OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо

Напишите в чат, если есть проблемы

Проверить, идет ли запись!

Утилиты для статического и динамического анализа защищенности веб-приложений: DAST/SAST/IAST

Колесников Александр

Правила вебинара

Активно участвуем

Задаем вопросы в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

Цели

1. Разобрать основные типы приложений для поиска уязвимостей
2. Познакомиться с особенностями и ограничениями
3. Провести тесты

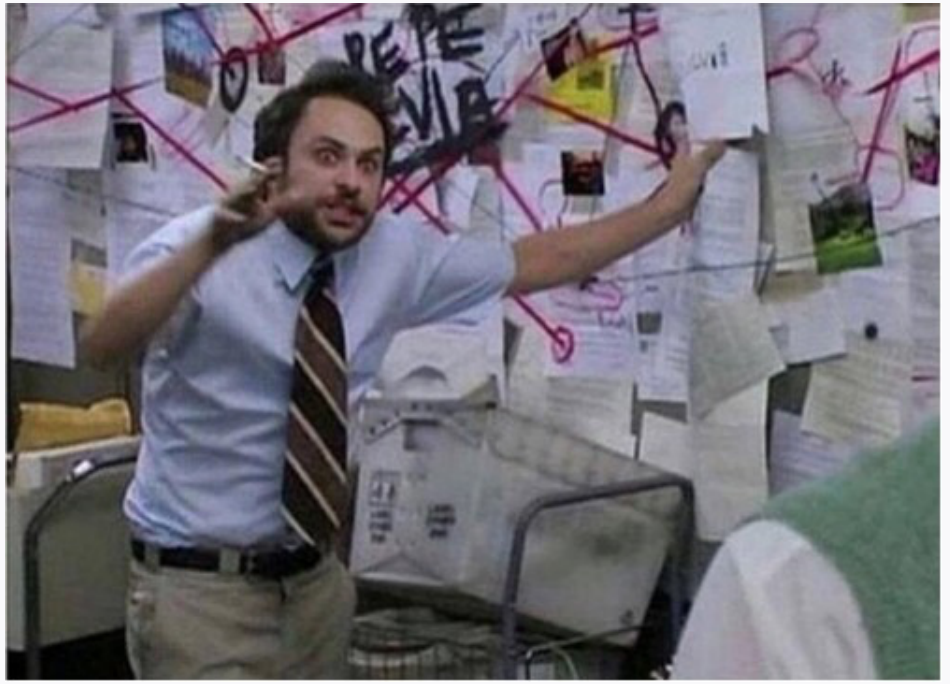

SAST
Static Application Security Testing

Одна программа не может исследовать другую программу!

Или может?

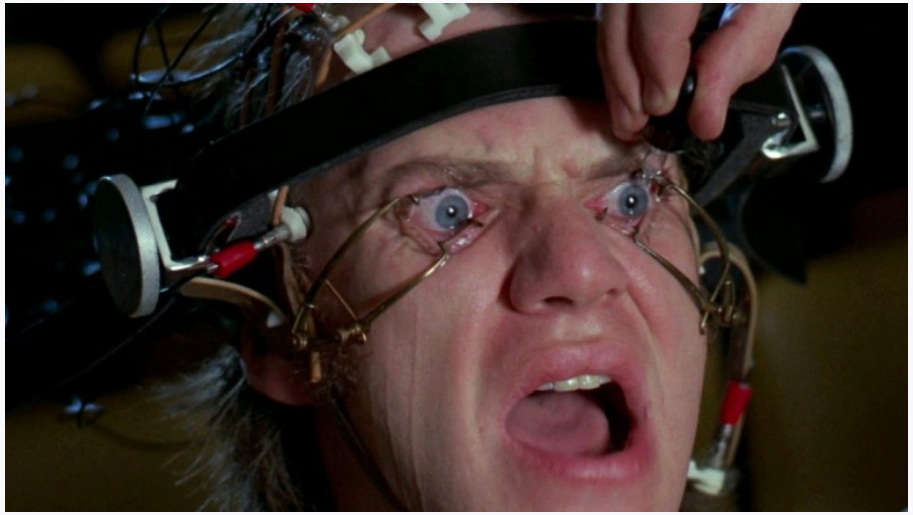
Теоретические ограничения

- **Статическое тестирование возможно:**
  - Фрагмент кода без циклов и рекурсии
  - Фрагмент с циклами или рекурсиями выход из которых не зависит от параметров
  - Условия выхода из цикла или рекурсии не превышают заданного порога



Статическое тестирование приложений

- **Сигнатурная проверка** - набор правил, которые содержат примеры кода
- **Исследование модели выполнения кода** - поиск входных параметров, которые вероятно могут привести к проблеме
- **Символическое исполнение** - использование отдельного символического языка для представления работы программы. Позволяет исследовать на ряде параметров.

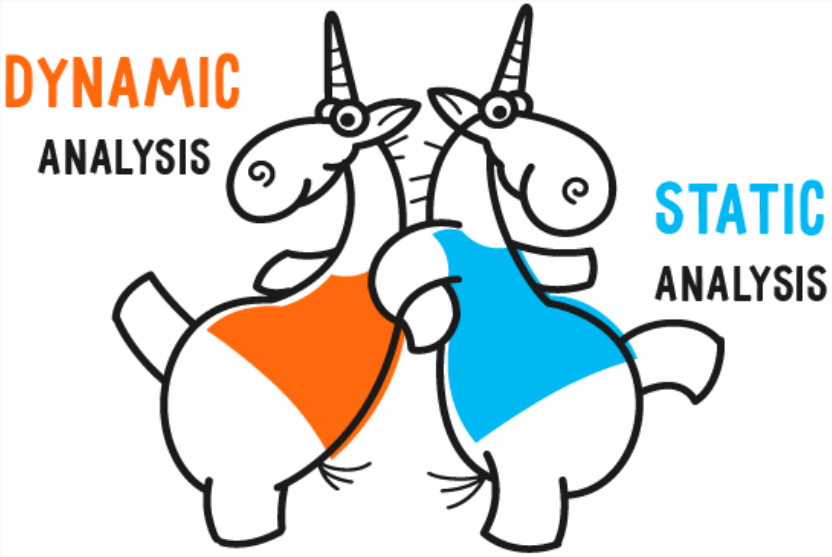


DAST
Dynamic Application Security Testing

Динамическое тестирование

- **Проверка на основе вредоносных значений** - отправление данных на развернутое приложение, регистрируются только падения и неопределенные состояния

- Нет никаких меток, сенсоров для регистрации причин падения. Нужно проводить Root-case анализ



IAST
Interactive Application Security Testing

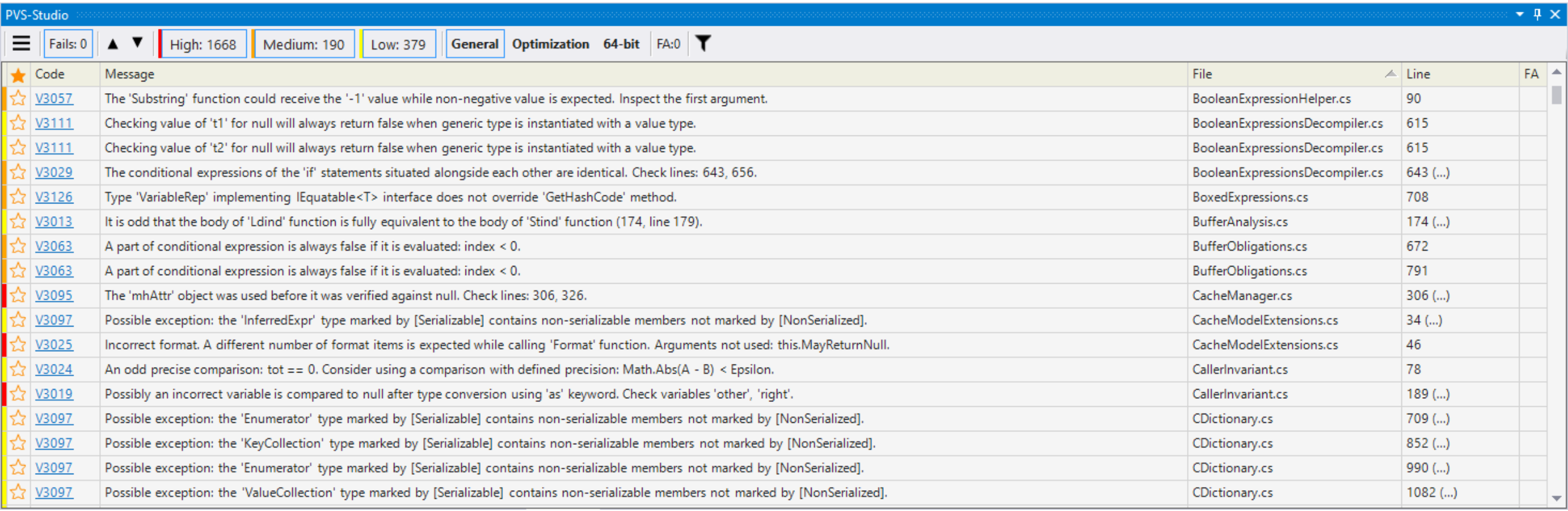
Интерактивное тестирование приложений

- Тестирование может проводиться как с исходным кодом так и без.
- Главное условие - наличие сенсоров, меток или другого механизма, который точно определяет проблему

Инструменты для тестирования приложений

PVS Studio

- Статический сканер:
  - C
  - C++
  - C#
  - Java



Code	Message	File	Line	FA
V3057	The 'Substring' function could receive the '-1' value while non-negative value is expected. Inspect the first argument.	BooleanExpressionHelper.cs	90	
V3111	Checking value of 't1' for null will always return false when generic type is instantiated with a value type.	BooleanExpressionsDecompiler.cs	615	
V3111	Checking value of 't2' for null will always return false when generic type is instantiated with a value type.	BooleanExpressionsDecompiler.cs	615	
V3029	The conditional expressions of the 'if' statements situated alongside each other are identical. Check lines: 643, 656.	BooleanExpressionsDecompiler.cs	643 (...)	
V3126	Type 'VariableRep' implementing IEquatable<T> interface does not override 'GetHashCode' method.	BoxedExpressions.cs	708	
V3013	It is odd that the body of 'Ldind' function is fully equivalent to the body of 'Stind' function (174, line 179).	BufferAnalysis.cs	174 (...)	
V3063	A part of conditional expression is always false if it is evaluated: index < 0.	BufferObligations.cs	672	
V3063	A part of conditional expression is always false if it is evaluated: index < 0.	BufferObligations.cs	791	
V3095	The 'mhAttr' object was used before it was verified against null. Check lines: 306, 326.	CacheManager.cs	306 (...)	
V3097	Possible exception: the 'InferredExpr' type marked by [Serializable] contains non-serializable members not marked by [NonSerialized].	CacheModelExtensions.cs	34 (...)	
V3025	Incorrect format. A different number of format items is expected while calling 'Format' function. Arguments not used: this.MayReturnNull.	CacheModelExtensions.cs	46	
V3024	An odd precise comparison: tot == 0. Consider using a comparison with defined precision: Math.Abs(A - B) < Epsilon.	CallerInvariant.cs	78	
V3019	Possibly an incorrect variable is compared to null after type conversion using 'as' keyword. Check variables 'other', 'right'.	CallerInvariant.cs	189 (...)	
V3097	Possible exception: the 'Enumerator' type marked by [Serializable] contains non-serializable members not marked by [NonSerialized].	CDictionary.cs	709 (...)	
V3097	Possible exception: the 'KeyCollection' type marked by [Serializable] contains non-serializable members not marked by [NonSerialized].	CDictionary.cs	852 (...)	
V3097	Possible exception: the 'Enumerator' type marked by [Serializable] contains non-serializable members not marked by [NonSerialized].	CDictionary.cs	990 (...)	
V3097	Possible exception: the 'ValueCollection' type marked by [Serializable] contains non-serializable members not marked by [NonSerialized].	CDictionary.cs	1082 (...)	

SonarQube

- Сканирование исходников для большого количества языков программирования
- SAST
- Дополнительно можно попробовать провести тестирование потока исполнения

Tenable

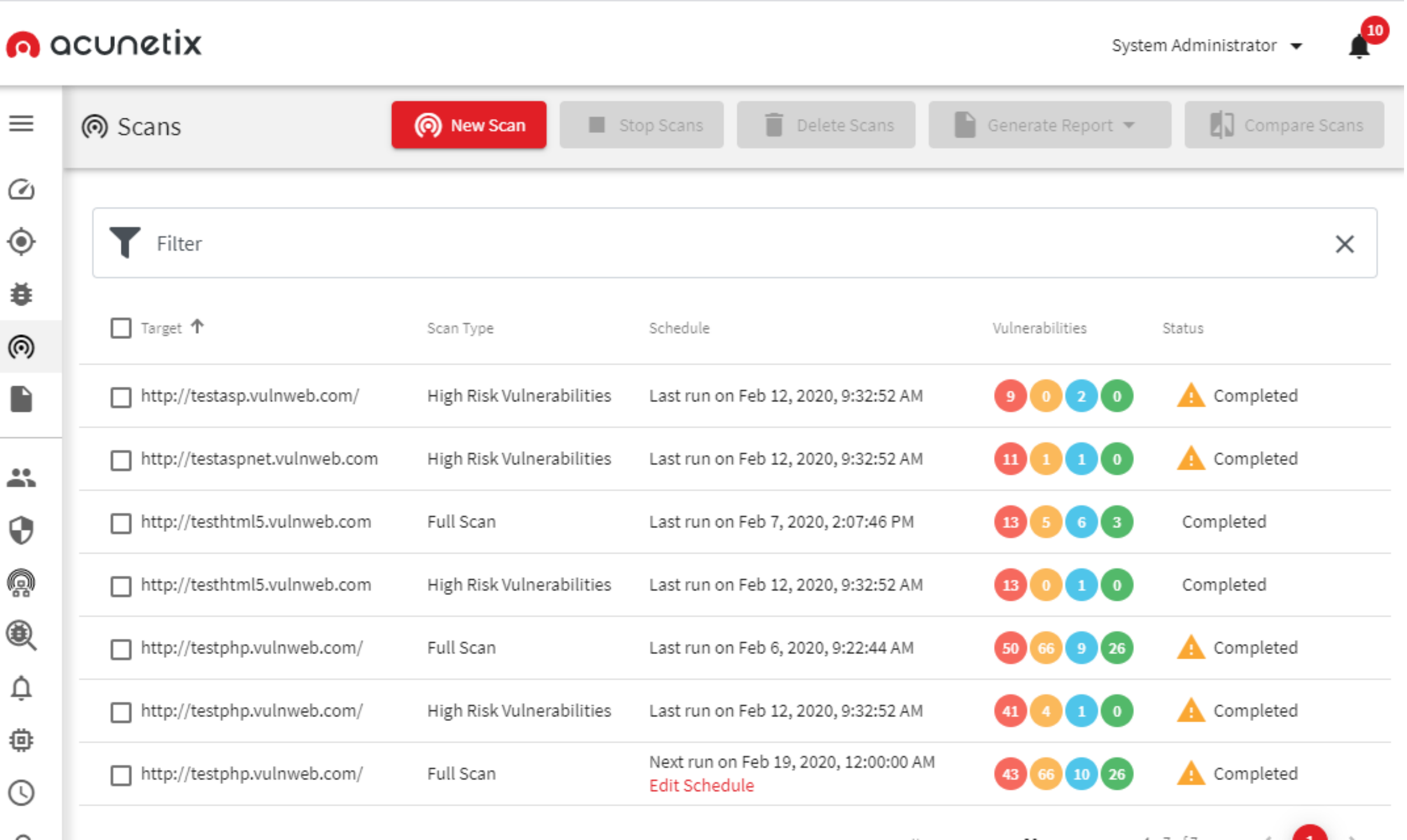
- Сканер общего назначения
- Проводит тестирование сервисов по типу черного ящика
- Проверяются как обычные приложения, так и web

OpenVAS

- Сканер общего назначения
- Проводит тестирование сервисов по типу черного ящика
- Тестирование, которе больше похоже на Fuzzing

Acunetix

- Сканер работает по типу черного ящика
- Ориентирован на уязвимости для web-сервисов

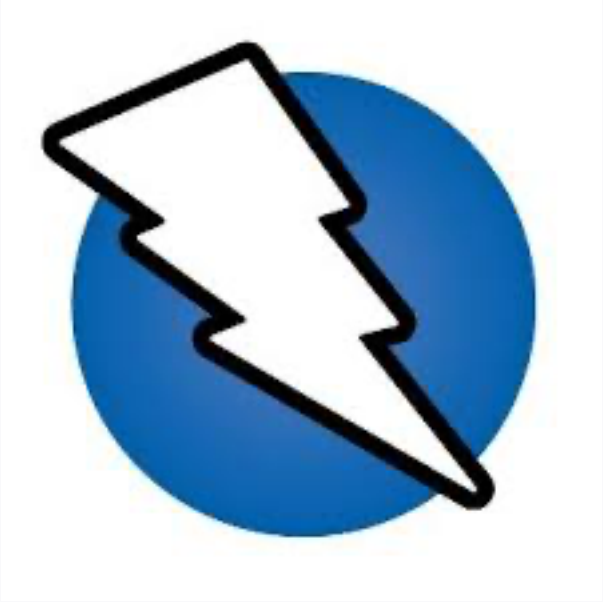

acunetix
System Administrator
10
Scans
New Scan
Stop Scans
Delete Scans
Generate Report
Compare Scans
Filter
Target
Scan Type
Schedule
Vulnerabilities
Status
http://testasp.vulnweb.com/
High Risk Vulnerabilities
Last run on Feb 12, 2020, 9:32:52 AM
9 0 2 0
Completed
http://testaspnet.vulnweb.com
High Risk Vulnerabilities
Last run on Feb 12, 2020, 9:32:52 AM
11 1 1 0
Completed
http://testhtml5.vulnweb.com
Full Scan
Last run on Feb 7, 2020, 2:07:46 PM
13 5 6 3
Completed
http://testhtml5.vulnweb.com
High Risk Vulnerabilities
Last run on Feb 12, 2020, 9:32:52 AM
13 0 1 0
Completed
http://testphp.vulnweb.com/
Full Scan
Last run on Feb 6, 2020, 9:22:44 AM
50 66 9 26
Completed
http://testphp.vulnweb.com/
High Risk Vulnerabilities
Last run on Feb 12, 2020, 9:32:52 AM
41 4 1 0
Completed
http://testphp.vulnweb.com/
Full Scan
Next run on Feb 19, 2020, 12:00:00 AM
Edit Schedule
43 66 10 26
Completed

Burp Suite

- Приложение для тестирований web приложений
- Предоставляет возможность конфигурации приложений
- Проверка без исходного кода

OWASP ZAP

- Автоматический сканер
- Ориентирован на web приложения
- Проводит тестирование для заданного набора входных параметров



Web Black box scanners

- Тестирование приложений без исходного кода:
  - Nikto
  - Dirb
  - Dirbuster
  - wFuzz
  - w3af

Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр