



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056.55

Snyk Code: КАК ЗАЩИТИТЬ КОД ОТ УЯЗВИМОСТЕЙ

Авдалян А.А.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: sharmanka228@gmail.com

Статья "Snyk Code" представляет собой обзор и анализ решений по обеспечению безопасности кода, предлагаемых платформой Snyk. В статье рассматриваются ключевые возможности и функции Snyk Code, включая его способность выявлять уязвимости, анализировать зависимые библиотеки и интегрироваться с различными системами CI/CD. Особое внимание уделяется методам автоматического обнаружения и исправления уязвимостей на этапе разработки, а также практическому применению платформы в различных сценариях программирования. Статья также обсуждает преимущества использования Snyk Code для повышения надежности и безопасности программного обеспечения, а также его влияние на общий процесс разработки.

Ключевые слова: Snyk Code, безопасность кода, уязвимости, анализ зависимостей, CI/CD, автоматическое исправление, разработка программного обеспечения, платформы безопасности.

Snyk Code: HOW TO PROTECT YOUR CODE FROM VULNERABILITIES

Avdalyan A.A.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

The article "Snyk Code" is an overview and analysis of code security solutions offered by the Snyk platform. The article discusses the key features and functions of Snyk Code, including its ability to identify vulnerabilities, analyze dependent libraries, and integrate with various CI/CD systems. Special attention is paid to the methods of automatic detection and correction of vulnerabilities at the development stage, as well as the practical application of the platform in various programming scenarios. The article also discusses the benefits of using Snyk Code to improve the reliability and security of software, as well as its impact on the overall development process.

Keywords: Snyk Code, code security, vulnerabilities, dependency analysis, CI/CD, automatic correction, software development, security platforms.

Введение

В эпоху стремительного роста числа угроз безопасности программного обеспечения и увеличения сложности современных приложений, обеспечение защиты кода становится одной из важнейших задач для разработчиков. Одним из инструментов, предоставляющих эффективные решения в этой области, является Snyk Code. Эта платформа специально разработана для выявления уязвимостей в исходном коде и зависимостях на ранних стадиях разработки, что позволяет минимизировать риски и улучшить безопасность приложений.

Snyk Code предлагает интегрированные инструменты для анализа кода, которые автоматизируют процесс обнаружения уязвимостей и предоставляют рекомендации по их устранению. Использование таких решений особенно важно в условиях современных циклов

разработки программного обеспечения, где быстрая интеграция и тестирование кода являются ключевыми факторами успеха[1].

В данном контексте, статья направлена на глубокий анализ возможностей и особенностей Snyk Code, а также его роли в поддержке безопасной разработки программного обеспечения. Мы рассмотрим, как Snyk Code справляется с задачей обнаружения уязвимостей, интеграции с системами CI/CD, и как его использование может повлиять на общий процесс разработки и безопасность программных продуктов.

Snyk Code: Обеспечение безопасности кода на каждом этапе разработки

Обзор Snyk Code

Snyk Code — это передовая платформа для анализа и защиты исходного кода, разработанная для помощи разработчикам в выявлении и устранении уязвимостей на ранних стадиях разработки. Платформа интегрируется с различными средами разработки и системами CI/CD, обеспечивая непрерывный мониторинг кода на предмет потенциальных угроз безопасности[3].

Основные функции и возможности

Snyk Code предлагает ряд ключевых функций, способствующих улучшению безопасности кода:

Статический анализ кода: Платформа проводит глубокий статический анализ кода, выявляя потенциальные уязвимости и ошибки еще до выполнения программы. Это позволяет разработчикам оперативно устранять проблемы на ранних стадиях[4].

Анализ зависимостей: Snyk Code также анализирует сторонние библиотеки и зависимости, используемые в проекте. Это важно, поскольку уязвимости в зависимостях могут стать точками входа для атак.

Интеграция с CI/CD: Платформа легко интегрируется с популярными системами непрерывной интеграции и доставки (CI/CD), такими как Jenkins, GitHub Actions и GitLab CI. Это обеспечивает автоматическое сканирование кода и зависимостей на каждом этапе разработки и развертывания.

Интерактивные рекомендации: Snyk Code предоставляет детализированные рекомендации по исправлению уязвимостей, что позволяет разработчикам легко понять и устранить найденные проблемы[2].

Обратная связь в реальном времени: Платформа обеспечивает обратную связь в реальном времени, что позволяет разработчикам немедленно реагировать на обнаруженные уязвимости и интегрировать исправления в кодовую базу.

Преимущества использования Snyk Code

Использование Snyk Code приносит множество преимуществ:

Улучшение безопасности: Постоянный анализ кода и зависимостей помогает предотвратить внедрение уязвимостей в конечный продукт, тем самым повышая общий уровень безопасности приложения.

Сокращение времени на исправление: Благодаря детализированным рекомендациям по исправлению и автоматизированному анализу, разработчики могут быстрее исправлять уязвимости, минимизируя время, затрачиваемое на безопасность.

Снижение рисков: Проактивное обнаружение и устранение уязвимостей снижает риск потенциальных атак и утечек данных, что особенно важно для соблюдения стандартов безопасности и требований нормативных актов.

Интеграция в рабочий процесс: Интеграция Snyk Code с системами CI/CD позволяет seamlessly интегрировать анализ кода в процесс разработки, что делает его частью повседневной работы команды разработчиков.

Практическое применение и примеры

Рассмотрим несколько сценариев, в которых Snyk Code может быть полезен:

Проекты с открытым исходным кодом: В проектах с открытым исходным кодом, где разработчики часто работают с внешними зависимостями, Snyk Code помогает обнаруживать уязвимости в этих зависимостях и своевременно их устранять.

Корпоративные приложения: Для крупных компаний, где безопасность данных критична, Snyk Code обеспечивает постоянный контроль над безопасностью кода, снижая риски утечек и атак[5].

Мобильные и веб-приложения: Разработчики мобильных и веб-приложений могут использовать Snyk Code для анализа как клиентской, так и серверной части приложений, обеспечивая комплексную защиту.

Заключение

Snyk Code представляет собой мощный инструмент для обеспечения безопасности кода, предлагая ряд функций, которые помогают разработчикам своевременно обнаруживать и устранять уязвимости. Его интеграция с системами CI/CD и возможность анализа как исходного кода, так и зависимостей делают его незаменимым в современном процессе разработки программного обеспечения. Использование Snyk Code способствует не только улучшению безопасности приложений, но и оптимизации процессов разработки, что в конечном итоге позволяет создавать более надежные и защищенные программные продукты.

Список литературы

1. Бударный Г. С. и др. Исследование концепции ядра в различных операционных системах //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 411-417.
2. Горбань С. А., Красов А. В., Цветков А. Ю. Оценка эффективности механизмов контроля правами доступа в ОС Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023). – 2023. – С. 345-348.
3. Шемякин С. Н. и др. Оценка расстояния единственности... Для некоторых блочных шифров //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 34-38.
4. Пестов И. Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.
5. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

References

1. Budarny G. S. et al. Research of the kernel concept in various operating systems //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 411-417.
 2. Gorban S. A., Krasov A.V., Tsvetkov A. Yu. Assessment of the effectiveness of access rights control mechanisms in Linux OS //Actual problems of infotelecommunications in science and education (APINO 2023). – 2023. – pp. 345-348.
 3. Shemyakin S. N. et al. Estimation of the uniqueness distance... For some block ciphers //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 34-38.
 4. Pestov I. E. Methodology for developing control effects on cloud infrastructure instances //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. - 2020. – No. 4. – pp. 72-76.
 5. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruевич, 1996.
-