

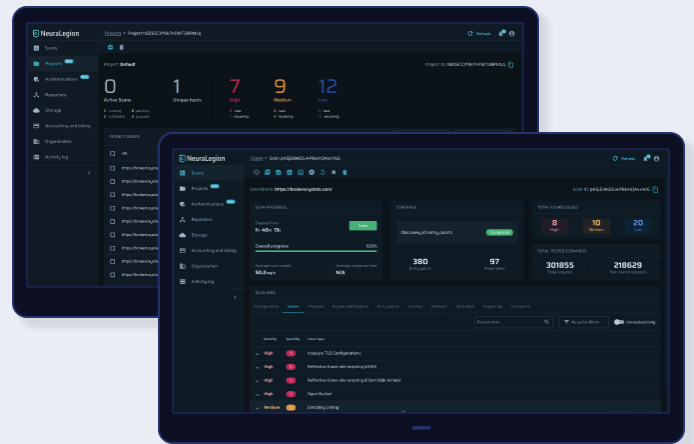


Эффективное и своевременное автоматизированное тестирование безопасности API и приложений

Bright — это первый сканер для динамического тестирования безопасности приложений (DAST), который позволяет специалистам, участвующим в цикле разработки, управлять процессом тестирования безопасности, автоматизированным для CI/CD-пайплайнов, а также выявлять и устранять проблемы безопасности на самых ранних этапах, обеспечивая оперативную безопасность в работе приложений и API.

Вы можете тестировать веб-приложения, одностраничные приложения, микросервисы, внутренние приложения и API-интерфейсы (REST, SOAP, GraphQL и веб-сокеты), а также проверить безопасность бизнес-логики с широким охватом уязвимостей.

Благодаря отсутствию ложных срабатываний каждый результат тестирования безопасности автоматически подтверждается, что устраняет необходимость в ручной проверке, экономит время специалистов по безопасности, позволяя разработчикам максимально эффективно внедрять DevSecOps и подход «Shift Left» (перенос процесса тестирования на ранние стадии разработки).



Автоматизация настройки и развертывания ПО и CI/CD требует применения инструментов для тестирования безопасности приложений, созданных для автоматизации, масштабируемости... и удобства разработчиков!

Учитывая, что разработчики запускают программное обеспечение в производство по несколько раз в день, традиционные сканеры безопасности быстро устаревают, что затрудняет процесс автоматизации и приводит к получению неточных результатов.

В свою очередь, периодическое сканирование безопасности приложений приводит к запоздалому и дорогостоящему обнаружению и устранению проблем, что усугубляет ситуацию с контролем безопасности и требует проведения технических доработок.

Тестирование со сдвигом влево «Shift Left»: используйте Bright



Отсутствие ложных срабатываний!

Автоматическое подтверждение результатов



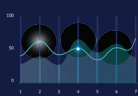
Сканирование приложений любых типов

Веб-приложения, внутренние приложения, одностраничные приложения



Беспроблемная интеграция CI/CD

Сканирование каждого запроса на включение изменений, сборки или слияния через интерфейс командной строки



Бизнес-логика

Тестирование безопасности



Сканирование всех API-интерфейсов

REST, SOAP, GraphQL, веб-сокеты



Тысячи атак

Широкий охват тестирования уязвимостей

Нам доверяют службы безопасности и разработчики:



Основные характеристики

Отсутствие ложных срабатываний

Как единственный сканер безопасности без ложных срабатываний, Bright автоматически проверяет каждую уязвимость, что исключает необходимость проведения дорогостоящей и длительной проверки вручную. Устраняет устаревшие оповещения, приоритизирует меры по устранению неисправностей, сокращению числа уязвимостей и технических недоработок.

Непревзойденное обнаружение видов атак

Полная поддержка файлов HAR, OpenAPI/Swagger и Postman. Для обеспечения полной автоматизации веб-сканер Bright использует запатентованную технологию автономного браузера, обеспечивающую активное взаимодействие с целевым объектом для создания нескольких цепочек взаимосвязей с приложением. Цепочки имитируют человеческие взаимодействия, включая анализ на основе объектной модели документа и JavaScript, а также автоматическое обнаружение, обмен данными и итерацию по интерактивным опциям и выпадающим спискам.

Выявление дополнительных уязвимостей, включая уязвимости бизнес-логики

Инструмент позволяет выявлять технические уязвимости в OWASP (API) Top 10, Mitre 25 и т.д., поддерживает автоматизированное тестирование безопасности бизнес-логики и предлагает наиболее полные и непревзойденные возможности тестирования на рынке.

Создан для разработчиков, которые доверяют ему свою безопасность

Bright — это облачное решение, которое легко интегрируется в процесс разработки. Несмотря на то, что специалисты службы безопасности получают детальный пользовательский отчет на приборных панелях на основе проектов, разработчики могут инициировать и контролировать сканирование с помощью CLI или управлять процессом разработки с помощью конфигурационных файлов .yaml в составе единиц для сканирования каждой сборки, запроса на внесение изменений или слияния для поддержания непрерывного и безопасного процесса разработки. Для немедленного устранения проблем предоставляются рекомендации в удобном для разработчиков формате.

Простое сканирование при получении доступа

Самая широкая в отрасли поддержка механизмов аутентификации позволяет легко сканировать защищенные логином части приложений и API, что обеспечивает максимальный охват.

Беспроblemная интеграция SDLC и CI/CD

Масштабируемая технология SaaS, предлагаемая Bright, интегрируется в процесс разработки, обеспечивая молниеносное сканирование каждой сборки. Интеграция комплексного и точного тестирования безопасности еще никогда не была такой простой, будь то решения «из коробки» со всеми привычными инструментами или через OpenAPI от Bright.

Точность и масштабируемость... АВТОМАТИЧЕСКИ!



Bright — сканер динамического тестирования безопасности приложений (DAST), который позволяет специалистам, участвующим в цикле разработки, управлять процессом тестирования безопасности, автоматизированным для CI/CD-пайплайнов, а также выявлять и устранять проблемы безопасности на самых ранних этапах, обеспечивая оперативную безопасность в работе приложений и API.

Раннее обнаружение уязвимостей в процессе разработки предполагает более дешевое их исправление и повышенную безопасность. Bright предоставляет масштабируемое решение, которому доверяют специалисты по безопасности и которое выбирают разработчики. Решение, предназначенное для быстрого выявления и устранения критических уязвимостей в приложениях, контроля качества или в производственной среде.

ВЫЯВЛЯЙТЕ СВОИ УЯЗВИМОСТИ С ПОМОЩЬЮ BRIGHT