

# ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

## БОНУСНЫЙ ВЕБИНАР

Безопасность frontend-приложений:  
особенности, угрозы и анализаторы класса  
FAST (Frontend Application Security Testing)





# ПРЕДСТАВИМСЯ!

Спикеры и гости вебинара



# ВАЛЕРИЙ ФИЛАТОВ

Developer Advocate

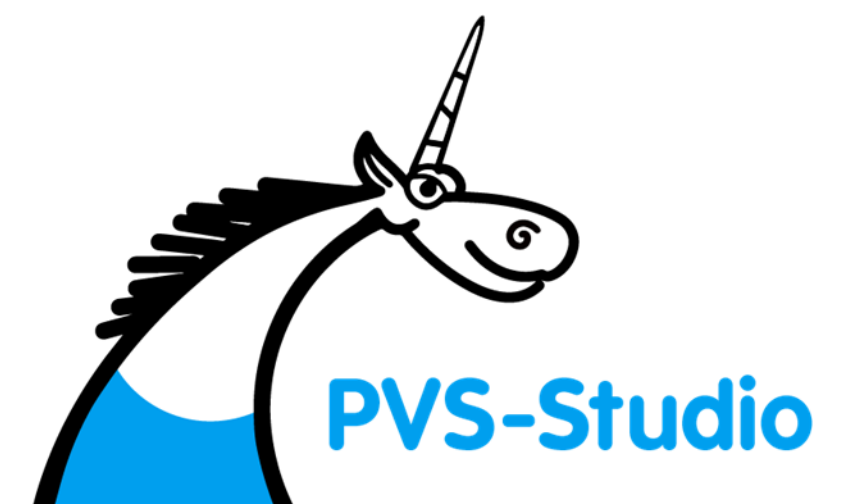
- Разработчик статического анализатора кода PVS-Studio.
- Рассказываю про технологии статического анализа и не только в статьях и на различных мероприятиях.



@feeelin



@feelindex



# 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.



# МИХАИЛ ПАРФЕНОВ

AppSec Lead

- Более 8 лет в AppSec/DevSecOps.
- Исследует методы анализа поведения кода для обнаружения угроз в клиентской части веб-приложений.
- Автор концепции Frontend Application Security Testing (FAST) и фреймворка моделирования угроз Frontend Kill Chain.
- Управляет разработкой первого российского FAST-анализатора в DPA Analytics.



@FrontSecOps





# #МНОГАБУКАФФ

## 5.11 Динамический анализ кода программы



## 5.11.1 ЦЕЛИ

- Обнаружение недостатков и уязвимостей в коде ПО в процессе его выполнения.



## 5.11.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Разработать регламент проведения динамического анализа кода ПО.
- Определить инструменты динамического анализа и фаззинг-тестирования, порядок их применения
- Определить перечень модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование.



## 5.11.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- Определить сценарии проведения тестирования для каждого исследуемого модуля (компонента) ПО средствами динамического анализа, включая инструменты проведения фаззинг-тестирования.
- Проводить динамический анализ с использованием инструментов динамического анализа
- Проводить повторный динамический анализ модулей (компонентов) ПО с целью контроля устранения ошибок.
- Проводить фаззинг-тестирование.

## 5.11.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

- При проведении фаззинг-тестирования использовать тестовые коллекции входных данных, подлежащие дальнейшим мутациям, для каждого из подвергаемых фаззинг-тестированию модуля (компонента) ПО (при использовании инструментов выполнения фаззинг-тестирования, использующих коллекции входных данных), вызывающие использование различных функциональных возможностей тестируемого модуля (компонента) ПО.



## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Регламент проведения динамического анализа кода ПО должен содержать следующие сведения:
  - обязанности сотрудников и их роли при проведении динамического анализа и фаззинг-тестирования;
  - критерии выбора инструментов динамического анализа, включая инструменты проведения фаззинг-тестирования;
  - критерии выбора методов и способов динамического анализа;
  - критерии выбора модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование;

## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Регламент проведения динамического анализа кода ПО должен содержать следующие сведения:
  - правила обработки срабатываний средств динамического анализа, требующих обработки (аварийная остановка, зависание и т. п.);
  - процедуры устранения найденных средствами динамического анализа ошибок;
  - периодичность проведения динамического анализа или события, при наступлении которых необходимо выполнять повторный динамический анализ (критерии проведения повторного динамического анализа);
  - периодичность проведения фаззинг-тестирования и критерии его завершения.



## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Перечень инструментов динамического анализа, включая инструменты проведения фаззинг-тестирования, должен включать:
  - наименования инструментов динамического анализа, их версии и их соответствие исследуемым модулям (компонентам) ПО;
  - параметры эксплуатации инструментов динамического анализа (для платформ, языков программирования и т. п.).

## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Перечень модулей (компонентов) ПО, которые необходимо подвергнуть динамическому анализу, включая фаззинг-тестирование, отвечающий требованиям регламента проведения динамического анализа, должен включать:
  - наименование модуля (компонента) ПО;
  - идентификатор модуля (компонента) ПО



## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Сценарии проведения тестирования для каждого исследуемого модуля (компонента) ПО средствами динамического анализа, включая инструменты проведения фаззинг-тестирования, обеспечивающие выполнение требований регламента проведения динамического анализа, должны включать:
  - идентификатор модуля (компонента) ПО;
  - наименование используемого инструмента;
  - параметры настройки инструмента;
  - критерии запуска и остановки тестирования.

## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Отчеты по результатам проведения динамического анализа должны включать:
  - срабатывания инструментов динамического анализа;
  - результаты анализа (обработки) выявленных ошибок (срабатываний динамического анализатора) для определенных регламентом типов ошибок, требующих обработки (аварийная остановка, зависание и т. п.).



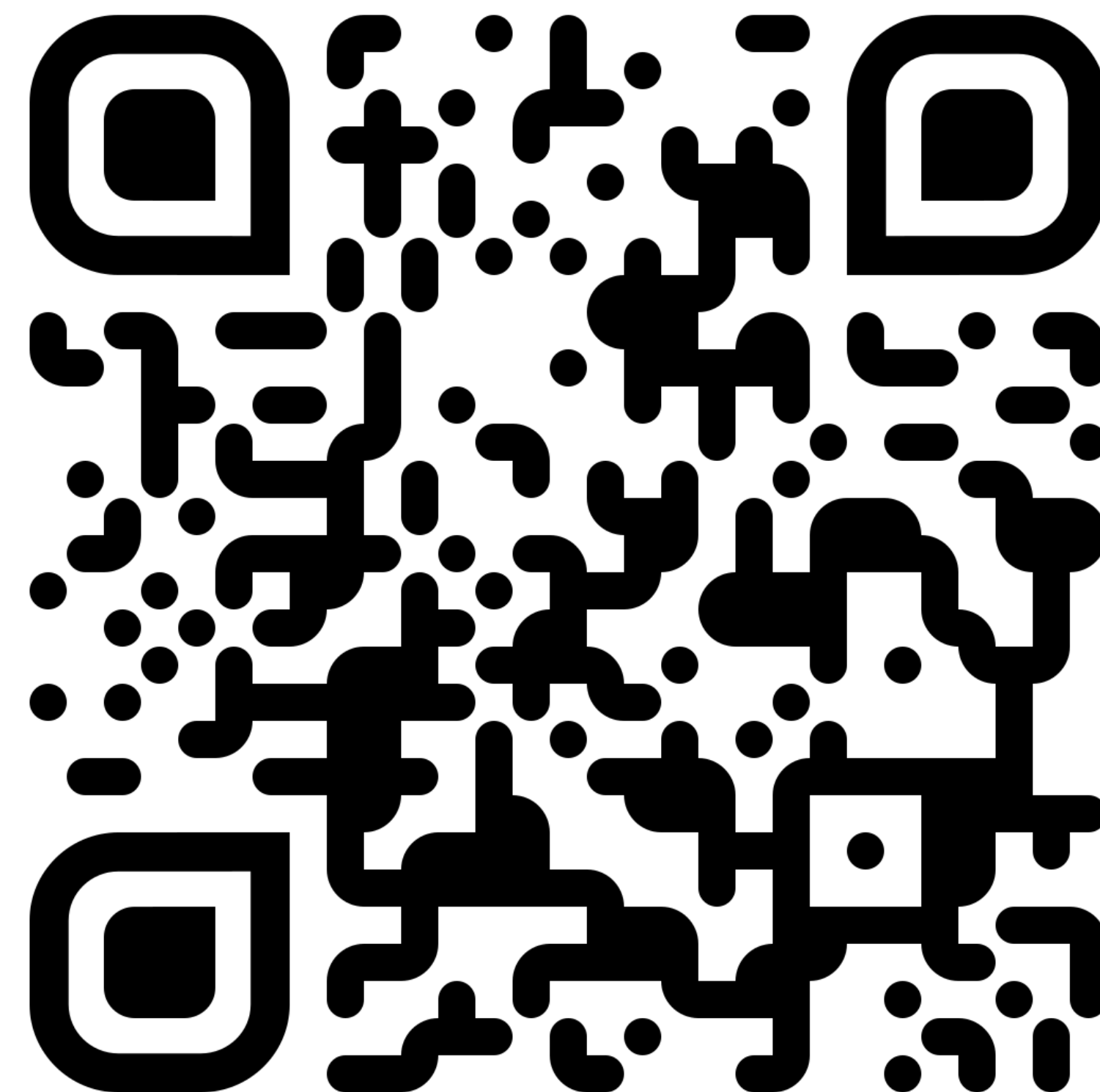
## 5.11.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ

- Отчеты по результатам проведения фаззинг-тестирования должны включать:
  - сведения о результатах работы инструментов фаззинг-тестирования (длительность проведения фаззинг-тестирования, количество аварийных завершений работы ПО, количество найденных путей выполнения и др.);
  - результаты анализа (обработки) аварийных завершений работы ПО, выявленных при проведении фаззинг-тестирования

ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

Вебинар 11.  
Динамический анализ  
кода программы



# СЛОВО СПИКЕРАМ!

Переходим к докладам





Сделай свой проект  
чистым и безопасным  
вместе с PVS-Studio



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

