

ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

Вебинар 13. Обеспечение безопасности сборочной среды программного обеспечения



Представимся!

Спикеры и гости вебинара



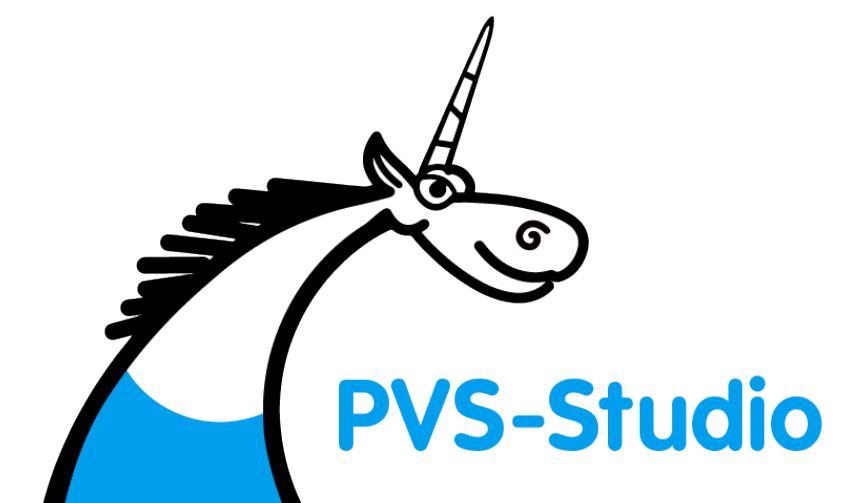
Владислав Богданов

Developer Advocate, Java Developer

- Разрабатываю ядро статического анализатора PVS-Studio для языка Java.
- Рассказываю про технологии статического анализа в статьях и на различных IT мероприятиях.



@vlade1
k



Виталий Пиков

Эксперт в области ИТ, ИБ, преподаватель

- Стаж преподавательской работы более 10 лет
- Заслуженный доцент Российского нового университета, преподаватель высшей школы
- Microsoft Certifications Earned: MCT, MCPS, MCSA, MCTS
- Автор более 30 научных публикаций



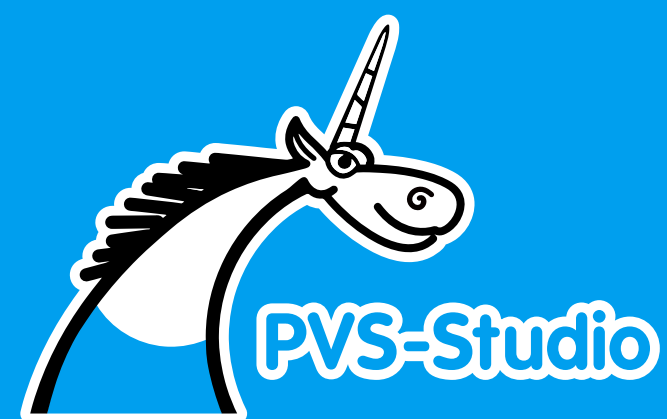
Роман Байталов

Архитектор системных решений в GitFlic, группа Астра

- 20+ лет в ИТ
- С 2012 по 2023 руководил отделом разработки для B2G, B2B и B2C секторов в компании, входящей в ТОП-10 крупнейших поставщиков услуг заказной разработки ПО в России
- Доклад: «Защищённая среда: как выстроить конвейер безопасной сборки с GitFlic»



О цикле вебинаров



Вокруг РБПО за 25 вебинаров: ГОСТ Р 56939-2024

- Организуют УЦ МАСКОМ и ООО «ПВС» (PVS-Studio)
- ГОСТ Р 56939-2024 описывает 25 процессов, необходимых для реализации разработки безопасного ПО, поэтому и 25 вебинаров
- Также, цикл включает в себя бонусные вебинары
- Мы открыты к сотрудничеству по разбору тем, пишите нам!

Записи предыдущих вебинаров



pvs-studio.ru/ru/webinar/rbpo/

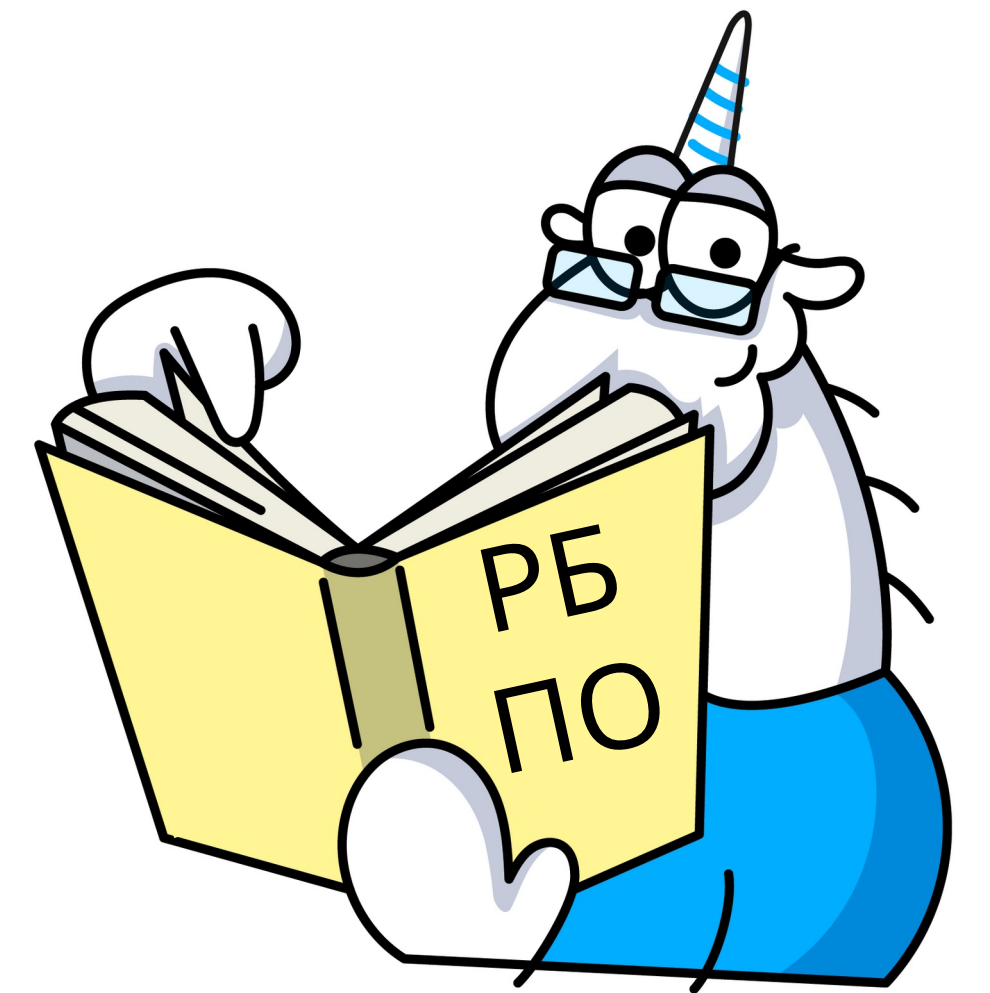
Процесс 13

Обеспечение безопасности сборочной среды программного обеспечения



5.13.1 Обеспечение безопасности сборочной среды программного обеспечения. Цели

- Обеспечение безопасности при сборке ПО, недопущение привнесения в результаты сборки ПО уязвимостей и ошибок со стороны сборочной среды.



5.13.2 Обеспечение безопасности сборочной среды программного обеспечения. Требования к реализации

- Разработать регламент обеспечения безопасности сборочной среды
- Зафиксировать описание ожидаемых результатов сборки ПО, прав доступа к среде сборки ПО и хранилищу результатов сборки ПО и ролей пользователей, участвующих в процессе сборки ПО
- Разработать схему сборочной среды

5.13.2 Обеспечение безопасности сборочной среды программного обеспечения. Требования к реализации

- Обеспечивать регистрацию всех выполняемых действий при сборке ПО в журналах аудита; журналы аудита должны храниться способом, обеспечивающим их целостность; сроки хранения журналов аудита должны быть зафиксированы в регламенте обеспечения безопасности сборочной среды
- Обеспечивать хранение результатов сборки ПО в выделенном хранилище — хранилище результатов сборки ПО

5.13.2 Обеспечение безопасности сборочной среды программного обеспечения. Требования к реализации

- Обеспечивать повторяемость сборки ПО (если применимо)
- Обеспечивать управление доступом к среде сборки ПО и хранилищу результатов сборки ПО на основе ролей пользователей
- Обеспечивать защиту каналов связи с внешними источниками данных для обеспечения конфиденциальности информации, обрабатываемой в сборочной среде.

5.13.3.1 Обеспечение безопасности сборочной среды программного обеспечения. Артефакты реализации

Регламент обеспечения безопасности сборочной среды должен содержать, как минимум, следующие сведения:

- обязанности сотрудников и их роли при проведении сборок ПО;
- порядок регистрации событий безопасности при реализации сборок ПО в журналах аудита;
- сроки хранения журналов аудита;
- описание мер безопасности, необходимых для реализации в сборочной среде.

5.13.3.2 Обеспечение безопасности сборочной среды программного обеспечения. Артефакты реализации

Информация о безопасности сборочной среды должна содержать:

- описание ожидаемых результатов сборки ПО;
- описание прав доступа к сборочной среде и хранилищу результатов сборки ПО, а также ролей пользователей, участвующих в процессе сборки ПО.

5.13.3.3 Обеспечение безопасности сборочной среды программного обеспечения. Артефакты реализации

Схематическое изображение сборочной среды должно содержать:

- элементы сборочной среды (серверы, узлы, виртуальные узлы, элементы среды контейнеризации и т. п.);
- связи между элементами сборочной среды, позволяющие отследить порядок (очередность) выполнения сборочных действий;
- компоненты сборочной среды, реализующие отдельные функции, в том числе меры безопасности (средства защиты информации, инструменты статического анализа и др.).

5.13.3.4 Обеспечение безопасности сборочной среды программного обеспечения. Артефакты реализации

Журналы аудита процессов сборки ПО должны содержать следующую информацию:

- дату и время начала и завершения сборки ПО;
- информацию о версии собираемого ПО (модуля ПО, компонента ПО);
- информацию об используемой конфигурации сборки ПО;
- информацию о шагах сборки ПО;
- информацию о событиях безопасности в соответствии с регламентом обеспечения безопасности сборочной среды.

5.13.3.5 Обеспечение безопасности сборочной среды программного обеспечения. Артефакты реализации

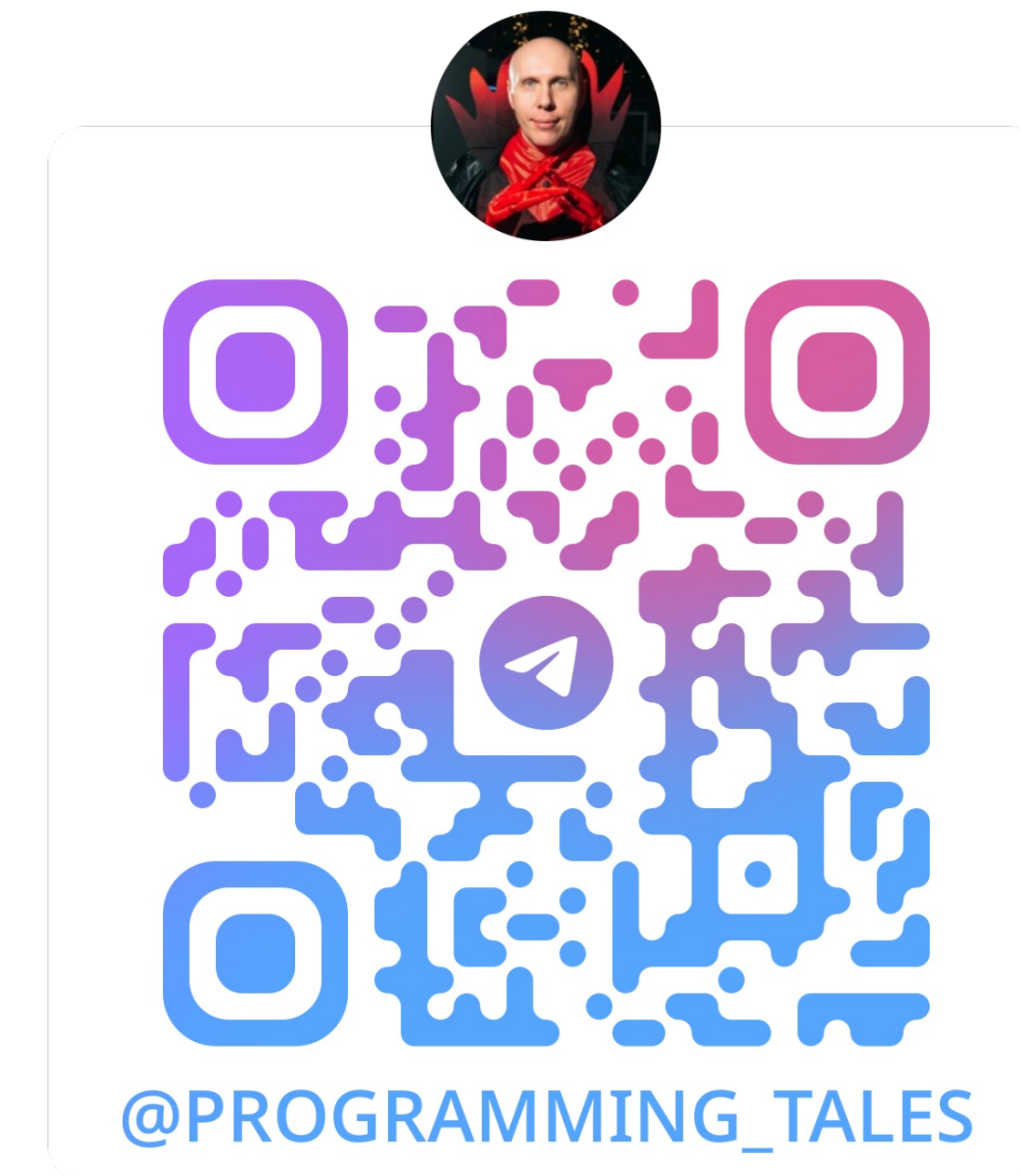
В качестве артефакта реализации требований, подтверждающих хранение результатов сборки ПО в выделенном хранилище, может использоваться журнал аудита сборки ПО, в котором указано место сохранения собранного модуля (компонента) ПО, результаты контрольного суммирования файлов, скачанных из хранилища результатов сборки ПО, и последующего сравнения их с контрольными суммами, указанными в журнале аудита сборки ПО или в графическом интерфейсе системы хранения результатов сборки ПО.

5.13.3.6 Обеспечение безопасности сборочной среды программного обеспечения. Артефакты реализации

В качестве артефактов реализации требований, подтверждающих повторяемость сборки ПО, могут использоваться журналы аудита выполненных сборок, сравненные друг с другом; результаты контрольного суммирования файлов, полученных при разных запусках сборок, и последующего их сравнения (по контрольным суммам, по бинарному представлению, по наименованию и размеру и др.).

Дополнительные материалы

- Телеграм-канал Андрея Карпова «**Бестиарий программирования**»:
 - Публикуется цикл постов, посвящённых РБПО.
 - Ссылка на пост «Процесс 13 — Обеспечение безопасности сборочной среды программного обеспечения»: https://t.me/programming_tales/408



Передаю слово следующему спикеру



Сделай свой проект
чистым и
безопасным вместе с
PVS-Studio



Сайт компании GitFlic



Сообщество GitFlic



Получи 10% скидку
на курсы «М БРПО»
в Учебном Центре
«МАСКОМ»

