



APPSEC  
EUROPE

# Addressing Security Requirements in Development Projects

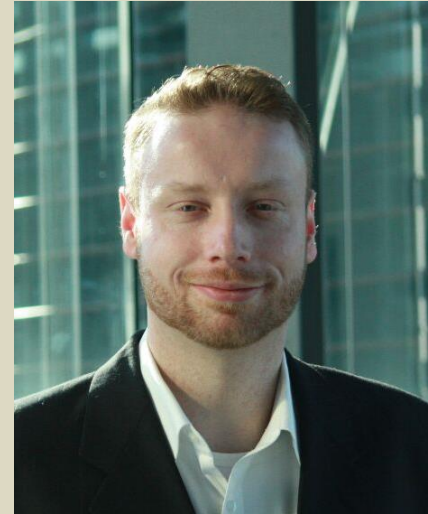
*Daniel Kefer, René Reuter*

# Whoami

**Daniel Kefer**



**René Reuter**







APPSEC  
EUROPE

# MOTIVATION

# Thesis

- Common security requirements often get forgotten
- There are a lot of them!
- We should make sure that these fit the dev workflow
- ... and automate as much as possible!



# Security Requirements

- **System properties**, e.g. Security Headers
- **Lifecycle activities**, e.g. Penetration Test
- Both land in your ticket system (probably just in different queues)



# Challenge

- Security standards are long (e.g. ASVS 3.0: 179 reqs)
- Optimization potential
- Filtering potential







APPSEC  
EUROPE

**OUR SOLUTION**

# Approach

- Security RAT (Requirement Automation Tool)
- Requirements are regarded on software artifact level
  - New artifacts
  - Existing artifacts being modified



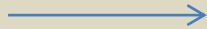


# Workflow



Security  
role

Define artifact



Report status



**Security RAT**

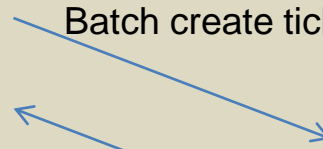
Create ticket & export file



Import file



Batch create tickets



Ticket status



**Artifact Queue**

Requirement set as YAML  
attachment

**Dev Queues**

Particular requirements  
as tasks





APPSEC  
EUROPE

**DEMO**





APPSEC  
EUROPE





# INTERNALS



# Technology

What Is JHipster?

————★————

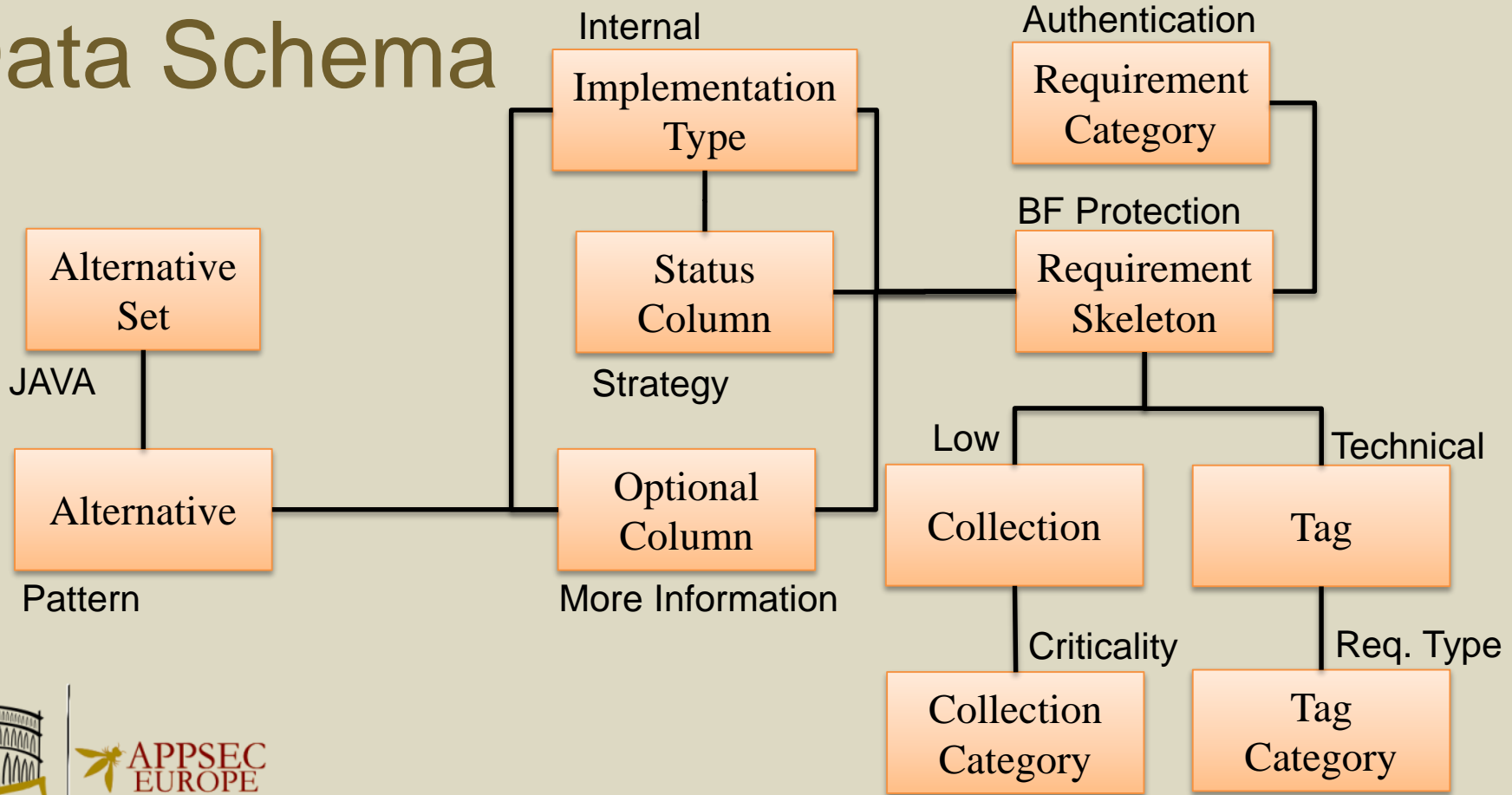
 +  +  = 

JHipster is a [Yeoman generator](#), used to create a [Spring Boot](#) + [AngularJS](#) project.

[HTTP://JHIPSTER.GITHUB.IO/](http://jhipster.github.io/)



# Data Schema



# Ticketing System Integration

- CORS (Cross Origin Request Sharing)
- SecurityRAT inherits user's rights in the ticketing system
- Need to allow GET and POST request in the Ticketing System (e.g. on the web server)





# Requirement Set

- You can start from scratch
- Or use the default one (provided as a MySQL dump and focused mainly on web development)



# Open Source Release

- <https://github.com/SecurityRAT>
- Currently with two projects:
  - SecurityRAT (the actual tool)
  - Security-Requirements (default requirement set)





APPSEC  
EUROPE

# FUTURE PLANS



# Work in Progress

- Docker Image for faster ramp up
- Own user management
- Documentation



# Requirements

- Working on quality of the default set
- Parametrization
- Quality vs Quantity
- Data Schema



# Integration

- Different Ticketing Systems (e.g. Bugzilla, TRAC)
- Wikis (e.g. TikiWiki, Confluence)
- Testing tools





# Community

- Attracting people to contribute, e.g.
  - Requirement sets for different developments, like embedded, stand-alone software, etc. (ASVS ?)
  - Development
  - Testing
  - Feature Requests



# Q&A

**Thank you for your attention!**

<https://github.com/SecurityRAT>

[dan.kefer@gmail.com](mailto:dan.kefer@gmail.com)

[reuter.rene@gmail.com](mailto:reuter.rene@gmail.com)

