Fortify Static Code Analyzer

Повышение качества кода и обеспечение безопасности создаваемых приложений с помощью Micro Focus Fortify

- Статистика

+ Более 84% всех нарушений безопасности происходят на уровне приложений[1]
+ Критические уязвимости веб-технологий затрагивают почти половину всех веб-приложений[2]
+ В 52% веб-приложений имеются проблемы, связанные с проверкой вводимых данных, межсайтовым скриптингом или SQL-инъекциями[3]
+ 33% приложений никогда не проверяются на наличие уязвимостей в системе безопасности[4]

1 *Отчет «Магический квадрант Gartner»*
2 *Отчет Micro Focus Cyber Risk 2015 г., февраль 2015 г.*
3 *Там же*
4 *Исследование: «Разработчики мобильных приложений не вкладываются в обеспечение безопасности», 20 марта 2015 г.*

Приложения создают риски и снижают безопасность

Требования и сложности в современной разработке ПО

- Реализация новых функций
- Повышение уровня сложности
- Жесткие временные рамки
- Сокращение бюджетов
- Задержки выпуска продуктов

Перечисленные факторы хорошо знакомы разработчикам, особенно тем, кто трудится над критически важными бизнес-приложениями. Создание современных программных продуктов осложняется необходимостью обеспечивать бесчисленное количество требований, поэтому на обеспечение безопасности зачастую не хватает времени. Между тем, угрозы эволюционируют, причем целью злоумышленников, как правило, является самое слабое звено — приложения. Fortify Static Code Analyzer (SCA) помогает защититься от наиболее серьезных угроз — от тех, которые несут в себе приложения для бизнеса.

Fortify Static Code Analyzer

Fortify SCA — это решение для статического анализа кода на наличие уязвимостей, предназначенное для групп разработки и специалистов по безопасности. Система проверяет код, помогая быстрее и легче обнаруживать уязвимости, определять их приоритеты и затем устранять.

Fortify SCA позволяет:

- выполнять частые сканирования исходного кода, в том числе на ранних этапах разработки;
- выяснять первопричину и место появления уязвимости вплоть до конкретной строки кода;
- находить корреляции между результатами и назначать им приоритет;
- ускорять разработку за счет более быстрого выполнения сканирования;
- оперативно устранять уязвимости;
- осваивать лучшие методики создания безопасного кода.

Для чего нужен статический анализ кода?

Статический анализ кода — это методика обнаружения уязвимостей непосредственно в исходном коде. Такой анализ регулярно проводится на ранних стадиях цикла разработки и на протяжении всего жизненного цикла приложения. В ходе его выполнения разработчики оперативно получают информацию об ошибках, допущенных на этапе создания кода.

Преимущества Fortify SCA

Универсальность

Имеющаяся в Fortify SCA поддержка широкого круга сред разработки, языков, платформ и фреймворков позволяет проводить анализ безопасности в средах, предназначенных как для создания ПО, так и для его продуктивной эксплуатации.

- Поддерживается 25+ языков программирования
- Более 911 тыс. интерфейсов API уровня компонентов
- Обеспечивается распознавание как минимум 961 вида уязвимостей
- Поддержка всех основных платформ, систем сборки и интегрированных сред разработки ПО

Точность
Fortify SCA характеризуется высокой точностью результатов и превосходит другие технологии статического тестирования на безопасность по разнообразию обнаруживаемых проблем. Назначая уязвимостям приоритет в зависимости от категории и степени риска, Fortify SCA предлагает готовый план действий по исправлению ошибок. Система работает, руководствуясь обширным, самым полным на текущий момент набором правил написания защищенного кода, который постоянно дополняется и обновляется специалистами исследовательского подразделения Micro Focus® Security Fortify Software Security Research.

Описание продукта
Гибкость
Fortify SCA органично встраивается в существующую среду разработки. Этот гибкий статический анализатор кода, запускаемый из командной строки, можно легко интегрировать в любую среду с помощью скриптов, подключаемых модулей и инструментов с графическим интерфейсом, что позволяет быстро приступить к использованию его возможностей.

Эффективность
Сокращение времени сканирования обеспечит необходимые преимущества организациям, желающим ускорить процессы обеспечения безопасности своих приложений. Fortify SCA помогает повысить эффективность труда разработчиков за счет использования инкрементального сканирования. Такое сканирование требует меньше времени, поскольку анализируются только те фрагменты кода, которые изменились с момента последней полной проверки. Это позволяет быстрее получать результаты сканирования, что дает возможность чаще выполнять проверки, повышая тем самым производительность труда разработчиков и способствуя более быстрому вводу ПО в продуктивную эксплуатацию.

Масштабируемость
В организациях могут применяться приложения разных типов: разработанные собственными силами, внешними подрядчиками, сторонними поставщиками, мобильные, с открытым кодом и т. п. При большом количестве и уровне сложности корпоративных приложений задачи тестирования и обеспечения безопасности становятся особенно трудными. Благодаря поддержке большинства популярных языков программирования Fortify SCA может обнаруживать бреши в приложениях всех типов, производя масштабирование по мере появления у предприятия новых потребностей.

Локальное установка и сервис SaaS
Предусмотрены различные схемы предоставления Fortify SCA в зависимости от тех задач, которые требуется решать клиенту.

- On Premises (локальный вариант) — для выполнения статических тестов безопасности кода приложений на площадке клиента.
- On Demand (SaaS): Fortify on Demand — это управляемый сервис проверки безопасности приложений, обеспечивающий легкий доступ к высокоточному статическому и динамическому тестированию, а также тестированию мобильных приложений, причем без первоначальных инвестиций и дополнительных затрат ресурсов и времени.

Поддерживаемые языки

- ABAP/BSP
- ActionScript/MXML (Flex)
- ASP.NET, VB.NET, C# (.NET)
- C/C++
- Classic ASP (с VBScript)
- COBOL
- ColdFusion CFML
- HTML
- Java (в т. ч. для Android)
- JavaScript/AJAX
- JSP
- Objective-C
- PHP
- PL/SQL
- Python
- T-SQL
- Ruby
- Scala
- Swift
- Visual Basic
- VBScript
- XML

Поддерживаемые среды разработки

- Eclipse
- IntelliJ Ultimate
- IntelliJ Community Android Studio
- IBM Rational Application Developer (RAD)
- IBM Rational Software Architect (RSA)
- Microsoft Visual Studio

Поддерживаемые инструменты сборки

- Ant
- Jenkins
- Maven
- MSBuild
- Xcodebuild

Fortify: таксономия уязвимостей ПО

Категории уязвимостей

Не существует общепринятых стандартов, определяющих, какие уязвимости являются критическими, а какие не являются. Различные организации публикуют собственные оценки, и расхождения ведут к путанице. Чтобы внести ясность в определение основных видов ошибок программирования, чреватых появлением уязвимостей, эксперты Fortify подготовили справочник «Семь пагубных королевств» (“The Seven Pernicious Kingdoms”), где универсальная классификация уязвимостей представлена в соответствии со стандартами OWASP, SANS, CWE и FISMA.

Международная лаборатория Fortify Software Security Research Group является одной из ведущих организаций по исследованию новых угроз безопасности. Знания, накопленные ее специалистами, вкладываются в решения семейства Micro Focus Security Fortify, благодаря чему механизмы поиска уязвимостей всегда способны выявлять самые новые угрозы. Сотрудники исследовательского отделения Fortify создали таксономию категорий уязвимостей — набор правил, дающий ясное представление о видах уязвимостей, которым могут быть подвержены приложения.

Дополнительно. Сведения о развитии таксономии: **www.vulncat.fortify.com/en**

О компании Micro Focus Security

Micro Focus является ведущим поставщиком решений в области безопасности и контроля соответствия современным требованиям. В числе клиентов компании — передовые предприятия, которым нужно минимизировать риск, связанный с использованием гибридных сред ИТ, а также защищать эти среды от новейших угроз. Micro Focus предлагает платформу класса Security Intelligence, созданную на базе лидирующих на рынке продуктов ArcSight, Fortify и Data Security.

Это уникальное решение выполняет интеллектуальную корреляцию событий, обеспечивая безопасность приложений и сетей для защиты современной гибридной инфраструктуры ИТ от изощренных кибератак.

Узнать больше о продукции Micro Focus Security можно на сайте **www.microfocus.com/securitysolutions.**

Дополнительные сведения

Решения Micro Focus Fortify способствуют укреплению доверия к программному обеспечению, от которого зависит успех вашего бизнеса.

Чтобы узнать больше, перейдите по ссылке www.microfocus.com/fortifysca

www.microfocus.com

Представительство
Micro Focus®
в Великобритании
+44 (0) 1635 565200

Представительство
в США
Rockville, Maryland
301 838 5000
877 772 4450

Дополнительную контактную информацию и адреса представительств см. по адресу **www.microfocus.com**