себя такие возможности управления:

- **Поле поиска по наименованию** служит для ограничения содержимого списка по наименованию;
- Кнопка **«Фильтр»** предназначена для вызова контекстного меню фильтра;

- Иконка **«Дерево»** напротив нужного компонента служит для перехода на страницу с графом (деревом) компонентов для конкретного компонента.

3.8 Опубликованные ресурсы

Раздел включает в себя список эндпоинтов, доступных по http/https запросам. Список включает в себя эндпоинты, использующие порты 80, 443 и другие. Помимо этого, содержит дополнительную информацию о каждом из эндпоинтов в списке, такую как дата определения эндпоинта, статус, источник (информация о группе репозиториев, репозитории и ветке, в которых был обнаружен дефект) и другое.

Основная страница раздела также включает в себя такие возможности управления:

- **Поле поиска по наименованию** служит для ограничения содержимого списка по наименованию;
- Кнопка **«Фильтр»** служит для вызова контекстного меню фильтра.

3.9 События

Раздел включает в себя список событий, произошедших на Платформе. Помимо этого, содержит дополнительную информацию о каждом из событий в списке, такую как раздел Платформы, код события, источник события и дату события.

Основная страница раздела также включает в себя такие возможности управления:

- **Поле поиска по наименованию** служит для ограничения содержимого списка по наименованию;
- Кнопка **«Фильтр»** служит для вызова контекстного меню фильтра.

4. Организация рабочего процесса на Платформе

4.1 Основной функциональный интерфейс

Основным функциональным элементом веб-интерфейса платформы выступает всплывающее окно подробного описания элемента списка.

Содержимое данного окна можно разделить на следующие группы:

1. Суммарная информация: включает в себя основные характеристики обнаруженного дефекта, компонента или эндпоинта. Представленный также **Переключатель статуса дефекта** предназначен для отражения фактического состояния дефекта:

- «Не проверено»;
- «Ложно»: дефект отсутствует;
- «Актуально»: дефект присутствует и создает угрозы информационной безопасности.

Состав характеристик может отличаться в зависимости как от типа элемента списка, так и от категории дефекта:

- Для дефектов, обнаруженных SAST-инструментами;
- Для дефектов, обнаруженных DAST-инструментами;
- Для дефектов, обнаруженных сканерам IAC;
- Для секретов;
- Для компонентов;
- Для опубликованных ресурсов;

2. Информация об уязвимости: включает в себя непосредственное описание уязвимости, которую влечет за собой дефект, а также рекомендации по смягчению угроз, возникающих по причине наличия дефекта.

3. Дополнительная информация: включает в себя пример безопасной реализации программного кода (программного кода, лишенного дефекта),

поле для заметок (комментариев), а также информацию об изменениях в описании дефекта.

Кроме того, для дефектов, обнаруженных DAST-инструментами, предоставляется дополнительная информация, такая как объект сканирования, отправленные запросы и полученные ответы.

4.2 Система «горячих» клавиш

На Платформе реализована система «горячих» клавиш для более оперативной обработки дефектов[2]. Схема представлена ниже:

Команда	Действие
A	Установка статуса «Ложно» для дефекта/компонента/эндпоинта, отрытого в окне подробного описания элемента списка.
D	Установка статуса «Актуально» для дефекта/компонента/эндпоинта, отрытого в окне подробного описания элемента списка.
W	Открытие окна подробного описания элемента для дефекта/компонента/эндпоинта выше текущего по списку.
S	Открытие окна подробного описания элемента для дефекта/компонента/эндпоинта ниже текущего по списку.
E	Открытие режима редактирования поля «Описание» в окне подробного описания элемента списка.
F	Открытие режима редактирования поля «Смягчение угроз» в окне подробного описания элемента списка.
G	Переход по ссылке, указанной в поле «Объект» в окне подробного описания элемента списка.

[2] Схема управления реализована для латинских раскладок клавиатуры.

5. Типовые сценарии выполнения работ на Платформе

5.1 Обработка дефектов выбранного репозитория

Алгоритм взаимодействия с Платформой с целью обработки дефектов выбранного репозитория состоит из следующих шагов (этапов):

1. Определение наименования целевого репозитория:

2. Поиск нужного репозитория на Платформе. Альтернативные методы:

- Через раздел «Группы»;

- Через раздел «Репозитории»;

3. Определение порядка обработки дефектов. Альтернативные методы:

- Единым списком на вкладке «Статистика»;

- Последовательная обработка сгруппированных по категориям дефектов на соответствующих вкладках раздела;

4. Обработка каждого дефекта. Последовательность действий:

- Выбор дефекта при помощи нажатия ЛКМ по строке с дефектом. Открывается окно подробного описания элемента списка;

- Ознакомление с описанием дефекта;

- Использование «горячей» клавиши G для перехода к исходному коду, определенному проблемным;

- Проверка наличия (или отсутствия) дефекта в программном коде;

- Возврат к окну подробного описания элемента списка, использование «горячей» клавиши A или D в зависимости от вердикта;

- (При необходимости) Использование «горячих» клавиш E и F открыть режим редактирования соответствующих полей и скорректировать информацию.

- Использование «горячей» клавиши S для перехода к следующему дефекту.