

# Трудности при интеграции SAST: разбираем и исправляем

**PVS-Studio**



**Глеб Асламов**  
C# Developer

# Уязвимости и SAST

## Уязвимости и SAST

Трудности при интеграции и их решение

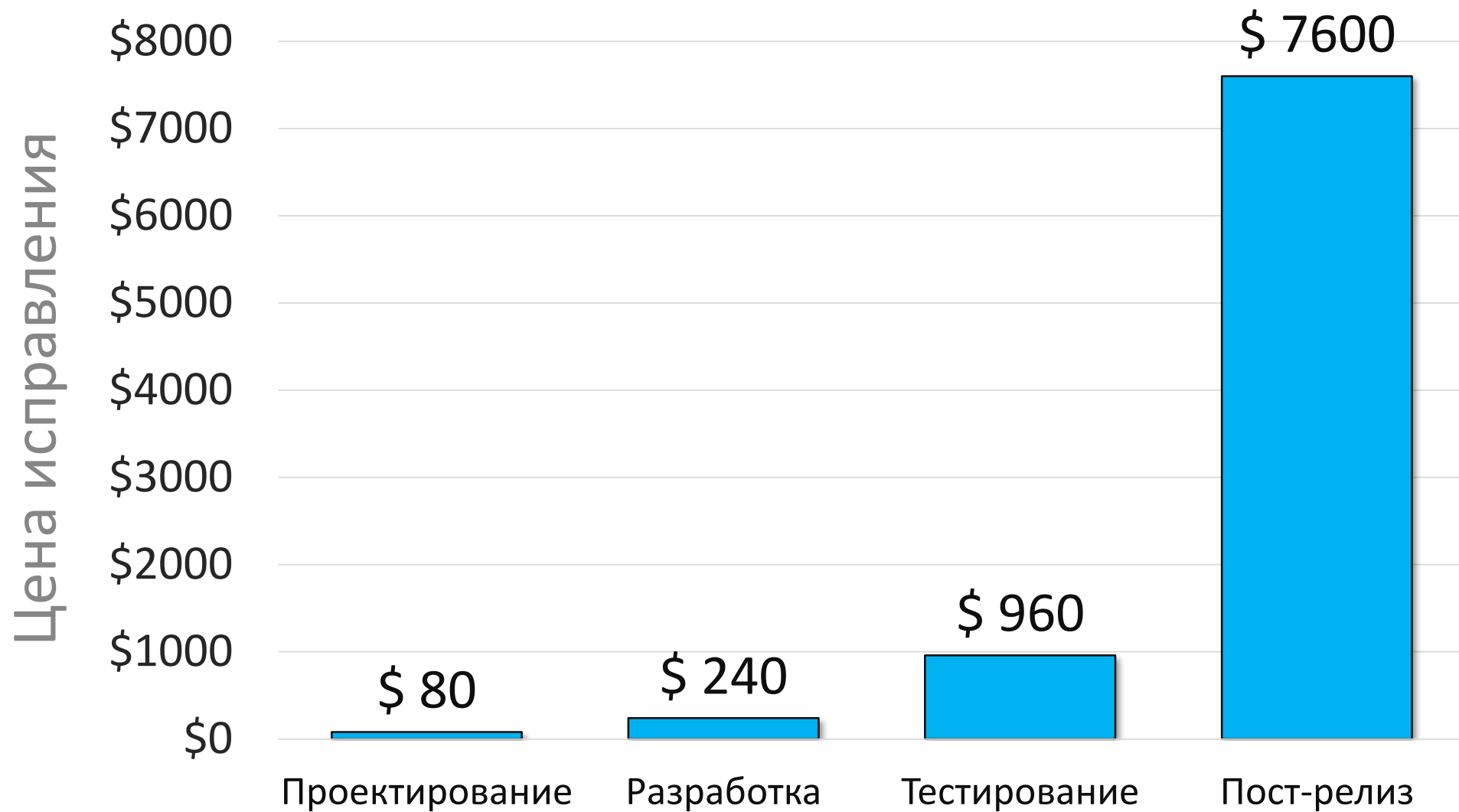
Уязвимости и SAST

Трудности при интеграции и их решение

Как быстро попробовать SAST инструмент

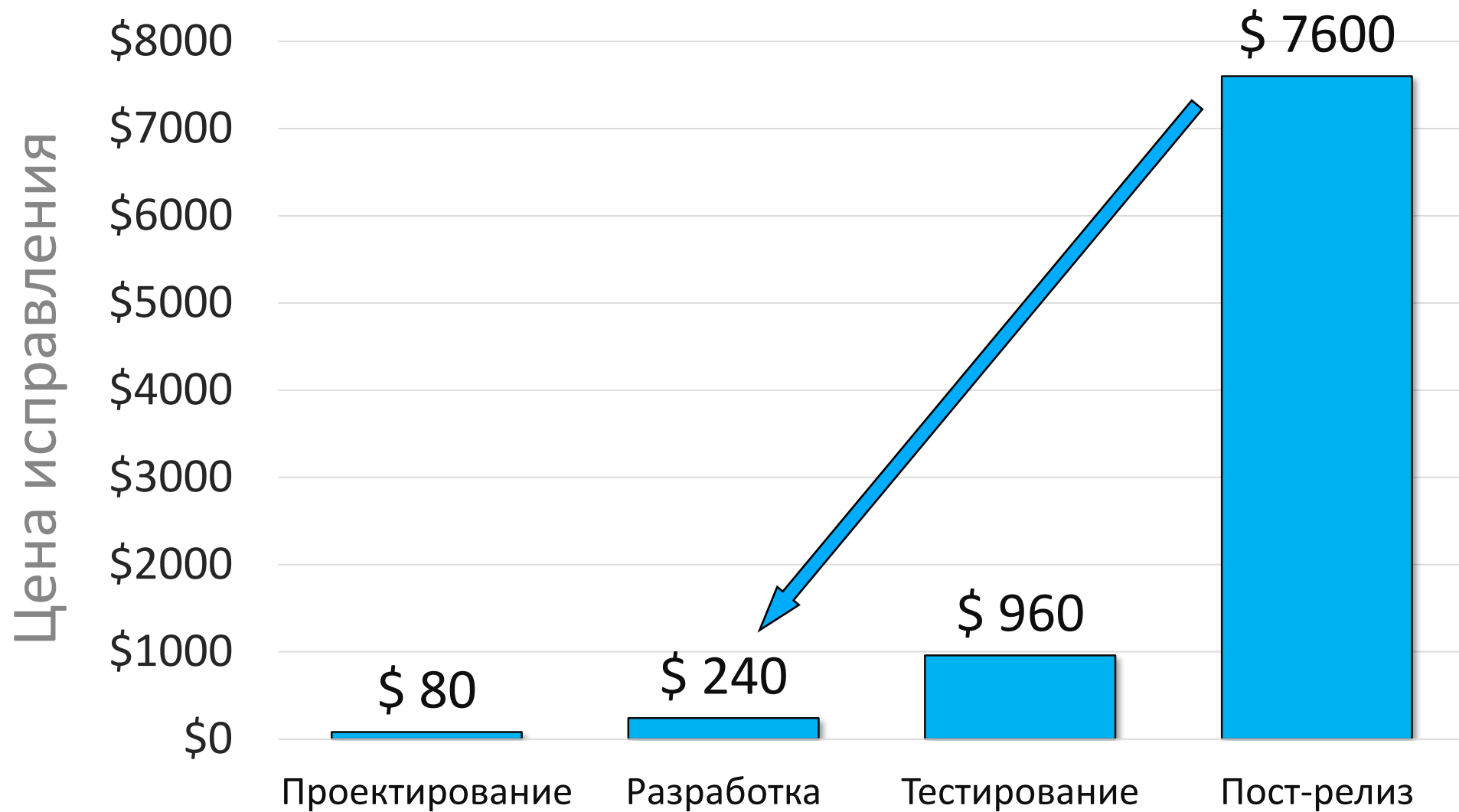
Почему уязвимости опасны?

# Сколько стоит исправить уязвимость?



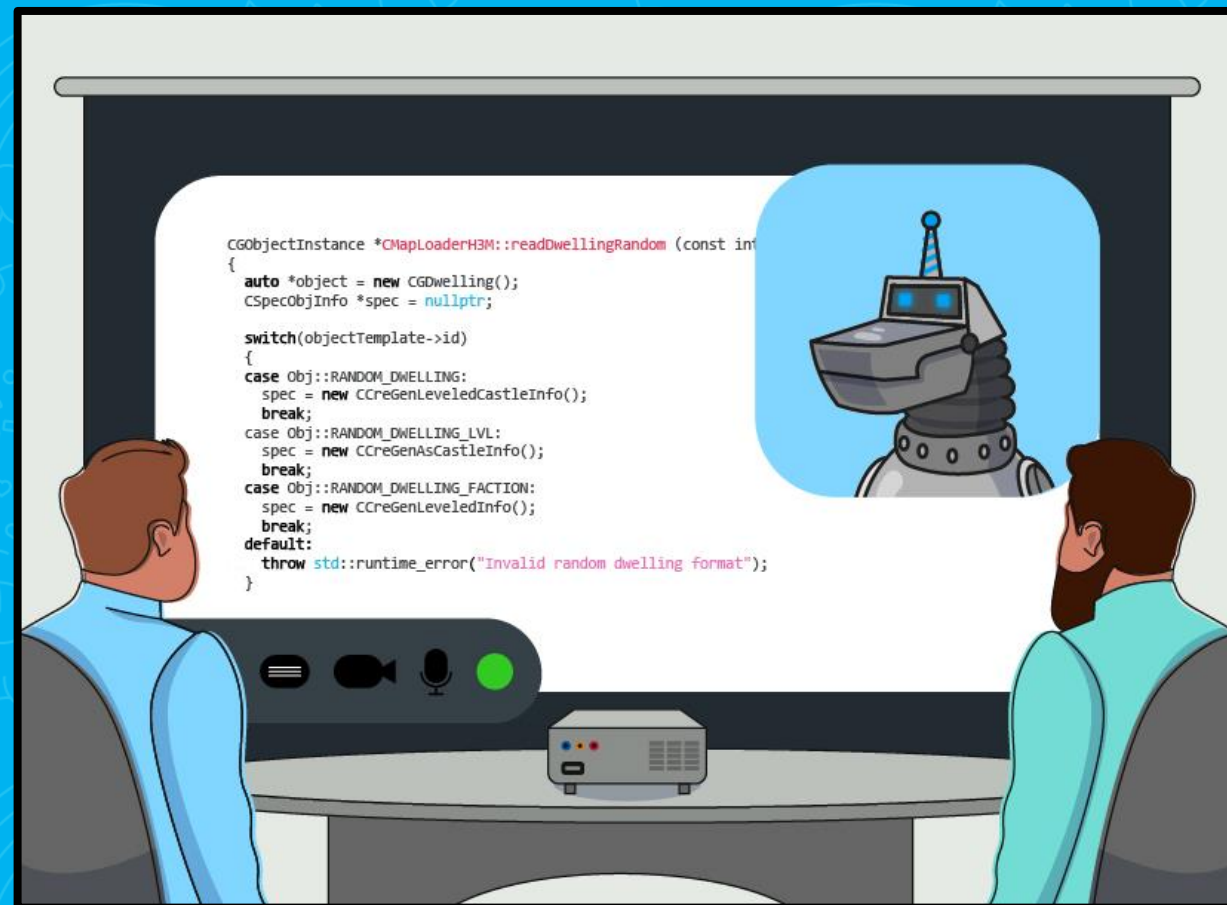
Источник - [NIST](#): National Institute of Standards and Technology

# Сколько стоит исправить уязвимость?



Источник - [NIST](#): National Institute of Standards and Technology

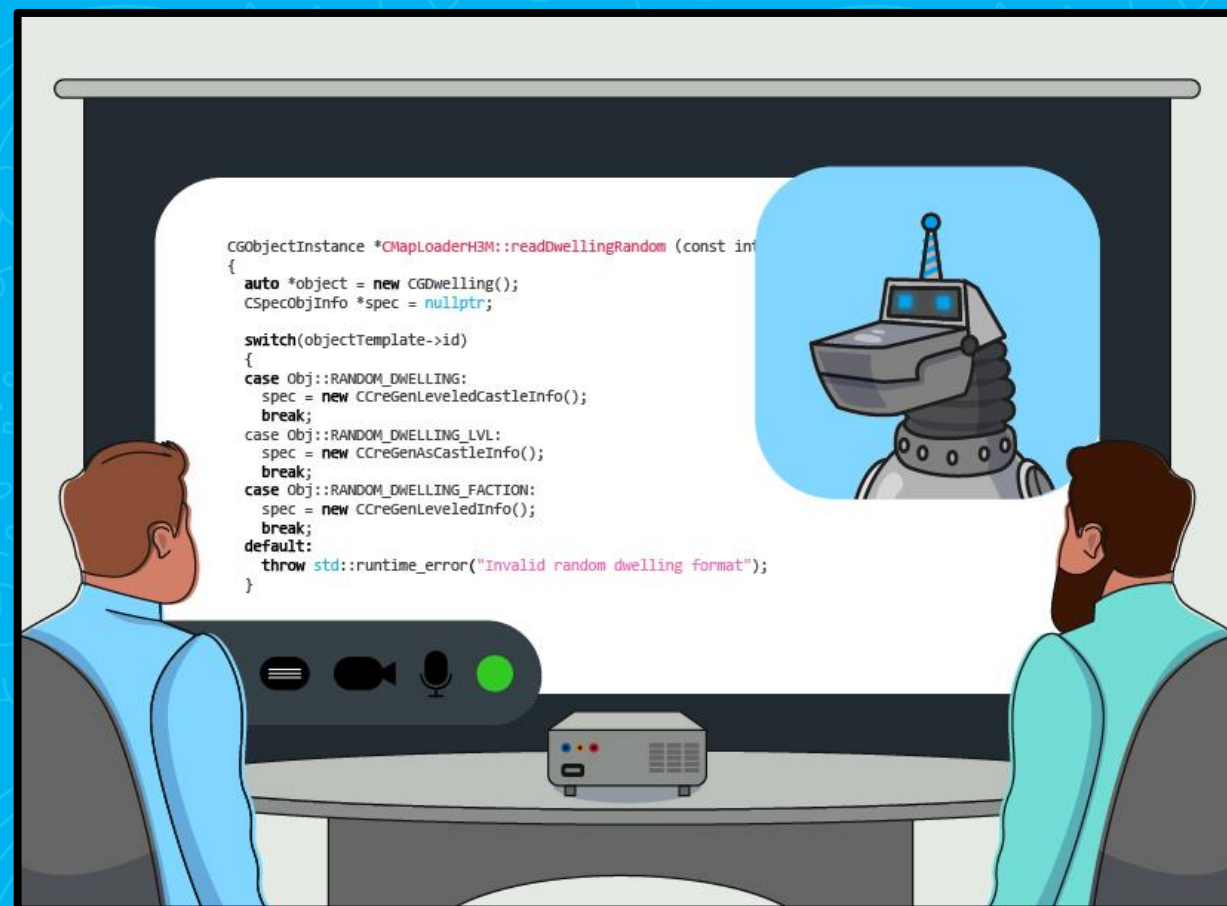
# Как искать уязвимости?





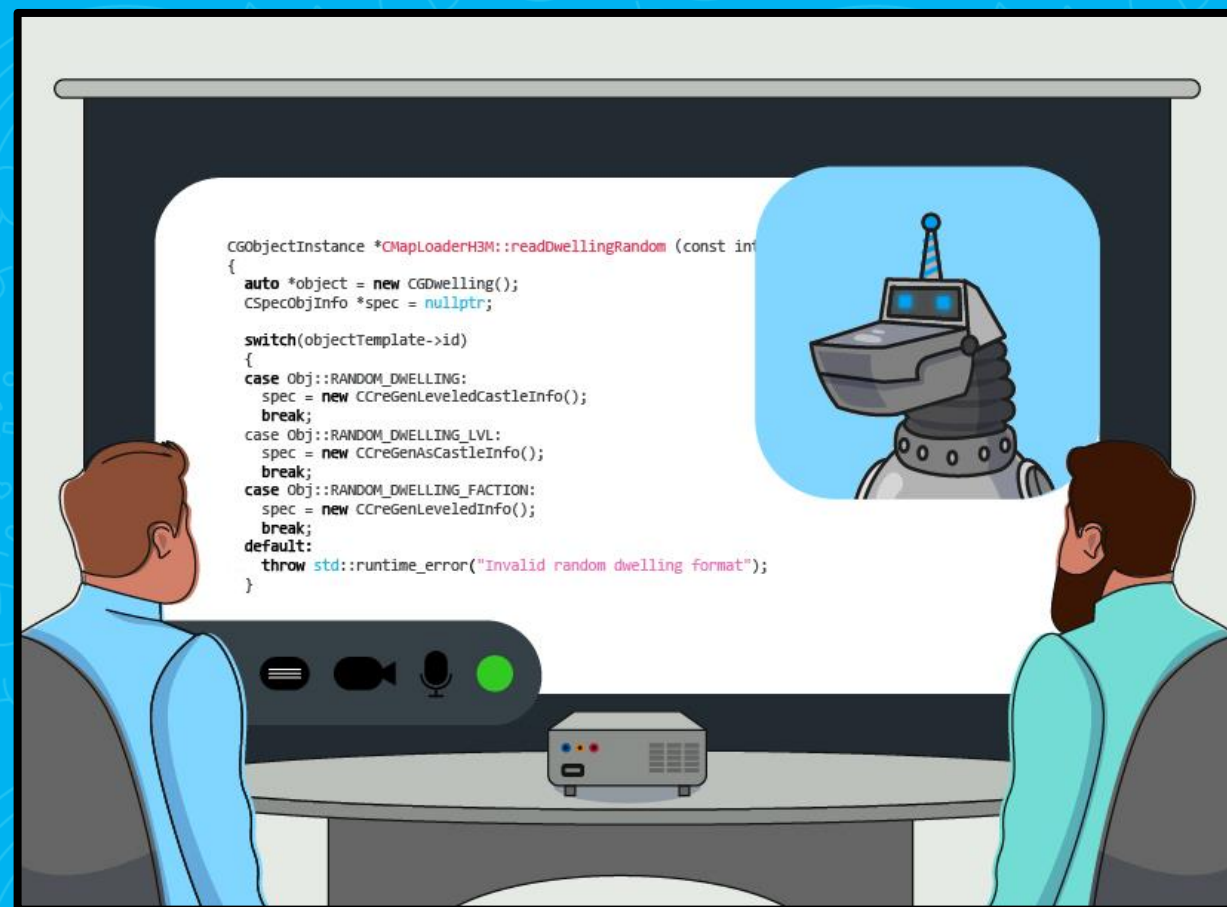
# Как искать уязвимости?

- Часто ошибки == уязвимости



# Как искать уязвимости?

- Часто уязвимости == ошибки
- Помогут найти тесты и анализаторы



# Что такое SAST?

## Жизнь без SAST

Сделать	В процессе	Сделано
Баг	Баг	Баг
Фича	Эпик	Баг
Баг	Баг	Баг



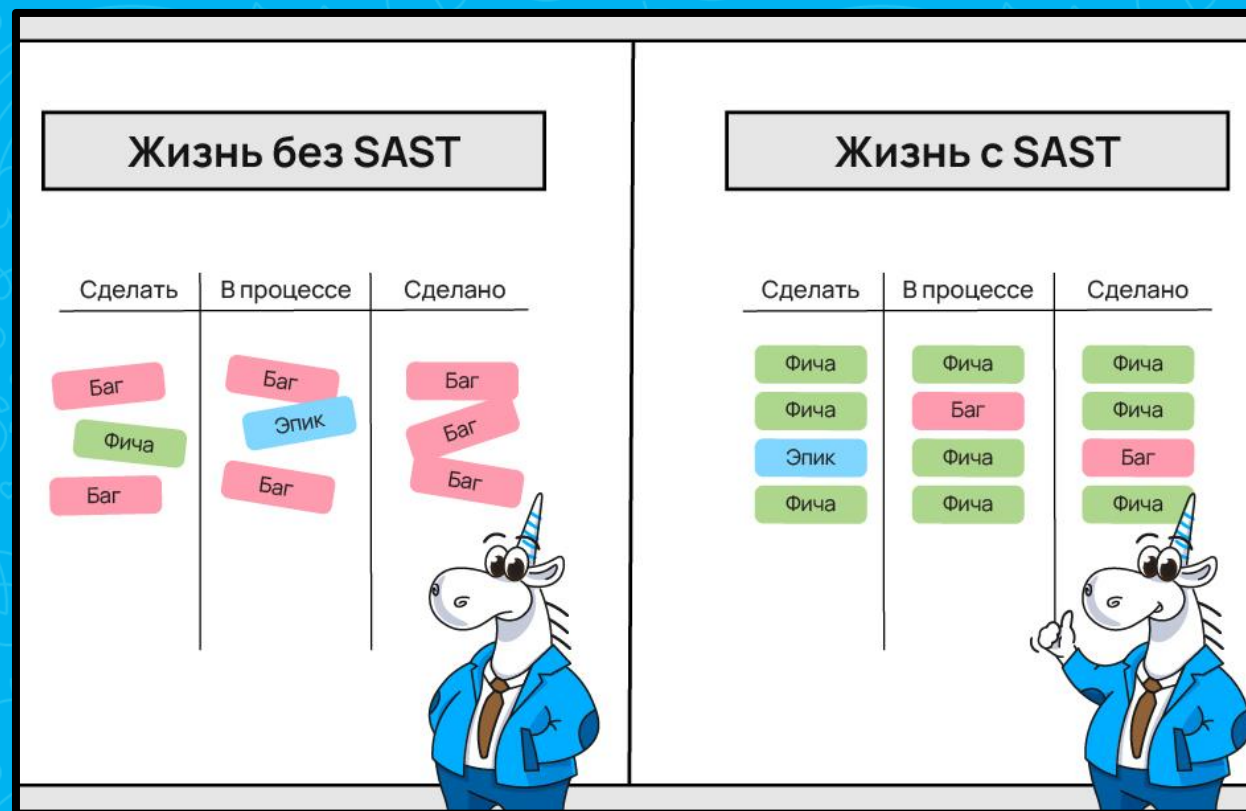
## Жизнь с SAST

Сделать	В процессе	Сделано
Фича	Фича	Фича
Фича	Баг	Фича
Эпик	Фича	Баг
Фича	Фича	Фича



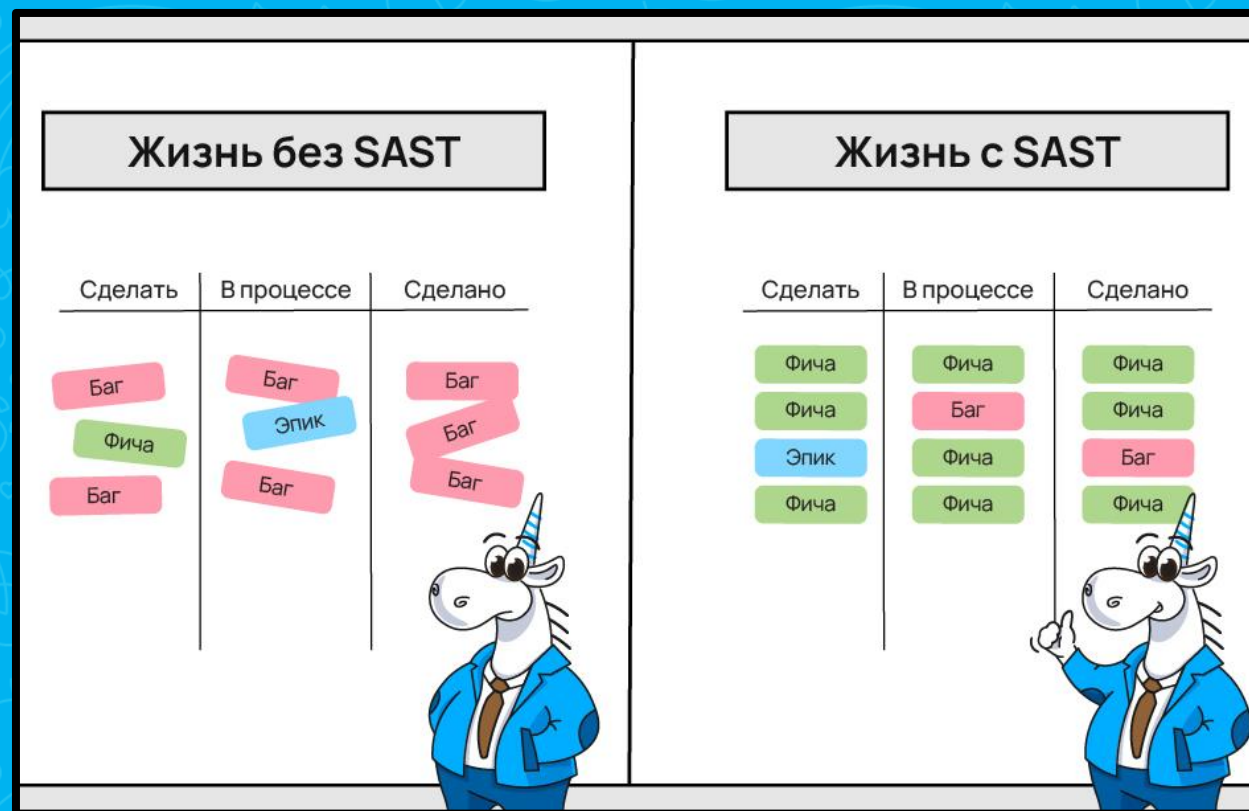
# Что такое SAST?

- Статический анализ, но про уязвимости



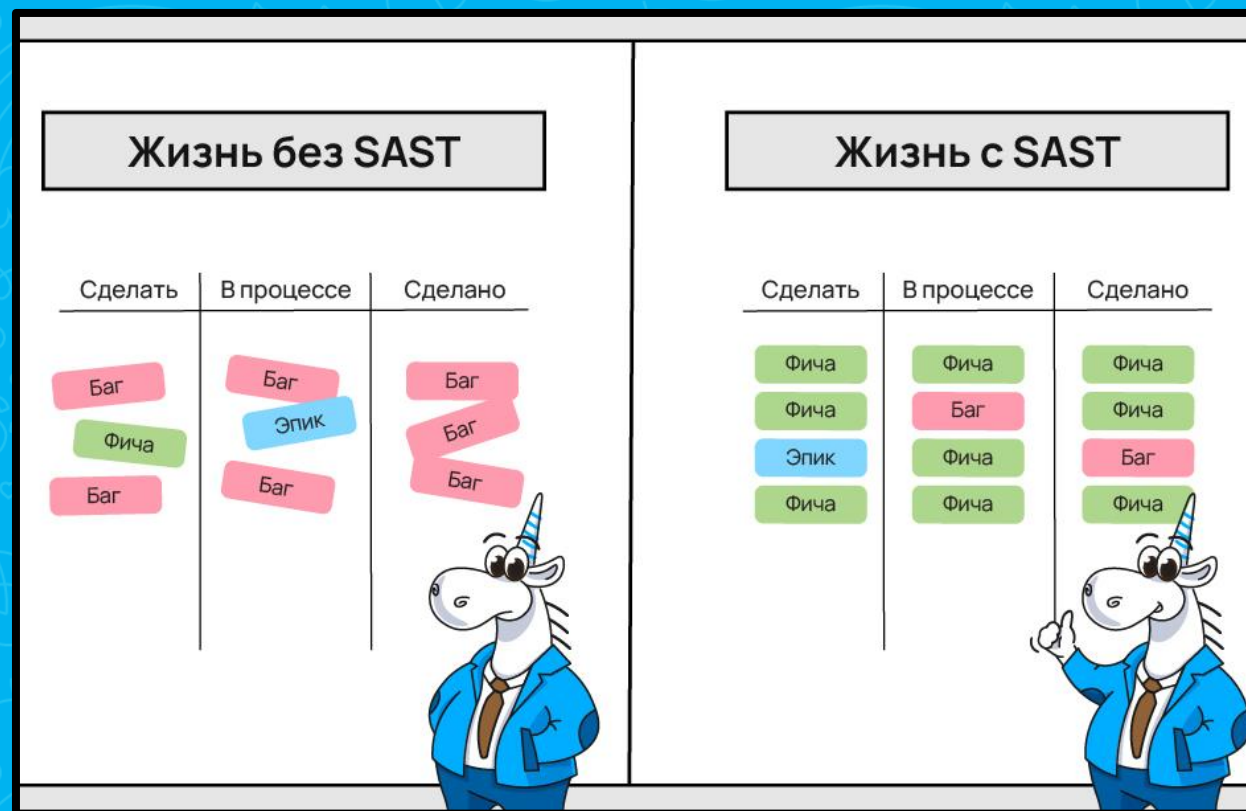
# Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код



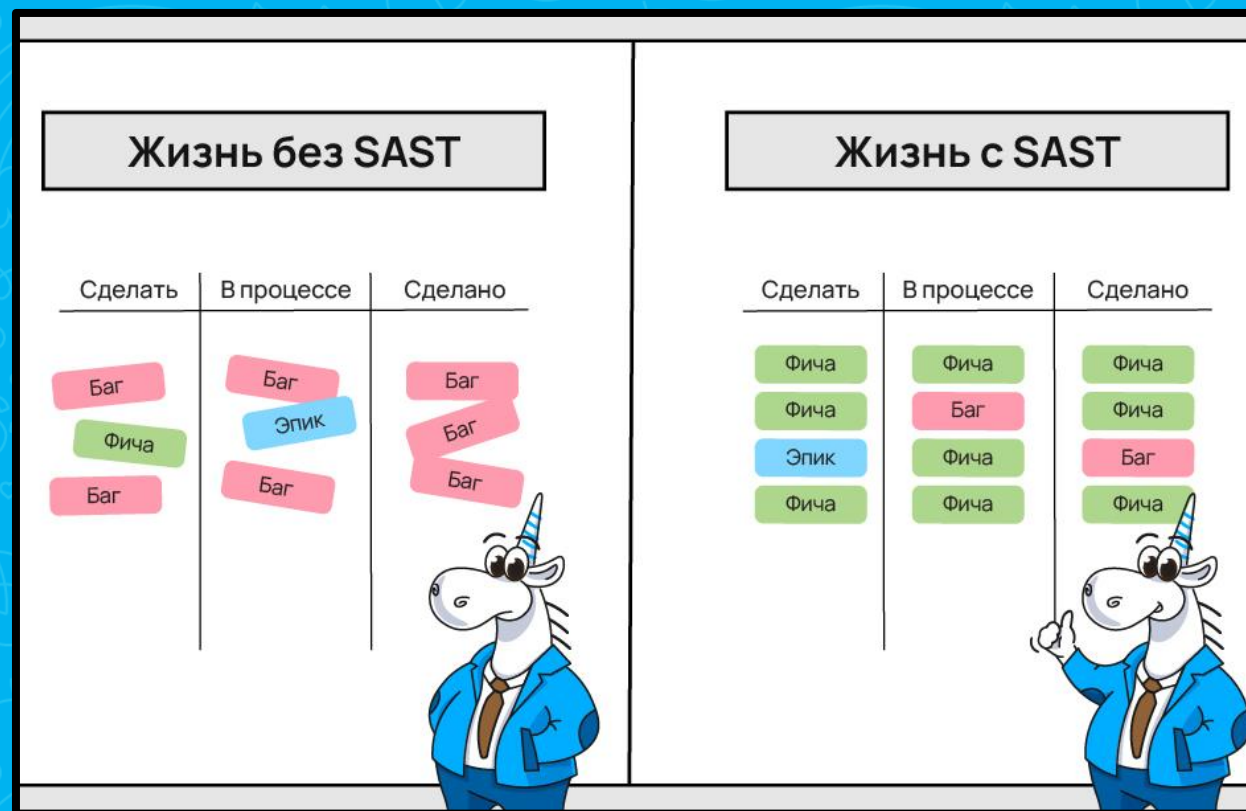
# Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие



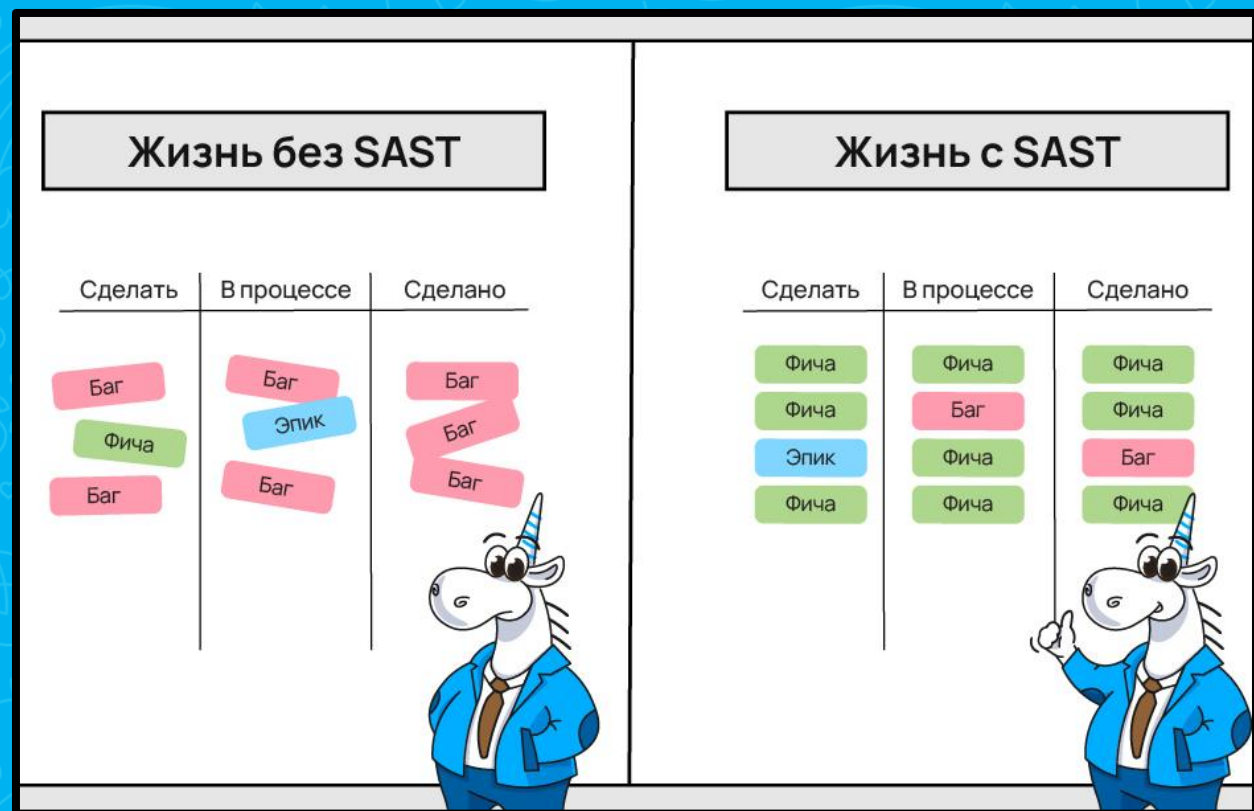
# Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей



# Что такое SAST?

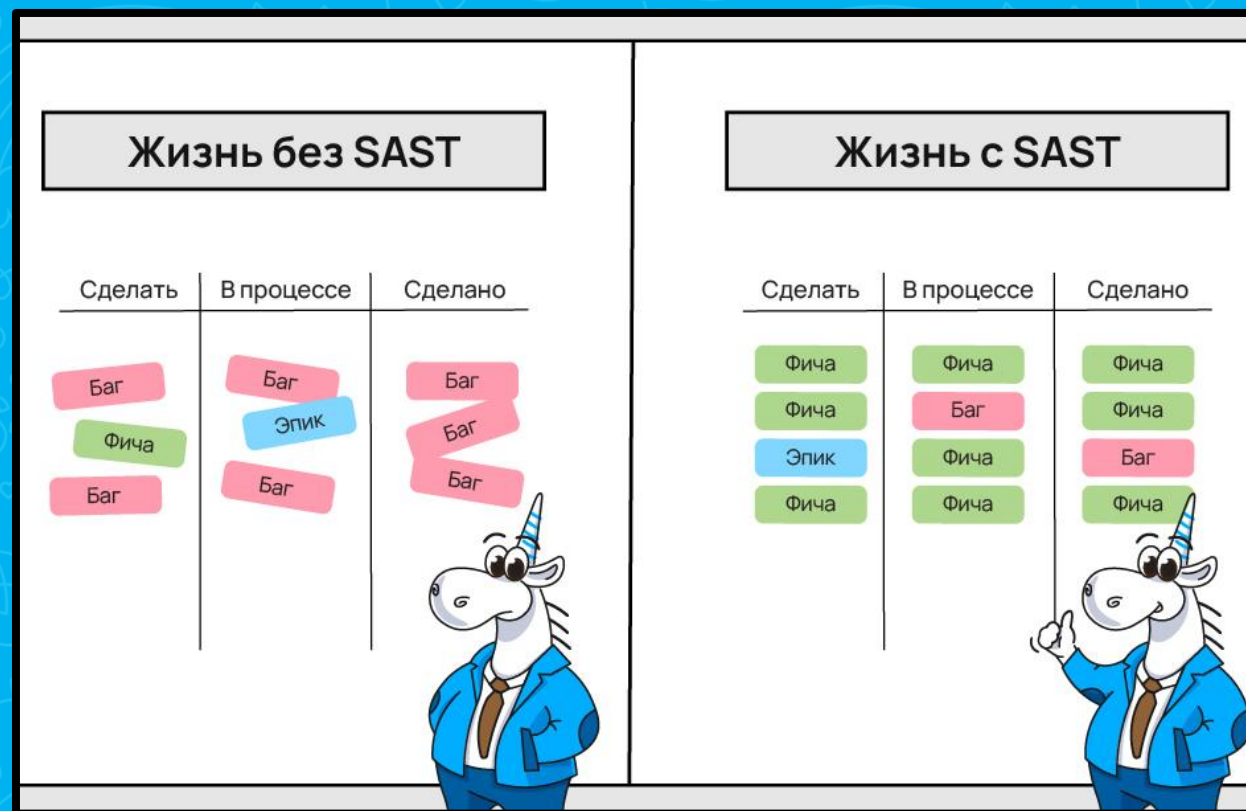
- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей
- Исправление до этапа тестирования





# Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей
- Исправление до этапа тестирования
- PVS-Studio – это SAST инструмент



## Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
```

```
....
```

```
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```




## Пример CWE в проекте FastReport

**ParagraphFormat** paragraphFormat; Поле



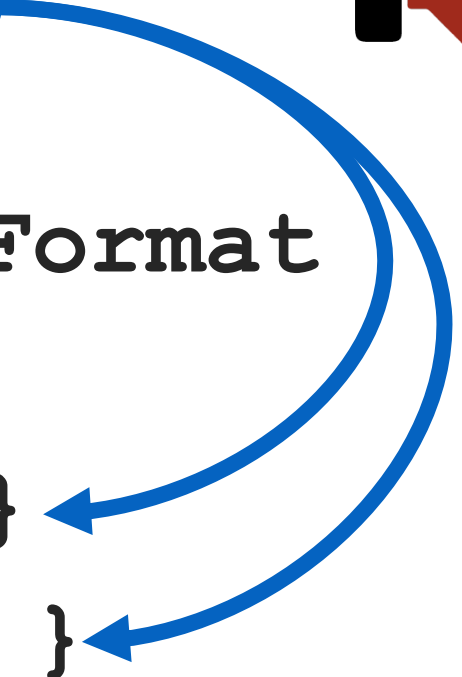
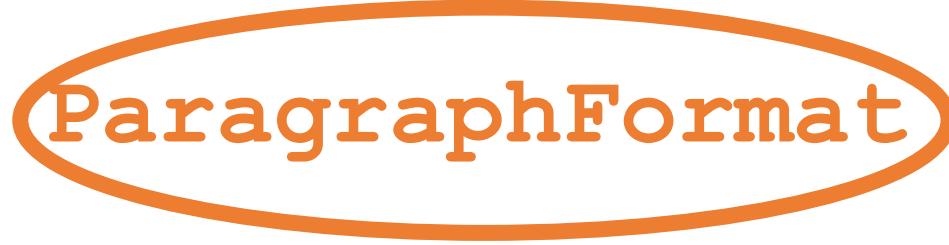
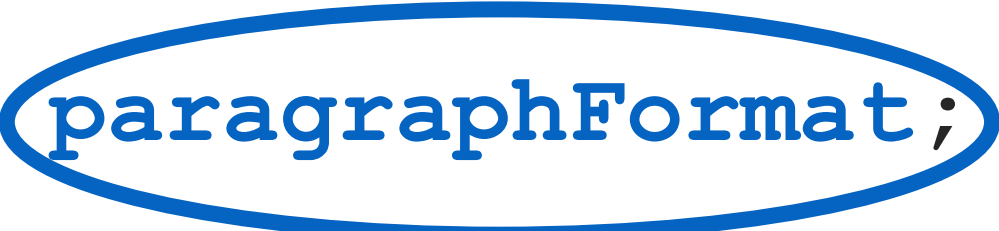
```
.....  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```

## Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat; Поле   
.....  
public ParagraphFormat ParagraphFormat  
{  
    СВОЙСТВО  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```

# Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;  
...  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```



# Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;  
...  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```



# Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;  
...  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```



## Пример CWE в проекте FastReport

```
static void Main(string[] args)
{
    TextObject textObj = new TextObject();
    textObj.ParagraphFormat = null;

    Console.WriteLine("Ok");
}
```

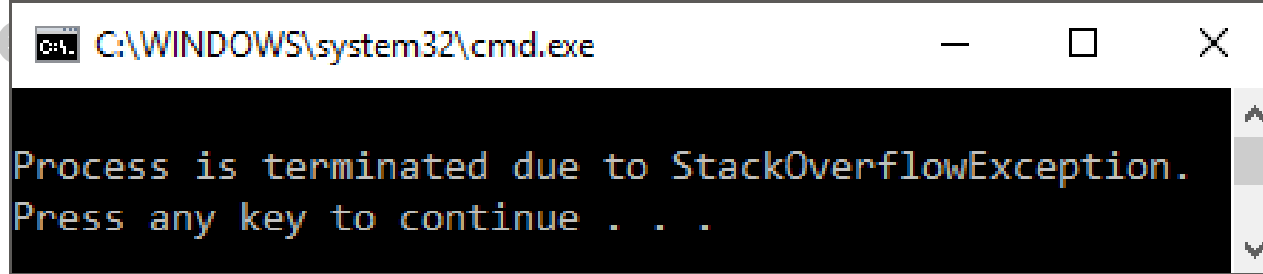




# Пример CWE в проекте FastReport

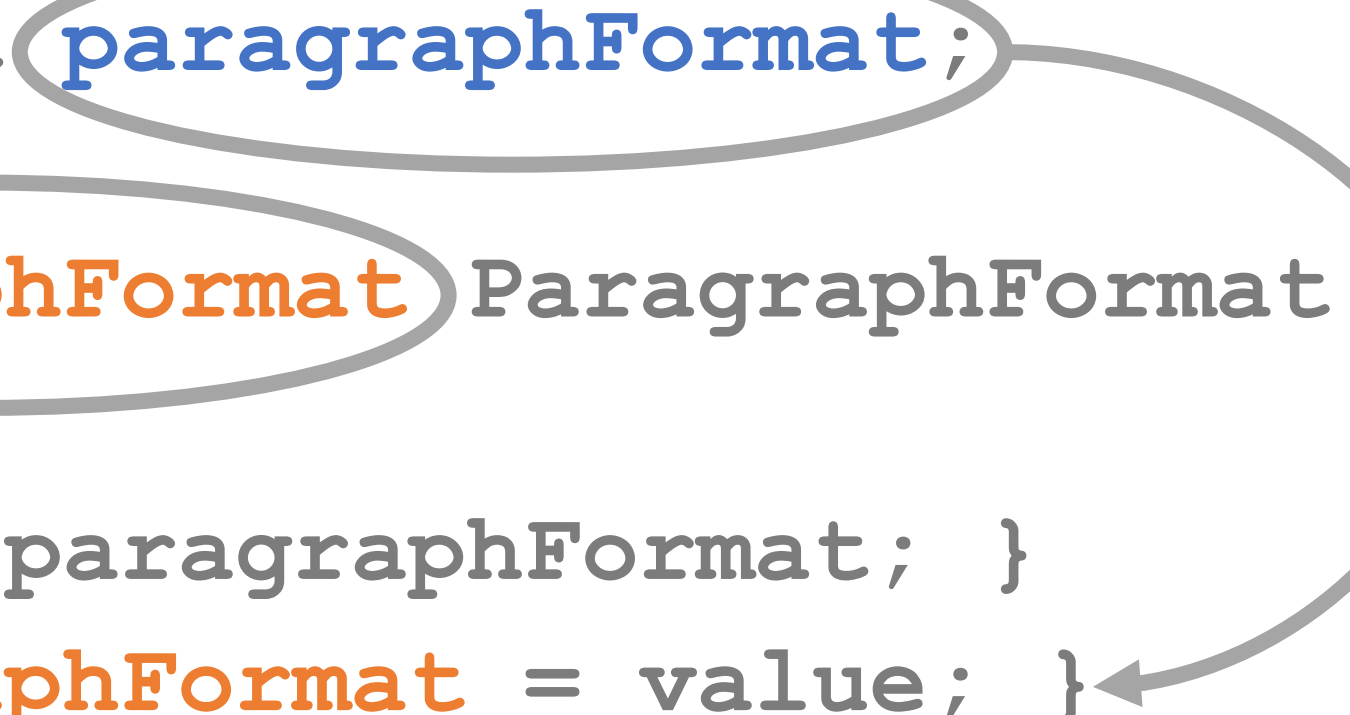


```
static void Main(string[] args)
{
    TextObject textObj = new TextObject();
    textObj.Text = "Ok";
    Console.WriteLine("Ok");
}
```



## Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;  
...  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }
```



Предупреждение PVS-Studio: V3010 [[CWE-674](#)]

Possible infinite recursion inside 'ParagraphFormat' property.

Разбираем проблемы при интеграции  
в legacy проект

PVS-Studio



Fails: 0



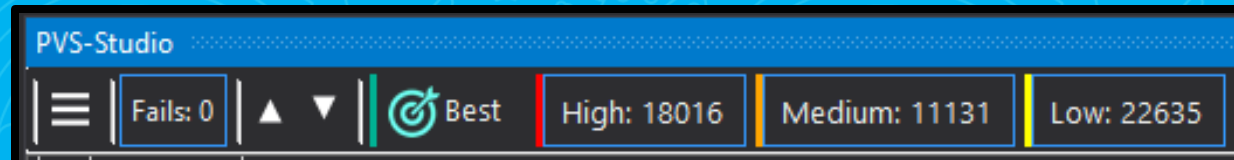
Best

High: 18016

Medium: 11131

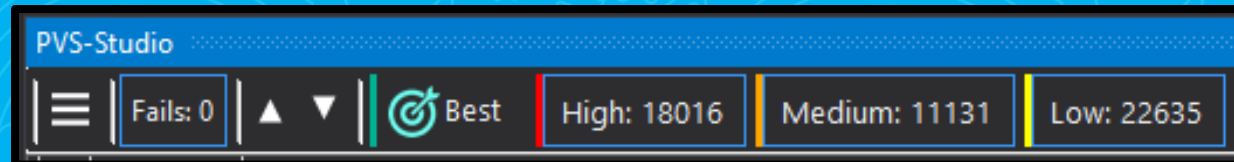
Low: 22635

# Опасность первого раза



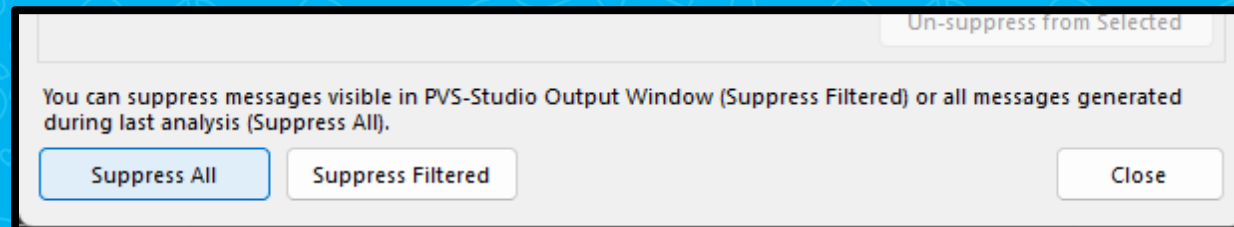
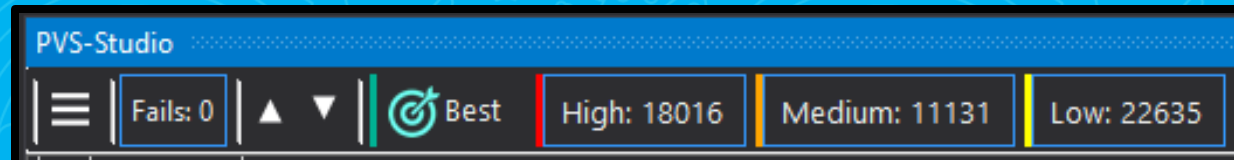
## Опасность первого раза

- Много срабатываний == нормально



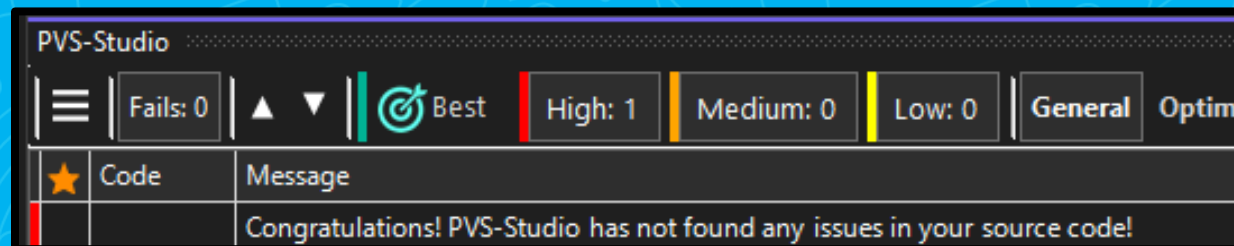
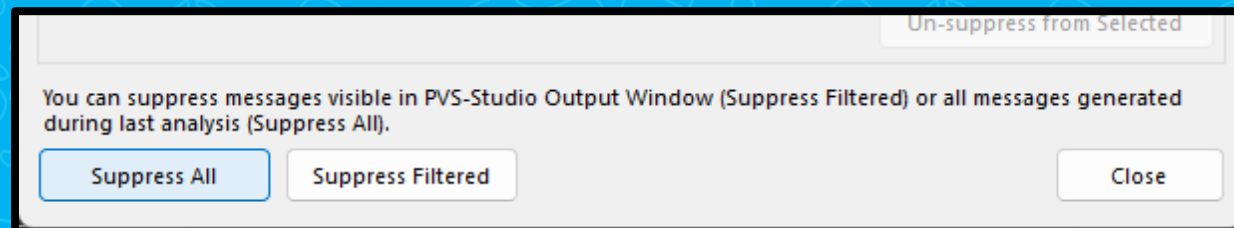
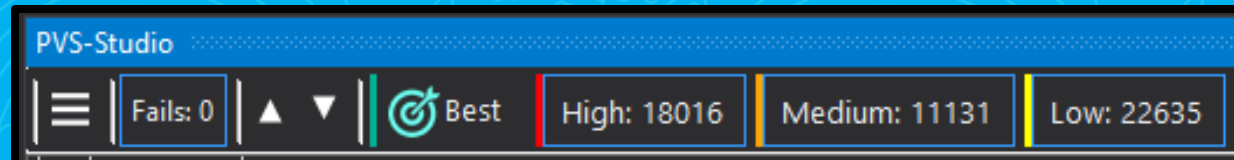
## Опасность первого раза

- Много срабатываний == нормально
- **Используем массовое подавление**



## Опасность первого раза

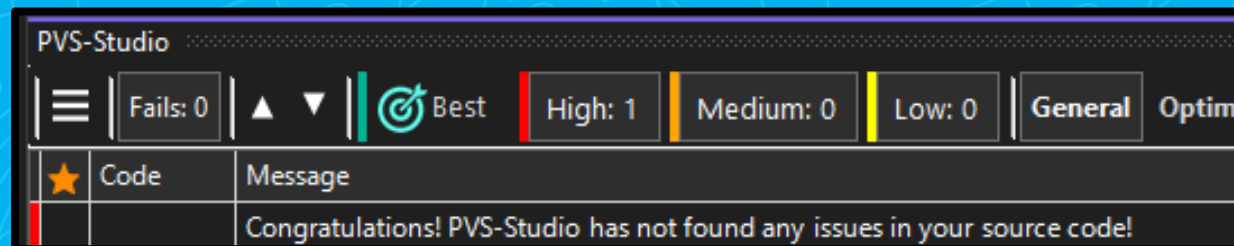
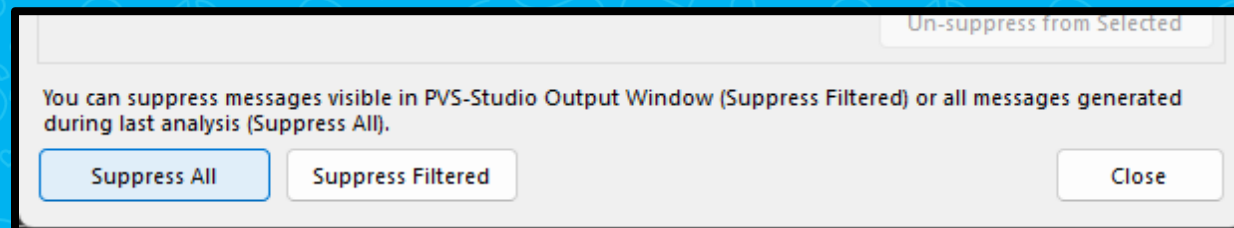
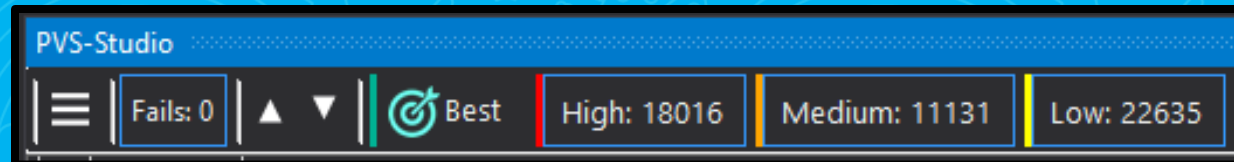
- Много срабатываний == нормально
- **Используем массовое подавление**
- Периодически возвращаемся и чиним



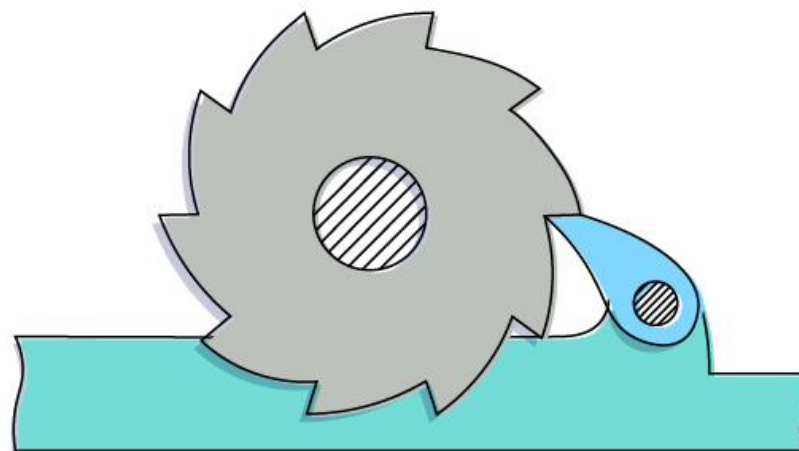


## Опасность первого раза

- Много срабатываний == нормально
- **Используем массовое подавление**
- Периодически возвращаемся и чиним
- Но есть и другой способ...

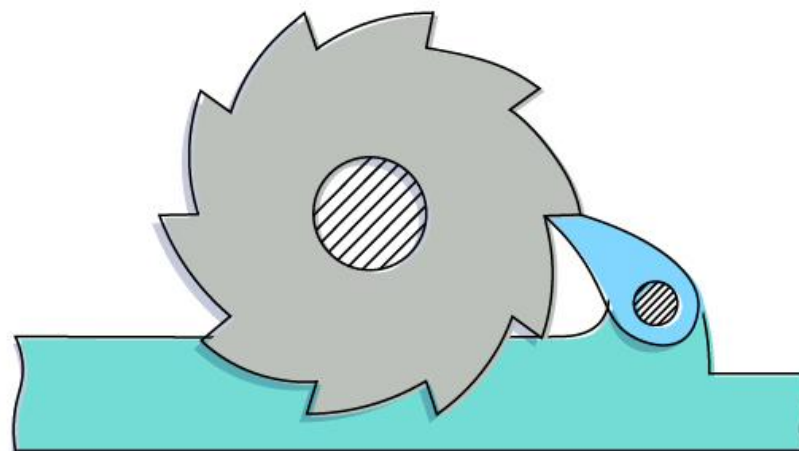


# Принцип Храповика



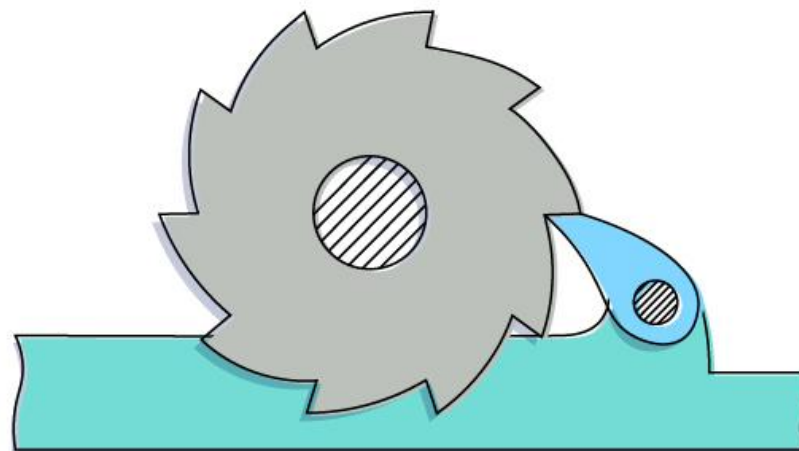
# Принцип Храповика

- Выполняем анализ



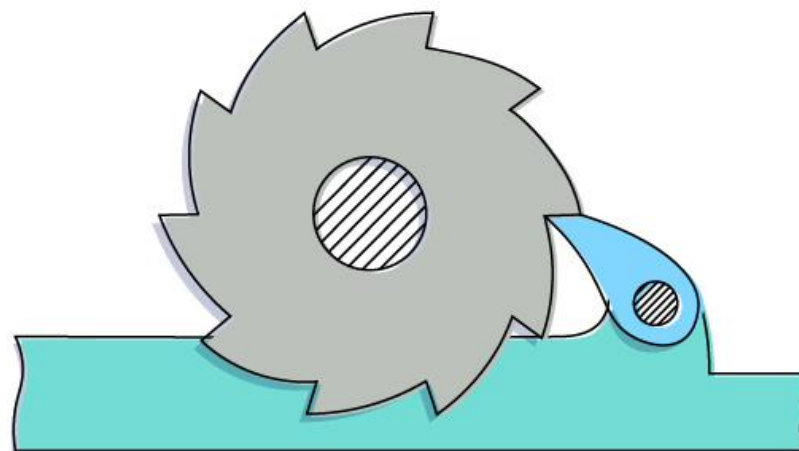
## Принцип Храповика

- Выполняем анализ
- **Заносим в систему контроля версий и устанавливаем порог вхождения**

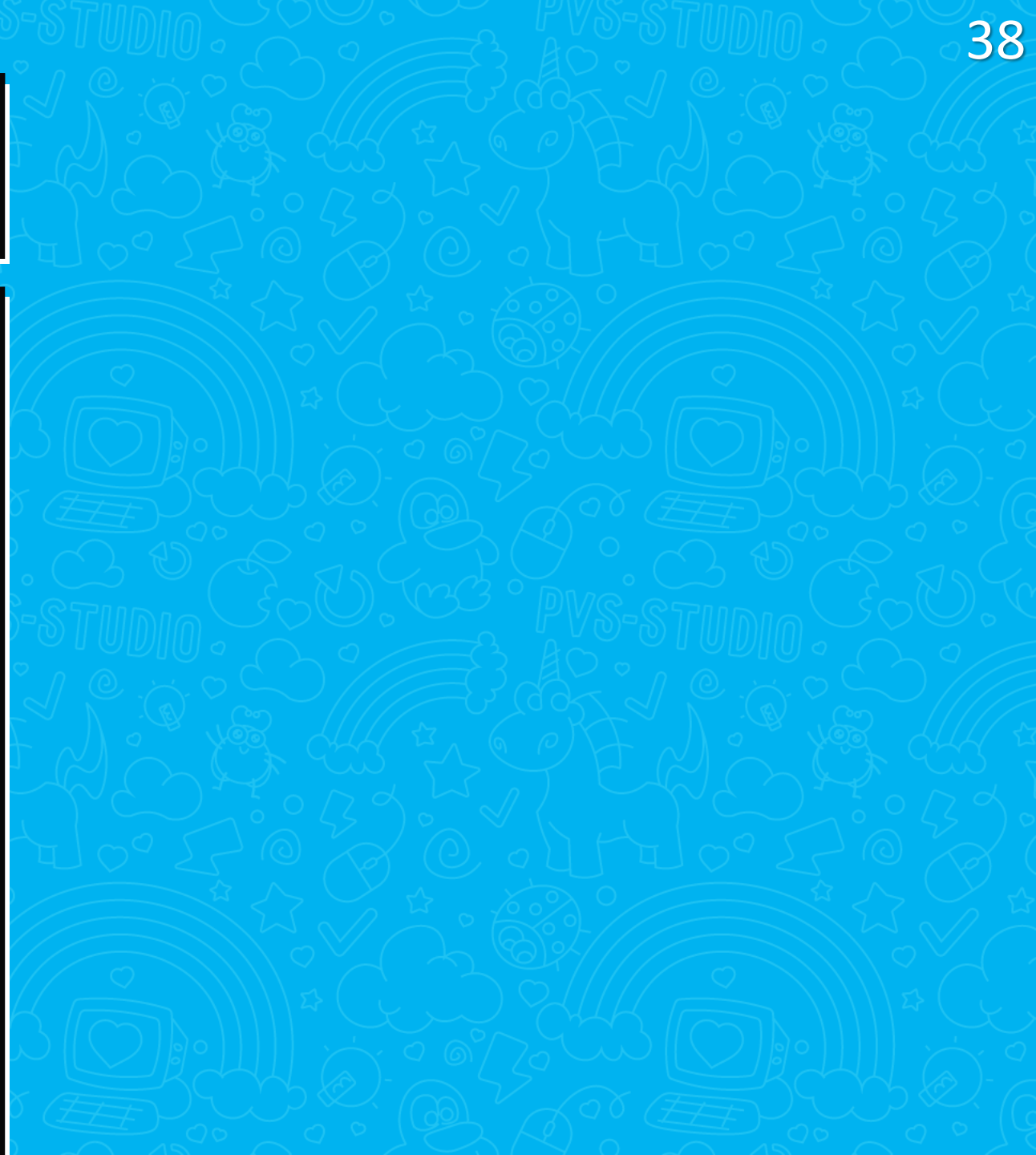
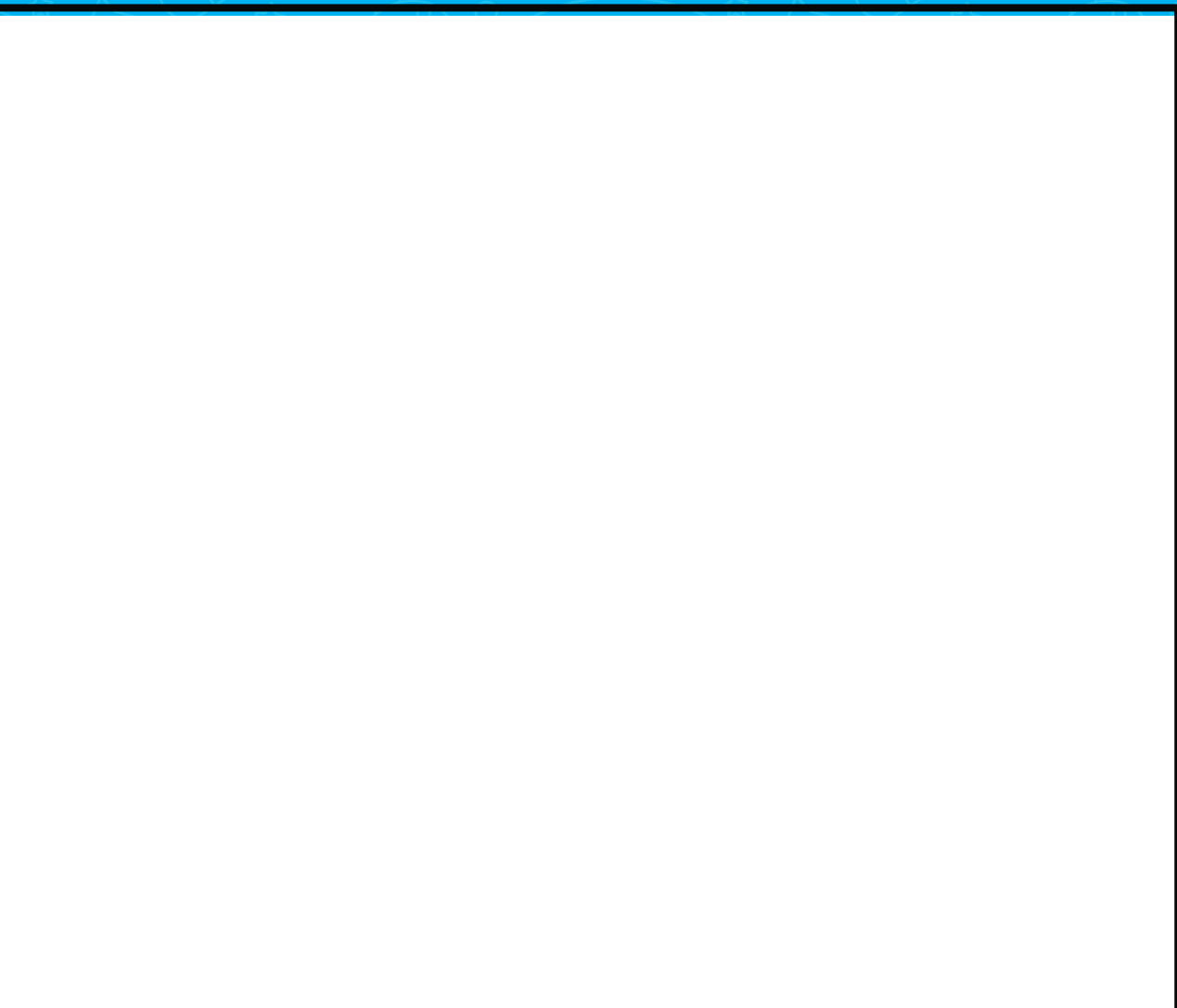


## Принцип Храповика

- Выполняем анализ
- **Заносим в систему контроля версий и устанавливаем порог вхождения**
- Исправляем!



# Ложные срабатывания

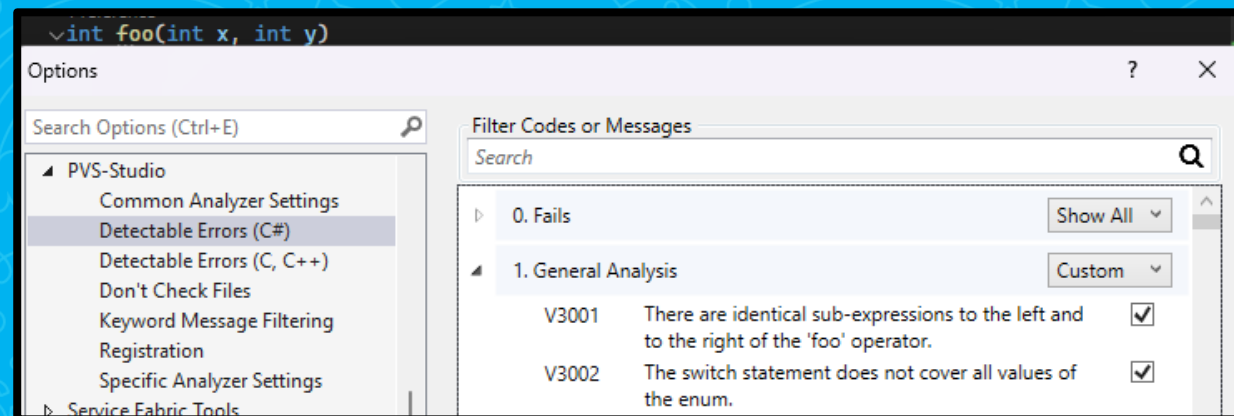


# Ложные срабатывания

- Особенность технологии

# Ложные срабатывания

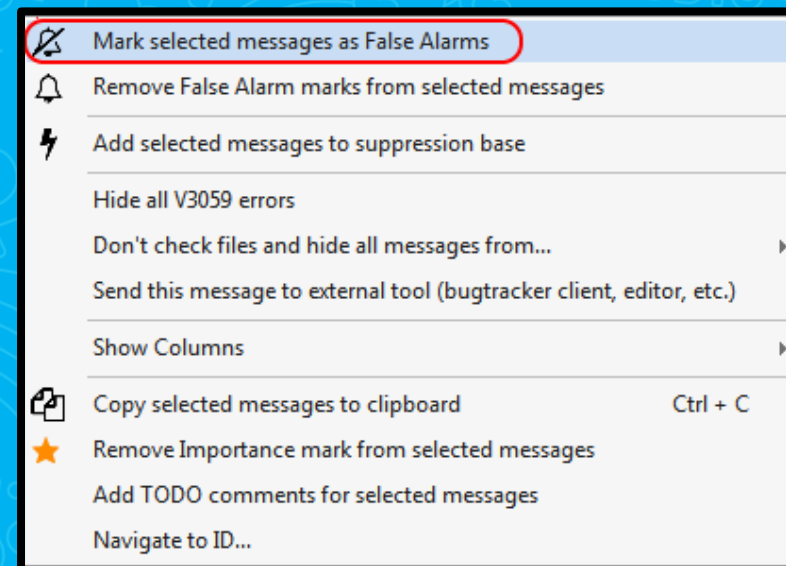
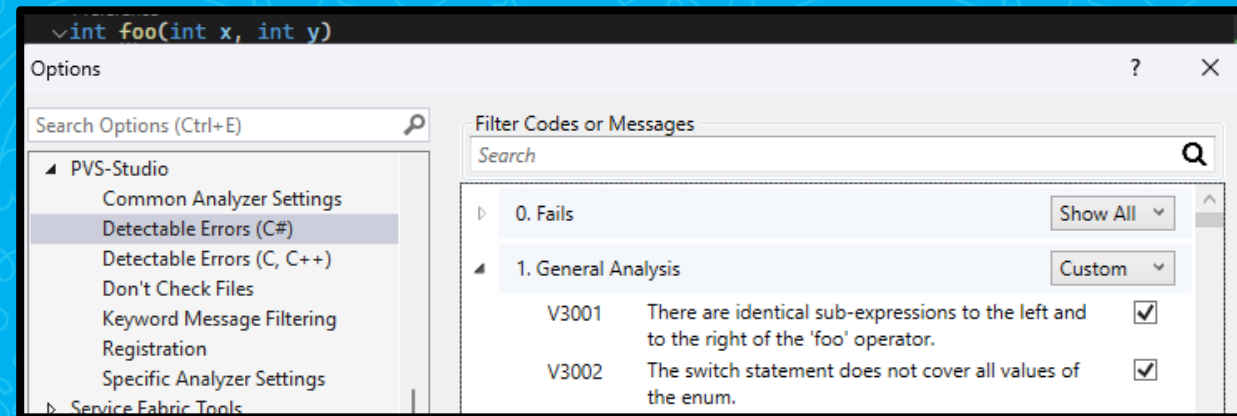
- Особенность технологии
- Настраиваем анализатор под проект





# Ложные срабатывания

- Особенность технологии
- Настраиваем анализатор под проект



# Долго время анализа



## Долго время анализа

- Больше проект == больше время



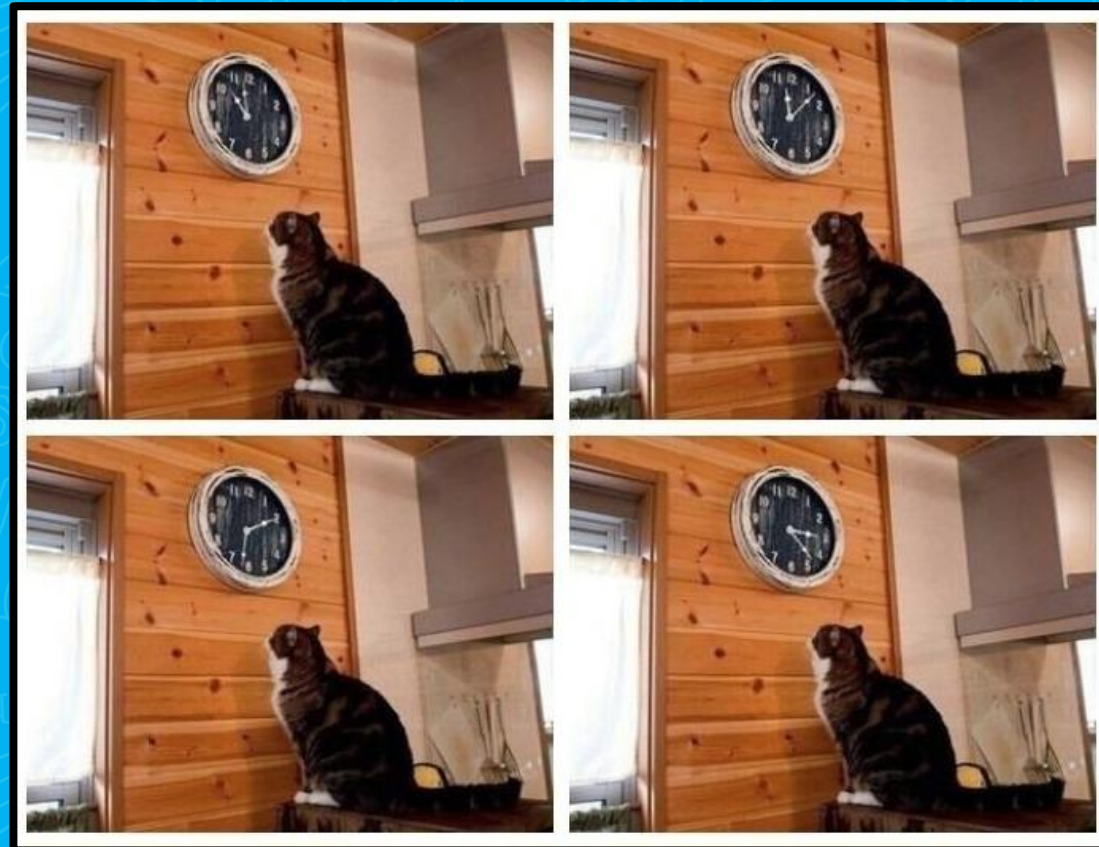
## Долго время анализа

- Больше проект == больше время
- **Инкрементальный анализ**

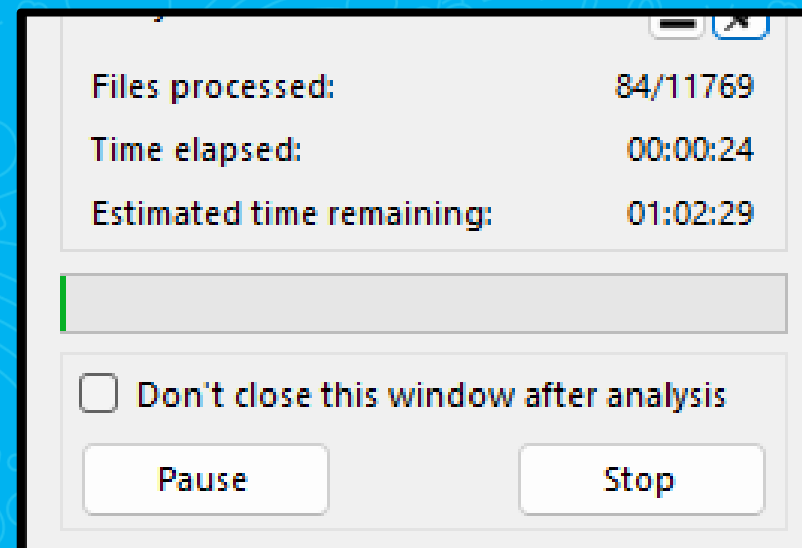
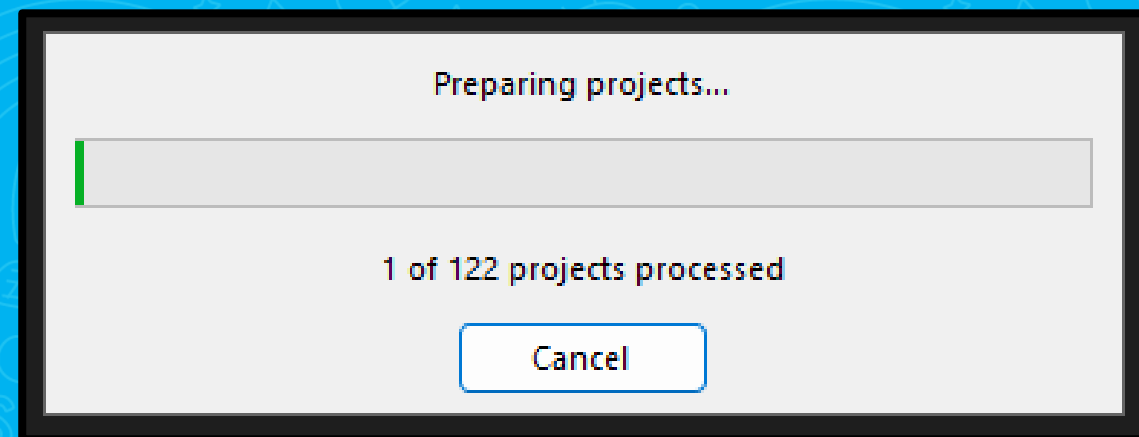


## Долго время анализа

- Больше проект == больше время
- **Инкрементальный анализ**
- Проверяйте только **изменённый код**

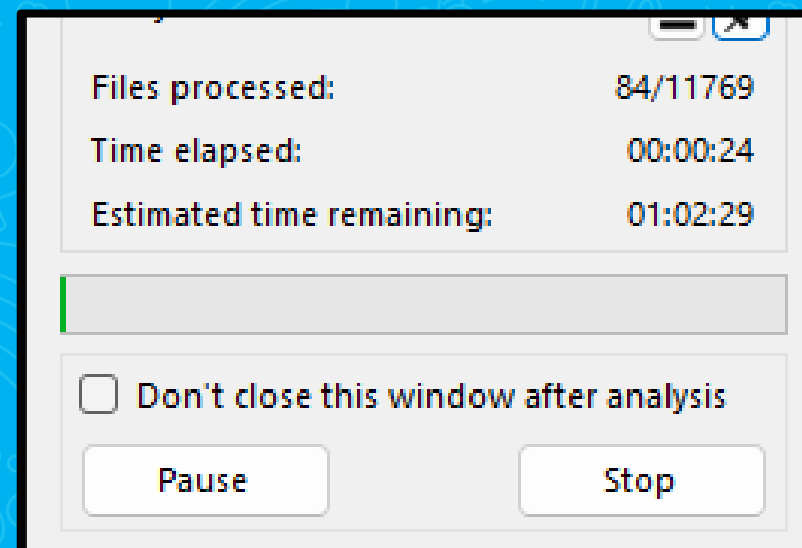
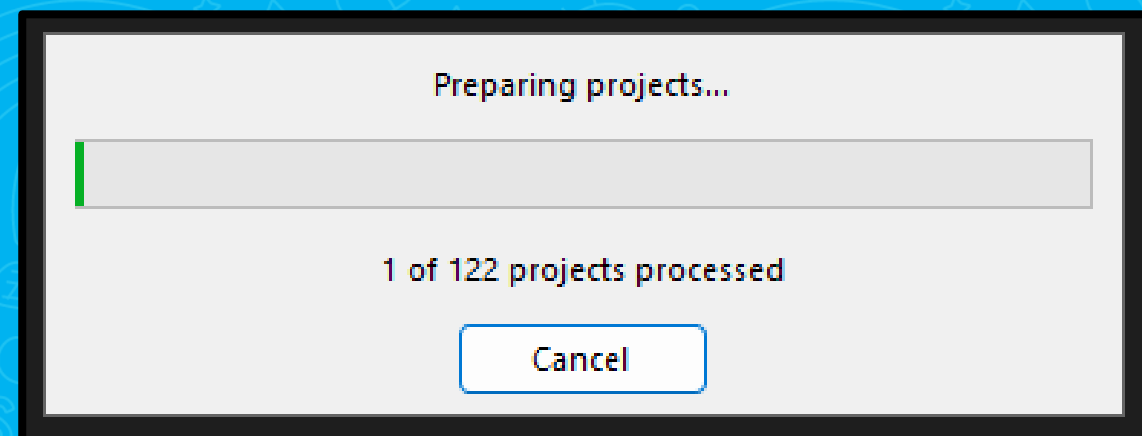


## «Избыточный» анализ



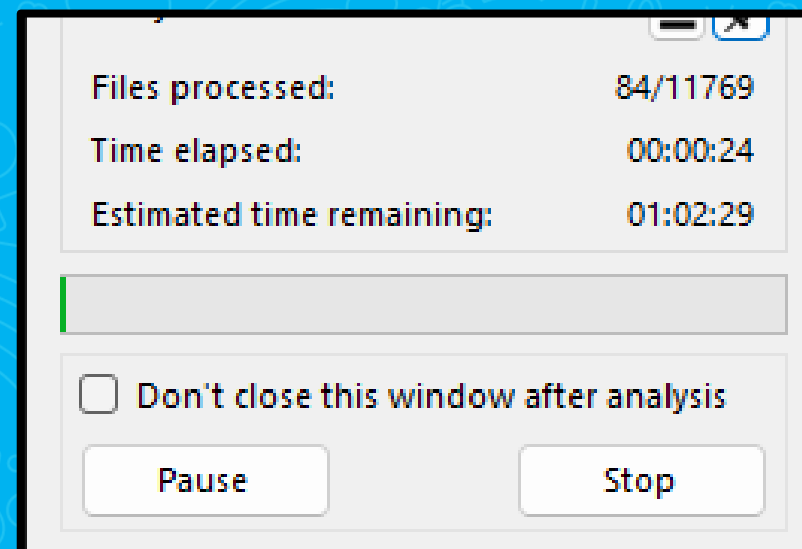
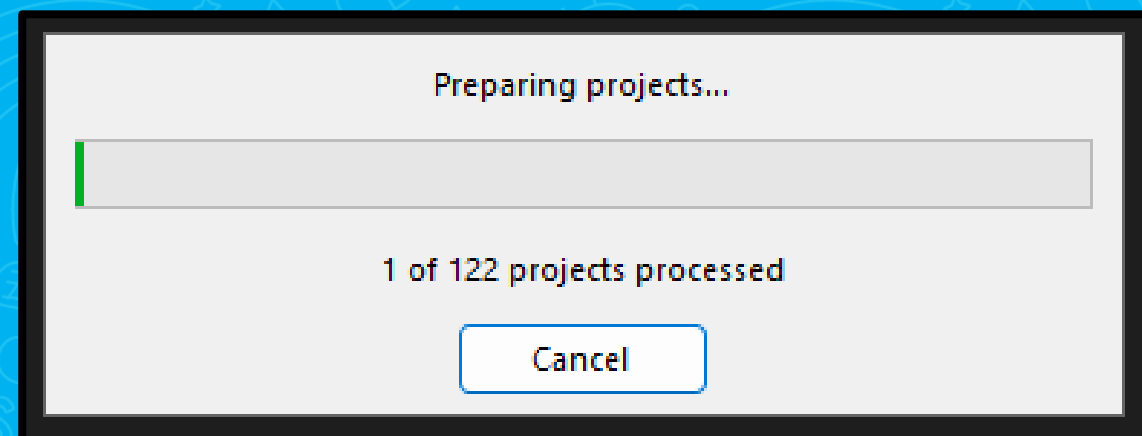
## «Избыточный» анализ

- Лишние файлы, внешние библиотеки



## «Избыточный» анализ

- Лишние файлы, внешние библиотеки
- Возвращаемся к настройке!





# Не хватает диагностик

- Анализатор не идеален
- Но все решаемо!
- Пишем в поддержку

Привет, спишь?)

Мне нужна диагностика которая найдет вот это:

```

@charset "utf-8";
@import url(../css/reset.css);
@import url(../css/layout.css);
@import url(../css/fonts.css);
@import url(../css/variables.css);
@import url(../css/mixins.css);
@import url(../css/animations.css);
@import url(../css/typography.css);
@import url(../css/tables.css);
@import url(../css/forms.css);
@import url(../css/buttons.css);
@import url(../css/headers.css);
@import url(../css/footers.css);
@import url(../css/print.css);

body {
  font-family: sans-serif;
  font-size: 16px;
  line-height: 1.2;
  color: #333;
  background-color: #fff;
}

h1 {
  font-size: 24px;
  font-weight: bold;
  margin: 0;
}

h2 {
  font-size: 20px;
  font-weight: bold;
  margin: 0;
}

h3 {
  font-size: 18px;
  font-weight: bold;
  margin: 0;
}

p {
  margin: 0;
}

a href="#" {
  color: #007bff;
  text-decoration: none;
}

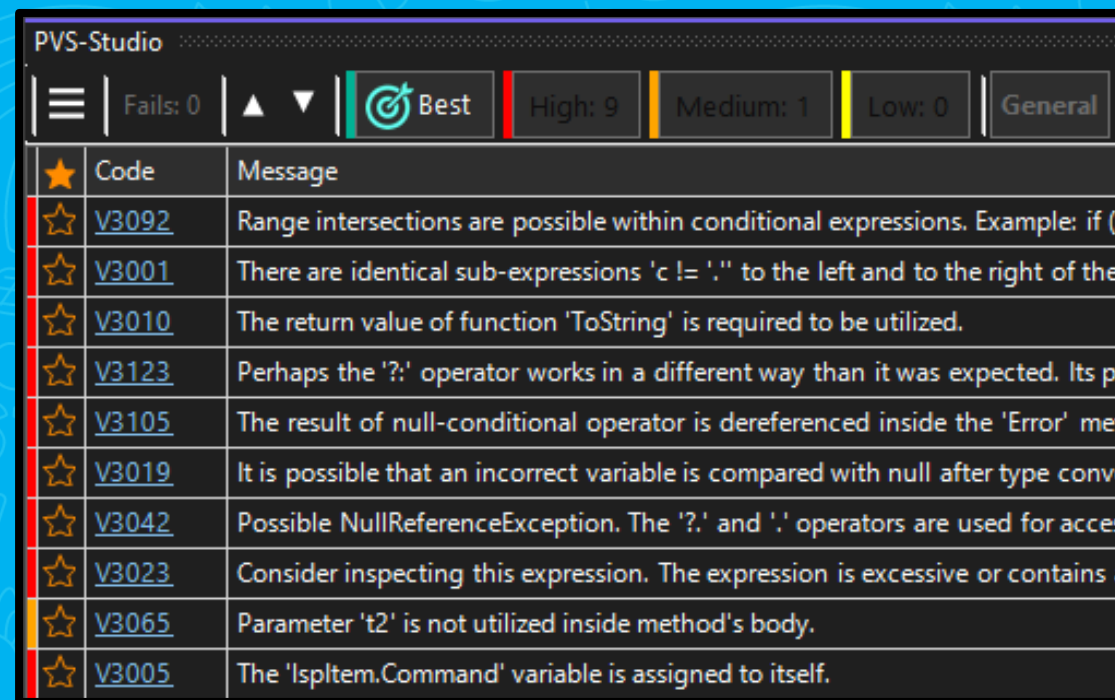
a href="#" :hover {
  color: #0056b3;
}

img alt="Logo" data-bbox="50 50 150 150"/>

```

## Как быстро попробовать?

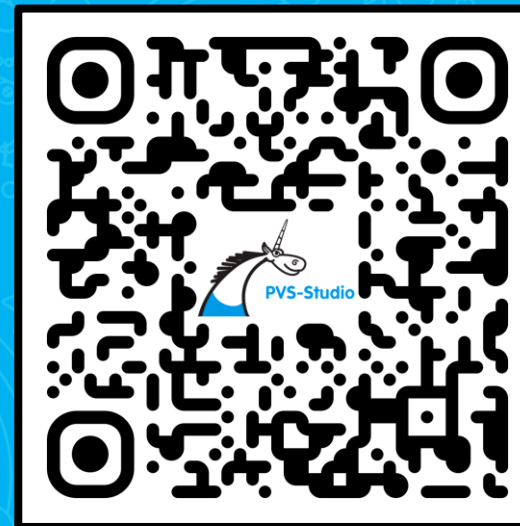
- Написать проект самому?
- Взять опен-сурс?
- Использовать на целевом?
- Попробовать TOP 10!



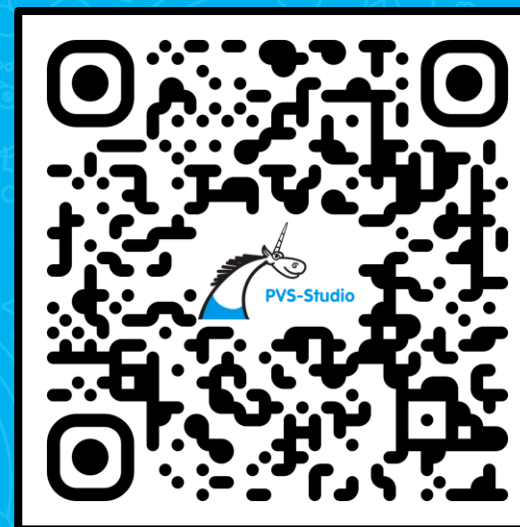
The screenshot shows the PVS-Studio interface with a list of 10 error messages. The interface includes a menu icon, 'Fails: 0', a 'Best' button, and a progress bar showing 'High: 9', 'Medium: 1', and 'Low: 0'. The error messages are as follows:

★	Code	Message
★	<a href="#">V3092</a>	Range intersections are possible within conditional expressions. Example: if (
★	<a href="#">V3001</a>	There are identical sub-expressions 'c != '.' to the left and to the right of the
★	<a href="#">V3010</a>	The return value of function 'ToString' is required to be utilized.
★	<a href="#">V3123</a>	Perhaps the '?' operator works in a different way than it was expected. Its pl
★	<a href="#">V3105</a>	The result of null-conditional operator is dereferenced inside the 'Error' met
★	<a href="#">V3019</a>	It is possible that an incorrect variable is compared with null after type conve
★	<a href="#">V3042</a>	Possible NullReferenceException. The '?' and '.' operators are used for acces
★	<a href="#">V3023</a>	Consider inspecting this expression. The expression is excessive or contains a
★	<a href="#">V3065</a>	Parameter 't2' is not utilized inside method's body.
★	<a href="#">V3005</a>	The 'Ispltem.Command' variable is assigned to itself.

**Устранение неисправностей при  
работе PVS-Studio**



**Советы по повышению скорости  
работы PVS-Studio**





Задавайте  
вопросы

# Q&A

Глеб Асламов

C# Developer & DevRel